دانشگاه جامع علمی کاربردی

طراحی و پیاده سازی زیرساخت شبکه های کامپیوتری

ویژه دانشجویان کامپیوتر و فناوری اطلاعات

و

علاقه مندان به موضوع شبکه های کامپیوتری

تدوین: علی ثاقب موفق

مقدمه:

شبکه کامپیوتری، ارتباط بین دو یا چند رایانه و یا تجهیزات رایانه ای است که تحت پروتکل ها و سیستم های عامل مشخص می توانند منابع سخت افزاری و نرم افزاری خود را به اشتراک گذارند. توجه داشته باشید که به تمامی تجهیزات سخت افزاری ونرم افزاری موجود در شبکه منبع (Resource) گویند و منبع آن چیزی است که قابلیت استفاده توسط چندین کاربر را دارد. هدف از ایجاد شبکه را می توان استفاده مشترک از منابع موجود، کاهش هزینه، قابلیت اطمینان، تسریع در انجام امور، قابلیت توسعه ارتباطات و به طور خلاصه افزایش بهره وری و کاهش هزینه دانست. مهمترین موضوع در شبکه های رایانه ای، به اشتراک گذاری منابعی است که به طور عادی درصد کمی از ظرفیت آنها استفاده می شود. مثل چاپگرها، ظرفیت پردازنده ها و حافظه های ذخیره سازی

انواع شبکه به لحاظ نحوه مدیریت و عملکرد:

۱- شبکه نظیر به نظیر work group (peer to peer)

۲-شبکه سِروری server- clients (server Based)

۱- شبکه peer to peer:

در این نوع از شبکه ها هر رایانه متصل به شبکه (ایستگاه کاری) می تواند به منابع سایر ایستگاه ها در شبکه دسترسی پیدا کند و کامپیوتر ویژه ای جهت نگهداری فایل های اشتراکی و مدیریت کاربران وجود ندارد. هر ایستگاه کاری می تواند هم سرویس دهنده وهم سرویس گیرنده باشد. از آنجائیکه در این مدل یک ایستگاه کاری مرکزی برای مدیریت عملیات شبکه وجود ندارد لذا هر کاربر ایستگاه کاری، مسئولیت مدیریت، امنیت و ارتقاء نرم افزارهای خود را به عهده دارد.

موارد کاربرد شبکه نظیر به نظیر:

- تعداد کامپیوتر کم باشد (کمتر از ۱۰)
- نیازی به مدیریت متمرکز نداشته باشیم.

- عدم امکان تأمین بودجه لازم
- امنیت اطلاعات برای سازمان دارای اهمیت کمی باشد و یا اینکه اطلاعات سازمان فاقد درجه محرمانگی باشد.
- اندازه سازمان کوچک باشد.

نیازمندی های سخت افزاری و نرم افزاری شبکه نظیر به نظیرpeer to peer:

- سیستم عامل پشتیبانی کننده گروه کاری یا work group
- پروتکل یکسان Tcp/Ip مورد استفاده ایستگاه های کاری شبکه
- تنظیمات ایستگاه های کاری و اینکه نام WorkGroup رایانه های موجود در شبکه یکسان باشد و تعریف متمایز کاربران
- تعریف و تنظیم منابع اشتراکی مثل فولدرهای به اشتراک گذاشته شده برای دیگران

۲_ شبکه سروری یا مبتنی بر سرویس دهنده

در این مدل شبکه، یک یا چند کامپیوتر بعنوان سرویس دهنده ، کلیه منابع اشتراکی شبکه را در خود نگهداری می کند. یک کاربر می تواند به سرویس دهنده دسترسی پیدا کرده و متناسب با سطح دسترسی خود، منابع و یا فایل های اشتراکی را از روی آن به دستگاه خود منتقل کند. در این مدل یک ایستگاه کاری (کامپیوتری که به شبکه متصل شده است) در خواست انجام دستور را به سرویس دهنده ارائه می دهد و سرویس دهنده پس از اجرای وظیفه مرتبط با آن درخواست، نتایج حاصل را به ایستگاه در خواست کننده بر می گرداند. این شبکه شامل یک تعداد سرویس دهنده (Host) و تعدادی تجهیزات ارتباطی (Node) و ملزومات ارتباطی(Media) است.

این شبکه ها دارای یک سِرور به عنوان مدیریت مرکزی و تعدادی ایستگاه کاری به عنوان سرویس گیرنده می باشد که از طریق رسانه های ارتباطی و تجهیزاتی به یکدیگر متصل می شوند. معمولاً کلیه نرم افزارها و بانک های اطلاعاتی بر روی کامپیوتر server قرار دارد و workstation ها به آن

متصل شده و از نرم افزارهای آن استفاده می کنند. کار server معمولاً کنترل و مدیریت منابع شبکه می باشد که این منابع شامل نرم افزارها، سخت افزارها، کاربران و اطلاعات است. معمولا در شبکه های سروری، کامپیوتر server از سایر کامپیوترها قدرتمندتر است و صرفا کار سرویس دهی کاربران شبکه را انجام می دهد و کاربری با آن کار نمی کند و در این حالت اصطلاحا به آن Dedicated server می گویند.

چند نمونه سیستم عامل شبکه:

Novell , Netware 3.11 3.5 4

Unix , Linux , Win2000 server adv. Win 2003, 2007,….. 2016 server

چند نمونه سیستم عامل ایستگاه کاری:

Ms-Dos, DR-Dos

Win 95, 98, Win xp ,Win 2000pro, win7, win 10

انواع سرویس دهنده ها(File server):

براساس نوع کاربردی که برای شبکه Server- Based در نظر می گیریم می توان Server مورد نظر را نصب و راه اندازی کرد .

مثل: File server، Application server، Print server، Data base server، Web server، mail server و ...

فایل سرور: عمومی ترین و کاربردی ترین نوع سِرور است که سرویس های فایلی و اطلاعاتی را ارائه می دهد. کاربران مختلف براساس سطوح دسترسی خود به این فایل ها دسترسی پیدا می کنند.

سرور برنامه های کاربردی: برنامه های کاربردی بر روی سرور قرار گرفته و کاربران نسبت نوع مجوز خود می توانند از آن ها استفاده نمایند.

سرویس دهنده کارهای چاپی: یعنی اینکه سرور (P.S) مدیریت کارهای چاپی و چاپگرها را بر عهده می گیرد. اینکه چه کاربری با چه اولویتی از کدام چاپگر و به چه صورت استفاده نماید.

سرویس دهنده بانک های اطلاعاتی: کلیه بانک های اطلاعاتی بر روی این سرور قرار گرفته و برنامه های کاربردی و کاربران از آن به نحو مقتضی استفاده می کنند.

سرویس دهنده صفحات وب: این سرور به منظور نگهداری صفحات وب و نرم افزارهای مرتبط در نظر گرفته می شود به طوری که کاربران بتوانند به آن متصل شده و از اینترنت و سرویس های مبتنی بر وب استفاده نمایند.

سرویس دهنده های پست الکترونیک: به منظور نگهداری و مدیریت mail های کاربران سازمان استفاده می شود.

سطوح و مجوزهای دسترسی: اینکه چه کاربری، به چه منبعی، در چه زمانی ، چه مکانی و با چه مجوزی و در چه سطحی بتواند دسترسی یابد که متناسب با شرح وظایف سازمانی کاربر می باشد.

ناظر و Admin (Adminstrator) همه مجوزهای دسترسی در تمام سطوح دسترسی را دارد و اوست که سایر کاربران را در شبکه تعریف و مجوزهای دسترسی آنها را تعیین می کند. کسی که سیستم عامل شبکه را نصب می کند، ناظر شبکه خواهد بود. مجوزهای دسترسی مثل نوشتن write، خواندن Read، تمامی مجوزها Full control، حذف Delete یا erase، مرورfile scan و ایجاد کردن Creat

مزایای شبکه سروری Server Based:

۱) امنیت بیشتر : اطلاعات و نرم افزارها در یک مکان و تحت کنترل واحد نگهداری می شود.

۲) مدیریت مرکزی Central Administration : مدیرشبکه (Admin) مسئول کل شبکه و نوع عملکرد کاربران می باشد.

۳) به اشتراک گذاشتن منابع Resource sharing: اعم از نرم افزاری و سخت افزاری که به

طور مشترک در اختیار کاربران قرار گیرد.

