Computer Network Technician

تکنسین عمومی شبکه های کامپیوتری

(به صورت عملی)

مؤلف و گردآوری کننده : سالار صداقتی

(it-sedaghati@outlook.com)

نسخه ۱,۱۲

به نام خدا

مقدمه

در این مجموعه سعی شده مطالب اولیه مورد نیاز برای راه اندازی شبکه در حد شرکت ها و مراکز کوچک که از سرور استفاده نمی کنند و هم چنین پایه ریزی شبکه های داخلی بزرگ بیان می گردد . بر اساس تجربیات اجرایی اینجانب، تاکید بر موارد و مشکلات اجرایی و عملی شده است . هم چنین از کتاب های Comptia Network + و شرکت مایکروسافت ، شبکه های کامپیوتری تانن بام، مبانی شبکه های کامپیوتری و مبانی پروتکلها درشبکه های کامپیوتری مهندس آرشین خوشرو استفاده شده است.

از این مجموعه می توانید برای آشنایی اولیه شبکه های کامپیوتری ، راه اندازی شبکه های Workgroup ، آمادگی برای امتحانات Network + و تکنسین عمومی شبکه های کامپیوتری و به عنوان پیش نیاز دوره های تخصصی شبکه از جمله MCSA (مایکروسافت) ، CCNA (سیسکو) و MTCNA (میکروتیک) ، استفاده کنید .

مطالب بر اساس ویندوز ۸ نوشته شده است.

فهرست

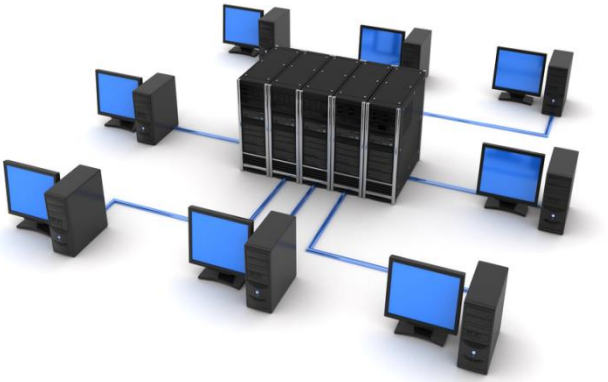
فصل اول

مباحث پایه شبکه های کامپیوتری

۱–۱ شبکه چیست؟

از دیرباز تبادل اطلاعات و ارتباطات مورد توجه بشر قرار داشته است . بعد از اختراع و گسترش کامپیوتر که داده های الکترونیکی به وجود آمد ، مهندسین به فکر تبادل این داده ها با کامپیوتر های دیگر افتادند که پایه ای بر ایجاد شبکه های کامپیوتری بود . با گذشت زمان این شبکه ها در ابعاد جغرافیایی و حجم تبادل داده، گسترش پیدا کرد .

مجموعه ای از کامپیوتر های مستقل که از طریق یک رسانه ی انتقال به همدیگر متصل شده و با یکدیگر به تبادل اطلاعات و داده می پردازند ، شبکه کامپیوتری گفته می شود . این شبکه ممکن است دو یا چند کامپیوتر در یک اتاق یا یک شبکه ی گسترده شده در تمام جهان به نام اینترنت باشد



یک نمونه از کاربرد شبکه می تواند شرکتی باشد که دارای بخش های فروش ، انبار و حسابداری است . سیستم های تک تک این بخش ها اطلاعاتی را تولید می کنند ولی نیاز است که این اطلاعات با هم یکپارچه سازی شوند . برای رسیدن به این یکپارچه سازی یک راه حل، استفاده از روش های قدیمی می باشد که خود افراد و مسئولین بخش ها اطلاعات را وارد نموده و با هم ادغام نمایند . اشتباهات فردی در وارد نمودن داده ها می تواند باعث اشتباه شدن در اطلاعات بدست آمده باشد .برای جلوگیری از این نوع مشکلات و به منظور سهل شدن کار ، شبکه نمودن سیستم های این بخش ها با هم و اشتراک منابع آن ها یک راه حل مناسب خواهد بود . هم چنین شبکه می تواند برای اشتراک تجهیزات فیزیکی نیز مورد استفاده قرار گیرد . برای مثال در یک خانه در صورتی که دو یا چند سیستم کامپیوتری موجود باشد ، نیازی به بودن چند پرینتر نمی باشد و شبکه نمودن آن ها و اشتراک یک پرینتر در آن شبکه باعث می شود که تمامی آن سیستم ها بتوانند از آن استفاده نمایند

۲-۱ اجزاء شبکه های کامپیوتری

در هر ارتباط شبکه ، یک کامپیوتر به سرویس یا اطلاعاتی نیاز دارد که این اطلاعات و سرویس را کامپیوتر دیگر در اختیار او قرار می دهد . در نتیجه اجزاء اصلی شبکه به صورت زیر می باشد .

۱-۳-۱ سرویس دهنده (Server)

کامپیوتر سرویس دهنده ، کامپیوتری است که سرویسی که کامپیوتر دیگر آن را نیاز دارد را در اختیار او قرار میدهد .

۱-۳-۲ سرویس گیرنده (Client)

یک سرویس گیرنده کامپیوتری است که از Server درخواست resource sharing سرویس یا اطلاعات خاصی ، که نیاز دارد را می کند .

نکته : وقتی سرویسی در اختیار سرویس گیرنده قرار می گیرد به این معنی نیست که حتماً Client این سرویس را درخواست کرده است چون ممکن است سرویس دهنده بدون درخواست Client تصمیم به اشتراک و ارائه آن گرفته باشد .

۱-۳-۳ محیط انتقال(Communication Media)

بستری که کامپیوتر ها به وسیله آن به هم متصل شده و تبادل اطلاعات روی آن انجام می پذیرد . این بستر می تواند سیمی یا بی سیم باشد .

۱-۳-۴ پروتکل (Protocol)

به قوانینی که برای یک ارتباط ایجاد شده در شبکه یا به صورت کلی برای کلیه ارتباطات شبکه اختصاص داده می شود تا ارتباط به صورت منظم و قابل مدیریت باشد . TCP/IP یک پروتکل کلی شناخته شده در شبکه می باشد که در ادامه بحث خواهد شد .

نکته : برای نمونه کامپیوتر B سرویسی نیاز دارد که کامپیوتر A این سرویس را در اختیار او قرار می دهد . در این ارتباط یک مجموعه قوانینی وجود دارد . منظور این نیست که همیشه کامپیوتر A سرویس دهنده) (Server و کامپیوتر B سرویس گیرنده (Client) می باشند بلکه ممکن است در یک ارتباط دیگرکامپیوتر A نیاز به سرویس داشته باشد که کامپیوتر B بتواند در اختیار او قرار دهد . در نتیجه وظایف این دو با هم عوض می شود .

۳-۱ انواع شبکه های کامپیوتری

شبکه های کامپیوتری از چندین دید متفاوت قابل تقسیم بندی هستند . در شبکه دو مورد از مهمترین موارد که نیاز به توجه زیاد دارند عبارتند از ابعاد جغرافیایی و سرویس دهی . به این جهت در ادامه تقسیم بندی از نظر ابعاد و از نظر مدل سرویس دهی بیان می نماییم .

۱-۳-۱ تقسیم بندی شبکه های کامپیوتری از نظر ابعاد و گستردگی فیزیکی

در این نوع تقسیم بندی ، فاصله ی بین کامپیوتر ها و اجزاء شبکه مورد توجه قرار دارد . با این دید شبکه های کامپیوتری به ۴ نوع PAN ، LAN ، MAN و WAN تقسیم می شوند .

۱-۱-۳-۱ شبکه های شخصی (PAN)

Personal Area Network (PAN) شبکه ای معمولاً محدود به یک میز می باشد . این شبکه متعلق به یک شخص است و تجهیزاتی که او از آنها روی میز خود استفاده می کند یک شبکه تشکیل می دهند . برای مثال ارتباط بی سیم بین ماوس و کیبرد یک PAN را تشکیل می دهند . هم چنین ارتباط بین PDA و کامپیوتر نیز از این نوع است .

۱-۱-۳-۲ شبکه های محلی (LAN)

LAN (Local Area Network) یک شبکه ی خصوصی محدود به یک اتاق یا یک ساختمان یا یک مجتمع می باشد که حداکثر ابعاد آن یک کیلومتر می باشد (البته در بعضی موارد ۲ یا ۳ کیلومتر هم می تواند باشد .) این شبکه ها معمولاً به منظور اشتراک منابع و مبادله ی اطلاعات مورد استفاده قرار می گیرد .

برای مثال شبکه ی کامپیوتر یک شرکت که محدود به یک ساختمان می باشد یا شبکه ی دو ساختمان کنار هم که به صورت یکپارچه شبکه شده اند یک LAN می باشد .

به دلیل این که ابعاد این نوع شبکه ها کوچک و محدود است پس کنترل و مدیریت آن ها آسان و عیب یابی سریع صورت می گیرد در نتیجه نگه داری از آن ها کار سختی نمی باشد .

۳-۱-۳-۱ شبکه های شهری (MAN)

Metropolitan Area Network (MAN) شبکه ای است که نسبت به LAN فاصله اجزا طولانی بوده و می توان گفت که دو یا چند LAN مختلف را به طوری که محدود به یک شهر باشند را یک MAN گویند .

برای مثال شبکه ی شهرداری تبریز که در مناطق مختلف شهر هرکدام به صورت LAN هستند و از طریق خطوط مخابراتی یا بی سیم به هم متصل شده اند . که یک MAN را تشکیل می دهند . شبکه ی تلویزیون کابلی و وایمکس نیز مثالی از MAN می تواند باشد .

۴-۱-۳-۱ شبکه های گسترده (Wide Area Network)

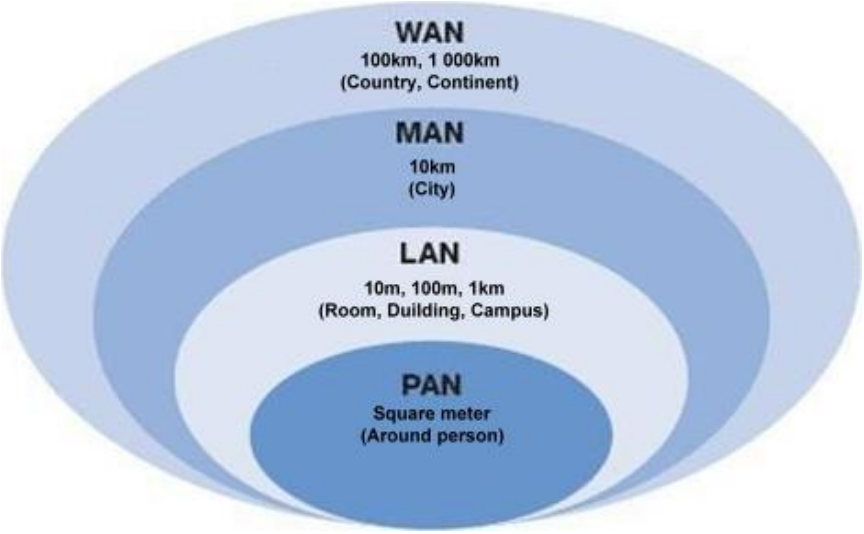
WAN گستره ی جغرافیایی بزرگتری نسبت به LAN و MAN دارد (مانند یک کشور یا یک قاره) . در اغلب شبکه های گسترده زیر شبکه های که می توانند هر کدام یک MAN باشند از دو بخش مجزا تشکیل می شوند : خطوط انتقال که بستر ارتباطی را تشکیل می دهند و تجهیزات سوئیچینگ که ارتباط بین خطوط انتقال را برقرار می کنند .

شبکه ی شهرداری های کشور مثالی از WAN می باشد اگر شهرداری های هر شهر که یک MAN را تشکیل داده اند به هم متصل شده اند . شبکه ی بین یک کارخانه و نمایندگی های آن در چند کشور نیز یک WAN می باشند .

اینترنت خود می تواند یک WAN محسوب شود ولی به دلیل گستردگی وسیع آن در بیشتر منابع آن را از دیگر انواع شبکه جداکرده و به آن شبکه ی شبکه ها گویند .

نکته : نمی توان گفت این سه نوع شبکه از لحاظ سرعت کدامیک بر دیگری برتری دارد ولی به دلیل این که پیاده سازی تکنولوژی با سرعت بالا در LAN ساده تر و کم هزینه تر است در نتیجه معمولاً سرعت LAN از MAN و WAN بیشتر می باشد .

سوال : دو سیستم یک بار از طریق کابل به هم وصل می شوند و بار دیگر از طریق دو اینترنت متفاوت ! در کدامیک سرعت بیشتر خواهد بود ؟

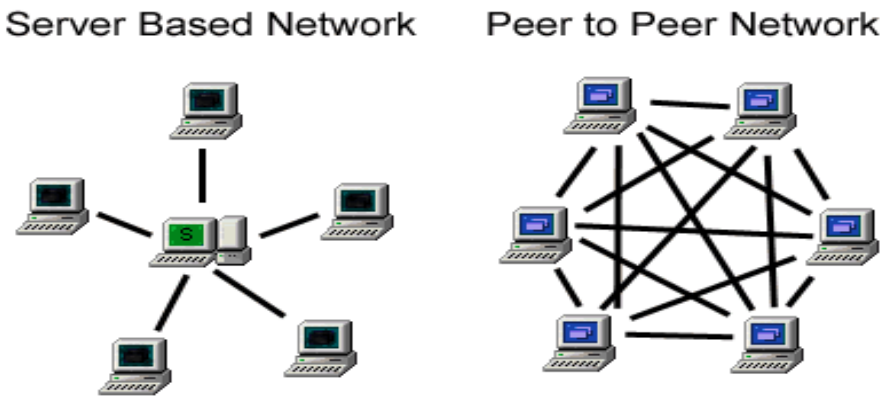


۲-۳-۱ تقسیم بندی شبکه ها از نظر سرویس دهی

از نظر سرویس دهی شبکه های کامپیوتری به دو دسته ی Peer to Peer و Server – Based تقسیم می شوند .

در نوع Peer to Peer (PtP) هر یک از سیستم های موجود در شبکه می توانند سرویس دهنده (Server) یا سرویس گیرنده (Client) باشند یعنی برای مثال سیستمی در یک زمان به عنوان سرویس دهنده عمل می کند . شاید در همان لحظه به عنوان سرویس گیرنده ی کامپیوتر دیگر نیز عمل کند .

در نوع سرویس دهی Server – Based ، یک یا چند سیستم فقط نقش سرویس دهنده (Server) در شبکه را دارند و بقیه ی سیستم ها نقش سرویس گیرنده (Client) دارند . در نقش ها تغییر نمی کنند . مزیت این نوع سرویس دهی ، مدیریت متمرکز آن است .



در این ساختار هدف هر لایه ارائه خدمات به لایه بالاتر خود می باشد . یک لایه ، زمانی باید ایجاد گردد که خدمت متفاوتی مورد نیاز است و در واقع هر لایه باید وظیفه مشخص داشته باشد .

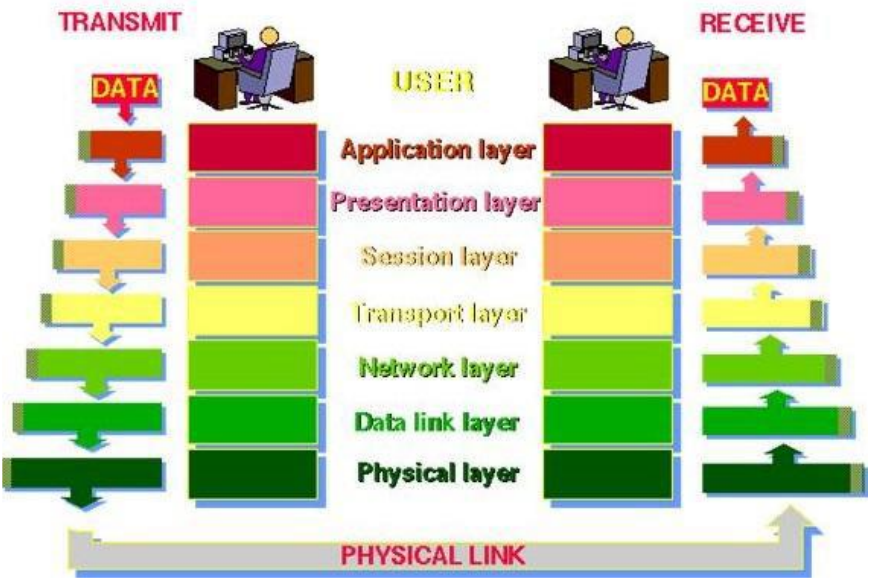
بین لایه های متناظر در گیرنده و فرستنده قوانینی نیز اعمال می شود که به آن ها پروتکل می گویند و به این مجموعه پروتکل ها به همراه لایه بندی و وظایف آن ها ، معماری شبکه (Network Architecture) گفته می شود .

دو مدل کلی در شبکه وجود دارد . OSI ، TCP/IP . OSI یک مدل مرجع بین المللی ۷ لایه می باشد که یک دید کلی از ساختار شبکه را بیان می کند و به پروتکل های خود وابسته نیست چون قبل از اختراع پروتکل هایش طراحی و ابداع شده است . مدل TCP/IP یک مدل چهار لایه ای بر اساس مدل OSI ولی منظم تر از آن می باشد چون این مدل بر اساس پروتکل هایش طراحی شده است و امروزه نیز بیشتر مورد استفاده قرار می گیرد . در ابتدا مدل OSI را بررسی می نماییم و در مباحث آینده به بررسی و کنکاش مدل TCP/IP خواهیم پرداخت .

۱-۴-۱ مدل OSI (Open System Inter connection)

مدل OSI براساس نظرات پیشنهادی سازمان بین المللی استاندارد ها (ISO) به عنوان اولین استاندارد بین المللی شبکه های چند لایه توسعه داده شده است . این مدل در سال ۱۹۹۵ به شکل امروز درآمد ، منظور از

سیستم های باز (Open System) این است که این سیستم ها قادر به ارتباط با سیستم های دیگر هستند .



۱-۱-۴-۱ لایه فیزیکی

لایه فیزیکی (Physical) وظیفه ی انتقال بیت های خام را از طریق کانال مخابراتی (رسانه ی انتقال) بر عهده دارد . در این لایه فقط ۰و۱ عبور می کنند و یک نکته این است که ۰ یا ۱ که فرستنده ارسال می کند باید به همان شکل در گیرنده دریافت شود . هم چنین یک طرفه یا دو طرفه بودن خط و چگونگی بر قراری و قطع ارتباط مواردی است که برای این لایه مهم می باشند .

۲-۱-۴-۱ لایه پیوند داده (Data Link)

بیت هایی که در لایه فیزیکی منتقل می شوند ، پر از خطا می باشند و نیاز است که این خطاها اصلاح شوند و به لایه شبکه تحویل داده شوند . لایه ی پیوند داده وظیفه ی اصلاح این خطاها را دارد . این لایه داده های ورودی را به بسته های کوچک که فریم نامیده می شوند می شکند و ارسال می کند . وظیفه دیگر این لایه این است که چگونه یک گیرنده کند را با یک فرستنده سریع هماهنگ کند . برای این منظور فرستنده باید از وضعیت بافر گیرنده قبل از ارسال اطلاع داشته باشد .

بافر

در لایه ی Data Link برای زمانی که داده ها به صورت پخش یا ارسال به همه (Broadcast) ارسال می شوند یک زیر لایه به نام کنترل دسترسی رسانه (Media Access Control) نیز مورد نیاز است که رسانه های انتقال را مدیریت نماید تا بستر ارتباطی کاملاً پر نشود و ازدحام رخ ندهد . در نتیجه لایه پیوند داده سه وظیفه ی اصلی قالب بندی داده ها ، خطا یابی و کنترل جریان (Flow Control) را بر عهده دارد .

۳-۱-۴-۱ لایه شبکه (Network)

لایه شبکه وظیفه کنترل زیر شبکه و هم چنین چگونگی هدایت بسته های اطلاعاتی را از مبداء به مقصد بر عهده دارد . در این لایه IP مبداء و مقصد مشخص و اضافه می شود . در لایه ی شبکه مسیریابی انجام می شود در

نتیجه می توان گفت روتر از تجهیزات این لایه محسوب می شود .در لایه ی سوم packet ایجاد می شود که ساختار آن در زیر مشخص است .

۱-۴-۱-۴ لایه انتقال (Transport)

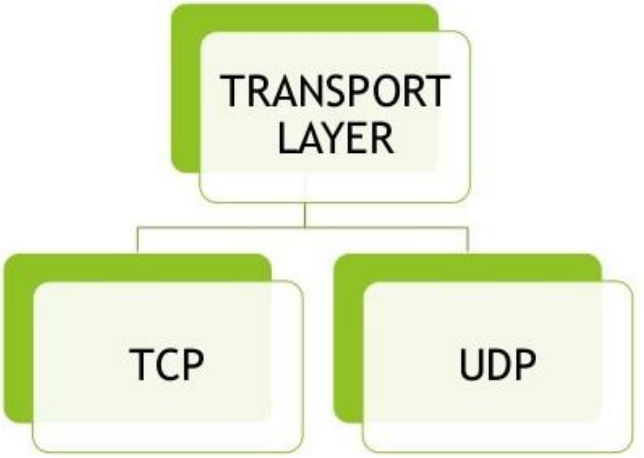
وظیفه اصلی لایه ی انتقال دریافت داده ها از لایه بالاتر و در صورت نیاز شکستن آن ها به اندازه های کوچکتر ، فرستادن آن ها به لایه شبکه و اطمینان حاصل کردن از این که داده ها به طور صحیح به طرف مقابل می رسند .

در این لایه نوع ارسال نیز مشخص می شود . دو نوع ارسال اتصال گرا (TCP) و بدون اتصال(UDP) وجود دارد .

TCP

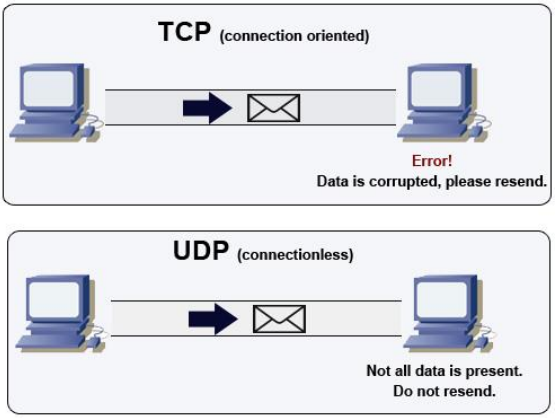
این نوع که معروف به سرویس اتصالگراست (Oriented Connection) ، از دست تکانی سه مرحله ای استفاده می کند به این معنی که قبل از شروع به ارسال داده ها ، یک اتصال اولیه ایجاد می کند و یک بسته به سمت مقصد می فرستد. مقصد زمانی که بسته را دریافت می کند یک Acknowledge به آن می فرستد به این معنی که بسته را دریافت کرده است . فرستنده یک بسته ی دیگر به معنی شروع کردن به ارسال می فرستد و از آن به بعد داده های خود را ارسال می کند . در این نوع ارسال گیرنده بعد از دریافت بسته ها برای هرکدام یک Ack می فرستد و در صورت

نرسیدن Ack یک بسته به فرستنده ، آن را دوباره ارسال خواهد کرد . نوع TCP امنیت بالا اما سرعت پایین (به دلیل انجام دست تکانی سه مرحله ای و Ack) دارد .



UDP

در این نوع ارسال هیچ گونه ارتباط اولیه ای بین مبداء و مقصد وجود ندارد یعنی بدون اتصال (Connection Less) است و فرستنده در اولین ارتباط شروع به ارسال داده های اصلی می کند و هیچ گونه Ack دریافت نمی کند . برای مثال برای مشاهده ی برنامه های زنده از طریق اینترنت اگر بسته ای که شامل چند پیکسل است به مقصد نرسد دیگر نیاز نیست آن بسته دوباره فرستاده شود به دلیل نرسیدن Ack . زیرا دیگر آن قسمت فیلم رد شده است . پس در این گونه موارد از UDP استفاده می شود و هیچگونه Ack فرستاده نخواهد شد در نتیجه سرعت بالا می رود .



۵-۱-۴-۱ لایه جلسه (Session)

زمانی که یک مکالمه ی تلفنی را آغاز می کنید و سلام می دهید یک جلسه بین شما و طرف مقابل آغاز می شود . شاید در این جلسه تصمیم بگیرید ده دقیقه فقط صحبت کنید یا با آغاز مکالمه نسبت به طرف مقابل رسمی یا غیر رسمی صحبت کنید . این موارد یک سری قوانینی است که شما برای آن جلسه وضع می کنید و با گفتن خداحافظ جلسه به پایان می رسد .

لایه ی جلسه مدل OSI نیز به همین صورت عمل می کند و یک سری قوانینی برای آن Session برقرار شده بین مبداء و مقصد وضع می شود . این لایه هم چنین در ارتباط های Half Duplex حساب نوبت ها را نگه می دارد .

وظیفه دیگر لایه جلسه این است که اجازه ندهد دوطرف یک عمل بحرانی را در آن واحد انجام دهند .لایه ی جلسه یک وظیفه مهم نیز دارد که به آن

همگام سازی می گویند . همگام سازی کمک می کند که در هنگام ارسال یک فایل بزرگ ، پس از از کار افتادن یا بروز مشکل ، انتقال دوباره از آخرین نقطه کنترلی ، تکرار شود .

۶-۱-۴-۱ لایه نمایش (Presentation)

لایه Presentation به قواعد و معنای اطلاعات فرستاده شده مربوط می شود . اطلاعاتی که در کامپیوتر های مختلف ایجاد می شود ، ممکن است به شکل های مختلف باشد . پس برای ممکن سازی ارتباط بین آن ها یا پستی سختار داده ها به شکل مجرد تعریف گردد و بر اساس یک استاندارد کد گذاری شود تا در طرف گیرنده همان داده های ارسالی درک شود .

هم چنین در لایه ی نمایش رمز نگاری و فشرده سازی داده ها نیز صورت می گیرد .

۷-۱-۴-۱ لایه کاربردی (Application)

این لایه شامل پروتکل ها و سرویس هایی است که مورد نیاز کاربران می باشد و تمامی برنامه های کاربردی در این لایه انجام می گیرد که در بخش سرویس های TCP/IP ، با چند مورد از آن ها آشنا خواهیم شد .

برای مثال در ارسال یک متن فارسی از طریق یک نرم افزار از ایران به فردی در کشور کانادا مراحل به این ترتیب پیش می روند:

در لایه برنامه های کاربردی طرف ارسال کننده نرم افزار خود را باز کرده و متن را نوشته و ارسال می کند. در لایه ششم (ارائه) این اطلاعات فشرده و رمز می شوند و نوع فشرده سازی و رمزنگاری در سرآیند این لایه نوشته می شود. همچنین اطلاعات کدینگ نیز در اینجا مشخص می شود که مثلا این نامه به زبان فارسی نوشته شده است تا طرف مقابل بداند چگونه باز کند. در لایه جلسه اطلاعات و قوانین مربوط به جلسه ی آغاز شده بین دو طرف نوشته می شود که مثلا زمان جلسه ۱۰ثانیه است و ...

در لایه انتقال نوع ارسال نوسته می شود تا گیرنده بداند با قوانین TCP (مثل ارسال Ack) کارکند یا UDP. در لایه سوم (Network) IP های مبدا و مقصد اضافه شده و packet تشکیل می شود. در لایه دوم آدرس های MAC مبدا و مقصد اضافه شده و فریم ایجاد می شود. بعدا در لایه فیزیکی فریم ها به صورت صفر و یک از طریق بستر فیزیکی به سمت مقصد روانه می شوند.

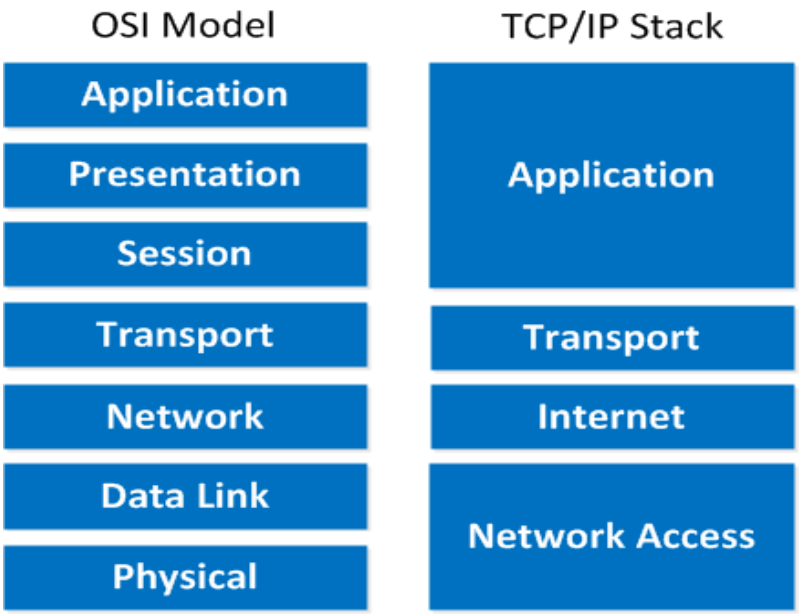
در سمت مقصد با تبدیل داده های به صورت قابل فهم برای کامپیوتر، در لایه پیوند داده MAC مقصد بررسی می شود و در صورت درست بودن (تعلق داشتن به آن سیستم) آن قسمت که فرستنده در واقع در لایه دو ایجاد کرده بود حذف شده و به لایه بالاتر تحویل داده می شود. در لایه

شبکه IP مقصد چک می شود و در صورت صحیح بودن آن قسمت نیز حذف شده و به لایه انتقال تحویل داده می شود. در لایه انتقال که فرستنده نوع انتقال را مشخص کرده بود گیرنده نیز آن را دریافت می کند تا بنداند چگونه با داده ها برخورد کند. در لایه جلسه قوانین مطرح شده به دست گیرنده نیز می افتد و در لایه ارائه گیرنده با نحوه اجرای داده ها آشنا شده و آن ها را در لایه برنامه کاربردی اجرا می کند.

مشکل اصلی لایه بندی OSI این است که بعضی از لایه ها وظایف زیادی انجام می دهند و حتی شامل چندین زیرلایه می باشند اما بعضی هم مثل لایه ی ۵و۶ تقریباً خالی بوده و دارای وظایف کمتری هستند . در نتیجه مدل TCP/IP به وجود آمد که در آن لایه های ۵ ، ۶ و ۷ در یک لایه گنجانده شده اند .

۲-۴-۱ مدل TCP/IP

مدلTCP/IP یک مدل چهار لایه ای است که در دانشگاه برکلی برای اولین بار روی سیستم عامل unix ارائه و سپس بر روی ویندوز گسترش یافت .
در این مدل مانند شکل ، لایه ی کاربردی تقریباً معادل با سه لایه ی نشست (Session) ، ارائه (presentation) و لایه ی کاربردی در مدل OSI و هم چنین لایه ی اینترنت (یا شبکه) معادل لایه ی شبکه ی مدل OSI می باشد .



به جای لایه های پیوند داده و فیزیکی که در OSI مطرح بودند ، در TCP/IP از یک لایه به نام واسط شبکه که عمل تبدیل سیگنال های الکتریکی به ۰ و ۱ به همراه بعضی اعمال دیگر انجام می دهد ، استفاده می شود.

۱-۲-۴-۱ کاربرد پروتکلTCP/IP

پروتکل TCP/IP مجموعه قوانینی است که در مدل TCP/IP اجرا می شوند . این پروتکل بر روی شبکه های کوچک و بزرگ قابل اجرا می باشد و اولین پروتکلی است که عمل Multicast می تواند انجام دهد .

۵–۱ توپولوژی شبکه

منظور از توپولوژی شبکه نحوه ی چیدمان device های موجود در شبکه می باشد . یعنی سیستم های شبکه به چه شکلی کنار یکدیگر قرار گرفته اند. در زیر چند توپولوژی اصلی شبکه را بررسی می کنیم .

Bus 1-5-1

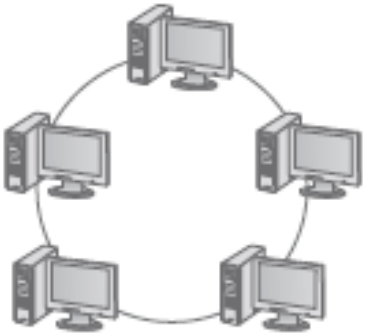
در توپولوژی Bus یا خطی سیستم ها به یک خط وصل شده اند و به صورت یکطرفه با هم ارتباط دارند .

هم چنین دو طرف این خط بسته می باشد که اصطلاحا گفته می شود Terminate شده است.

پس یک مشکل بزرگ این نوع ساختار یک طرفه بودن ارتباط بین سیستم ها می باشد . مشکل بعدی این است که اگر خطی (کابلی) قطع شود کل شبکه از کار خواهد افتاد .

Ring 2-5-1

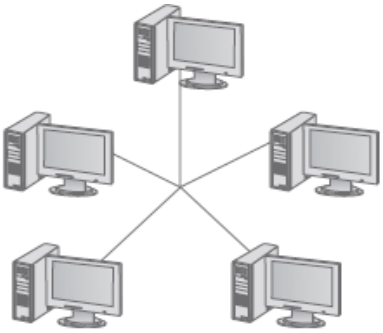
در این توپولوژی یکی از مشکلات Bus حل شه است و اول و آخر توپولوژی Bus به هم وصل شده است تا سیستم ها بتوانند هر یک به همدیگر داده بفرستند و ارتباط داشته باشند .



Ring در اول به صورت یکطرفه بود اما این یک طرفه بودن و برگشت ناپذیر بودن باعث شد که سرعت انتقال داده کاهش یابد در نتیجه بعد ها Ring دوطرفه نیز ایجاد شد . Ring همان مشکل قطع توپولوژی Bus را دارد و اگر یکی از کابل ها قطع شود کل شبکه از کار خواهد افتاد .

Star 3-5-1

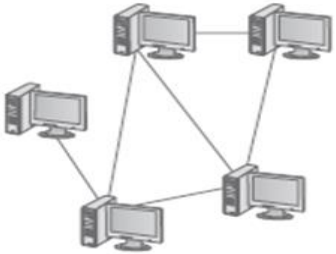
در توپولوژی Star یک device مرکزی وجود دارد که تک به تک سیستم های شبکه مستقیماً به آن وصل می شوند و آن device ارتباط بین آن ها را برقرار می کند این device می تواند Switch ، Hub و . . . باشد .



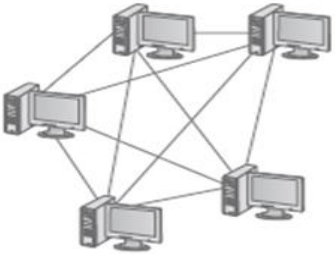
نکته : نیاز نیست که device حتماً در مرکز قرار گرفته باشد .
این توپولوژی مشکلات توپولوژی های قبلی را برطرف می کند . زمانی که یکی از کابل های ارتباطی قطع می شود ، فقط ارتباط آن سیستم با شبکه قطع خواهد شد نه کل شبکه . هم چنین اگر کل شبکه مختل شود یا کار نکند مشکل مشخصا از همان device مرکزی خواهد بود . در نتیجه رفع ایراد (troubleshooting) این نوع شبکه ها آسان خواهد بود .
مشکل اصلی توپولوژی Star این است که اگر device مرکزی مشکل پیدا کند ، کل شبکه از کار خواهد افتاد .

MESH 4-5-1

در این به هم بندی گره ها (سیستم ها یا device های دیگر) به صورت مستقیم بدون واسطه به همدیگر وصل شده اند . Mesh دو نوع است یکی Fully Mesh که تمامی سیستم ها بدون استثناء به هم وصل شده اند و دیگری Partially Mesh که در آن یک سیستم ممکن است به صورت مستقیم به تمامی سیستم های دیگر وصل شود یا این که فقط به تعدادی از آن ها متصل گردد .
مشکل بزرگ این نوع توپولوژی در شبکه های سیمی هزینه ی بالای آن است زیرا به تعداد سیستم ها نیاز به کارت شبکه و کابل وجود دارد .
توپولوژی Mesh در شبکه های بی سیم مورد استفاده قرار می گیرد .



Partially Mesh



Fully Mesh

۱–۶ استاندارد های شبکه

تعداد زیادی سازنده و تامین کننده قطعات و تجهیزات شبکه وجود دارد ، که فکر می کنند می دانند چگونه باید کار خود را انجام دهند . اما بدون یک عامل هماهنگ کننده ، این وضعیت می تواند به یک آشوب واقعی بیانجامد ، و در نهایت هیچ کاری هم انجام نشود . تنها راه برای خلاصی از چنین وضعیتی ، توافق بر سر استاندارد های شبکه است .

استاندارد ها نه تنها اجازه می دهد تا تجهیزات مختلف بتوانند با هم کار کنند ، بلکه فروش محصولات منطبق با استاندارد را نیز افزایش می دهند – و فروش بیشتر یعنی تولید انبوه ، کاهش هزینه ها ، طراحی بهتر ، کاهش قیمت ها و افزایش مجدد درخواست (مگر اقتصاد چیزی غیر از این است).

یکی دیگر از بازیگران بزرگ در صحنه استاندارد های جهانی ، موسسه ی مهندسان برق و الکترونیک (IEEE) است ، که بزرگترین سازمان حرفه ای دنیا محسوب می شود . علاوه بر انتشار کتب و مجلات متعدد و برگزاری

صدها کنفرانس علمی در سال ، IEEE یک گروه تدوین استاندارد نیز دارد که در زمینه ی مهندسی برق و کامپیوتر فعالیت می کند . برای مثال ، کمیته ی ۸۰۲ وظیفه تدوین استاندارد شبکه های LAN را در IEEE بر عهده دارد ، که گروه های کاری آن را در شکل ملاحظه می کنید . میزان موفقیت گروه های کاری ۸۰۲ چندان بالا نیست ، و داشتن عدد ۸۰۲.x تضمینی برای موفقیت یک استاندارد نیست . البته استثنا هایی هم در این زمینه وجود دارد ، که استاندارد های ۸۰۲,۳ و ۸۰۲,۱۱ از آن جمله اند .

در جدول استانداردهای ۸۰۲ IEEE را مشاهده می کنید. استاندارد های مهم با علامت ستاره مشخص شده اند. آن هایی که با فلش رو به پایین مشخص شده اند این روزها استفاده نمی شوند. و ۸۰۲,۸ مدت هاست که از مباحث شبکه حذف شده است.

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

۱-۶-۱ اترنت

استاندارد هایی در زمینه ی شبکه های LAN وجود دارد که مهمترین آن ها عبارتند از : Ethernet ، Token Ring ، Token Bus ، ARC-NET که امروزه از Ethernet به دلیل قابلیت های آن استفاده می شود .

شرکت های DEC ، Intel ، Xerox یک استاندارد واحد وضع کردند و نام آن را DIX Ethernet گذاشته اند که امروزه با Ethernet شناخته می شود .

سازمان IEEE بعد ها Ethernet را به صورت استاندارد بین المللی با نام IEEE802.3 در آورد .

نحوه ی ارسال (Signal transmit) در Ethernet به صورت Digital است یعنی به صورت گسسته به صورت ۰و۱ داده ها ارسال می شوند و با یک احتمال خطای کم در گیرنده دریافت می شوند و در سمت گیرنده اصطلاحاً سیگنال بازسازی می شود .

Ethernet یک استاندارد به صورت Baseband است .

نکته : تفاوت Baseband و Broadband در این است که در اولی در یک بسته ارتباطی فقط یک نوع سیگنال در جریان می تواند باشد . اما در Broadband انواع سیگنال می تواند باشد بدون این که به همدیگر تاثیر منفی بگذارند و مثل کابل تلفن که هم DSL و هم صوت از آن عبور می کند بدون این که تاثیری بر روی هم بگذارند .

Ethernet به همبندی های Bus ، Star ، PTP و Mesh را پشتیبانی می کند . Ring دو طرف را نیز پشتیبانی می کند اما در Ring یک طرف نمی تواند کار کند .

در مبحث کابل ها، زیرکمیته های استاندارد Ethernet بیان شده است.