۴) استفاده در مقیاس های بزرگ و سازمانی

وظایف ناظر شبکه (Administration):

ناظر شبکه مسئولیت حفظ و ارتقاء سخت افزار و نرم افزارهای شبکه را دارد. همچنین وظایف زیر را متناسب با تخصص و تجربه خود انجام می دهد. در صورتی که شرکت و یا سازمان بزرگ باشد بخشی از این وظایف به سایر متخصصین شبکه تفویض می شود.

۱- تعریف کاربران در شبکه

۲- تعیین سطوح دسترسی کاربران در شبکه و ارائه مجوزهای دسترسی به کاربران

۳- مدیریت برنامه ها و نرم افزارهای سرور

۴- انجام عملیات Back up گیری در دوره های زمانی خاص

۵- ارتقاء سرور به لحاظ سخت افزاری و نرم افزاری

۶- رفع اشکالات احتمالی در شبکه

۷- توسعه شبکه

۸_ طرح نقشه شبکه برای ایجاد و ارتقاء شبکه

۹_ بروز رسانی تجهیزات شبکه اعم از Active , Passive

۱۰_ اعمال امنیت شبکه

پارامترهای انتخاب شبکه:

۱- تعداد کامپیوترها ۲- امنیت اطلاعات ۳- مدیریت متمرکز ۴- بودجه لازم

۵- اندازه سازمان ۶- کنترل مرکزی ۷- ماموریت سازمان ۸_ نوع کسب و کار

اینها متناسب با اهمیت خود می توانند نقش موثری بر انتخاب نوع شبکه کامپیوتری داشته باشند.

انواع شبکه به لحاظ Scope و محدودیت های جغرافیایی:

۱_ شبکه های PAN: Personal area Network: شبکه ای که وسعت آن محدود به ابعاد انسان و برای کاربردهایی است که کاربران برای خود دارد مثل بلوتوث، هدرز فری، موس بی سیم و ...

۲_ شبکه های HAN(Home area Network): شبکه ای با محدوده عملکرد یک منزل مثل تلفن بی سیمی خانگی، آیفون و....

۱- شبکه های LAN(local area Network) : شبکه ای که محدود به یک محدوده جغرافیایی خاص است. صرفاً کاربران داخل آن محدوده از آن استفاده می کنند نظیر شبکه Lan یک شرکت در محدود به یک ساختمان ۳ طبقه است. این شبکه دارای محدوده جغرافیایی خاص است. مثل شبکه یک دانشگاه، شرکت یا مرکز آموزشی

۴_ شبکه های CAN (Campus area Network): این شبکه محدوده وسیعتری از یک ساختمان دارد و شامل یک منطقه می شود مثل شبکه منطقه عسلویه، ایران خودرو، ذوب آهن که شامل چندین ساختمان و شرکت در یک منطقه وسیع می باشد و مستلزم شبکه ارتباطی بزرگتری است.

۲- شبکه های MAN:(metropolitan area Network) شبکه ناحیه شهری، شبکه ای است که محدوده آن یک شهر است. مثل شبکه تلفن شهری، شبکه شهرداری مناطق و ....

۳- شبکه های WAN(wide Area Network): شبکه ناحیه گسترده شبکه ای که فاقد محدودیت جغرافیایی است به طوری که می توان از راه دور به آن متصل شد.مثل اینترنت، اینترانت، اکسترانت

Pan < Han < Lan < Can < Man < Wan

همبندی یا توپولوژی شبکه:

اسامی دیگر آن عبارتند از نقشه یا طرح شبکه و Design, layout, Physical layout , map

نحوه ارتباط، آرایش و شکل قرار گیری کامپیوترها در یک شبکه کامپیوتری را توپولوژی آن شبکه می گویند و انواع آن عبارتند از:

۱- توپولوژی Bus (Linear Bus)

۲- توپولوژی Star ستاره (کاربردی تر است)

۳- توپولوژی Ring حلقه

۴- توپولوژی Mesh ترکیبی

البته ترکیبی از همبندی های بالا نیز می تواند بعنوان همبندی جدید مطرح شود. در همبندی شبکه های نظیر به نظیر همبندی های درختی، ترکیبی و نقطه به نقطه نیز وجود دارد.

۱- توپولوژی Bus: مسیر

قدیمی ترین و ساده ترین توپولوژی شبکه های کامپیوتری است و در این روش کامپیوترها به وسیله رسانه ارتباطی مشترک (کابل کواکسیال RG 58) به طور ساده یکی به دیگری متصل می شود. در انتهای دو سر کامل اتصال دهنده Terminator (ترمیناتور) وصل می گردد. با توجه شکل ظاهری، آن را توپولوژی خطی نیز می گوییم. مزیت آن سادگی نصب و راه اندازی، هزینه کمتر جهت کابل کشی، توسعه آسان مسیر شبکه و پیچیدگی فنی کمتر است و از معایب آن این است که در صورت قطع شدن هر نقطه از کابل کل شبکه قطع خواهد شد و اینکه تعداد کامپیوترها موجود در شبکه در عملکرد شبکه موثر است و افزایش آن ها منجر به کاهش کارآیی و سرعت شبکه خواهد شد. نکته قابل توجه اینکه کامپیوتر نقشی در سیگنال های عبوری در کابل ندارد یعنی هیچ گونه عملی بر روی آن انجام نمی دهد بنابراین خاموش بودن و خرابی کامپیوتر تأثیری بر عملکرد کل شبکه نخواهد گذاشت.

اتصالات و اتصال دهنده های مورد نیاز شبکه Bus:

۱- BNC: جهت اتصال کابل شبکه کواکسیال به کامپیوتر

۲- Terminator: جهت بستن دو انتهای کابل

۳- Barrel: اتصال دو قطعه کابل مجزا به یکدیگر

۴_ T Connector : اتصال دهنده واسط برای اتصال BNC به کارت شبکه

۲- توپولوژی ستاره یا star:

در توپولوژی ستاره، هرکامپیوتر یا تجهیز رایانه ای به یک دستگاه مرکزی به نام Hub یا switch با کابل های شبکه مجزا وصل می شوند. مزایای آن نسبت به توپولوژی باس عبارت است اینکه قطعی یک نقطه از کابل ارتباطی کامپیوتر تا دستگاه مرکزی منجر به قطعی کل شبکه نخواهد شد و صرفاً همان کامپیوتر از شبکه قطع می گردد. امکان مدیریت و نظارت مرکزی خواهیم داشت. از معایب آن می توان به هزینه نصب و راه اندازی، پیچیدگی فنی و قابلیت توسعه آن با توجه به کابل کشی های مجزا اشاره کرد. در این توپولوژی از رسانه ارتباطی UTP یا STP یا FTP استفاده می کنیم.

FTP: Foiled twisted pair STP: shielded twisted pair UTP: unshielded twisted pair

سایر اتصال دهنده های لازم عبارتند از RJ 45 یا Jack connector، Socket (wall plate)

همچنین عموماً از Rack (رک) برای استقرار و جایگذاری تجهیزات ارتباطی استفاده می شود.

۳- توپولوژی Ring:

این توپولوژی شبیه به توپولوژی Bus می باشد با این تفاوت که دو سر ابتدا و انتهای آن به همدیگر متصل هستند به لحاظ ظاهری توپولوژی Ring مشابه Star است ولی در عمل یک Ring داریم که ارتباط کامپیوترها را برقرار می نماید. این حلقه و Rinf در دستگاه مرکزی قرار دارد. در Ring هر کامپیوتر بصورت Active عمل می کند و بر روی رسانه ارتباطی اثر می گذارد. لذا با توجه به ویژگی های فوق می توان مزایا و معایب زیر را برای آن در نظر گرفت. **مزیت آن** عدم قطعی دراثر ازدیاد

ترافیک در شبکه ، سرعت بالاتر شبکه نسبت به توپولوژی ماقبل و عیب آن پیچیدگی نصب و راه اندازی و اینکه در اثر خرابی کامپیوتر کل شبکه fail خواهد شد.

٤- توپولوژی Mesh:

در این توپولوژی (همبندی) هر کامپیوتر به روش های مختلف و از مسیرهای متنوع به سایر کامپیوترها و شبکه متصل می شود به طوری که افزایش مصرف کابل را در این نوع همبندی خواهیم داشت همچنین با توجه به ارتباطات متعدد بین سیستم ها، امنیت فیزیکی شبکه به لحاظ قطعی کابل، زیاد خواهد شد یعنی در صورت قطع شدن یک یا چند مسیر شبکه، شبکه از سایر مسیرهای جایگزین برای انتقال اطلاعات اقدام می نماید. مثل توپولوژی اینترنت.