فصل دوم

کابل ها و تجهیزات شبکه

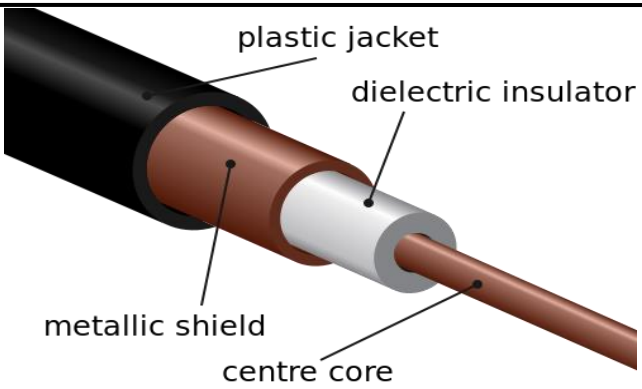
۲–۱ کابل ها و connector های شبکه

در شبکه های سیمی ارتباط شبکه به وسیله ی انواع کابل می تواند برقرار شود . هر کابل به وسیله ی یک connector به سیستم یا device های شبکه وصل می شود . در این قسمت انواع اصلی این کابل ها و connector های مختص آنها را مورد بررسی قرار می دهیم .

سه نوع کابل در شبکه های کامپیوتری مورد استفاده قرار می گیرد که عبارتند از : کابل های کواکسیال ، کابل های زوج سیم بهم تابیده شده و کابل های فیبر نوری که به دو نوع اول کابل های مسی نیزگفته می شود .

۲-۱-۱ کابل های کواکسیال

کابل های کواکسیال یا کابل های هم محور در شبکه های اولیه برای شبکه کردن مورد استفاده قرار می گرفتند . امروزه از این کابل ها برای آنتن های موجود در شبکه استفاده می کنند (آنتن تلویزیون نیز از این نوع است .) ساختار کلی کابل های کواکسیال در شکل زیر مشخص است .



جریان الکتریکی از طریق core از سمت فرستنده به سمت گیرنده ارسال شده و مسیربرگشت را از طریق Shield طی می کند . Shield هم چنین از ایجاد نویز در core جلوگیری می کند . در این نوع کابل ها هر چقدر قطر core و متناسب با آن غلظت بافت الیاف فلزی Shield بیشتر باشد آن کابل در مسافت های طولانی تری قابل استفاده خواهد بود . دو نوع کابل از نظر ضخامت وجود دارد :

۱) کابل کواکسیال نازک معروف به Thin با قطر ۶,۵ mm

۲) کابل کواکسیال ضخیم معروف به Thick با قطر ۱۳ mm

کابل thin به دلیل سبک و انعطاف پذیر بودن نسبت به thick و هم چنین به علت پایین بودن قیمت بیشتر مورد استفاده قرار می گیرد ولی در فواصل طولانی جواب نخواهد داد .

نوعی از کابل thin معروف به RG58 در شبکه های کامپیوتری اولیه مورد استفاده قرار می گرفت که در سه نوع RG58 U (Solid core) ، RG58 A/U (Standard core) و RG58 C/U (نسخه ی نظامی A/U) عرضه می شد .

کابل های thick نیز در دو نوع RG11 و RG8 در شبکه های کامپیوتری استفاده می شد .

نکته : مشهورترین connector کابل های کواکسیال، BNC می باشد .

۲-۱-۲ کابل های Twisted Pair

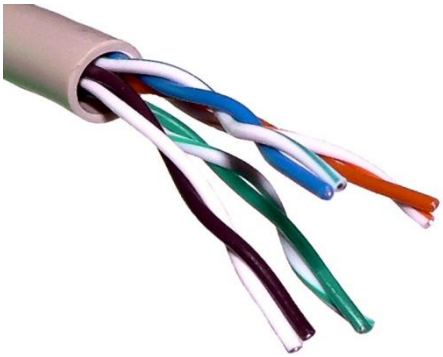
رایج ترین نوع کابل در شبکه های کامپیوتری کابل های زوج سیم بهم تابیده شده (Twisted pair) می باشند که در آن ها چند جفت کابل وجود دارد و هر جفت به هم تابیده شده اند . دلیل به هم تابیدگی این است که میدانی در اطراف خود القاء نکنند و تاثیرات اثرات نویز القاء شده را روی خود خنثی نمایند . در عوض یک عیب بزرگ این کابل ها ایجاد هم شنوایی (Cross Talk) است .

کابل های TP در انواع مختلفی موجود هستند که اصلی ترین انواع آنها عبارتند از :

(Unshielded Twisted Pair) UTP 1-2-1-2

کابل های UTP هیچگونه محافظ (shield) بین زوج سیم ها وروکش پلاستیکی ندارند . در نتیجه در برابر نویز زیاد مقاوم نبوده و کارایی آن ها کاهش خواهد یافت . در عوض این نوع کابل ها قیمت پایین تری نسبت به

بقیه دارند و انتخا خوبی برای محیط های داخلی و کم نویز به حساب می آیند . امروزه نیز بیشترین استفاده از کابل های UTP می شود .

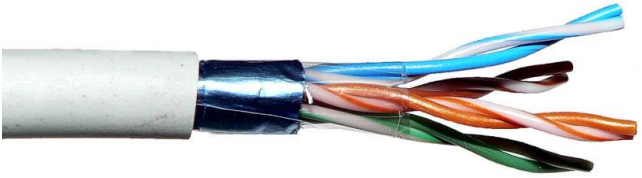


(Shielded Twisted Pair) STP 2-2-1-2

کابل های STP برعکس کابل های UTP دارای یک محافظ بین زوج سیم ها و روکش محافظ هست و این محافظ نسبت به نوع محیط انتخاب می شود . برای مثالShield هایی برای محیط های مرطوب ، یا محیط های دارای نویز های فرکانسی و . . . درست می شوند و بسته به شرایط محیط این نوع کابل ها انتخاب می شوند .

FTP 3-2-1-2 (Foilded Twisted Pair)

در این نوع کابل ها از Foil برای کاهش نویز محیط بین زوج سیم ها و روکش پلاستیکی استفاده می شود . این کابل ها کمی ارزان قیمت تر از نوع STP هستند و در برابر نویز مقاومت کمتری خواهند داشت .



کابل های TP در category های متفاوتی عرضه شده است که هر کدام از این اقسام در ساختار تعداد زوج سیم ها ، حداکثر مقدار داده ی انتقالی و . . . با هم تفاوت دارند که در جدول زیر نشان داده شده اند .

Category	Makeup	Data rate	Network compatibility
Cat-1	2 pair	1 Mbps	Analog voice
Cat-3	4 twisted pairs	10 Mbps – 2 pair	10BaseT
Cat-5	4 twisted pairs	10 Mbps – 2 pair 100 Mbps – 2 pair	10BaseT 100BaseTX
Cat-5e	**4 twisted pairs**	**10 Mbps – 2 pair** **100 Mbps – 2 pair** **1 Gbps – 4 pair**	**10BaseT** **100BaseTX** **1000BaseTX**
Cat-6	**4 twisted pairs**	**1 Gbps – 4 pair** **10 Gbps – 4 pair** (55m)	**1,000BaseTX** **10,000BaseTX**
Cat-6a	**4 twisted pairs**	**10 Gbps – 4 pair**	**10,000BaseTX**

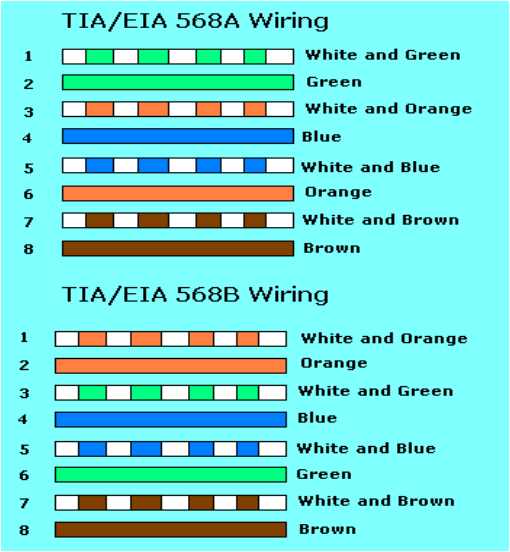
The Evolution of Ethernet Standards to Meet Higher Speeds				
Date	IEEE Std.	Name	Data Rate	Type of Cabling
1990	802.3i	10BASE-T	10 Mb/s	Category 3 cabling
1995	802.3u	100BASE-TX	100 Mb/s*	Category 5 cabling
1998	802.3z	1000BASE-SX	1 Gb/s	Multimode fiber
	802.3z	1000BASE-LX/EX		Single mode fiber
1999	802.3ab	1000BASE-T	1 Gb/s*	Category 5e or higher Category
2003	802.3ae	10GBASE-SR	10 Gb/s	Laser-Optimized MMF
	802.3ae	10GBASE-LR/ER		Single mode fiber
2006	802.3an	10GBASE-T	10 Gb/s*	Category 6A cabling
2015	802.3bq	40GBASE-T	40 Gb/s*	Category 8 (Class I & II) Cabling
2010	802.3ba	40GBASE-SR4/LR4	40 Gb/s	Laser-Optimized MMF or SMF
	802.3ba	100GBASE-SR10/LR4/ER4	100 Gb/s	Laser-Optimized MMF or SMF
2015	802.3bm	100GBASE-SR4	100 Gb/s	Laser-Optimized MMF
2016	SG	Under development	400 Gb/s	Laser-Optimized MMF or SMF
Note: *with auto negotiation				

زیرشاخه های ۸۰۲,۳

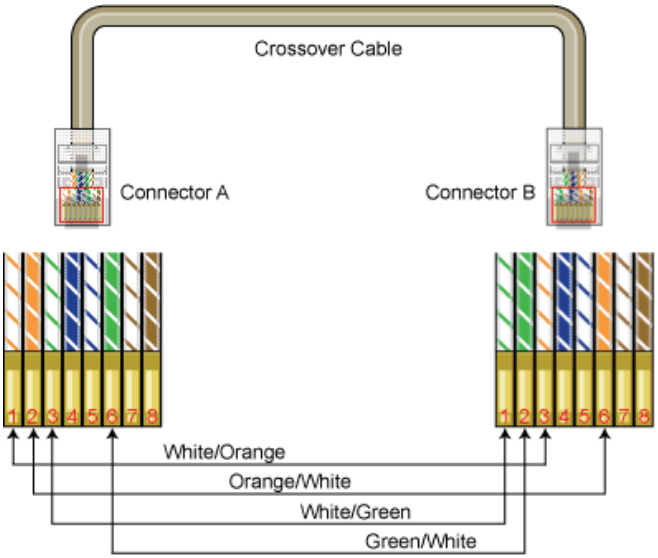
۲-۴-۲-۱ استاندارد سوکت زنی کابل های TP

سازمان TIA (Telecommunications Industry Association) استاندارد های سوکت زنی کابل های TP را مشخص کرده است . سوکتی که برای این نوع کابل ها استفاده می شود معروف به RJ-45 می باشد و استاندارد وضع شده برای سوکت زنی TIA/EIA T568 نام دارد .

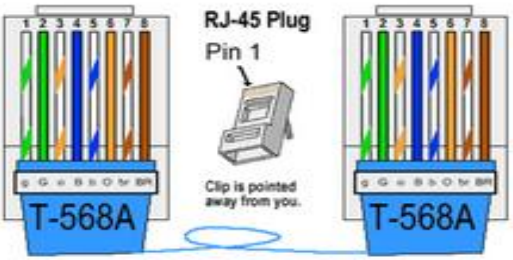
استاندارد TIA/EIA T568 در دو نوع A و B است که در شکل مشاهده می کنید :



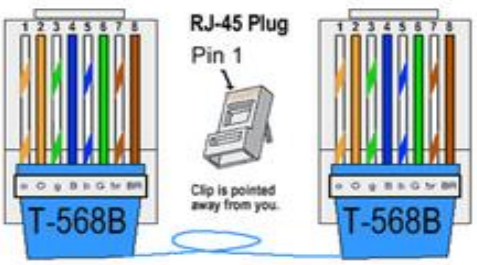
در device های غیر مشابه می توانید در هر دو سمت سوکت زنی را طبق استاندارد A یا در هر دو سمت B زد . اما در دو device مشابه مثل دو عدد PC برای این که ارتباط آن ها طبق استاندارد و به خوبی ایجاد شود آن ها را با کابلی که یک طرف آن استاندارد A و طرف دیگر B باشد به هم وصل می کنند . به کابلی که یک طرف آن A و طرف دیگر B باشد اصطلاحاً Cross Over گویند و کابلی که هر دو طرف آن مشابه باشد (یعنی هر دو A یا هر دو B) ، کابل straight گفته می شود .



Crossover



Straight (A)



Straight (B)

سوال : چرا در سیستم های مشابه کابل Cross Over نیاز است ؟

در استاندارد کابل های شبکه طبق شکل زیر از پین اول و دوم داده ها ارسال و از پین های سوم و ششم دریافت می شوند . در سیستم های مشابه اگر به صورت straight سوکت زده شود در سیستم ارسال کننده اگر داده ها از پین اول و دوم ارسال شود در سمت گیرنده به همان دو پین اول فرستاده می شود که در این دو مثال اولی فقط ارسال تعریف شده است نه دریافت !

نکته : در کارت شبکه های جدید اگر هم دو سیستم مشابه straight زده شود دوباره مشکلی پیش نمی آید و سیستم خودش کابل های دریافتی و ارسالی را شناسایی می کند ، ولی برای عملکرد خوب بهتر است طبق استاندارد عمل شود .

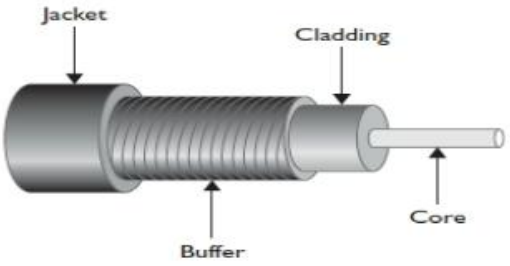
سوال (۱): پین های ۴ ، ۵ ، ۷ و ۸ برای چه عملی استفاده می شوند ؟

سوال(۲): برای ارتباطات زیر از کدام نوع straight یا Cross Over استفاده می شود ؟

PC to PC
Switch to Switch
Modem to Laptop

۳-۱-۲ فیبر نوری (Fiber Optic)

فیبر نوری از ترکیبات پلاستیک فشرده تا سلیس ساخته می شود . این کابل ها توانایی هدایت نور را با سرعت بالا دارند و از این امکان می توان برای ارسال داده ها از طریق این کابل ها استفاده کرد . یک کابل فیبر نوری از سه قسمت اصلی تشکیل شده است . قسمت مرکزی آن هسته (core) نام دارد که داده ها از طریق آن عبور می کنند ، قسمت پوشش دهنده ی هسته clad می باشد که انعکاس دهنده ی نور در داخل هسته است . بالا ترین قسمت کابل فیبر نوری ،Buffer است که کابل را پوشش داده و از نویز جلوگیری می کند .

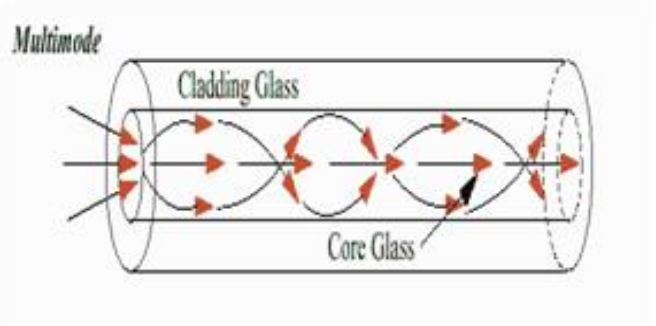


دو نوع فیبر نوری وجود دارد که عبارتند از :

Multi Mode و Single Mode

(MM) Multi Mode 1-3-1-2

اگر شعاع هسته کمی بزرگ باشد طوری که بیش از یک شاخه نور بتواند از آن عبور کند به این نوع فیبر اصطلاحاً Multi Mode گفته می شود . نوری که برای این نوع کابل استفاده می شود می تواند LED یا Laser باشد که نوع LED آن ارزان ترین نوع فیبر نوری به حساب می آید .

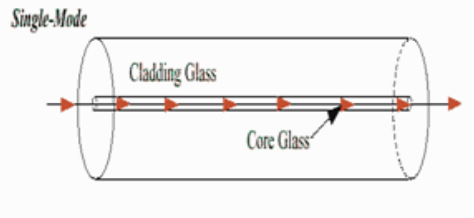


با این که فیبر MM می تواند اطلاعات زیادی را در زمان کوتاه به مقصد برساند ، اما فقط قادر به جوابگویی در مسافت های کم می باشد .هم چنین در نوع LED به دلیل این که چندین شاخه نور (پالس نور) در یک زمان و کنار هم دیگر می توانند عبور کنند (به دلیل بزرگ بودن شعاع) باعث هم پوشانی (Over Lapping) پالس های خروجی خواهد شد .

که برای جلوگیری از آن از لیزر به جای LED استفاده می شود که باعث بالا رفتن هزینه خواهد شد .

(SM) Single Mode 2-3-1-2

در کابل های Single Mode شعاع هسته را تا حد امکان کوچک کرده طوری که تقریباً فقط یک شاخه از نور بتواند از آن عبور کند . در نتیجه فقط از نور لیزر در این نوع استفاده می شود که تمامی این موارد باعث می شودبه دلیل طی کردن مسیر مستقیم این شاخه های نور و نخوردن آن ها به clad ، مسافتی که می توانند برسند افزایش می یابد . پس کابل های SM برای مسافت های طولانی استفاده می شود ، البته قیمت و هزینه ی آنها بالاتر است .



نکته (۱): سه connector پر استفاده ی فیبر نوری ST ، SC و LC هستند .

✓ST 

✓SC 

✓LC 

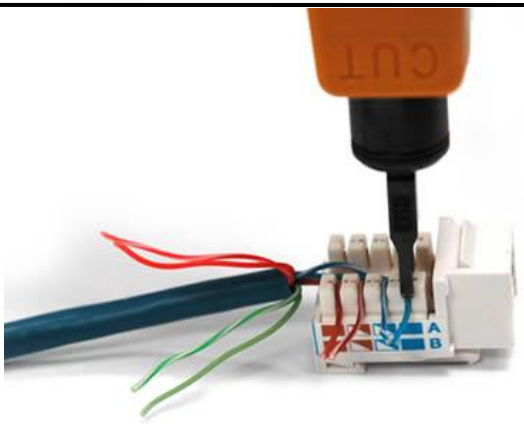
نکته (۲) : فیبر نوری می تواند به PC و سرور ها نیز علاوه بر روتر ها . سوئیچ ها وصل شود اما به کارت های شبکه ی مخصوص به خود است .

چند مورد تجهیزات Passive دیگر

Keystone Jack

قسمتی از کابل در شبکه که در معرض بیشترین آسیب قرار دارد کنار سیستم client ها و سوکت آن ها می باشد . برای مثال در یک ساختمان دو طبقه ، سوئیچ اصلی در طبقه اول قرار دارد و در طبقه ی دوم نیز کامپیوتر های کارکنان وجود دارد که بین سوئیچ و آن کامپیوتر ها کابل کشیده شده است . همان طور که گفته شد در سمت کامپیوتر کارکنان امکان آسیب دیدن کابل زیاد است چون مثلاً کارکنان معمولاً کابل را از سیستم جدا وصل می کنند . هم چنین امکان کشیده شدن کابل و . . . وجود دارد . در صورت ایراد پیدا کردن کابل در این محل ها در بیشتر موارد به دلیل یک تکه بودن کابل رفع ایراد آن سخت خواهد بود . در نتیجه تا کنار سیستم می توان به صورت مستقیم کابل کشید ولی در کنار سیستم یک Keystone Jack زده می شود و کابل بر آن اصطلاحاً patch شده و از آن یک سوکت به بیرون می دهد . پس یک کابل کوتاه از Keystone Jack به سیستم وصل می شود که در صورتی هم که کابل به دلایل مطرح شده مشکل پیدا کند به راحتی تعویض می شود .

نکته : با استفاده از Insertion tools کابل ها به Keystone ، چفت می شود .



Keystone Jack در سه نوع می باشد . یک نوع در داخل داکت قرار می گیرد ، نوع بعدی به دیوار نصب می شود . نوع آخر به صورت پریز مانند است که منظم تر دیده می شود .

Rack

رک محفظه ای است که سرور ها وتجهیزات دیگر شبکه مثل سوئیچ ، روتر ، مودم ، Firewall سخت افزاری و . . . درون آن قرار می گیرند و در نتیجه

از صدمات فیزیکی در امان می مانند . هم چنین در رک سیستم تهویه ی مناسب تعبیه می شود که باعث بالا رفتن کارائی سیستم های داخل آن می شود .

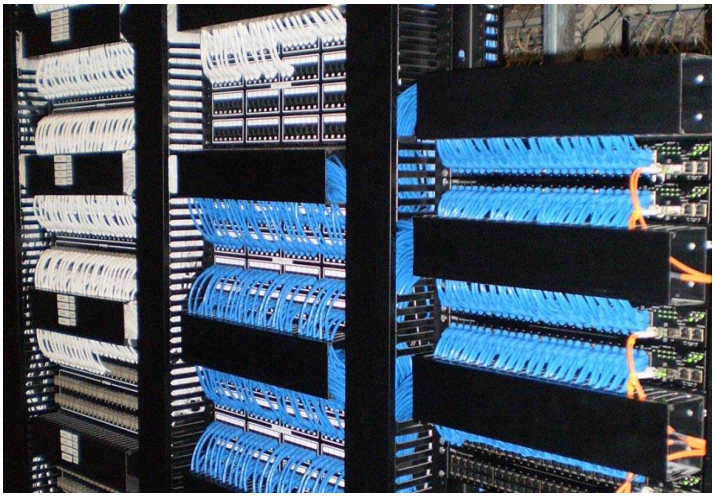
رک در دو نوع دیواری و ایستاده وجود دارد و واحد اندازه گیری آن Unit است که هر یونیت حدوداً برابر ۵ سانتی متر است .

Patch Panel

برای منظم کردن آرایش کابل های داخل رک از Patch Panel استفاده می شود . طوری که کابل های شبکه ابتدا به Patch Panel چفت می شوند و سپس با استفاده از یک کابل Patch Cord به سوئیچ یا روتر و . . . وصل می شوند . در بالای Patch Panel برای هر کابل می توان نام آن را نوشت که باعث نظم خواهد شد .

Patch Cord

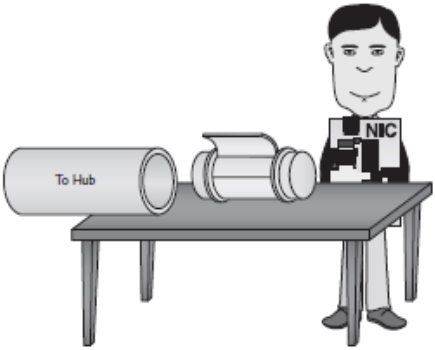
کابل هایی که به صورت آماده به بازار می آیند و سوکت های آن ها توسط کارخانه سازنده زده شده و معمولاً دوام بالاتری دارند معروف به کابل Patch Cord هستند.



Device 2-2 های شبکه

۱-۲-۲ کارت شبکه (NIC)

هر سیستم یا دستگاهی که بخواهد در یک شبکه فعالیت کند نیاز است که یک کارت شبکه داشته باشد . کارت شبکه یک device است که دارای چند چیپ مجزا می باشد و اعمال در یافت و ارسال اطلاعات از طریق بسته را بر عهده دارد .



هر کارت شبکه یک آدرس منحصر به فرد در دنیا را دارد که به آن آدرس فیزیکی یا MAC Address گفته می شود . این آدرس فیزیکی ۴۸ بیت می باشد که ۲۴ بیت اول آن OUI (Organization Unique Identifier) که نشان دهنده ی ، کارخانه ی سازنده کارت شبکه و ۲۴ بیت بعدی را خود کارخانه ی سازنده اختصاص می دهد که به صورت منحصر به فرد تعیین می گردد .

MAC Address شامل اعداد بین ۰ تا ۹ و حروف A – F می باشد .

برای مشخص کردن آدرس MAC یک سیستم از چند روش می توان استفاده کرد که سه روش معمول بیان می شود .

روش اول :

به تنظیمات کارت شبکه های خود وارد شوید (راحت ترین روش تایپ کردن NCPA.CPL در استارت است .) ، روی کارت شبکه ی خود راست کلیک کرده و Status را انتخاب کنید ، در صفحه ی باز شده دکمه ی Details را فشار دهید . در سطر physical address آدرس فیزیکی آن کارت شبکه را مشاهده می کنید .

نکته : در صورتی که کارت شبکه مورد نظر connect باشد این قسمت را می توان مشاهده کرد .

روش دوم :

به قسمت command prompt ویندوز رفته (تایپ CMD در Run یا استارت) و در آن جا تایپ کنید :

Ipconfig /all

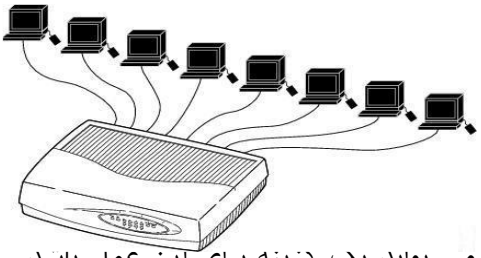
همان طور که مشاهده می کنید تنظیمات و آدرس MAC کارت شبکه یا کارت های شبکه شما را نشان می دهد .

روش سوم :

وارد CMD شده و تایپ کنید :

getmac

این مورد نیز فقط آدرس های فیزیکی (MAC) کارت یا کارت های شبکه شما را نشان می دهد .



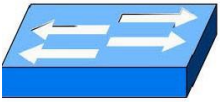
Hub 2-2-2

در توپولوژی star همان طور که بیان شد نیاز به یک device مرکزی می باشد که ارتباط را بین سیستم ها برقرار کند . Hub می تواند یک دزینه برای این عمل باشد . تمام سیستم ها به Hub وصل می شوند و ارتباطات را برقرار می کند . زمانی که یکی از سیستم ها می خواهد بسته ای را به سیستم دیگر بفرستد ، هاب این بسته را به کل پورت هایش کپی می کند . اصطلاحاً این بسته به همه broadcast می شود . سیستمی که این بسته به اول تعلق دارد آن بسته را باز می کند ولی بقیه بسته را بیرون می اندازد .

دو مشکل اصلی در ساختار Hub وجود دارد . اولی این که وقتی داده ها در شبکه broadcast می شوند بار شبکه زیاد خواهد شد که این می تواند باعث کندی شبکه و ازدحام شود ، مشکل دوم این است که داده هابه هم ارسال می شوند در نتیجه امنیت کاهش می یابد .

Repeater 3-2-2

Repeater همان مثل Hub عمل می کند ولی در توپولوژی Bus استفاده می شود .



Switch 4-2-2

دستگاه Switch پر استفاده ترین device در شبکه محسوب می شود و مشکلات هاب را حل کرده است . Switch نیز در توپولوژی star مورد استفاده قرار می گیرد و تمامی دستگاه ها از طریق سیم به این device متصل شده و ارتباط بینشان برقرار می شود .سیستم (۱) که می خواهد داده هایی را به سیستم (۲) بفرستد سوئیچ داده های ارسالی را فقط به پورت سیستم (۲) کپی خواهد کرد . در صورتی که سیستم (۱) بخواهد داده ها را به سیستم های ۲ ، ۴ و۱۵ بفرستد ، سوئیچ داده ها را به پورت های این سه مورد کپی می کند . حتی در صورتی که سیستم (۱) بخواهد داده هایی را به تمامی سیستم های شبکه ارسال کند (broadcast) دوباره سوئیچ این مورد را عملی خواهد کرد . در نتیجه سوئیچ Unicast ، Multicast و

broadcast را انجام می دهد . سوئیچ معمولا با تعداد پورت ها و سرعت آن ها مشخص می شود.

نکته: سوئیچ هایی که در شماره مدل آن ها حرف G وجود دارد، دارای پورت هایی با سرعت یک گیگابیت در ثانیه هستند.

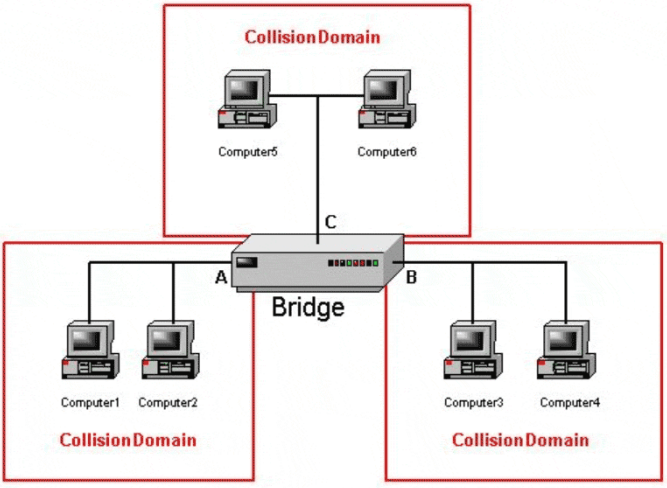
از یک دید سوئیچ دو نوع است . سوئیچ لایه ۲ که در لایه ی ۲ مدل OSI کار می کند و با آدرس MAC داده ها را به مقصد می رساند و سوئیچ لایه ی ۳ که با IPطرف گیرنده ، داده ها را به او ارسال می کند یعنی در لایه ی سه مدل OSI (لایه شبکه) کار می کند و چند شبکه را به هم متصل می تواند بکند .

از دید دیگر سوئیچ ها در دو نوع cut through (on the fly) و store and forward هستند . در نوع cut through سوئیچ بسته های آمده را به پورت های مقصد کپی می کند و هیچ گونه اعمالی روی آنها انجام نمی

دهد . اما در نوع store and forward ، بسته های رسیده به سوئیچ در سوئیچ ذخیره می شوند و یک سری اعمالی مثل رمز نگاری ، فشرده سازی و . . . را سوئیچ روی آن ها انجام داده سپس به سمت طرف گیرنده ارسال می کند .

Bridge 5-2-2

تفاوت bridge و Switch دقیقاً مثل تفاوت Hub و Repeater است . bridge در توپولوژی bus مورد استفاده قرار می گیرد .



Router 6-2-2

سوئیچ لایه ۲ و Hub ، ارتباط سیستم های یک شبکه را برقرار می کند . Router برای ارتباط دو یا چند شبکه ی متفاوت مورد استفاده قرار می گیرد . این device ها معمولاً دارای چیپ هایی برای انجام اعمال مسیریابی هستند و تفاوت اصلی آن ها با سوئیچ لایه سه در این است . سوئیچ لایه ۳ با این که می تواند دو یا چند شبکه را مسیردهی نماید اما به دلیل نبودن چیپ های قدرتمند برای این کار ، اگر مسیر ها کمی پیچیده باشند ، سوئیچ لایه ۳ وظایف خود را درست انجام نمی دهد . پس روتر در لایه ی سوم مدل OSI کارکرده و از IP مبداء و مقصد برای رساندن بسته ها به مقصد استفاده می کند . شرکت سیسکو و میکروتیک دو شرکت فعال در زمینه ساخت روتر محسوب می شوند.

توجه: روتر Broadcast را از خود عبور نمی دهد.

نکته : مودم نیز یک نوع روتر محسوب می شود که در مباحث آتی دلایل آن مشخص می شود .

فصل سوم

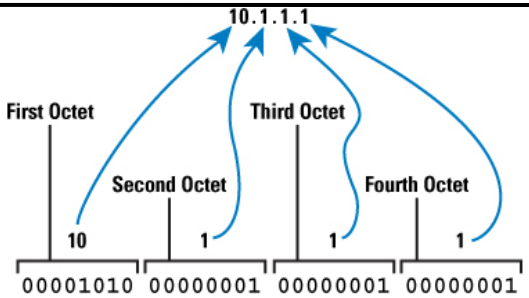
IP (Internet Protocol)

۱–۳ آدرس IP

IP یک آدرس منحصر به فرد در داخل یک شبکه است که در لایه ی ۳ کار می کند . پس یک تفاوت مهم بین آدرس MAC و IP در این است که MAC در کل دنیا منحصر به فرد است ولی IP فقط در یک شبکه منحصر به فرد می باشد .

آدرس های IP در دو ورژن ۴ و ۶ موجود هستند که در این جا به بررسی ورژن ۴ یا همان IPv4 به صورت خلاصه خواهیم پرداخت و سرویس هایی را نیز روی این مورد پیاده خواهیم کرد . IPv4 دارای ۴ اکتت است که هر اکتت دارای ۸ بیت می باشد در نتیجه این ورژن IP دارای ۳۲ می باشد. پس هر اکتت می تواند بین ۰ تا ۲۵۵ باشد.

نکته: در یک دسته بندی IP ها را به دو دسته Valid و InValid تقسیم میکنند. IP های ورژن ۴ در صورتی Valid گفته می شوند که از ۴ اکتت تشکیل شوند که هر اکتت بین ۰ تا ۲۵۵ باشند.



IPv4 در ۵ کلاس دسته بندی شده است که عبارتند از :

Class A	1.0.0.0 - 126.۲۵۵.۲۵۵.۲۵۵
Class B	128.۰.۰.۰ - ۱۹۱.۲۵۵.۲۵۵.۲۵۵
Class C	19.۲۰.۰.۰ - 223.۲۵۵.۲۵۵.۲۵۵
Class D	224.۰,۰.۰ - ۲۳۹.۲۵۵.۲۵۵.۲۵۵
Class E	240.۰.۰.۰ - ۲۵۴.۲۵۵.۲۵۵.۲۵۴

یعنی برای مثال ۱۳۰,۱۲۰,۱۴۰,۱۱ در کلاس B و IP ۱۹۲,۱۶۸,۱۰۰,۱۹ در کلاس C قرار دارد .

Subnet mask

در واقع هر IP خود به تنهایی معنی ندارد و به همراه Subnet mask خود معنی پیدا می کند . یک سیستم برای این که تشخیص دهد دو IP در یک شبکه قرار دارند یا نه ، خود IP ها را تک به تک با Subnet mask شان AND می کند .

نکته : در عمل AND در صورتی که هر دو عدد ۱ باشد جواب ۱ خواهد بود . در غیر این صورت ۰ می باشد .

بعد از این که هر IP را به Subnet mask مربوط به خودش AND کرد جواب های به دست آمده را با هم مقایسه می کند . در صورت برابر بودن جواب ها ، دو IP در یک شبکه قرار دارند .

Subnet mask های default کلاس ها در جدول زیر نوشته شده اند . به صورت خلاصه می توان گفت که در Subnet mask ، NID ها برابر ۲۵۵ و HID ها برابر صفر می باشند .

Class	Subnet Mask decimal	No. of Hosts per Network	No. of Networks	Start -End Address
A	255.0.0.0	16 Million	127	1.0.0.0 - 126.255.255.255
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255
C	255.255.255.0	254	2 Million	192.0.0.0 - 223.255.255.255
D	Reserved for multicast groups			224.0.0.0 - 239.255.255.255
E	Reserved for future use, or Research and Development Purposes			240.0.0.0 - 254.255.255.254

NID در کلاس A شامل اکتت اول ، در کلاس B شامل دو اکتت اول و در کلاس C شامل سه اکتت اول می باشد یعنی برای مثال در کلاس C یک IP مثال می زنیم :

۱۹۲.۱۶۸.۱.۱۶ /۲۴

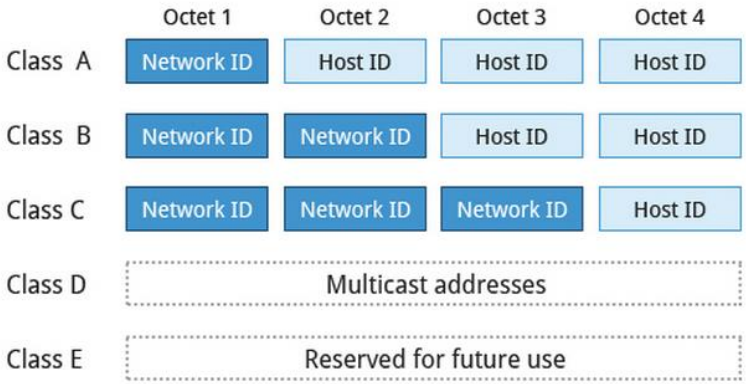
NID (Net ID) : ۱۹۲.۱۶۸.۱

HID نیز به اکتت هایی به جز NID اطلاق می شود :

HID (Host ID) : 16

منظور از NID ، کد شناسایی شبکه می باشد یعنی برای این که دو یا چند سیستم در یک شبکه قرار گیرند باید NID آن ها برابر شود .

HID نیز کد شناسایی Client های شبکه می باشد .



NN (Network Name) برابر با نام شبکه است برای نوشتن NN ، باید NID را عیناً نوشته ولی به جای HID صفر قرار دهیم .

برای مثال NN در IP ۱۹۲,۱۶۸,۱,۱۶ /۲۴ برابر با ۱۹۲,۱۶۸,۱,۰ /۲۴می باشد .

برای پیدا کردن آدرس Broadcast یک شبکه یعنی آدرسی که اگر برای آن بسته ای ارسال کنیم به همه در شبکه ارسال خواهد شد نیز NID را عیناً نوشته ولی به جای HID ، ۲۵۵ قرار خواهیم داد . در مثال قبل آدرس Broadcast خواهد شد : ۱۹۲,۱۶۸,۱,۲۵۵ /۲۴

مثال : در IP زیر NID ، HID ، NN و Broadcast address مشخص شده است : ۱۵۰,۱۰۰,۱,۴ /۱۶

چون در کلاس B است پس در اکتت اول NIP و دوتای بعدی HID خواهند شد و داریم :

NN: 150.100.0.0 /16

Broadcast address : 150.100.255.255 /16

تمرین : NID ، HID ، NN و Broadcast address را برای IP های زیر مشخص کنید :

۱۰.۲۷.۱۶.۱ /۸

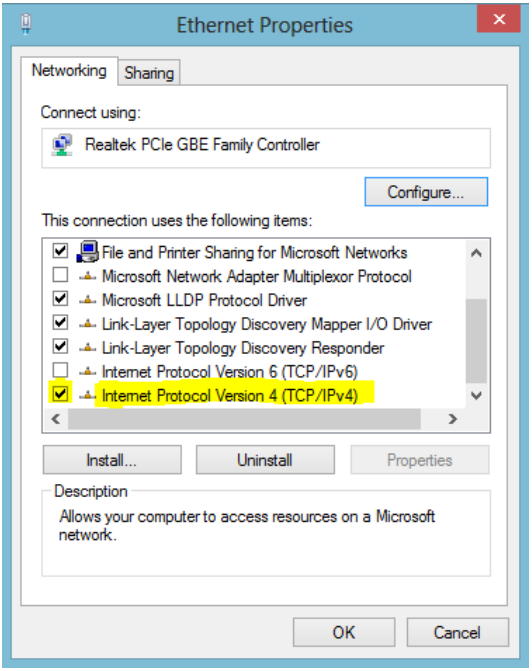
۲۰۰.۰.۰.۱ /۲۴

نکته : رنج ۱۲۷,۰,۰,۰ تا ۱۲۷,۲۵۵,۲۵۵,۲۵۵ معروف به IP های Loop back هستند . این رنج مشخص کننده ی خود سیستم می باشند و از آن ها در شبکه استفاده نخواهیم کرد .