توپولوژی ترکیبی:

استار باس، Star- Bus : در این نوع توپولوژی شبکه چندین switch بصورت سری به همدیگر وصل می شوند. سوئیچ ها بصورت Bus و خطی به هم وصل شده اند. قطعی بین آنها در قطعی شبکه می تواند مؤثر باشد در عین اینکه قسمت های مجزا می توانند مستقلا کار کنند.

استار استار، Star- Star: در این روش سوئیچ ها از طریق یک دستگاه مرکزی دیگر به همدیگر متصل می شوند. هزینه Star- Star بیشتر است چون یک switch اضافی داریم. در این روش اگر یک سوئیچ قطع شود، صرفا کامپیوترهای متصل به همان سوئیچ قطع شده و بقیه به راحتی به کار خود ادامه می دهند و صرفا ارتباط با رایانه های متصل به آن سوئیچ مشکل خواهد داشت.

در شبکه های peer to peer نوع اتصال اهمیت چندانی ندارد و کامپیوترها می توانند از روش Bus یا Star بر همدیگر متصل شوند. نقش کاربران و نحوه مدیریت فایل ها و امنیت سیستم های مربوطه در این نوع شبکه اهمیت بسزایی دارد و هر کاربر مسئول به اشتراک گذاری منابع سخت افزاری و نرم افزاری متصل به سیستم خود می باشد.

رسانه های ارتباطی: (Media):

کابل یا وسیله ای که کامپیوترها و تجهیزات سخت افزاری را به یکدیگر متصل می کند بر اساس نوع، قابلیت و جنس به انواع مختلف تقسیم می شود. سه نوع از کابل های معروف عبارتند از:

۱)کابل کواکسیال (Coaxial Cable RG58)

این کابل عموماً در توپولوژی Bus استفاده می شود و حداکثر طول قابل استفاده ۱۸۵ متر، مقاومت اهمی ۵۰ Ω و نویز پذیری و تداخل بسیار کم و دارای دو نوع Thin(نازک) و Thick(ضخیم) است. برای استفاده کابل جهت مسافت های بیش از ۱۸۰ متر از دستگاهی به نام Repeater استفاده می کنیم. کابل کواکسیال با مقاومت اهمی ۵۰ برای مخابرات دیجیتال و با مقاومت اهمی ۷۵ برای مخابرات آنالوگ مثل تلوزیون کابلی استفاده می شود.

موضوع CrossTalk یعنی اثر امواج الکتریکی ناشی از کابل های مجاور و Noise یعنی تاثیر ولتاژ زیاد لحظه ای در اثر قطع یا وصل برق درباره این کابل مطرح است. کابل کواکسیال ضخیم جهت اتصال دو شبکه lan با مسافت طولانی تر و یا در مواردی که فاصله کامپیوتر ها از یکدیگر زیاد است استفاده می شود و حداکثر طول قابل استفاده ۵۰۰ متر است، مقاومت اهمی ۵۰ اهم است و نویزپذیری بسیار کم و مقاومت فیزیکی بیشتر از کابل نازک است.

۲) کابل به هم پیچیده (Cat5/6/7 -UTP/ STP)

این نوع کابل در شبکه Star استفاده می شود و حداکثر طول قابل استفاده ۱۰۰ متراست و دو نوع کابل معمولی و Cross داریم که کابل cross برای اتصال دو دستگاه مشابه (کامپیوتر به کامپیوتر یا سوئیچ به سوئیچ) و کابل معمولی برای اتصال دو دستگاه نامتشابه (کامپیوتر به سوئیچ) بکار می رود. در این کابل به هم تابیدگی سیستم ها به علت جلوگیری از نویز و cross talk است و نویز پذیری آن کم است. کابل تلفن RJ11 با دو زوج سیم است که قابلیت انتقال صدا را دارد. البته کابل STP مقاوم تر است

ولی کابل UTP بیشتر استفاده می شود چون انعطاف پذیری بیشتری دارد. این کابل براساس نرخ انتقال داده به جندین گروه تقسیم می شوند که به هر کدام یک Category می گویند و به اختصار از سه حرف اول استفاده می شود. Cat 1, Cat2, Cat3, Cat4, Cat5, Cat6 , ... به ترتیب دارای سرعت های ۲و ۴و ۱۰ و ۱۶و ۱۰۰ می باشند. cat 5 عمومی تر از سایرین می باشد با سرعت حداکثر 100 Mbps: Mega bit per second و نوع Cat 7, cat 6 برای مسافت های طولانی تر و تا 1 Gbps می تواند سرعت داشته باشد.

۳. فیبر نوری (Fiber optic) :

از این نوع کابل ها برای شاهراه اصلی و Back bone شبکه و یا اتصالات بین شبکه ای و بین طبقات یک ساختمان استفاده می شود. هر رشته کابل فیبر نوری صرفاً یا ارسال داده و یا دریافت داده را انجام می دهد لذا وجود دو رشته از فیبر نوری برای شبکه الزامی است. با این حال معمولا ۴ رشته سیم استفاده می شود که دو رشته آن به عنوان پشتیبان و Back up درنظر گرفته میشود. کابل فیبر نوری دارای ویژگی های منحصر به فرد زیر است:

۱/ جنس آن ترکیبی از شیشه و پلاستیک

۲/ سرعت انتقال داده از 100 Mhps تا 1 Gbps و بیشتر (۱۰ تا ۱۰۰ Gbps)

۳/ قابل استفاده در مسافت های طولانی (چند کیلومتر)

۴/ عدم نویز پذیری (به سبب جنس آن و استفاده از سیگنال نوری جهت انتقال داده).

۵/ عدم امکان دزدی اطلاعات از طریق کابل فیبر نوری Not tapped

۶/ مقاومت فیزیکی بالا (استفاده در اعماق دریا و شرایط مختلف آب و هوایی)

۷/ گران قیمت (کابل و تجهیزات و اتصالات مرتبط با آن)

۸/ یک طرفه

انواع انتقال اطلاعات: Data Transmition:

۱. ساده یا simplex : فرستنده(sender) صرفاً ارسال اطلاعات می کند و در خصوص نحوه دریافت آن توسط گیرنده(Reciver) پاسخگو نیست. (مثال: تلویزیون و رادیو).

۲. نیمه دو طرفه یا half duplex : ارسال و دریافت اطلاعات می تواند توأماً ولی غیر همزمان وجود داشته باشد یعنی زمانی که ارسال کننده اطلاعات را می فرستد دریافت کننده صرفاً در حالت دریافت، اطلاعات است و بر عکس مثل بی سیم.

۳. تمام دو طرفه یا full duplex : ارسال و دریافت اطلاعات می تواند توأماً و همزمان وجود داشته باشد. مثل تلفن

انتقال سیگنالینگ:

- انتقال دیجیتال: Base Band Transmition
  - ✓ از کل عرض باند (Band width) یا همه ظرفیت خط استفاده می شود.
  - ✓ انتقال دو طرفه است.
  - ✓ پالس های جدا از هم
  - ✓ استفاده از امواج نوری یا الکتریسیته
  - ✓ تقویت کننده سیگنال Repeater است
- انتقال آنالوگ: Broad Band Transmition
  - ✓ پالس های پشت سرهم متوالی
  - ✓ از بخشی از عرض باند استفاده می شود
  - ✓ انتقال یکطرفه
  - ✓ استفاده از امواج نوری یا الکترو مغناطیسی

- ✓ برای ارسال و دریافت توأم با دوکابل مـــجزا یکی برای ارســـال و یکی برای دریافت یا تقســـیم رسانه به دو فضای فرکانسی و هر کدام برای ارسال یا دریافت که با استفاده از کانال بندی رسانه فیبر نوری صورت می گیرد.
- ✓ قابلیت استفاده چندگانه از آن مثل تلویزیون کابلی به طوریکه هم اینترنت باشد هم تلویزیون.

Bandwith: میزان سرعت انتقال داده bps

انواع سوئیچینگ:

سوئیچینگ مداری یا Circuit Switching :

وقتی صحبت از Circuit Switching می شود شما می توانید دقیقا مکانیزمی مشابه خط تلفن قدیمی را در نظر بگیرید. شما هر زمانی که بخواهید از خط استفاده کنید گوشی را بر می دارید و شماره یا کانال مربوط به مقصد را انتخاب می کنید و ارتباط می گیرید و در این ارتباط کانال ارتباطی برقرار شده بین شما و مقصد، صرفا مختص شما می باشد و شما می توانید از پنهای باند موجود و سایر منابعی که در بستر این ارتباط وجود دارد بصورت اختصاصی استفاده کنید و هرگاه که کارتان برای انتقال داده تمام شد ارتباط تلفن یا کانال را قطع می کنید. از مزیت های چنین سیستمی این است که شما امکان استفاده از لینک ارتباطی بصورت مقطعی و زمانبندی مشخص را خواهید داشت اما مشکل این شبکه ها محدودیت تعداد کسانی است که می خواهند از لینک ارتباطی استفاده کنند، در واقع در هر زمان ممکن است یک نفر و یک ارتباط از مبدا به مقصد برقرار شود و باقی افراد ممکن است مجبور باشند پشت خط باقی بمانند و منتظر خالی شدن لینک باشند. در Circuit Switching مسیر انتقال داده کاملا از قبل مشخص است و به هیچ عنوان نیازی به مسیریابی برای ارسال داده نمی باشد.

سوئیچینگ بسته ای یا Packet Switching :

وقتی صحبت از Packet Switching می شود دقیقا شما ساختار شبکه های کامپیوتری را تصور کنید که هر داده ای تبدیل به بسته های کوچک شده و درون شبکه ارسال می شود و با توجه به آدرس مبدا و مقصد و شماره و ساختار بسته اطلاعاتی در مسیر ارتباطی که به احتمال زیاد بسته های سایر کامپیوترها نیز وجود دارند ارسال خواهد شد و کامپیوتر مقصد نیز با توجه به آدرس مقصد بسته را دریافت می کند. در این نوع شبکه ها بسته ها بصورت مجزا و جدا جدا برای مقصد واحد ارسال می شود. با توجه به اینکه در یک مسیر ارتباطی بسته های متفاوت و متعددی از کامپیوترهای مختلف وجود خواهد داشت بنابراین ما به پروتکل هایی نیاز داریم تا بسته های اطلاعاتی را از مبدا تا مقصد هدایت کنند که در واقع همان پروتکل های مسیریابی در این لایه محسوب می شود .

روش های دسترسی: (Access Method)

قانون دسترسی یا (Access Ruls) و اینکه یک کامپیوتر چگونه به رسانه شبکه دسترسی داشته و در آن داده وارد نماید و یا اینکه از آن رسانه ارتباطی (کابل) داده (DATA) اخذ کند. به طور کلی سه روش دسترسی به خط وجود دارد:

۱_روش گوش دادن به خط یا CSMA/ CD : carrier sense multiple Access / Collisssion Detection : این شیوه در توپولوژی star, Bus استفاده می شود. در این روش کامپیوتر از طریق کارت شبکه رسانه ارتباطی را دائم چک می کند (sense) و در صورت خالی بودن خط نسبت به ارسال پاکت های اطلاعاتی اقدام می کند. پس از دریافت پاکت متوسط گیرنده آن و اعلام به کامپیوتر فرستنده، خط مجدداً خالی شده و آماده استفاده مجدد خواهد بود. وضعیت کشف برخورد ، شرایطی است که دو کامپیوتر همزمان خط داشت کرده و خالی بودن آن را تشخیص دهند نسبت به ارسال داده اقدام خواهند نمود. لذا برخورد (collision) پیش خواهد آمد که برای رفع آن به مدت زمان کوتاه و تصادفی هر دو متوقف شده و سپس نسبت به ارسال مجدد داده اقدام می کنند.

۲_روش عبور نشانه یا Token passing : در روش token passing که در همبندی Ring استفاده می شود یک پاکت داده ای خاص به نام Token در شبکه به گردش درمی آید. کامپیوتری که بخواهد ارسال داده داشته باشد بایستی ابتدا token و علامت را در اختیار گرفته و سپس ارسال داده نماید چنانچه داده به مقصد رسید و تأیید آن دریافت گردید، کامپیوتر ارسال کننده، مجدداً token را وارد شبکه می نماید. این token با سرعت بسیار زیاد در (حدود ۵۰۰ هزار دور در ثانیه) در شبکه به گردش درمی آید. از آن جایی که صرفا یک token وجود دارد لذا کامپیوترهای متقاضی استفاده از رسانه بایستی منتظر دریافت آن بمانند. لذا در حالت ترافیک بالا نیز شبکه کار خواهد کرد و قطع نمی شود.

۳_روش اولویت بر مبنای تقاضا یا Demand priority (اولویت تقاضا) : این شیوه در شبکه های سرعت بالا استفاده می شود . در روش Demand priority که مشابه روش token passing می باشد نوبت ارسال (token) به کامپیوتری محول می گردد که متقاضی ارسال داده بر روی رسانه شبکه می باشد. این روش پیچیده تر ولی سرعت آن بالاتر می باشد.

موسسه استاندارد گذاری IEEE: موسسه ای است که قوانین مربوط به شبکه را وضع می نماید. انجمن مهندسین برق و الکترونیک (Institue of Electrical and Electronic Engineering) نسبت به برقراری استانداردهای شبکه مثل اترنت اقدام می کند.

اترنت: Ethernet: قراردادی است که نقل و انتقال داده ها را در فعالیت های مختلف شبکه تعریف می نماید.مثل:

802.3 csmA/ cD (star & Bus)
802.5 token passing
802.11 شبکه های بی سیم
802.15 Blue tooth
10 Base 5 500 /۲ کابل کواکسیال ضخیم Base Band
10 Base T twisted pair

100 Basex fast Ethernet۱۰۰

10 Basefl Fiber optic line

نحوه ارسال پیام در شبکه: DATA یاMessage

برای ارسال پیام در شبکه اولین کاری که صورت می گیرد تقسیم داده به واحدهای کوچکتر است که به آنها Packet می گویند. تقسیم بندی داده به پاکت یعنی ابتدا داده را به واحدهای کوچکتر تقسیم و سپس نسبت به ارسال آنها اقدام می نماییم.که این مهم به دلایل زیر است:

- ✓ اعمال مدیریت بر روی داده
- ✓ به منظور جلوگیری از انسداد کابل
- ✓ سهولت ارسال مجدد داده در مواقع خطا
- ✓ کشف راحت خطاها

پاکت ها (packet) شامل فیلدهای زیر می باشد:

۱/ آدرس مبدأ source Address

۲/ آدرس مقصد Destination Address

۳/ داده Data

۴/ اطلاعات انتقال داده Addressing & Routing

۵/ اطلاعات مربوط به مونتاژ داده اصلی Assembly & DeAssemble

۶/ اطلاعات کشف خطا cyclic Redundancy check CRC

فیلدهای دیگری نیز برای کنترل و اطمینان از صحت دریافت پاکت وجود دارند که در سربرگ پاکت آورده شده اند.

نرم افزارهای شبکه: به دو دسته تقسیم می شوند:

۱/ **نرم افزارهایی که بر روی سِرور نصب می شوند:** این نرم افزارها روی کامپیوتر سرور نصب و راه اندازی شده و بایستی بتوانند مدیریت کاربران و منابع شبکه را به همراه نحوه دسترسی کاربران و سطوح ایمنی شبکه تعریف نمایند و شامل:

سیستم عامل شبکه Network oprating system (N.O.S): این سیستم عامل علاوه بر دارابودن ویژگی های سیستم عامل معمولی بایستی بتواند عملیات مدیریت منابع شبکه را انجام دهد و در عین حال قابلیت چند کاربره و چند وظیفه ای داشته باشد. سیستم عامل شبکه یا Preemptive است که در این حالت سیستم عامل می تواند کنترل پردازشگر را از یک برنامه در مقابل اجرا خارج نماید. (بدون توجه به برنامه) و یا nonpreemptive که درآن صرفاً برنامه در حال اجرا بایستی کنترل را به سیستم عامل معرفی کند در غیر این صورت سیستم عامل منتظر می ماند. سیستم عامل ناول که قدیمی ترین و کاربردی ترین سیستم عامل شبکه که امنیت آن بسیار مناسب شبکه های متوسط و بزرگ است و stability و قابلیت آن به طوری که می توان مدتها و ماهها آن را روشن نگه داشته و کاربران متعدد با آن کار نمایند. سیستم عامل NT: اولین سرور مایکروسافت با ویژگی گرافیکی که Client آن NT client می باشد. سیستم عامل های win 2000 server تا WIN 2016 Server بدنبال آن عرضه شدند و مراحل پیشرفت سیستم های عامل سروری ادامه دارد.