نکته مهم : همان طور که مشخص شد ، در هر IP ، تمام HID ها صفر یا تمامی آن ها ۲۵۵ باشد ، به ترتیب معروف به NN و Broadcast IP هستند و نمی توان از آن ها در دادن IP به سیستم ها استفاده کرد . برای مثال از کلاس C ما می توانیم به ۲۵۴ سیستم IP داده و استفاده کنیم چون HID که برای Client ها استفاده می شود می تواند ۲۵۶ تا عدد (۰

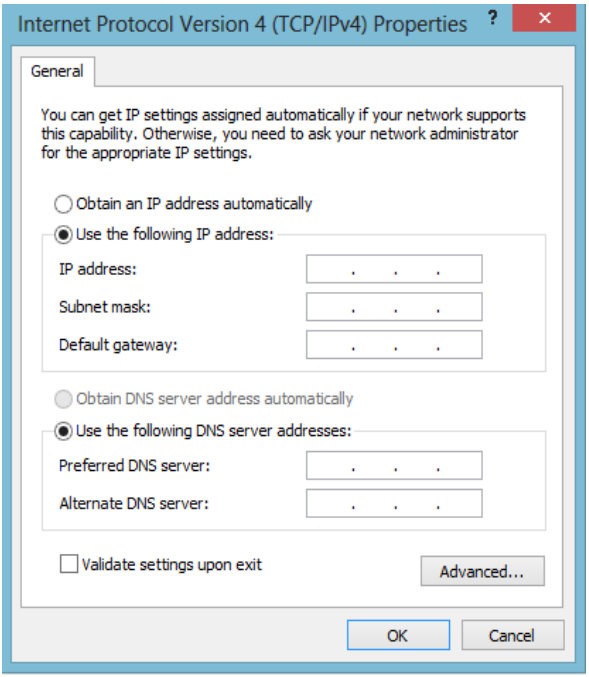
تا ۲۵۵) بگیرد ولی خود صفر و ۲۵۵ را نمی توانیم بدهیم پس داریم ۲۵۶-۲=۲۵۴

برای اختصاص دادن IP به کارت شبکه ی سیستم خود ابتدا وارد تنظیمات کارت های شبکه شوید . (در جستجو تایپ کنید NCPA.CPL) روی کارت شبکه ی خود راست کلیک کرده و properties را انتخاب نمایید . سپس گزینه ی Internet Protocol Version 4 را انتخاب کرده و وارد properties آن شوید .



در این قسمت با انتخاب گزینه ی اول یعنی obtain an IP address automatically به سیستم اجازه می دهیم که اگر یک سروری (DHCP)

در شبکه آدرس IP را به سیستم ها به صورت خود کار اختصاص می دهد ، از آن سرور IP بگیرد .



با انتخاب گزینه ی دوم یعنی use the following IP address خودتان به صورت دستی IP مورد نظرتان را اختصاص دهید . در قسمت IP address ، آدرس IP را نوشته و در قسمت دوم Subnet mask آن را قرار دهید .

در Default Gateway آدرس روتر یا مودمی که اینترنت را برای شبکه ی شما ارائه می دهد یا شبکه ی شما را به یک شبکه ی دیگر وصل می کند را

وارد نمایید . با اختصاص Gateway به سیستم می گویید که در صورتی که یک IP درخواست شود ولی در شبکه شما نباشد ، آن را به مودم یا روترتان تحویل دهد .

در پایین نیز آدرس IP سرور DNS خود را در صورت وجود خواهید نوشت .

نکته : در صورت نیاز به اختصاص چند آدرس IP برای کار در شبکه های متفاوت در قسمت Advanced آن ها را وارد کنید .

Subnetting

در بعضی از شبکه ها نیاز است که شبکه به زیر بخش هایی تقسیم شود که از هم دیگر جدا شده و نتوانند به هم دسترسی پیدا کنند اما همگی در قالب یک شبکه باشند . به این کار زیر شبکه بندی یا Subnetting گفته می شود .

فرض کنید یک شرکت دارای ۴ بخش حسابداری ، فروش ، اداری و هیئت مدیره است و در نظر دارد شبکه ی این ۴ بخش را به دلایل مدیریتی و امنیتی از هم جدا کند . برای این کار به کل زیر عمل خواهیم کرد : (IP شرکت ۲۴/ ۱۹۲,۱۶۸,۱,۰ است) .

$$۲ \text{ ^ } ? \geq ۴$$

یعنی ۲ به توان چه عددی از ۴ (تعداد زیر شبکه ها یا همان بخش های شرکت) بزرگتر مساوی خواهد بود.

عدد به دست آمده mask bit نام دارد . در این مثال : mask bit = 2
Subnet mask پیش فرض این IP برابر ۲۵۵,۲۵۵,۲۵۵,۰ است پس از روی آن Subnet mask جدید را پیدا خواهیم کرد : (که معادل /۲۶ خواهد بود که معادل تعداد یک هاست .)
دو بیت (همان به تعداد mask bit) از Host ID را برداشته و ۱ می کنیم که در این مثال برابر خواهد بود با :

۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱,۱۱۱۱۱۱۱۱,۱۱۰۰۰۰۰۰

پس Subnet mask جدید را بدست آوردیم که معادل ۲۵۵,۲۵۵,۲۵۵,۱۹۲خواهد بود.
حالا IP ها و زیر شبکه ها را پیدا خواهیم کرد :
همان طور که مشاهده می کنید از ۲ بیت جدا شده ۴ حالت که معادل ۴ زیر شبکه است داریم

۱۹۲.۱۶۸.۱. ۰۰ ۰۰۰۰۰۰
۱۹۲,۱۶۸,۱. ۰۱ ۰۰۰۰۰۰
۱۹۲,۱۶۸,۱. ۱۰ ۰۰۰۰۰۰
۱۹۲,۱۶۸,۱. ۱۱ ۰۰۰۰۰۰

در نتیجه ۴ زیر شبکه بدست آمد .
برای هر زیر شبکه نام زیر شبکه ، اولین آدرس معتبر از آن زیر شبکه ، آخرین آدرس معتبر و آدرس broadcast آن زیر شبکه را پیدا می کنیم .

زیر شبکه اول :

نام زیر شبکه اول 192.168.1.0 /26 : 000000 ۱۹۲ .۱۶۸.۱.۰۰

اولین آدرس معتبر 192.168.1.1 /26 : 192.168.1.00 000001

آخرین آدرس معتبر ۱۹۲,۱۶۸,۱,۶۲/۲۶ : ۱۹۲,۱۶۸,۱,۰۰ ۱۱۱۱۱۰

آدرسbroadcast ۱۹۲,۱۶۸,۱,۶۳/۲۶ : ۱۹۲,۱۶۸,۱,۰۰ ۱۱۱۱۱۱

زیر شبکه دوم :

نام زیر شبکه دوم ۱۹۲,۱۶۸,۱,۶۴/۲۶ : ۰۰۰۰۰۰ ۱۹۲,۱۶۸,۱,۰۱

اولین آدرس معتبر ۱۹۲,۱۶۸,۱,۶۵/۲۶ : ۰۰۰۰۰۱ ۱۹۲,۱۶۸,۱,۰۱

آخرین آدرس معتبر ۱۹۲,۱۶۸,۱,۱۲۶/۲۶ : ۱۱۱۱۱۰ ۱۹۲,۱۶۸,۱,۰۱

آدرسbroadcast ۱۹۲,۱۶۸,۱,۱۲۷/۲۶ : ۱۱۱۱۱۱ ۱۹۲,۱۶۸,۱,۰۱

و همین طور دو زیر شبکه ی بعدی بدست می آید .

نکته : در Subnetting ، زیر شبکه های متفاوت هیچ گونه دسترسی به هم ندارند و حتی هم دیگر را ping هم نمی توانند بکنند .

Supernetting

فرض کنید در شبکه ای ۵۰۰ سیستم وجود دارد و همان طور که بیان شد ، شما در کلاس C می توانید ۲۵۴ عدد IP بدهید . پس مجبور خواهید شد از کلاس B استفاده کنید . اما در این کلاس IP های زیادی هدر خواهد رفت . هم چنین زیاد بودن رنج IP ها در بعضی موارد مثل زمانی که برنامه های خاصی تمامی IP های موجود را برای انجام اعمال خاصی جست و جو می کنند ، بار شبکه زیاد خواهد ش . در نتیجه بهتر است رنج IP ها کاهش یابد . برای این کار از Super netting استفاده می شود .

Super netting با قسمت Net ID کار می کند و از آن بیت هایی را به نسبت نیازش به HID خواهد داد .در این مثال در حالت عادی HID در کلاس C ، ۸ بیت دارد که $۲^۸-۲=۲۵۴$ می شود . اما اگر ۹ بیت HID باشد $۲^۹-۲=۵۱۰$ پس جوابگوی ۵۰۰ عدد سیستم این شبکه خواهد بود . پس ۱ بیت از NID به HID اختصاص خواهیم داد : (فرض کنید IP=192.168.100.0/24)

بیت در نظر گرفته شده می تواند دو حالت داشته باشد یعنی یا ۱ یا ۰

۱۹۲.۱۶۸.۰۱۱۰۰۱۰۰.۰۰۰۰۰۰۰۰

۱۹۲.۱۶۸.۰۱۱۰۰۱۰۱.۰۰۰۰۰۰۰۰

پس شبکه ی جدید بین ۱۹۲,۱۶۸,۱۰۰,۰/۲۳ تا ۱۹۲,۱۶۸,۱۰۱,۲۵۵ /۲۳خواهد بود .

نام شبکه ی جدید ۱۹۲,۱۶۸,۱۰۰,۰/۲۳ ، اولین IP معتبر ۱۹۲,۱۶۸,۱۰۰,۱/۲۳ ، آخرین IP معتبر ۲۳/ ۱۹۲,۱۶۸,۱۰۱,۲۵۴ و آدرس broadcast این شبکه ۲۳/ ۱۹۲,۱۶۸,۱۰۱,۲۵۵ خواهد بود .

Subnet mask جدید در این شبکه نیز ۲۵۵,۲۵۵,۲۵۴,۰ می شود یعنی ۱۱۱۱۱۱۱۱,۱۱۱۱۱۱۱۱,۱۱۱۱۱۱۱۰,۰۰۰۰۰۰۰۰ که معادل ۲۳/ خواهد بود .

نکته : با انجام Super netting تمام IP های بین اولین و آخرین آدرس معتبر می توانند با هم ارتباط داشته باشند و حتی هم دیگر را ping نمایند.

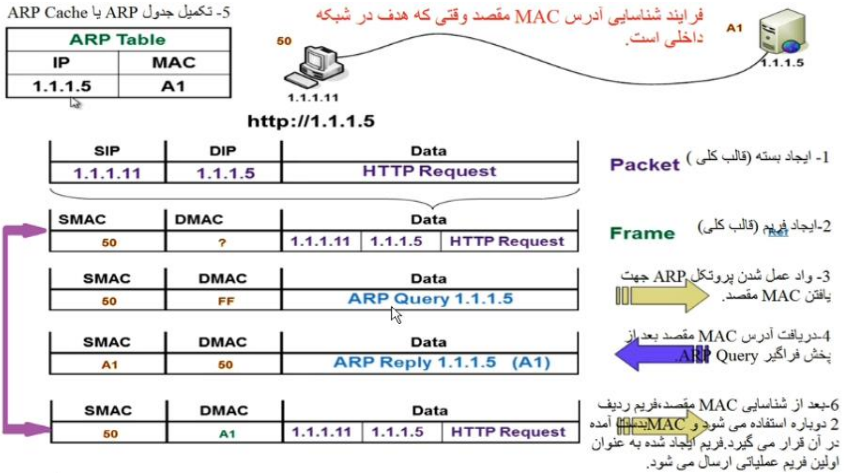
ARP ۲-۳

سوئیچ های لایه ی ۲ همان طور که از نامشان مشخص است در لایه ی ۲ کار می کنند و باید آدرس MAC مقصد را بدانند تا به آن بسته ارسال کنند . در حالت عادی کامپیوتر فقط MAC خود را می داند و زمانی که یک PDU به سمت مقصد می خواهد ارسال کند معمولاً فقط IP مقصد را در اختیار دارد .

APR پروتکلی است که آدرس های MAC سیستم های شبکه را با IP آن ها مشخص می کند . APR به این شکل کار می کند :

زمانی که یک سیستم در شبکه می خواهد برای اولین بار با سیستم دیگر ارتباط برقرار کند در حالی که فقط آدرس IP آن را دارد ، ابتدا یک PDU

به شکل زیر به تمامی سیستم ها ی شبکه ای که سوئیچ لایه ۲ دارد Broadcast می کند . برای Broadcast کردن در شبکه ای که دارای سوئیچ لایه ۲ است یعنی با MAC کار می کند نیاز است که آدرس MAC مقصد را در PDU ، FF:FF:FF:FF بگذارد یعنی Broadcast بکند و به همه ی سیستم های شبکه بفرستد .



سیستم های شبکه این PDU را دریافت کرده و بعد از چک کردن MAC مقصد در لایه ی ۲ که خود آن ها را هم شامل می شود ، به لایه ی سوم رفته و IP مقصد را بررسی می کنند . IP مقصد اگر IP آنها بود که اجازه می دهند به لایه های بالا رفته و Data را باز می کنند ، در غیر این صورت PDU ارسال شده را به بیرون می اندازند .

زمانی که سیستم هدف Data را باز کند ، در ARP ، در قسمت Data یک دیتای کم حجم بنام ARP Query گذاشته شده است و سیستم با

بازکردن آن متوجه خواهد شد که منظور سیستم ارسال کننده بدست آوردن آدرس MAC او است پس یکPDU در جواب آن به سیستم اول ارسال خواهد کرد و در آن MAC آدرس مبداء همان آدرسی خواهد بود که سیستم اول دنبال آن می گردد و در قسمت Data ، جواب ARP خواهد نوشت . پس سیستم اول MAC آدرس سیستم دوم را پیدا کرده و آن را در جدول ARP خود به همراه IP آن می نویسد و در دفعات بعدی از آن جدول استفاده خواهد کرد .

نکته : قبل از برقراری هر گونه ارتباط در این نوع شبکه ها ، اولین کار چک کردن جدول ARP می باشد .

- ✓ برای مشاهده جدول ARP در یک سیستم وارد CMD شده و تایپ کنید .

ARP –a یا ARP –g

- ✓ برای پاک کردن کل جدول:

ARP -d

نکته : برای پیدا کردن آدرس MAC مقصد زمانی که سیستم مقصد در یک شبکه ی دیگر می باشد این فرایند در دو مرحله صورت می گیرد ، یکی در میان سیستم مبداء و روتر و دیگری بین روتر و سیستم مقصد .

فصل چهارم

Workgroup و Sharing

دو نوع ساختار مدیریت کاربران شبکه وجود دارد که عبارتند از : Workgroup و Domain .

Workgroup : در این نوع ساختار تمامی کامپیوتر های موجود در شبکه با هم ارتباط دارند بدون این که سیستمی به عنوان سیستم احراز هویت مرکزی موجود باشد . به این معنی که احراز هویت کاربران تک تک کامپیوتر ها در خود هر کامپیوتر انجام می شود .

Domain : بر اساس سرویس Active Directory بنا نهاده شده است . در این ساختار یک کامپیوتر مرکزی که معمولاً دارای سخت افزار قوی تر نسبت به بقیه ی کامپیوتر های شبکه است و احراز هویت Account های کاربران را بر عهده دارد .

در Domain ، Account هایی برای کاربران در سرور مرکزی ساخته می شود . اما کاربران از تمامی کامپیوتر های موجود در شبکه که عضو Domain شده اند می توانند وارد Account خود شوند نه از یک سیستم خاص ، مگر این که محدودیت هایی برای این کار اعمال شود .

در این دوره راه اندازی شبکه Workgroup بررسی خواهد شد.

۱–۴ راه اندازی Workgroup

برای راه اندازی یک شبکه Workgroup باید به سه مورد مهم دقت نماییم.

۱) IP سیستم ها

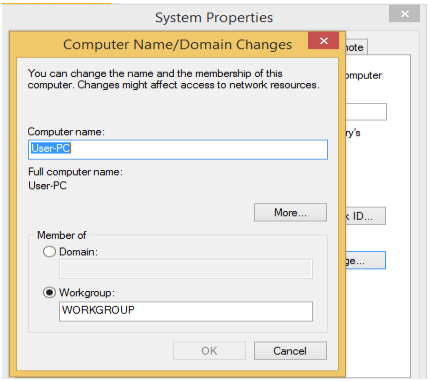
IP تمامی سیستم هایی که می خواهیم با آنها Workgroup راه اندازی کنیم باید در یک رنج شبکه قرار داشته باشند . در سناریوی عملی که ما می خواهیم اجرا کنیم IP سیستم ها را در رنج شبکه ۱۹۲,۱۶۸,۴۳,۰ /۲۴ انتخاب می نماییم .

نکته : برای این که سیستم ها در شبکه بتوانند با هم ارتباط داشته باشند باید IP های هم رنج داشته باشند .

۲) Workgroup Name

نام Workgroup سیستم هایی که تشکیل شبکه ی Workgroup می دهند باید برابر باشند .

با راست کلیک روی This PC (My Computer به قسمت Properties می رویم و از قسمت Change طبق شکل می توانیم نام Workgroupرا تعریف نماییم.



نکته(۱): تغییر دادن نام کامپیوتر

و همچنین عضو کردن آن به دامین در این قسمت صورت می گیرد.

نکته(۲): معمولاً در راه اندازی شبکه Workgroup یک شرکت ، نام Workgroup را به نام آن شرکت ثبت می کنند .

در اینجا همان نام Workgroup را قرار می دهیم .

۳) تنظیمات دسترسی

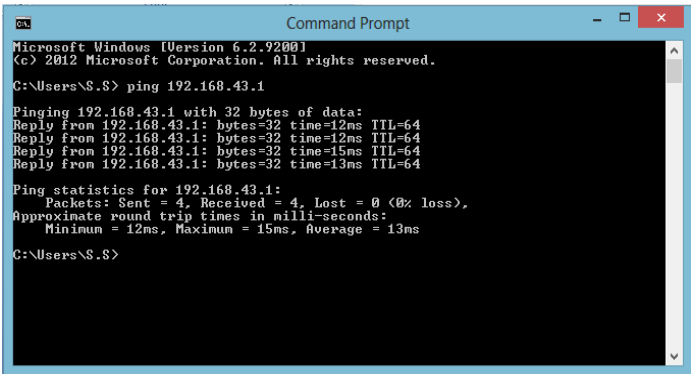
همان طور که گفته شد فایروال سیستم با فایروال نرم افزار هایی مثل Smart Security و ... ارتباطات با سیستم (هم ورودی و هم خروجی) را کنترل می کنند و به صورت پیش فرض اجازه ی دسترسی به سیستم را از اکثر پورت ها نخواهند داد . برای این منظور برای راه اندازی شبکه ی مورد نظرمان ، ابتدا باید فایروال سیستم را خاموش نماییم تا از برخی دسترسی ها و ارتباطات جلوگیری نکند و یا اینکه فایروال خود را برای پروتکل ICMP و پورت Sharing ، config نماییم و اجازه ی دسترسی به آن ها بدهیم . البته معمولا به صورت پیش فرض این موارد در فایروال اجازه داده شده اند. (در مبحث Firewall چگونگی config آن مطرح شد .)

ما در این سناریو Firewall را خاموش می نماییم و نرم افزار دیگری برای انجام عمل Firewall نداریم . حالا یک شبکه ی Workgroup راه اندازی شد . برای این که بودن ارتباط بین سیستم ها را مشخص کنیم از دستور ping در CMD ویندوز استفاده می کنیم . برای انجام این عمل وارد محیط Command Prompt ویندوز شده و دستور:

Ping IP

را تایپ می کنیم . (به جای IP آدرس IP سیستم مقابل نوشته می شود.)

در صورت وجود ارتباط جواب زیر را دریافت می نماییم .



Reply که مشاهده می کنید به این معنی است که سیستم شما به آن سیستم یا Device بسته های ۳۲ بایتی می فرستد و سیستم مقابل در یک زمان نشان داده شده به سیستم شما جواب میدهد. پس نشان می دهد که ارتباط وجود دارد. دستور ping چند سوئیچ مهم دارد که در بسیاری از مواقع استفاده از آنها لازم می باشد .

ping-t : این دستور مشهور به ping به صورت ممتد است . با استفاده از ایت دستور ما به صورت ممتد ping می گیریم و مثلاً در مواقعی که در شبکه مشکل وجود دارد از این دستور استفاده کرده و زمانی که مشکل رفع شد ping مان جواب خواهد داد .

ping-a : این دستور نام کامپیوتر سیستم مقابل را به ما نشان می دهد . در بعضی موارد در شبکه نیاز است که نام کامپیوتر طرف مقابل را بدست آوریم . برای این منظور به جای این که به صورت فیزیکی پشت آن سیستم بنشینیم از این دستور استفاده می کنیم .