۲/ نرم افزارهایی که بر روی ایستگاه کاری نصب می شوند: نرم افزارهای ارتباطی شبکه ، این نرم افزارها بایستی با نرم افزارهای شبکه و سیستم عامل شبکه هماهنگی کامل داشته باشد بطوری که بتوانند به سرور متصل شده و نرم افزارها و اطلاعات آن بطور اشتراکی استفاده نمایند. این نرم افزارها متناسب با سیستم عامل شبکه می تواند متفاوت باشد. همچنین نرم افزارهای client بسته به نوع O.S کامپیوتر نیز فرق می نماید. پس از نصب نرم افزارهای مذکور(نرم افزار + پروتکل + تنظیمات) بر روی

Client، ایستگاه کاری قادر به اتصال به شبکه (سرور) خواهد بود. طبیعی است جهت ارتباط با سرور نیاز به Account داریم. یعنی (username & Password).

پس از نصب نرم افزار بر روی ایستگاه کاری، ایستگاه کاری را تحت همان account شناخته و با آن ارتباط برقرار می نماید. بسته به مجوزهای صادر شده به Account مذکور که طبعا توسط Administor تنظیم شده است. کاربر مورد اشاره می تواند در شبکه با برنامه ها و نرم افزارهای مربوط کار نماید. برخی نرم افزارهایی که روی client هستند عبارتند از:

الف) Rediector : نرم افزار ایستگاه کاری است که ابتدا دستور صادر شده توسط کاربر را تفسیر و سپس تعیین می نماید که این دستور برای کامپیوتر local است یا برای شبکه (Network). در صورتی که دستور مورد نظر برای شبکه باشد، آن را به فایل سرور جهت اجراء ارسال می نماید.

ب) Designator: در این قسمت نگاشت های مختلف از روی volume شبکه به درایوهای منطقی هارد (local) انجام می شود. از آخرین درایو مربوط به درایوهای local کامپیوتر مربوط به شبکه است.

Drive m→ prg: \ personel

Drive n→ sys

Drive k →Dat

ج) Peripherds: تجهیزات جانبی شبکه : آن دسته از فرامینی که قرار است با تجهیزات سخت افزاری شبکه ارتباط برقرار نمایند مثل گرفتن print بر روی چاپگر print server شبکه و یا ارتباط با تجهیزات ارتباطی شبکه مانند مودم، کارت شبکه.

سایر نرم افزارهای ایستگاه کاری، نرم افزارهای کاربردی هستند که برای کار در محیط شبکه طراحی و پیاده سازی شده اند و اصطلاحا برنامه های تحت شبکه می باشند.

بازدید از شبکه یا Site Survey: برای بازدید از شبکه یک سازمان یا شرکت بایستی موارد ذیل را نیز مدنظر قرار دهیم:

۱/ نام واحد سازمانی و شرح مختصر از عملکرد آن

۲/ نوع شبکه و توپولوژی

۳/ تجهیزات سخت افزاری موجود.

۴/ تعداد سِرورها و نوع هر کدام، N.O.S مورد استفاده.

۵/ کاربران- تعداد آنها و نحوه دسترسی به شبکه

۶/ نرم افزارهای مورد استفاده

۷/ بررسی تجهیزات WAN.

۸/ Server ROOM و امکانات آن.

۹/ نظر شما در رابطه با شبکه مورد نظر

۱۰/ نظر شما در رابطه با بهبود شبکه مذکور یا توسعه آن.

لایه های OSI: Open system Interconnection (اتصال بین سیستم های باز)

این استاندارد توسط سازمان ISO و به صورت هفت لایه درنظر گرفته شد. این لایه های OSI عبارتند از :

7/ Application Layer,	All	Away
6/ Presention Layer	People	Pissa
5/ session layer	Seem	Sussage
4/ transport layer	T0	Throw
3/ Network layer	Need	Not
2/ Data link layer	Data	Do
1/ Physical layer	Processing	Please

لایه کاربردی: Application layer (7)

الف) این لایه سرویـــس هایی را فراهم می کنـد که جهت برنامه های کاربـــردی شبکه می باشد مثل SNMP , flp یا Smtp.

ب) نزدیک ترین سطح به کاربر است.

ج) برنامه های شبکه ای کاربر ابتدا با این لایه برخورد می نماید

د) اینکه فایل های ارسالی و یا دریافتی مربوط به کدام برنامه کاربردی کامپیوتر است و به چه صورت بایستی نمایش یابد از وظایف این لایه به شمار می رود

ه) در این لایه message یا DATA آماده جهت استفاده در برنامه های کاربردی است

و) این لایه متناظر با لایه همنام خود در کامپیوتر مبدأ می باشد بنابراین در کامپیوتر مبداء این لایه، اصل DATA و یا message را برای انجام عملیات تقسیم بندی می گیرد و در کامپیوتر مقصد این لایه، داده آماده را دریافت می کند.

پروتکل و فعالیت هایی که در لایه کاربردی هستند عبارتند از: برنامه های smtp, snmp, ftp برای پروتکل tcp/ ip نوشته شده اند. ftp (file transfer protocol)، جهت دسترسی مستقیم به کامپیوتر مقصد به کار می رود و از این دستور جهت دریافت و یا ارسال مستقیم فایل از کامپیوتر به کامپیوتر استفاده می گردد. snmp (simple Network management protocol) ، پروتکل مدیریتی شبکه است. smtp (simple message transfer protocol ، پروتکل انتقال ساده پیام ها/ مثل دستور ping

Icmp (Internet control message protocol ، انتقال packetهای کنترلی بین روترها جهت کشف مسیرهای مناسب کنترل جریان داده ها. روترها از Icmp packet جهت چک کردن روترهای

اطراف استفاده می کنند و تنظیم سرعت انتقال داده ها بین دو Router و هماهنگ سازی جریان داده ها نیز از طریق ارسال Icmp محقق می شود.

لایه کاربرد در تمام برنامه های کاربردی در تعامل یا اینترنت استفاده می شوند.

لایه نمایش: (presentation layer) (6)

ای لایه وظیفه قابلیت رویت و نمایش داده بر روی سیستم مقصد را به عهده دارد.

الف) در این لایه تبدیل و تغییر فرمت نمایش اطلاعات، رمزگذاری یا رمز گشایی بر روی اطلاعات انجام می گیرد.

ب) وظیفه این لایه قابل نمایش نمودن اطلاعات داخل message می باشد.

ج) فرمت دهی، تعیین character set و تعیین نحوه نمایش DATA مربوط به این لایه می باشد.

د) در مواردی که سیستم های عامل نامتجانس بر روی کامپیوترهای مبدأ و مقصد وجود داشته باشد وظایف این لایه کاملا مشخص است.

ه) دیتا ، DATA قابل رؤیت توسط کاربر می گردد.

لایه نشست (جلسه): session layer (5)

الف) این لایه بالاترین سطح Dialog یا ارتباط دوجانبه بین کامپیوترها را فراهم می کند.

ب) وظیفه آن بازکردن، استفاده و بستن یک اتصال بین دو کامپیوتر می باشد.

ج) قرار دادن نقاط check (check point) در فواصل انتقال داده انجام می گیرد این کار برای این است که در صورت اشکال در ارسال پاکت ها از همان نقطه بروز مشکل مجددا ارسال گردند و کل دیتا دیگر منتقل نشود.

د) باب گفتگوی دیتایی بین دو کامپیوتر باز، استفاده و بسته می شود.

Open, Use And Close the session

لایه حمل داده: Transport(4)

الف) تقسیم داده به واحدهای کوچکتر (Packet) و انتقال آنها از کامپیوتر مبدأ به مقصد.

ب) این انتقال بایستی درست و صحیح باشد. اطمینان از انتقال صحیح DATA در این لایه انجام می شود. در صورت بروز اشکال Packet مجددا منتقل می شود.

ج) کارهای خطایابی؛ تست ارسال و تقسیم داده نیز انجام می گیرد.

د) انتقال داده بصورت end- to – end با حفظ ترتیب ارسال packetها و تأیید کامل داده که از پروتکل های tcp یا UDP استفاده می گردد. Tcp انتقال مطمئن داده Connection Based است یعنی پس از ارسال داده، از دریافت آن نیز مطمئن می شود. Connection Based: یعنی ایجاد یک اتصال (connection) بین مبدأ و مقصد ارسال داده و اطمینان از دریافت آن (ack دریافت می شود).

UDP (uniform Datagram protocol): پروتکل غیر مطمئن؛ یعنی انتقال داده بدون دریافت تأییدیه انجام می شود. Connection less ایجاد نمی شود. پروتکل UDP برای انتقال Packet های مکرر کوچک مناسب است چون سریع تر از Tcp است همچنین سایز آن نیز کوچکتر از Tcp است ولی برای Packetهای بزرگتر و امنیتی مناسب نمی باشد.

لایه شبکه: (3) (Network layer)

الف) مسیر یابی Packet ها در شبکه به طوری که حداکثر کارآیی (سرعت انتقال) و حداقل ترافیک را در شبکه داشته باشیم. این لایه شامل جدول مسیر یابی یا (routing table) است که حاوی تمامی ipهای شبکه های مجاور می باشد.

ب) در این لایه کوتاهترین مسیر (کم هزینه ترین) انتخاب و سپس Packetها به سمت آن مسیر هدایت می شوند.

ج) آدرس دهی و مسیر یابی Addressing & Routing از وظایف این لایه است. تبدیل(ip آدرس) منطقی به آدرس نیز یکی از فعالیت هایی است که بایستی انجام شود.

د) مسیریاب ها ، Routerها در این لایه کار می کنند.

ه) قادر به ارتباط داده ها بین شبکه های مختلف می باشد.

به عبارت خلاصه تر کار این لایه مدیریت ترافیک شبکه، مسیریابی شبکه، انتخاب مناسب ترین مسیر (Route)- تبدیل آدرس منطقی به فیزیکی- با هدایت داده در مسیر است.

لایه پیوند داده ها: DATA link layer (2)

الف) این لایه آدرس دهی جزئی (داخل شبکه ای) را انجام می دهد.

ب) همچنین Packetها را تبدیل به frame های داده با قالب مشخص می نماید.

ج) در این لایه داده (frame) آماده برای ارسال در شبکه می گردد.

این لایه عموما شامل دو زیر لایه می باشد:

کنترل دسترسی رسانه Media access control: MAC : sublayer

کنترل پیوند منطقی Logical link control: LLC : sublayer

این لایه، داده را از طریق لایه فیزیکی و کارت شبکه منتقل می نماید. اینکه پس از انتقال داده به شبکه مقصد، داده ها به چه کامپیوتری در شبکه مقصد ارسال شوند از وظایف این لایه است. Bridge در این لایه کار می کند. Switch های ابتدایی نیز در این لایه کار می کنند و اصطلاحا به آنها سوئیچ های لایه دو می گویند. آدرس کارت شبکه (آدرس فیزیکی) در قسمت MAC تعریف می شود.آدرس کارت شبکه که در کل دنیا منحصر به فرد می باشد. انتقال بیت ها از رسانه سخت افزاری و ایجاد frame اطلاعاتی معین، ارتباط با کارت شبکه، کابل و نوع انتقال، کنترل رسانه ارتباطی(خط)، دریافت بیت ها و تشکیل frame از وظایف لایه پیوند داده ها به شمار می آید.

لایه فیزیکی: Physical layer

الف) ارسال داده به شکل بیت های صفر و یک، از طریق کارت شبکه به رسانه ارتباطی.

ب) تعیین نوع انتقال (سریال) انتقال بیت ها- ارتباط با کارت شبکه از وظایف این لایه است.

ج)این لایه را لایه سخت افزار نیز می گویند. این لایه نزدیکترین لایه به سخت افزار و در ارتباط مستقیم با سخت افزارهای شبکه می باشد.

د) Repeater در این لایه کار می کند. و پایین ترین لایه از لایه های شبکه OSI است.

فعالیت هایی که در هر لایه اتفاق می افتد عکس همان فعالیت ها در لایه متناظر از کامپیوتر مقصد اتفاق می افتد. زبان هر لایه را لایه متناظر می فهمد. هر لایه صرفا با دو لایه مجاور خود (بالا- پایین) ارتباط دارد.

معماری لایه ای: Layering: پروتکل هایی که لایه بندی بوده و هر لایه در عین تعامل با لایه های بالا و پایین، مستقل عمل کند را دارای معماری لایه ای گویند. Layering Architecture

در این حالت ساختار لایه ای برای پروتکل ها منظور می شود به طوری که هر پروتکل یا لایه با پروتکل های مجاور ارتباط دارد. همچنین لایه ها در این وضعیت مستقل از یکدیگرند. معمولا در ساختار لایه ای پروتکل ها حجم بالا و سرعت کم را خواهیم داشت. ولی ارتقاء هر لایه می تواند مستقل از سایر لایه ها انجام شود بطوری که تغییر در یک لایه، تأثیری در عملکرد کل لایه ها و پروتکل نخواهد داشت.

پروتکل Protocol: قانون و رویه ارتباطات است به طوری که نحوه ارتباط و چگونگی استفاده از رسانه ارتباطی را تعریف می نماید.

پروتکل های شبکه ای دو نوع هستند: NonRoutable protocol , Routable protocol

مسیر یا Route: وقتی دارای چند شبکه lan باشیم، اینکه از چه راهی از شبکه مبداء به شبکه مقصد برسیم و ارتباط داده ای از یک شبکه به شبکه دیگر را route می گویند. حال پروتکل هایی را که

اجازه دهند Data از یک شبکه (Lan) به شبکه دیگر (lanهای دیگر) منتقل شود را Routable گویند و در مقابل پروتکلی است که قادر به عبور از میان شبکه ها نمی باشد را غیر قابل مسیریابی NonRoutable می گویند . این پروتکل ها صرفا قادر به انتقال Data (داده) درون یک شبکه هستند. هر کدام از انواع پروتکل های مذکور می توانند Connectionless یا Connection-Based باشد.

بدون اتصال یا Connectionless : «بدون اتصال» ، در این حالت پروتکل پس از ارسال داده منتظر جواب یا تأیید دریافت نمی گردد و دارای ویژگی حجم کمتر و سرعت بیشتر می باشد مثل پروتکل ip اتصال گرا یا Connection- Based: در این حالت پروتکل پس از ارسال داده (DATA) منتظر دریافت تأییدیه (Ack) می شود. به این پروتکل ها مطمئن یا reliable گویند. مثل Tcp با ویژگی سرعت کمتر و حجم بیشتر.

لایه های OSI در سیستم عامل WIN NT:

3/ File system layer → Application, presention, session

2/ Transport layer→ transport, Network

1/ Network interface layer→ DATA link, physical

پشته پروتکل یا Protocol stack: به چندین پروتکل که با همدیگر کار می کنند، پشته پروتکل یا Protocol stack می گویند. طبیعی است در این حالت وظایف پروتکل ها مستقل از یکدیگر است. مثل Tcp/Ip یا Ipx/Netx

انقیاد و قید کردن Binding protocol : انتساب یک پروتکل به کارت شبکه را Bind کردن گویند. بدیهی است که پس از نسبت دادن پروتکل به کارت شبکه، آن Network card با آن پروتکل مذکور نسبت به ارسال و یا دریافت DATA عمل خواهد کرد. در صورت Bind کردن چند پروتکل به یک کارت شبکه، اولویت ها در نظر گرفته می شود.

پروتکل Tcp/ Ip: Transmition control protocol / Internet protocol IP:

یکی از مشهورترین پروتکل های ارتباطی شبکه است که در اینترنت نیز از آن به عنوان پروتکل ارتباطی استفاده می شود و دارای ویژگی های "Industrial Standard" است یعنی دارای قابلیت استاندارد صنعتی است و open protocol است یعنی یک پروتکل باز است به عبارت دیگر وابسته به شرکت خاصی نمی باشد و در اختیار هیچ کمپانی نیست و اصطلاحا de- facto است. همچنین قابلیت ارتباط بین کامپیوترها بدون توجه به سیستم های عامل دستگاه را دارد. مثل امکان ارتباط بین سیستم های عامل نامتجانس win..... Ms- Dos و Apple . پروتکل Tcp/Ip قابل توسعه (Scalable) است یعنی امکان توسعه وگسترش شبکه از Lan به Wan با پروتکل ICP/Ip امکان پذیر است. از مشکلات و نکات آن اندازه بزرگ و سرعت نسبتا کم این پروتکل است.

به پروتکل Tcp/ ip، پروتکل inter networking گویند. به سبب اینکه قابلیت ارتباط چندین شبکه را دارد. پروتکل tcp/ ip به صورت لایه ای است که دارای ۴ لایه می باشد که عملکرد هر کدام مشابه با عملکرد لایه های مشابه آن درOSI است. به واسطه اینکه TCP/IP در زمان مناسب و در محل مناسب ارائه گردید، این پروتکل عمومیت و کاربری عملیاتی یافت و لایه های آن عبارتند از:

Application ==== Application, Presentation, Session Layer
Transport ==== transport layer
Internet ==== Network layer
NIC Layer ==== Datalink, physical layer

پروتکل ARP: (Address Resolution Protocol)

جهت تبدیل آدرس ip دستگاه به آدرس فیزیکی (آدرس کارت شبکه) استفاده می شود. قابل ذکر است که آدرس های کارت شبکه منحصر به فرد می باشد. IP → MAC Address

IP از طریق ARP تبدیل به آدرس فیزیکی می شود.