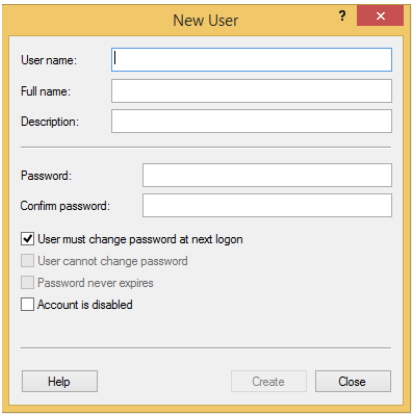
ping-l : همان طور که قبلاً ذکر شده ping معمولی بسته های ۳۲ بایتی را می فرستد . در بعضی مواقع نرم افزار های تحت شبکه ی ما بسته هایی بیش از این مقدار ارسال و دریافت می کنند . به این دلیل ما می توانیم مقدار بایت بسته های ping را افزایش دهیم .

نکته : به جای size فقط از ۰ تا ۶۵۵۰۰ بایت می توانیم قرار دهیم.

ایجاد کاربر

برای ایجاد کاربر جدید برای هر سیستم مراحل زیر را انجام می دهیم :

- روی(This PC (My Computer راست کلیک کرده وارد قسمت Manage شوید .
- وارد شاخه Local users and group شده و Users را باز کنید .
- راست کلیک کرده و New Users را انتخاب کنید .
- در صفحه ی باز شده در قسمت Username نام کاربری را وارد کرده و
- در قسمت password و confirm password پسورد مورد نظر را برای آن کاربر وارد کنید .



- در پایین ۴ مورد وجود دارد :

User must change password at next log on : به این معنی که کاربر در اولین Log on به سیستم باید پسورد خود را عوض کند .

User can't change password : کاربر به هیچ وجه نمی تواند پسورد خود را عوض کند .

Password Never expire : پسورد کاربر هیچ موقع منقضی نخواهد شد.

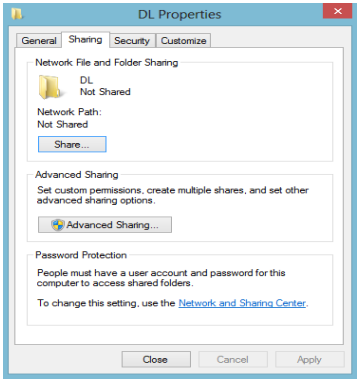
Account is disable : کاربر مورد نظر ایجاد می شود ولی با انتخاب این گزینه کاربر نمی تواند از Account خود استفاده کند و وارد سیستم شود .

نکته (۲) : با راست کلیک کردن روی کاربر ایجاد شده و رفتن به قسمت properties می توان سطح دسترسی های کاربر مورد نظر را تغییر داد .

موارد مربوط به دسترسی ها و کاربران در دوره ی ویندوز بیان می شود .

۲-۴ راه اندازی Sharing

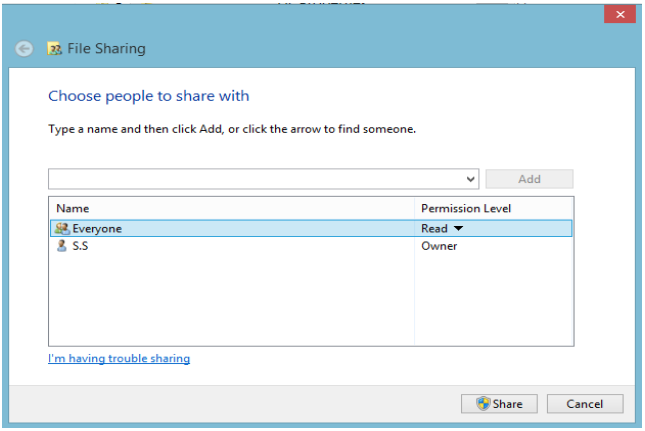
یک نیاز مهم در اکثر شرکت ها و مکان هایی که شبکه راه اندازی می کنند ، به اشتراک گذاشتن فایل ها و folder هایشان است . برای مثال در یک شرکت نقشه کشی ، هر فرد قسمتی از نقشه ساختمان را کار می کند و آن را به فرد دیگری تحویل می دهد و او یک قسمت دیگر آن را کامل می کند . یک روش استفاده از cool disk می باشد اما این مورد نیز مشکلات مربوط به خود را دارد و باعث کاهش سرعت انجام کار نیز می شود . بهترین روش شبکه کردن سیستم های آن ها است تا بتوانند فایل های خود را به اشتراک بگذارند برای این کار دو راه حل وجود دارد . راه اول این است که یک folder در یکی از سیستم ها که معمولاً در ساعات کاری روشن است به اشتراک گذاشته شود و همه روی آن folder فایل های خود را به اشتراک بگذارند که در واقع مدیریت این folder و حتی ویروس یابی آن راحت تر خواهد بود . روش بعدی این است که در هر سیستم یک folder (برای مثال به نام آن سیستم) به اشتراک گذاشته شود و از طریق آن بقیه با آن ارتباط داشته باشند . برای به اشتراک گذاشتن ساده یک folder روی آن راست کلیک کرده و وارد Properties شوید . بعد وارد تب Sharing شده و گزینه ی Share را انتخاب کنید .



در قسمت add می توانید کاربرانی که می توانند به این folder دسترسی داشته

باشند را انتخاب کنید ، سپس در پایین نوع دسترسی آن ها را مشخص کنید .

دسترسی Read یعنی این که کاربر مشخص شده فقط می تواند folder و محتویات آن را بازکرده و ببیند . Read/Write به این معنی است که کاربر مورد نظر هم محتویات را می تواند ببیند و هم آن ها را تغییر یا حتی پاک کند .



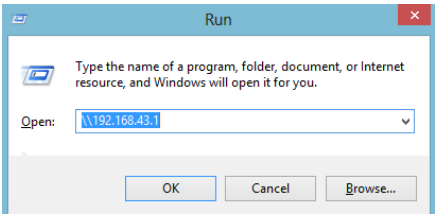
در آخر Share را زده و از آن جا خارج شوید . در نتیجه folder مورد نظر برای گروه یا کاربری که انتخاب نموده اید به اشتراک گذاشته شد .

نکته (۱) : برای به اشتراک گذاشتن گزینه ی Advanced Sharing نیز وجود دارد که می توان permission ها را کامل کنترل کرد ولی از مجال این دوره خارج است .

نکته (۲) : برای به اشتراک گذاشتن پرینتر در شبکه روی printer راست کلیک کرده و به printer properties رفته و از تب Sharing ، گزینه ی Share this printer را بزنید .

برای این که بتوان به folder ها و حتی پرینتر های به اشتراک گذاشته ی یک سیتم متصل شد دو روش کلی و معمول وجود دارد :

روش اول : در Run یا حتی در آدرس بار پنجره ی (This PC Computer) تایپ شود :



// IP سیستم طرف مقابل

// نام کامپیوتر سیستم طرف مقابل

منظور از طرف مقابل همان سیستمی است که قصد بازکردن folder های به اشتراک گذاشته ی آن را دارید .

روش دوم :

Network را در سیستم خود باز کرده و منتظر بمانید تا تمامی سیستم های موجود در شبکه را بیاورد .پس با بازکردن هریک ، تمامی فایل ها و folder های به اشتراک گذاشته توسط او خواهید دید .

نکته (۱) : در ویندوز ۷ و ۸ یک قسمت به نام Advanced Sharing Settings وجود دارد که در آن قسمت می توان اجازه ی به اشتراک گذاری در سیستم و برخی از تنظیمات مربوط به آن گنجانده شده است .

مسیر این قسمت :

Control Panel / Network and sharing center / Change advanced sharing settings

نکته (۲) : در صورت مشاهده نکردن سیستم ها در قسمت Network به قسمت Advanced sharing settings رفته و Network discovery را turn on نمایید .

۳-۴ چند Command مهم

Netstat

دستور netstat برای مشاهده ارتباطات آماده و همچنین ارتباطات برقرار شده با سیستم مورد استفاده قرار می گیرد. با این دستور می توان ارتباطات تروجان ها، برنامه ها و شخص های مخرب که قصد تخریب یا به دست آوردن اطلاعات سیستم را دارند، شناسایی و آن ها را قطع کرد. برای استفاده از این دستور وارد CMD شده و کلمه netstat را تایپ کنید. دستور netstat چند سوئیچ مهم دارد که عبارتند از:

Netstat –n : این دستور به جای نام کامپیوتر، IP سیستم طرف مقابل را در اختیار ما قرار می دهد.

Netstat –b : این سوئیچ فایلی که با آن IP در ارتباط است را نشان می دهد.

Netstat –a : تمامی ارتباطات برقرار شده و آماده برای ارتباط را نشان می دهد.

Traceroute

این دستور که در سیستم عامل های مایکروسافتی به صورت tracert نوشته می شود مسیر شما تا سیستم مقصد را نشان می دهد و hop های بین شما را مشخص می کند. از این دستور برای عیب یابی استفاده می شود. بدین گونه که اگر ارتباط با سیستمی در خارج از شبکه قطع شده است میتوان بررسی کرد که این ارتباط تا کجا سالم است و مشکل در کدام قسمت می تواند باشد (به جای بررسی تک تک قسمت ها) نحوه اجزای این دستور:

tracert (ip or name)

مثال: tracert google.com

Ipconfig

این command موارد مربوط به تنظیمات کارت شبکه را نشان می دهد که دارای چندین سوئیچ است که به چند مورد مهم اشاره می کنیم :

Ipconfig /all : تمامی IP ها وآدرس های MAC کلیه کارت های شبکه ی سیستم به همراه برخی جزئیات آن ها را نشان می دهد .

Ipconfig /release : برای آزاد و صفر کردن آدرس های IP کارت شبکه از سرور DHCPاستفاده می شود . یعنی IP که سیستم از سرور DHCP گرفته است را پاک می کند .

Ipconfig /renew : این سوئیچ سعی می کند دوباره از سرور DHCP آدرس IP بگیرد .

Ipconfig /displaydns : این دستور محتویات داخل DNS Cache را نشان می دهد .

نکته : در این Cache نام DNS ها (سایت ها و DNS های داخلی شبکه) به همراه IPآن ها در اولین ارتباط نوشته می شود تا در ارتباطات بعدی به جای جست و جوی دوباره آن ها از این قسمت درخواست شود تا سرعت بالا رود .

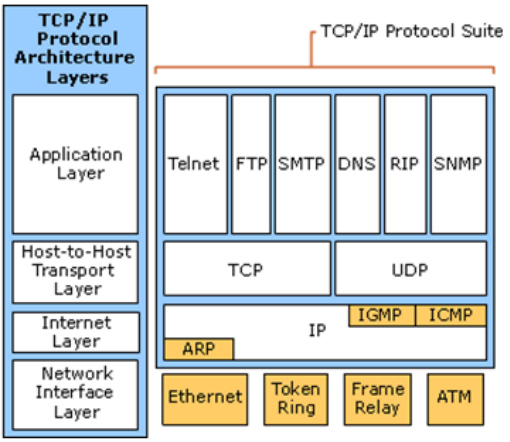
Ipconfig /flushdns : این دستور DNS Cache را پاک می کند .

فصل پنجم

TCP/IP

TCP/IP ۱-۵

همان طور که در فصل اول بیان شد این مدل از ۴ لایه تشکیل شده است که در شکل نیز مشخص است.



پروتکل TCP/IP یک پروتکل پیچیده است که می تواند الگوریتم های متنوع مسیریابی و انتقال براساس Connection Oriented و Connection Less را انجام دهد. این پروتکل برای تمامی ابعاد شبکه،

اعم از شبکه های بزرگ و کوچک استفاده می شود. همچنین اولین پروتکلی است که قادر به اجرای Multicating است.

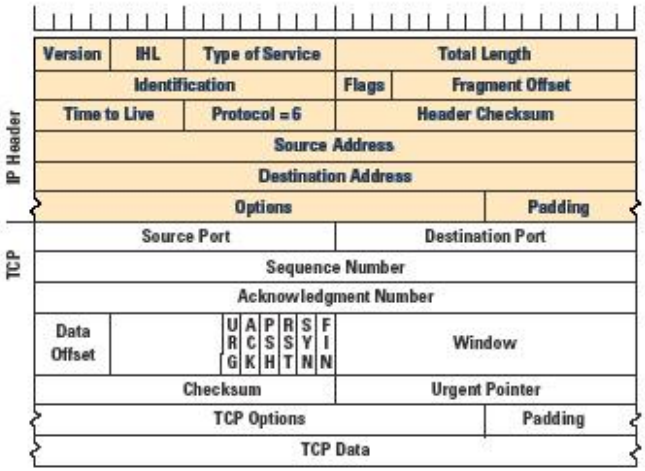
یادآوری

Unicast : ارسال به یک سیستم

Broadcast : ارسال برای تمامی سیستم های شبکه

Multicast : ارسال به گروهی از سیستم های شبکه

نکته: شکل بسته TCP را در شکل زیر مشاهده می کنید. برای اطلاعات بیشتر در کتاب شبکه های کامپیوتری تانن بام قسمت مربوطه را مطالعه نمایید.



۲–۵ سرویس های TCP/IP

سرویس در واقع خدماتی است که در شبکه می تواند انجام شود . هر سرویس برای این که اجرا شود باید از یک پورت کامپیوتر سرویس دهنده خارج و وارد یک پورت کامپیوتر سرویس گیرنده شود .

پورت یک درگاه ورودی یا خروجی است که عمل رد و بدل شدن اطلاعات از طریق آن صورت می گیرد . به هر پورت یک عددی اختصاصی داده می شود که آن عدد بین ۱ تا ۶۵۵۳۵ می تواند باشد . برای انجام اعمال مدیریتی و امنیتی ، به هر یک از سرویس های اصلی شبکه یک پورت خاصی اختصاص داده می شود که این پورت ها بین ۱ تا ۱۰۲۳ هستند و معروف به پورت های شناخته شده می باشند . رنج بعدی پورت ها بین ۱۰۲۴ تا۴۹۱۵۱ می باشند . زمانی که شما از یک سرویس استفاده می کنید ، مشخصاً سرویس دهنده از پورت شناخته شده ی مختص آن سرویس در سیستم خود به شما سرویس می دهد ولی سیستم شما معمولا یک پورت به صورت random از ۱۰۲۴ تا ۴۹۱۵۱ انتخاب کرده و از طریق آن ، سرویس را دریافت می کند .

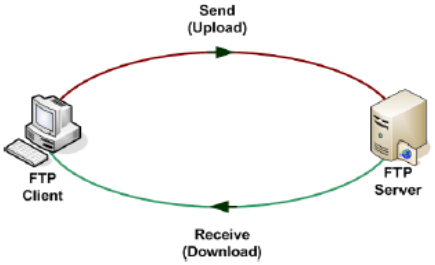
سری سوم پورت ها بین ۴۹۱۵۱ تا ۶۵۵۳۵ هستند که به ندرت توسط برنامه ها مورد استفاده قرار می گیرند و در بعضی سرویس ها استفاده می شود. معمولاً توسط Trojan ها یا virus ها نیز استفاده می شوند .

در ادامه به چند مورد از سرویس های مهم TCP/IP اشاره می کنیم .

FTP 1-2-5 (یا TFTP)

FTP (File Transfer Protocol) انتقال فایل را در شبکه بخصوص شبکه ی اینترنت انجام می دهد و بودن یک سرویس مجزا برای این عمل باعث می شود سیستم های مختلف که دارای سخت افزار های متنوع هستند در قالب یک سرویس و یک استاندارد به تبادل فایل بپردازند .

FTP در واقع عمل upload و download را انجام می دهد و از دو قسمت تشکیل شده است : FTP Client و FTP Server . به عمل ارسال اطلاعات از FTP Client به FTP Server ، upload و هم چنین به عمل ارسال اطلاعات ازFTP Server به FTP Client ، download گفته می شود .



سرویس FTP از دو پورت شناخته شده ی TCP 20,21 استفاده می کند که TCP 20 برای ارسال و دریافت اطلاعات و TCP 21 برای ارسال فرامین مورد استفاده قرار می گیرد .

نکته: برای دسترسی به سرویس FTP در مرورگر خود به این شکل آدرس را وارد نمایید:

ftp:// Address

که آدرس به صورت آدرس IP یا نام سرور FTP نوشته می شود.

HTTP 2-2-5 (Hyper Text Transfer Protocol)

سرویس HTTP برای دستیابی به اطلاعات از طریق browser استفاده می شود . در این سرویس HTTP Client همان browser می باشد و HTTP Server همان سرور وب سایتی است که به آن وصل می شویم .

سرویس HTTP از پورت ۸۰ TCP استفاده می کند .

HTTPS 3-2-5 (Hyper Text Transfer Protocol Secure)

HTTPS نیز مانند HTTP پروتکلی برای استفاده از وبسایت ها می باشد . HTTPS بین کلاینت و سرور دیتای وب سایت دارای HTTPS را رمز می کند تا اطلاعات را کسی نتواند در میان این دو قسمت شنود کند .

وب سایتی که خواستار استفاده از این سرویس هست نیاز دارد که یک SSL برای خود خریداری کند . SSL دو عمل انجام می دهد . اول این که داده

های بین سرویس گیرنده های وب سایت و وب سایت را رمز می کند . دومی این که به وب سایت اعتبار می دهد و آن را تضمین می کند . SSL های رایگان نیز وجود دارند که فقط عمل رمزنگاری را انجام می دهند ولی اعتباری به وب سایت مورد نظر نمی دهند.

HTTPS از پورت ۴۴۳ TCP,UDP استفاده می کند .

نکته : با وجود امنیت بالای HTTPS ولی چون سرعت انتقال این پروتکل پایین تر از HTTP است پس فقط در صفحات نیاز به امنیت بالا مثلاً صفحه ی پرداخت بانک از آن استفاده می شود .

(Tele Network) Telnet 4-2-5

Telnet روشی برای وصل شدن به سیستم ها و device ها در شبکه می باشد به صورتی که هیچ گونه پردازشی روی اطلاعات در سیستمی که Telnet می زند صورت نمی گیرد و تمامی موارد در سیستم مرکزی یا همان سیستمی که به آن با Telnet وصل شده ایم صورت می گیرد . به سیستمی که Telnet می زند Telnet Client وسیستمی که به آن Telnet می زنیم Telnet Server گفته می شود .

Telnet از پورت ۲۳ TCP استفاده می کند .

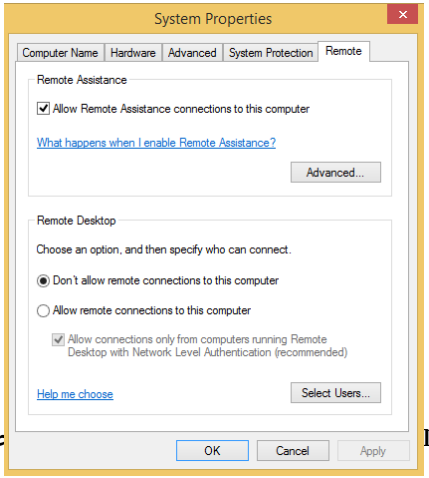
روش ارتباط به وسیله Telnet : IP Telnet

5-2-5 RDP (Remote Desktop Protocol)

RDP همان Telnet می باشد که در محیط گرافیکی انجام می شود و به صورت کاملاً گرافیکی به سیستم مقابل وصل می شود .

RDP نیز مثل دیگر سرویس ها یک Client دارد که نیازمند سرویس است و یک سرور که سرویس RDP را ارئه می دهد .

برای راه اندازی سرور RDP نیاز است که در سیستمی که می خواهیم به آن remote بزنید و اجازه ی آن را بدهید برای این کار روی This PC راست کلیک کرده و گزینه ی properties را انتخاب کنید . در قسمت Remote Settings اجازه ی دسترسی به تمامی سیستم ها یا به سیستم های خاصی برای سرویس Remote Desktop را بدهید .



حال در سیستم nt خواهد ریموت بزند با استفاده از برنامه ی Remote Desktop Connection ، آدرس IP یا نام کامپیوتر سرور RDP (همان سیستمی که میخواهیم به آن ریموت

بزنیم) را وارد کرده و به آن Connect می شویم . RDP از پورت ۳۳۸۹ TCPبه صورت پیش فرض استفاده می کند .

(Simple Network Time Protocol) SNTP 6-2-5

دقیق بودن ساعت و تاریخ در تمامی سیستم های شبکه ، یک مورد بسیار مهم محسوب می شود . مخصوصاً در شبکه هایی که برای مثال اطلاعات حسابداری تبادل می شود نیاز به ساعت دقیق بیشتر احساس می شود . هم چنین برای برقراری امنیت و انجام log گیری نیز به ساعتی دقیق نیاز داریم.

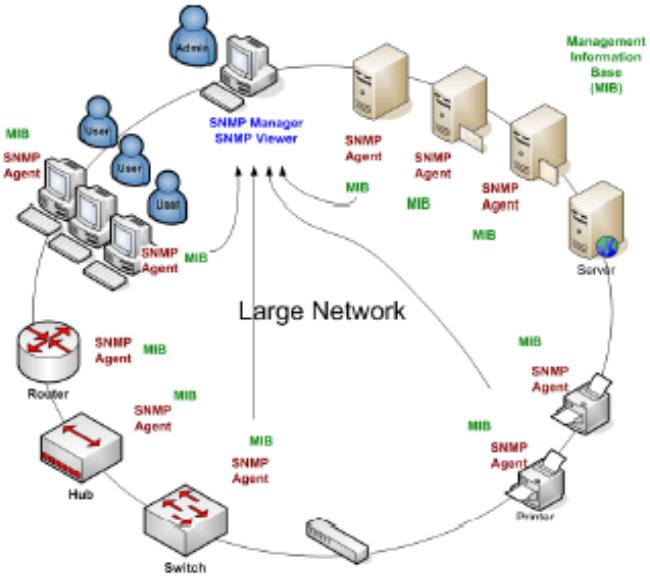
سرویس SNTP (NTP هم گفته می شود) ساعت سیستم ها را با خود برابر می کند و معمولاً خود نیز با یک سرور معتبر ساعت خود را تنظیم می کند .

سرویس SNTP از پورت TCP 37 و UDP 123 استفاده می کند .

(Simple Network Management Protocol) SNMP 7-2-5

برای این که امنیت شبکه خود را بالا ببرید و هم چنین بهترین کارایی را از شبکه ی خود دریافت کنید نیازمند برنامه های مدیریتی هستید . پروتکل SNMP یک سرویس مدیریتی است که در مورد شبکه شما اطلاعاتی را جمع آوری کرده و آن ها را تجزیه و تحلیل کرده و آن ها را به شکل منظم شده در اختیار شما قرار می دهد . حتی در بعضی موارد نرم افزار هایی که از

این پروتکل استفاده می کنند ، راه حل هایی را برای افزایش کارایی و امنیت شبکه ارائه می دهند .



SNMP از دو بخش تشکیل شده است : SNMP Agent که روی سیستم های شبکه نصب می شود و اطلاعات هر سیستم را جمع آوری می کند و SNMP Manager که اطلاعات تمامی Agent ها را جمع آوری کرده و به تجزیه و تحلیل کردن آن ها می پردازد .

برای فعال سازی Agent در سیستم های مایکروسافت به مسیر زیر رفته و Management Protocol Simple Network را فعال کنید .

Control Panel / Programs and Features / Turn Windows Features on or off

نکته: بعد از عمل اطلاعات مدیریتی کاربران در یک بانک اطلاعاتی به نام MIB در خود سیستم ها ذخیره می شود و هنگام درخواست Manager به او تحویل داده می شود.

سپس درSNMP Manager نرم افزار مدیریتی شبکه را نصب کرده تا به گرد آوری اطلاعات بپردازد . یکی از بهترین نوع این نرم افزارها Solarwinds می باشد.

نکته(۱): به SNMP Manager ، SNMP Viewer نیز گفته می شود.

SNMP از پورت های UDP 161 و UDP 162 استفاده می کند .

نکته(۲): برای استفاده از سرویس های TCP/IP نیاز است به پورت های آن ها در Firewall اجازه دهید که در ادامه به نحوه تنظیم فایروال اشاره می کنیم.

Firewall 3-5

Firewall به دو صورت نرم افزاری یا سخت افزاری ، به کنترل شبکه می پردازد . Firewall هایی که بیشتر مورد استفاده قرار می گیرند به صورت نرم افزاری هستند که فایروال خود ویندوز یکی از پرکاربردترین آن هاست . Firewall معمولاً فقط پورت های امن و مورد استفاده ی سرویس های خاص را باز کرده و بقیه ی پورت ها را می بندد و اجازه ی استفاده و وارد شدن از آن ها را از شبکه و اینترنت نخواهد داد .

برای خاموش یا روشن کردن Firewall ویندوز از طریق control panel وارد Windows Firewall شوید . در سمت چپ Turn Windows Firewall on or off را انتخاب کرده و در صفحه ی باز شده خاموش یا روشن کردن Firewall را می توانید انتخاب کنید .

برای تنظیم Firewall و اجازه دادن به پورت ها و سرویس های خاص در همان صفحه ی اول Firewall وارد Advanced setting شوید .

دو قسمت In bound Rules و Out bound Rules را مشاهده می کنید که اولی برای کنترل ترافیک های ورودی از شبکه به سیستم و دومی برای کنترل ترافیک خروجی از سیستم به شبکه استفاده می شود .

برای مثال برای این که اجازه بدهیم کسی سیستم ما را در شبکه ping کند وارد In bound شده ، New Rule را انتخاب می نماییم و مراحل را به ترتیب زیر پیش می بریم :

Rule type : custom
Program : all programs
Protocol and Ports : Protocol type : ICMP V4
Customize : Echo Request
Scope : Local IP : any
remote IP : Any

یعنی این را برای تمامی کسانی که قصد ping از سیستم ما را دارند اعمال کنید .

یعنی اجازه نده و ببند .

Action : block the connection

یعنی این رول را برای Domain یا شبکه خصوصی و یا شبکه اینترنت اعمال کند . Profile : Domain , Private , Public

که هر سه را انتخاب کنید .

در آخر نیز یک نام برای رول خود انتخاب و Finish نمایید .

رول مورد نظر ساخته شد و از این به بعد کسی نخواهد توانست کامپیوتر شما را ping کند .

مثال دیگر اجازه دادن به پورت ۳۳۸۹ است که پورت Remote Desktop می باشد . این پورت معمولاً با فعال سازی سرویس RDP باز می شود ولی در صورتی که فایروال شما این اجازه را نداد ، به جای این که فایروال را خاموش کنید ، به این پورت اجازه ی دسترسی بدهید .

برای این کار وارد New Rule شده و گزینه ی Port را انتخاب کنید . در بالا TCP یا UDP بودن آن را مشخص کرده و در قسمت پایین دو گزینه را پیش رو خواهید داشت :

All Local ports

یعنی تمامی پورت های TCP یا UDP (که در بالا مشخص گردید)

با انتخاب گزینه بعدی می توانید یک یا چند پورت را که با (،) از هم جدا کرده اید را تایپ کنید . برای مثال در این جا ما ۳۳۸۹ را مشخص کرده ایم

و بقیه مراحل را مثل مثال قبلی طی می کنیم و در قسمت Action ، Allow the connection را انتخاب می نماییم به این معنی که تمامی ارتباطات را که با این پورت انجام می گیرد اجازه داده خواهد شد .

به همین شکل ، هر سرویس می توان اجازه ارتباط با سیستم را داد .

نکته : برای اجازه دادن یا بستن ارتباط یا شبکه برنامه هایمان نیز به این شکل می توانید عمل کنید . فقط در قسمت Rule type ، Program را انتخاب کرده و ادامه دهید .

فصل ششم

شبکه های بی سیم

امروزه شبکه های بی سیم به صورت گسترده مورد استفاده قرار می گیرند . این نوع شبکه ها به آسانی قابل پیاده سازی هستند و هزینه ی نسبتاً پایینی نسبت به شبکه های سیمی دارند . در شبکه های بی سیم یک device اطلاعات را به امواج رادیویی تبدیل می کند و در سمت Client ها یک کارت شبکه ی بی سیم این امواج را دریافت کرده و آنها را برای استفاده ی سیستم کامپیوتری خود آماده می کند .

شبکه های WLAN چون مشکلات کابل کشی را ندارند و دارای پیاده سازی ساده ای هستند در نتیجه افراد زیادی علاقه مند به راه اندازی آنها

هستند . البته این نوع شبکه ها چند عیب از جمله امنیت پایین ، سرعت کم و نویز زیاد را دارند که روز به روز این معایب کاهش می یابند .

۱-۶ باند فرکانسی

برای این که deviceها با هم در شبکه بی سیم در ارتباط باشند نیازمند برقراری ارتباط در یک فرکانس هستند . هر فرکانس می تواند متعلق به یک باند فرکانسی (گروهی از فرکانس ها) باشد .

در مبحث بی سیم چند باند فرکانسی وجود دارد که برای شبکه های عادی معمولاً از باند فرکانسی ۲,۴ استفاده می شود که بیشتر device های بی سیم از جمله گوشی ها و لپ تاپ ها آن را support می کنند .

همان طور که بیان شد هر باند فرکانسی شامل چند فرکانس مشخص است که اصطلاحاً به هر کدام از آن ها یک channel گفته می شود . در ادامه به بررسی دو باند فرکانسی مشهور در شبکه می پردازیم :

۱-۱-۶ باند فرکانسی ۲,۴ GHz

باند فرکانسی ۲,۴ پرکاربرد ترین باند فرکانسی موجود می باشد و اکثر device ها آن را support می کنند . حتی وسایلی مانند microwave ، موس بی سیم و ... نیز معمولاً از این باند فرکانسی استفاده می کنند .

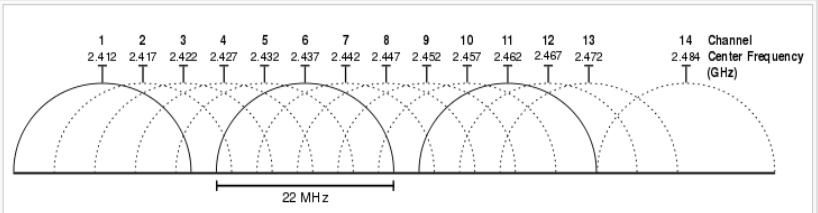
برای تنظیم کردن device های وایرلس مثل Access point یا مودم بی سیم در صورت پشتیبانی آن ها از فرکانس غیر از ۲,۴ ، این نکته را باید در نظر داشته باشیم که موبایل ها ، لپ تاپ ها و اکثر کارت های شبکه ی وایرلس موجود در بازار فقط فرکانس ۲,۴ را پشتیبانی می کنند .

باند فرکانس ۲,۴ دارای ۱۴ Channel اصلی می باشد . که در جدول زیر مشخص شده اند . که در کشور ما ۱۱ کانال اول مورد استفاده قرار می گیرد.

Channel	Frequency (MHz)	North America	Japan	Most of world & Iran
1	2412	Yes	Yes	Yes
2	2417	Yes	Yes	Yes
3	2422	Yes	Yes	Yes
4	2427	Yes	Yes	Yes
5	2432	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes
8	2447	Yes	Yes	Yes
9	2452	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467	No	Yes	Yes
13	2472	No	Yes	Yes
14	2484	No	11b only	No

کانال های مجاور در این فرکانس روی همدیگر تاثیر نویز دارند پس بهترین کانال هایی که روی همدیگر تاثیری ندارند کانال های ۱ ، ۶ و۱۱ می باشند .

با توجه به شکل زیر زمانی که کانالی را انتخاب می کنیم نیاز است به تاثیر کانال های اشغال شده روی همدیگر توجه داشته باشیم . برای مثال در صورتی که کانال ۶ ، ۱۱ و ۱۰ در محلی که قصد راه اندازی وایرلس را داریم پر باشند پس ما بهتر است کانال ۱ را انتخاب نماییم . ولی در صورتی که محیط شلوغ باشد کانالی را انتخاب می کنیم که device دیگری که از آن استفاده می کند از ما دور باشد و تاثیر نویز آن کمترین باشد .



Graphical representation of 2.4 GHz band channels overlapping

نکته : برای یافتن کانال مناسب و بار روی کانال ها نرم افزار های زیادی برای ویندوز و حتی آندروید موجود است .

۲-۱-۶ باند فرکانسی ۵ GHz

باند فرکانسی ۵ GHz بیشتر در ارتباطات لینک های وایرلس و بعضی ارتباطات داخل شبکه ها مورد استفاده قرار می گیرد . این باند فرکانسی چون نسبت به ۲,۴ کمتر اشغال می شود در نتیجه مورد توجه شبکه کاران می باشد .

باند فرکانسی ۵ GHz دارای پهنای زیادی است در نتیجه می تواند دیتای زیادی را حمل کند اما مسافتی که قادر به طی کردن است کمتر از ۲,۴ می باشد .

(Wireless Fidelity) : Wi-Fi 2-6

Wi-Fi یک استاندارد برای ارتباطات بی سیم در فواصل کوتاه است و بیشتر برای به اشتراک گذاشتن اینترنت برای کامپیوتر ها و گوشی ها استفاده می شود .

تفاوت Wireless با Wi-Fi در این است که Wireless مفهوم کلی تری داشته و در مفهوم اصلی می توان گفت Wi-Fi نیز جزئی از Wireless می باشد . Wi-Fi معمولا اینترنت را در یک محدوده ی کوچک مثل یک ساختمان به اشتراک میگذارد و یک شبکه بی سیم نیز در این محدوده راه اندازی میکند. اما به محدوده های بزرگتر Wi-Fi گفته نمی شود.

IEEE 802.11

سازمان IEEE یک استاندارد به نام ۸۰۲,۱۱ برای شبکه های بی سیم مورد استفاده در فواصل نزدیک (Wi-Fi) وضع کرده است که آن ها را به همراه مشخصاتشان در جدول زیر مشاهده می کنید . برای مثال ۸۰۲,۱۱ در باند فرکانسی ۲,۴ کار میکند و دارای پهنای باند ۲۰ می باشد. حداکثر مقدار داده ای که این استاندارد می تواند حمل کند ۵۴ مگابیت در هر ثانیه است.

نکته: حداکثر Data Rate های ذکر شده در جدول فقط در شرایط آزمایشگاهی که شرایط کاملا ایده آل محصوب می شود قابل دستیابی است.

TABLE – IEEE 802.11 PHY STANDARDS

Release date	Standard	Band (GHz)	Bandwidth (MHz)	Modulation	Advanced antenna technologies	Maximum data rate
1997	802.11	2.4	20	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4	20	DSSS	N/A	11 Mbits/s
1999	802.11a	5	20	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4	20	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4, 5	20, 40	OFDM	MIMO, up to four spatial streams	600 Mbits/s
2012 (expected)	802.11ad	60	2160	SC, OFDM	Beamforming	6.76 Gbits/s
2013 (expected)	802.11ac	5	40, 80, 160	OFDM	MIMO, MU-MIMO, up to eight spatial streams	6.93 Gbits/s

۶-۳ Device های شبکه های بی سیم

۶-۳-۱ کارت شبکه ی بی سیم

کارت های شبکه ی بی سیم که به آن ها WNIC هم گفته می شود برای ارسال و در یافت سیگنال از WNIC های دیگر یا AP مورد استفاده قرار می گیرند و آن سیگنال ها را به داده های معنی دار برای کامپیوتر تبدیل می کند . WNIC ها در دو نوع داخلی و خارجی موجود هستند . نوع داخلی به اسلات های مادربرد سیستم وصل می شود و نوع خارجی معمولاً به صورت USB به سیستم وصل می شود .

(AP) Access Point 2-3-6

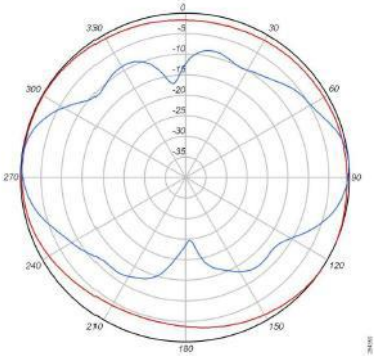
APها مانند سوئیچ در شبکه های سیمی عمل کرده و ارتباط بین Client ها را برقرار می کنند . یعنی برای این که سیستم های شبکه که هر کدام دارای WNIC هستند با هم شبکه نیاز است همگی به یک AP وصل شوند . AP ها علاوه بر برقراری شبکه ی وایرلس می توانند شبکه ای که خود نیز در یافت می کنند را نیز بین شبکه ی وایرلس خود Share کنند . برای مثال یک AP می تواند از طریق کابل شبکه به مودم موجود در شبکه وصل شده و اینترنت آن مودم را در شبکه ی وایرلس که AP راه انداخته Share کند .

۳-۳-۶ آنتن

سه نوع کلی آنتن در شبکه های بی سیم مورد استفاده قرار می گیرند که عبارتند از :

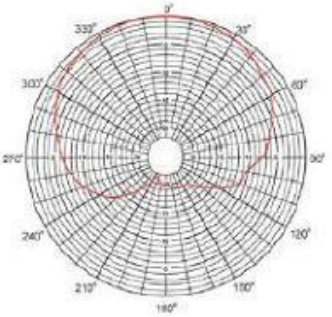
Omni directional

این نوع آنتن در شبکه های داخلی (تجاری و خانگی) بیشتر استفاده می شود . پوشش دهی این آنتن ها به شکل کره می باشد و تقریباً تمامی دور آنتن را پوشش می دهد .



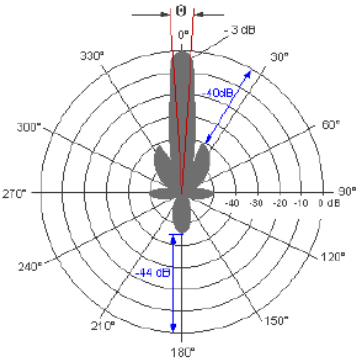
این انتن ها شامل چراغ خیابان ها فقط پوشش دهی شان به سمت جلوی خود است . برای مثال اگر بخواهید در یک اتاق جلسه فقط آن هایی که دور میز جلسه نشسته اند از شبکه ی وایرلس استفاده کنند یک آنتن Semi به سقف آن جا نصب کنید .

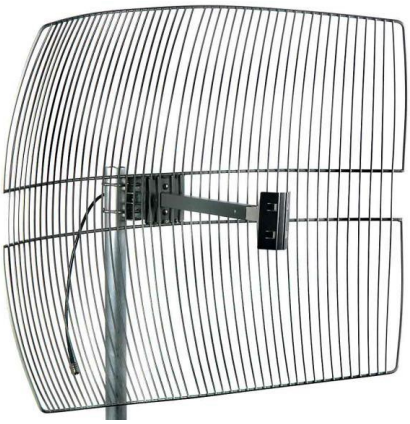
نکته : بعضی از این نوع آنتن ها قابلیت تنظیم شعاع پوششی را نیز دارند .



Highly directional

این نوع آنتن ها برای اتصال نقطه به نقطه مورد استفاده قرار می گیرند و باید هر دو نقطه در یک خط باشند که بتوانند ارتباط برقرار کنند .

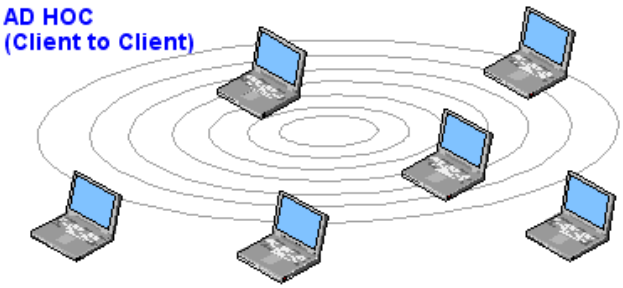




۶-۴ مد های شبکه های بی سیم

۶-۴-۱ مد Ad hoc

در این ساختار تمامی سیستم ها بدون هیچ واسطی به صورت مستقیم با هم ارتباط دارند .



برای راه اندازی Ad Hoc در ویندوز ۸ دستورات زیر را در CMD وارد کنید :

Netsh wlan set hostednetwork mode=allow ssid=networkname key=Password

Netsh wlan start hostednetwork

که دستور اول یک شبکه Ad Hoc با نام (Network Name) و پسورد (Password) ایجاد می کند و دسته ی دوم این شبکه را start می کند .