پروتکل Reverse Address Resolution Protocol: RARP در این جا عکس عمل ARP انجام می شود یعنی آدرس سخت افزاری به آدرس ip تبدیل می گردد.

$$\text{MAC Address} \xrightarrow{RARP} \text{Ip Address}$$

پروتکل اینترنتی IP: Internet protocol : این پروتکل به صورت connection less، packet forwarding عمل می کند. بطوری که در این پروتکل پس از ارسال packet، منتظر دریافت تأییدیه نمی ماند پس به این گونه پروتکل ها، نامطمئن یا پروتکل بیشترین تلاش (Best effort) می گویند.

پاکت ip شامل ؛ آدرس مبدأsource Address ، آدرس مقصد Destination Address، داده ، مشخصه پاکت Packet identification IP و TTl (time to live) است.

علاوه بر اجزای اصلی فوق، سایر اجزای فرعی مربوط به کنترل خطا و مسیریابی است. جزء TTL، که مخفف Time To Live می باشد، زمان لازم برای اینکه یک packet فرصت داشته باشد تا به مقصد برسد را تعیین می کند و مقدار آن در کارایی شبکه و حضور پاکت های سرگردان موثر است. پاکت IP به اندازه پیش فرض 128 ثانیه (یا 128 .hop) T.T.L= 128 می تواند در شبکه وجود داشته باشد و پس از سپری شدن این زمان packet دور انداخته می گردد.

آدرس های ip: آدرس ip نسخه ۴ که در آن آدرس ها شامل ۴ ناحیه می باشد که هر کدام می تواند عدد بین صفر تا ۲۵۵ را به خود بگیرد. دو نوع ip داریم:

معتبر یا valid : به آن Valid. Ip می گویند و منحصر به فرد می باشد و توسط سازمان هماهنگ کننده ipهای اینترنتی ارائه میشود. معمولاً همراه با پهنای باند اختصاصی و خط ارتباطی مربوطه تعدادی آدرس valid. ip نیز اختصاص می یابد که طبعا مستلزم قبول هزینه آن می باشد، ipهای موجود که استفاده می شود از نوع IPV4 است. Register, valid ip و ثبت شده می باشد بطوری که بسیاری از کمپانی های بین المللی صرفاً مراودات نرم افزاری و update های نرم افزاری را از طریق valid, ip

انجام می دهند (مثل تلفن مستقیم و تلفن داخلی در ادارات سازمانی). Valid, ip به مراتب کاراتر از آدرس invalid ip می باشد.

غیر معتبر یا invalid ip : یک ip شخصی تعریف شده است و بطوری که کاربر می تواند آزادانه ip را بر روی سیستم خود اعمال می نماید (مثل تلفن – داخلی) از این آدرس ها می توان به عنوان invalid ip استفاده نمود.

[192. 168. 0.0]

[10.1. 0.0]

[175. 16. 0.0]

[169. 0.0.0]

ماسک زیرشبکه یا Subnet mask: برای اینکه از محدوده ip های موجود به نحو مؤثر استفاده شود. subnet mask را به کار می بریم.

آدرس IP : 192 . 168 . 42 . 1

آدرس Subnet Mask : 255 . 255 . 255 . 0

این subnet mask به معنای داشتن 255 آدرس ip با آدرس 192 .168. 42. X می باشد.

تعداد ایستگاه کاری = 2^{24} و تعداد شبکه = $2^{8} \rightarrow$ کلاس A Subnet Mask: 255.0.0.0

تعداد ایستگاه کاری = 2^{16} و تعداد شبکه = $2^{16} \rightarrow$ کلاس B Subnet Mask: 255.255.0.0

تعداد ایستگاه کاری = 2^{8} و تعداد شبکه = $2^{24} \rightarrow$ کلاس C Subnet Mask: 255.255.255.0

کلاس D برای Broad cast و کلاس E برای تحقیقات آزمایشگاهی است.

کلاس A از آدرس 1.0.0.1 تا آدرس ۱۲۶/۲۵۵/۲۵۵/۲۵۴ که قابلیت پشتیبانی از۱۶ میلیون میزبان در هر یک از ۱۲۷ شبکه را دارد.

کلاس B از آدرس 128.1.0.1 تا ۱۹۱/۲۵۵/۲۵۵/۲۵۴ است و قابلیت پشتیبانی از ۶۵،۰۰۰ میزبان در هر ۱۶،۰۰۰ شبک را دارد.

کلاس C ازآدرس 192.0.1.1 تا آدرس ۲۲۳/۲۵۵/۲۵۴/۲۵۴ است و قابلیت پشتیبانی از ۲۵۴ میزبان در هر یک از ۲ میلیون شبکه را دارد.

کلاس D ازآدرس 224.0.0.0 تا آدرس ۲۳۹/۲۵۵/۲۵۵/۲۵۵ است و برای گروه های چندپخشی رزرو شده است.

کلاس E ازآدرس 240.0.0.0 تا ۲۵۴/۲۵۵/۲۵۵/۲۵۴ است و برای استفاده در آینده و با اهداف تحقیق و توسعه استفاده می شود.

بنابراین آدرس دهی کلاس های IP:

کلاس A : در این کلاس ۸ بیت اول آن برای netID و ۲۴ بیت آخر آن hostID است و اینکه بیت اول مربوط به netID آن صفر است. در نتیجه فضای آدرس دهی آن از ۱ تا ۱۲۶ را در بر می گیرد .

کلاس B : در این کلاس آدرس دهی، ۱۶ بیت اول آن برای netID و ۱۶ بیت آخرآن برای hostID است و بیت اول netID یک و بیت دوم صفر است. در نتیجه از ۱۲۸ تا ۱۹۱ را در بر می گیرد .

کلاس C : در این کلاس آی پی، تعداد ۲۴ بیت اول آن netID و ۸ بیت آخر hostID است و دو بیت netID آن یک و بیت سوم صفر است. در نتیجه محدوده آدرسی از ۱۹۲ تا ۲۲۳ را در بر می گیرد.

کلاس D : در این کلاس سه بیت netID آن یک و بیت چهارم صفر است. در نتیجه از ۲۲۴ تا ۲۳۹ را در بر می گیرد. این کلاس دارای کاربرد خیلی کمتری نسبت به سه کلاس قبلی می باشد. بیشتر برای ارتباطات Multicast و ارتباطات ویدئویی از این کلاس استفاده میشود.

کلاس E : در این کلاس چهار بیت netID آن یک است. در نتیجه فضای آدرسی آن از ۲۴۰ تا ۲۵۵ را در بر می گیرد. این کلاس حتی از کلاس D هم کاربرد کمتری دارد.

رنجIP های از پیش رزرو شده:

برخی از آی پی ها و دامنه‌ها برای اهداف و کاربردهای ویژه‌ای رزرو شده اند که عبارت اند از:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

هر گاه یک آدرس آی پی (IPA) در اکتت آخر خود ۲۵۵ باشد، آدرس فوق از نوع Broadcast است. از آدرس های Broadcast جهت ارسال یک بسته یا پیغام به همه کامپیوترها استفاده میشود.

آدرس آی پی دروازه شبکه یا Ip Gate way : این ip مربوط به سرور است یعنی کامپیوترهای دستگاه کاری بایستی در قسمت ip Gate way خود آدرس ip، سروری را که از طریق آن به بیرون از شبکه مرتبط می شوند را در نظر بگیرند.

نکته: همه کامپیوترهای متعلق به یک شبکه طبیعتا دارای subnet یکسان وآدرس ip Gate way مشابهی هستند.

NetBios : (Network Basic input output system)، یک رابطه و Interface شبکه ای است که در سیستم عامل ویندوز استفاده میشود و پروتکل های Tcp/ip ،NW Link و NetBeui از طریق این رابطه با برنامه های کاربردی و سرویس های ویندوز در ارتباط هستند. NetBios یک پروتکلsession layer می باشد و در لایه نشست کار می کند. بنابراین پروتکل های Routable را حمایت می نماید. مثل (Tcp/ip) این پروتکل در سیستم های عامل ویندوز وجود دارد.