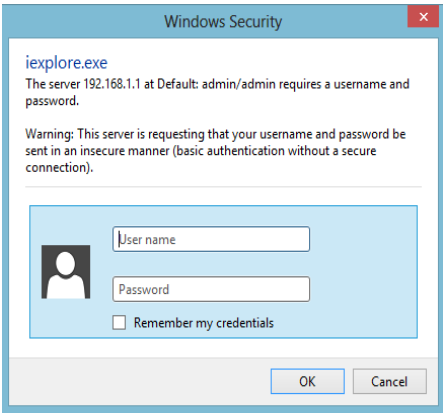
۶-۴-۲ مد Infrastructure

در این مد یک device بی سیم مثل AP یا مودم بی سیم گذاشته و سیستم ها به آن مودم یا AP به صورت بی سیم وصل می شوند . در نتیجه AP ارتباط بین سیستم ها را برقرار می کند . برای config کردن AP چند مرحله مهم وجود دارد که بیان می کنیم :

مرحله اول

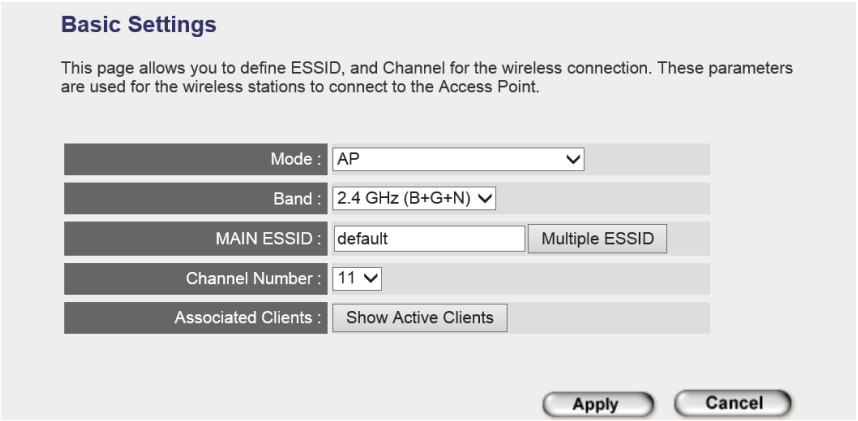
وارد قسمت تنظیمات AP شوید . برای این کار آدرس پیشفرض AP را در مرورگز خود نوشته و Enter کنید . (آدرس IP پیشفرض AP در دفترچه

ی آن نوشته می شود .) هنگام ورود یک username و password از شما سوال می شود که این نیز در دفترچه AP نوشته شده است .



مرحله دوم

وارد تنظیمات اولیه AP شده و معمولاً تنظیمات مربوط به انتخاب باند و فرکانسی ، SSID و Channel را مشاهده خواهید کرد .



باند فرکانسی : همان طور که بیان شد معمولاً از باند های فرکانسی ۲,۴ استفاده می شود .

اما در کنار انتخاب این باند استاندارد آن نیز انتخاب می شود .

(n , g , b)

نکته : اگر فقط استاندارد N انتخاب شود به این معنی نیست که چون از لحاظ سرعت و قابلیت ها از بقیه بالاتر است بقیه را نیز پوشش می دهد . در نتیجه برای این که هر سه پوشش یابد b,g,n را باید انتخاب کرد .

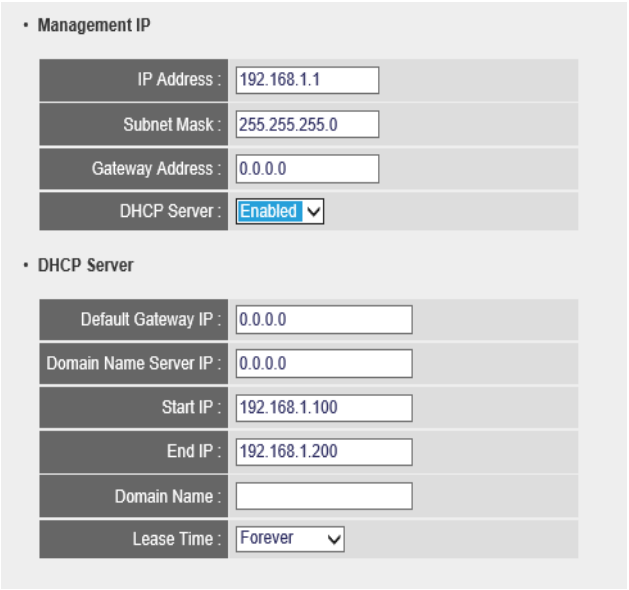
SSID (Service Set Identifier) : SSID همان نامی است که در فضا پخش می شود . در واقع در شبکه های وایرلس یک بسته که شامل SSID و نوع رمز نگاری وایرلس است در فضا پخش می شود و اصطلاحاً Broadcast می گردد .

نکته : می توان جهت بالا بردن امنیت ، از Broadcast شدن SSID جلوگیری کرد . که معمولاً گزینه ای با این نام در تنظیمات پیشرفته وجود دارد . با disable آن طرف مقابل به همراه دانستن رمز بی سیم ، SSID آن را نیز باید بداند .

Channel : در مورد Channel ها و انتخاب آن ها در مباحث قبلی بحث گردید . در این جا کانال مناسب را انتخاب کنید .

مرحله سوم (تنظیمات IP)

AP به صورت default یک IP دارد که معمولاً ۱۹۲,۱۶۸,۱,۱ می باشد . برای تغییر این IP به قسمت مدیریت IP مراجعه کنید .



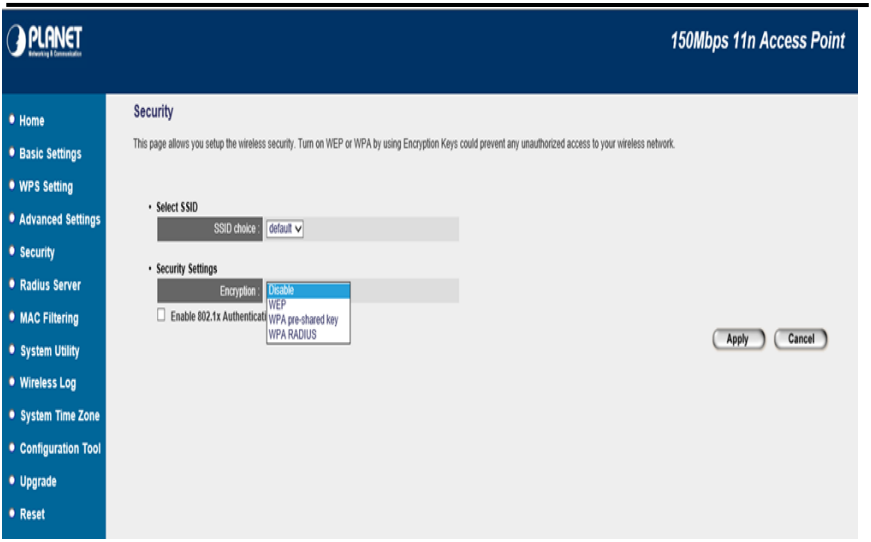
در این قسمت به همراه تغییر IP خود AP می توانید Gateway آن را نیز که معمولاً مودم موجود در شبکه است تعیین کنید .

کامپیوتر دارای کارت شبکه بی سیم ، لپ تاپ ، موبایل و . . . که بخواهند به این AP وصل شوند ، برای استفاده از امکانات آن باید یک IP در رنج شبکه ی AP داشته باشند . در نتیجه یا باید به صورت دستی یک IP در رنج شبکه ی AP وارد کنند که مشکلاتی را نیز به همراه خواهد داشت و یا این که خود AP به صورت اتوماتیک به آن ها IP دهد که این مورد نیز در همان قسمت تنظیمات IP موجود است . در این قسمت DHCP را

Enable کرده و محدوده ی IP را مشخص کنید . هم چنین می توانید آدرس Gateway و DNS را نیز برای کاربران تنظیم نمایید .

مرحله ی چهارم (پسورد)

دو نوع پسورد در تنظیمات AP ها وجود دارد . اولی پسورد ورود به تنظیمات آن است که برای بالا بردن امنیت حتماً باید عوض شود .
نکته : در بعضی AP ها می توان username تنظیمات را نیز عوض کرد .
پسورد دیگر پسورد شبکه ی وایرلس است . برای این که شخص ثالثی اجازه ی ورود به شبکه ی بی سیم موجود در AP را نداشته باشد نیازمند پسورد گذاری به آن خواهید بود .
بسته به نوع AP معمولاً دو نوع پسورد گذاری در آن ها وجود دارد . نوع اول استفاده از یک سرور احراز هویت (Radius) است . در این نوع به جای این که خود AP احراز هویت کاربران را انجام دهد به یک سرور احراز هویت که دارای الگوریتم های مختلف رمز نگاری است تحویل می دهد تا در صورت تایید آن سرور به کاربر اجازه داده شود .



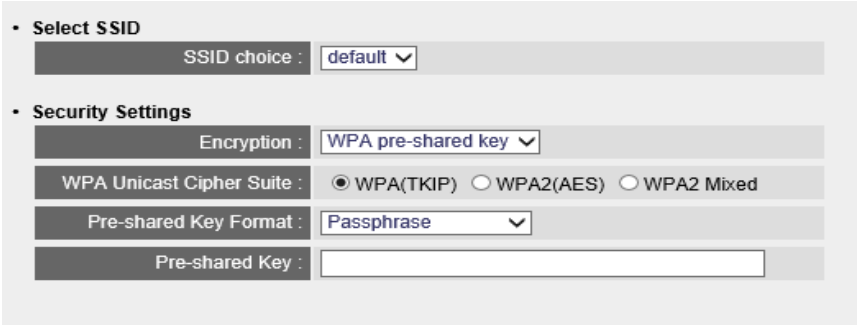
نوع دوم که مشهور به Preshared Key نیز هست ، بدین صورت عمل می کند که در AP یک پسوردی config می شود و هر device که بخواهد وارد آن شود باید آن پسورد را وارد کند .

معمولاً ۴ نوع رمزنگاری در مودم های بی سیم و AP ها وجود دارد که می توان انتخاب کرد .

نوع اول WEP است که دارای کمترین امنیت می باشد اما به دلیل این که بعضی از کارت شبکه های قدیمی انواع دیگر رمز نگاری را پوشش نمی دهند ، مجبور به استفاده از آن در این نوع شبکه ها هستیم .

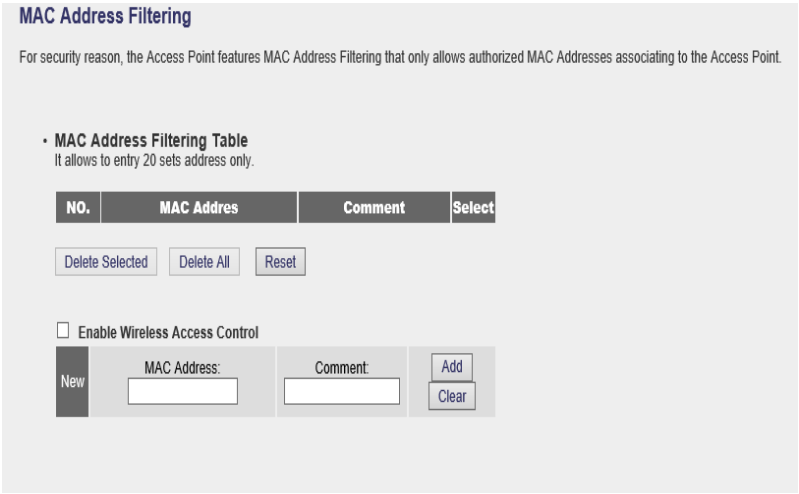
نوع بعدی WPA است که از رمز نگاری TKIP استفاده می کند که نسبت به WEP امن تر است . نوع دیگر WPA2 است که از رمز نگاری پیشرفته AES استفاده می کند که یک نوع رمز نگاری نسبتاً امن می باشد .

هم چنین یک نوع دیگر به نام (WPA2 mix) وجود دارد که از ترکیب AES و TKIP بهره می برد و امن ترین نوع محسوب می شود و بهتر است از این مورد استفاده شود .



مرحله پنجم (MAC فیلتر)

برا بالا بردن امنیت AP و مودم های بی سیم بهتر است آدرس فیزیکی (MAC) سیستم هایی که از آن استفاده می کنند را در قسمت MAC Address Filtering وارد کرده و آن را Enable کنید . در نتیجه فقط device هایی که شما وارد کرده اید می توانند از AP استفاده کنند .


MAC Address Filtering
For security reason, the Access Point features MAC Address Filtering that only allows authorized MAC Addresses associating to the Access Point.
MAC Address Filtering Table
It allows to entry 20 sets address only.
NO.
MAC Addres
Comment
Select
Delete Selected
Delete All
Reset
Enable Wireless Access Control
New
MAC Address:
Comment:
Add
Clear

پیوست

مودم چیست ؟

مودم مخفف Modular – De modular یعنی وسیله ای که سیگنال ها را مدوله یا دمودله می کند .

رایج ترین نوع مودم که در ایران استفاده می شود مودم های آنالوگ هستند . این نوع مودم ها به خطوط آنالوگ تلفن شهری وصل شده و کار تبدیل اطلاعات دیجیتال به آنالوگ را بر عهده دارند .

ما به ساختار مودم بیشتر از جنبه ی شبکه ای می پردازیم . مودم در واقع از دو قسمت تشکیل شده است . قسمت اول قسمتی است که به تلفن وصل شده و تبدیلات مورد نیاز را انجام می دهد . قسمت دوم قسمتی است که به

شبکه ی داخلی متصل گردیده و سرویسی که از قسمت اول دریافت می کند را به شبکه ی داخلی ارائه می دهد .

Connection های معمول در مودم

PPPOE

برای استفاده از اینترنت در Ethernet از این Connection استفاده می شود . PPPOE نسبت به مودم های Dial-up مزایای زیادی از جمله سرعت بالا و پرداخت هزینه بر اساس credential دارد . این connection اینترنت دریافتی از سمت ISP را به Ethernet داخلی تحویل می دهد . پس برای استفاده از این سرویس باید ساختار شبکه ی داخلی بر اساس Ethernet باشد .

PPPOA

این connection نیز همان طور که مشخص است اینترنت دریافتی از شبکه مخابرات (از سمت ISP) را به شبکه ی داخلی از نوع ATM می دهد .

Bridge

در این حالت هیچ نوع connection در مودم ساخته نشده و مودم سرویس اینترنت را به سمت یک client ارسال می کند و آن client برای استفاده از این اینترنت نیاز است که یک PPPOE Connection در سمت خود ایجاد نماید .نکته : در این حالت فقط یک سیستم می تواند از سرویس اینترنت استفاده کند .

ساختار داخلی مودم

سال ها پیش برای این که هر سیستم اینترنت داشته باشد نیاز بود که برای هر کدام یک خط تلفن مجزا به همراه اینترنت اختصاص داده شود . زیرا هر سیستم باید IP مجزا و منحصر به فرد در دنیا داشت . در واقع از نوع bridge استفاده می شد . اما یک مشکل بزرگ این ساختار تمام شدن IP های ورژن ۴ بود . برای مثال یک شرکتی که ۲۰ عدد کامپیوتر داشت و همه نیازمند اینترنت بودند باید ۲۰ عدد اینترنت (هر کدام با یک IP مجزا)

خریداری می کرد . در نتیجه یک پروتکل به نام NAT (Network Address Translation) ایجاد شد .

NAT

چند سال پیش تصمیم گرفته شد IP های ورژن ۴ به دو قسمت public و private تقسیم شوند . IP های public باید در کل دنیا منحصر به فرد باشند و در یک لحظه به یک سیستم خاص تعلق داشته باشند . اما IP های private فقط در شبکه های داخلی منحصر به فرد می باشند .

برای مثال همان شرکتی که ۲۰ عدد کامپیوتر داشت با استفاده از قابلیت NAT می تواند فقط یک عدد اینترنت بگیرد با یک IP از نوع public که شرکت ارائه دهنده ی اینترنت به او خواهد داد . اما آن اینترنت را می تواند از هر تعداد کامپیوتری که در شبکه ی داخلی خود دارد استفاده نماید . در واقع دو نوع آدرس IP خواهیم داشت . یکی در سمتی از مودم که به سمت مخابرات است و دیگری در سمتی که به سمت شبکه داخلی مان می باشد . در نتیجه یک پروتکل مسیریابی مورد نیاز است که این دو نوع IP را به هم متصل کند (اصطلاحاً Route دهد) . این پروتکل NAT نام دارد .

یک مشکل NAT این است که آدرس های private شبکه از بیرون دیده نمی شوند و برای مثال اگر سیستمی از شبکه ی داخلی تان یک کار غیرمجازی در دنیای اینترنت انجام شود ، از بیرون فقط public IP شما

دیده خواهد شد نه IP سیستم طرف مورد نظر . پس نیاز است که در شبکه ی داخلی انواع log گیری ها راه اندازی شود .

آدرس های private در جدول زیر مشخص هستند . آدرس های غیر از این سه مورد آدرس های public خواهند بود .

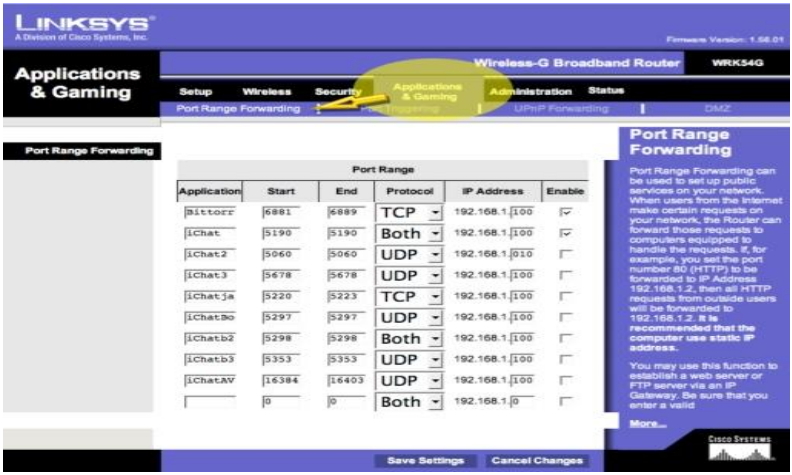
RFC1918 name	IP address range	number of addresses	largest CIDR block (subnet mask)	host id size	mask bits
24-bit block	10.0.0.0 - 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits
20-bit block	172.16.0.0 - 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits
16-bit block	192.168.0.0 - 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits

نکته (۱) : آدرس های public به وسیله ی ISP ها از DHCP سرور استفاده کرده و در مدت های مشخصی عوض می شوند (به دلیل امنیت) . البته امکان خریداری Static IP وجود دارد که یک آدرس IP مشخص و به شما خواهد داد و تعویض نخواهد شد .

نکته (۲) : مودم های DSL زمانی که در حالت PPPOE قرار می گیرند عملیات NAT را انجام می دهند .

Port Forwarding

همان طور که بیان شد زمانی که از NAT استفاده می شود سیستم ها به طور مستقیم با بیرون از شبکه ی داخلی ارتباط ندارند و یک Route بین آن ها وجود دارد . هم چنین NAT مانند یک Firewall عمل کرده و ارتباطاتی که از بیرون برقرار می شود را مستقیماً از خود عبور نمی دهد .



برای مثال اگر بخواهید کسی که از بیرون public IP شما را بزند با پورت ۳۳۸۹ و وارد Remote Desktop یکی از سیستم های شبکه شما شود نیازمند استفاده از این قابلیت مودم خواهید بود . برای این کار به قسمت Port Forwarding مودم رفته و private IP آن سیستم داخلی را بدهید و پورت ۳۳۸۹ را وارد کنید . در نتیجه زمانی که فردی از بیرون

بخواهد به کامپیوتری که مشخص کردید RDP بزند ، مودم مستقیماً او را به آن سیستم راهنمایی می کند .

مثلاً اگر آدرس public شما ۱۰۰.۱۷۹.۷.۵ و آدرس سیستم مورد نظر شبکه ی داخلی ۱۹۲,۱۶۸,۱,۶۰ باشد به این شکل تنظیم می کنیم :

Remote Host : 100.۱۷۹.۷.۵

External Port : 3389 می توانید یک رنج نیز بدهید

Internal Host : 192.۱۶۸.۱.۶۰

Internal Port : 3389

نکته : برای انجام این کار ها نیاز است که یک Static IP از ISP خود خریداری نمایید زیرا در صورتی که public IP شما بعد از مدتی عوض شود نخواهید توانست از این سرویس دوباره استفاده کنید و باید IP جدید را بدانید.

توجه : تنظیمات مربوط به LAN و WLANمودم مشابه با تنظیمات AP می باشد که در بخش های قبل بیان شده است.