NW Link : (Netware link)، این پروتکل جهت هماهنگی سیستم های مبتنی بر سیستم عامل ویندوز با سیستم های مبتنی بر سیستم عامل Novell می باشد که توسط شرکت مایکروسافت طراحی و پیاده سازی گردیده است. لذا جهت اتصال workstation های windows به شبکه Novell مثل

ناول نت ور نسخه ۵ (Novell Netware 5) نیاز به قرار دادن این پروتکل داریم. در واقع NW link همان تغییر نام یافته IPx/ spx می باشد که در سیستم عامل ویندوز لحاظ شده است.

Net BEUI: (Network Basic Extended user Interface) ، یکی از پروتکل های خاص ویندوز است این پروتکل در لایه Transport layer کار می کند. از ویژگی های آن این است که پاکت ها را مسیر دهی بین شبکه ای نمی کند و Non Routable است یعنی قادر به عبور پاکت ها از شبکه ها نمی باشد. از مزایای آن سایز کوچک packet ها و سرعت بالای آنها است. لذا برای ارسال پیام ها و داده های کوچک مناسب است. همچنین در شبکه های نظیر به نظیر (peer- to peer) به عنوان پروتکل ارتباطی استفاده می شود.

DNS : (Domain Name Service) ، این سرویس جهت تبدیل نام آدرس های شبکه متناظر با آدرس Ip های اختصاصی می باشد در صورت عدم تنظیم DNS و یا عدم وجود آن، نمی توان از آدرس های حرفی برای رفتن به سایت استفاده نمود و صرفا بایستی از ip Address ها استفاده کنیم.

تجهیزات ارتباطی: (Communication Devices) ، تجهیزاتی که ارتباط بین کامپیوترها را به عنوان گره های پایانی برقرار می نماید. این تجهیزات ارتباطی را گره های میانی نیز می گویند و برخی ازآنها عبارتند از مودم، Switch/ Hub، Bridge ، BRouter, Routerو Gate way

۱) مودم (Modem) : (Modulator and Demodulator)

از مودم برای ارتباط بین کامپیوترهای راه دور از طریق رسانه های مختلف ارتباطی استفاده می شود که معروف ترین آن خطوط تلفن می باشد. در این حالت، کار مودم تبدیل سیگنال های دیجیتال به آنالوگ و برعکس می باشد. بطوری که، سیگنال های دیجیتال از کامپیوتر به مودم ارسال شده و سپس مودم این سیگنال ها را به آنالوگ تبدیل کرده و از خط تلفن به سمت مقصد یا مودم گیرنده هدایت می کند. سپس مودم مقصد سیگنال های آنالوگ دریافتی را به سیگنال دیجیتال تبدیل می نماید تا در کامپیوتر

مقصد مورد استفاده قرار گیرد. به لحاظ محل استقرار و نحوه قرار گیری مودم بر روی سیستم کامپیوتر، مودم ها به ۲ نوع تقسیم می شوند:

الف) داخلی internal : داخلی ، مودم هایی که به شکل یک کارت (Modem card) داخل اسلات Mother Board" slot" قرار می گیرند.

ب) خارجی external: مودم هایی که به صورت یک دستگاه مجزا در خارج کامپیوتر قرار گرفته و با استفاده از کابل مخصوص مودم به کامپیوتر متصل می شود. البته این دو نوع مودم به لحاظ عملکردی مشابه هستند. مودم داخلی بیشتر استفاده خانگی و شخصی دارد و مودم خارجی، بیشتر استفاده اداری و شرکتی دارد و معمولا کیفیت، قدرت و سرعت آن بیشتر است و اینکه به راحتی از یک کامپیوتر به کامپیوتر دیگر منتقل می شود.

تقسیم بندی مودم ها به لحاظ فنی و عملکردی :

۱) **مودم های آسنکرون** (Asynchronous modem) : در این مودم ها ارسال سیگنال به صورت غیر زمان بندی انجام می شود. بطوری که برای انتقال داده از stop Bit, start Bit استفاده می شود. مودم های غیر زمانبندی یا Asyn modem ها مجهز به تولید clock pulse نمی باشند و clock زمان بندی ندارند. (Timing clock)

۲) **مودم های سنکرون** (Synchronous modem) : این نوع مودم ها در محیط های آنالوگ استفاده می شود. مودم های دیجیتالی بوده که از خطوط دیجیتال (leased line) و خطوط اختصاصی جهت انتقال داده استفاده می نمایند.این مودم ها سنکرون هستند یعنی از (Timing) استفاده می نمایند. در این حالت stop Bit, start Bit های متوالی نداریم و صرفاً از Timing clock برای جداسازی فریم ها و انتقال packet استفاده می شود. طبعاً این روش برای دیتا های متعدد بزرگتر مناسب می باشد مودم های سنکرون دارای سرعت بیشتری نسبت به مودم های Async است و اتلاف زمان محاسبه

مربوط به بیت شروع و پایان stop Bit, start Bit نداریم در این جا از روش های کنترل خطا جهت اطمینان از صحت Data ارسالی استفاده می شود.

معمولاً شرکت های ارائه دهنده سرویس های اینترنتی مثل Isp ، icp و pap ها از مودم های دیجیتالی استفاده می کنند و این مودم ها به لحاظ ظرفیت انتقال داده و سرعت قیمت بیشتری دارند. برخی از سرعت مودم ها به طور مثال 28,800 bps: bit per second و مثلا بعد از فشرده سازی 115,000 بیت در ثانیه bps بودند. مودم های sync استفاده خانگی کمتری دارند. باد ریت یا Boud rate، نرخ انتقال بیت ها و زمان انتقال یک بیت است.

مودم های ADSL سرعت بالا :

این مودمها توانایی انتقال داده چندرسانه ای (multimedia) با سرعت بالا رادارند مثلا تاMbps 1.

برای داشتن چنین قابلیتی ضروری است تا هر دو طرف خط مجهز به مودم ADSL باشند.

این واژه مخفف Asymetric Digital Subscriber Line است و رسانه ارتباطی مورد استفاده از این نوع مودم می تواندخط تلفنی باشد.

تقویت کننده :Repeater، این دستگاه در لایه اول یا همان لایه فیزیکی، کار می کند لذا جهت ارتباط خطوط شبکه ای، با روش دسترسی یکسان به کار می رود. این دستگاه صرفاً سیگنال ورودی ضعیف شده را تقویت (attenution) و در خروجی ارائه می دهد.

هاب : **Hub** ، مشابه Repeater است با این تفاوت که به صورت چندگانه (multi) عمل می کند و سیگنال ورودی را بر روی همه پورت ها پخش می کند و دو نوع داریم:

هاب فعال **Active** : تقویت سیگنال انجام می دهد و متصل به برق می شود .

هاب غیرفعال **Passive** : صرفا عبور سیگنال انجام می دهد.

از آنجائیکه هاب در لایه فیزیکی کار می کند بنابراین قادر به اتصال بین شبکه ها نمی باشد. Hub ها بر اساس تعداد Port ها و سرعت متفاوتند.

پل: Bridge

این دستگاه جهت کنترل و تفکیک ترافیک شبکه می باشد. ترافیک شبکه را در مسیرهای مختلف تقسیم می کند Bridge یا پل با توجه به پاکت های ورودی آدرس های آنها را تشخیص داده و همچنین سگمنت (segment) مربوطه را متوجه می شود، لذا در صورت داشتن آدرس packet، آن را به مسیر مشخص (segment مربوطه) هدایت می کند. پل در لایه دوم عمل می کند در بخش MAC لایه DATA link کار می کند . لذا قادر به ارسال packet به یک مسیر خاص می باشد. Bridge دارای جدول look up table است که مشخصه مسیرهای مختلف و آدرس ها را در آن نگهداری می نماید. بنابراین این دستگاه بر خلاف Repeater دارای حافظه (RAM) است. البته این حافظه به تدریج اطلاعاتش در شبکه تکمیل می شود. در صورتی که Bridge آدرس مقصد را نتواند شناسایی کند، پاکت را برای تمامی مسیرها می فرستد. حافظه هاب به تدریج در شبکه تکمیل می شود به طوریکه آدرس های از قبل استفاده شده را در حافظه نگه می دارد. دفعه بعد و موقع استفاده از آن آدرس ذخیره شده نیاز به جستجوی مجدد و پیدا کردن ندارد. پل یا Bridge داخل شبکه کار می کند. اکنون بیشتر از سوئیچ برای این منظور استفاده می شود.

Switch: مشابه Bridge عمل می کند ولی دارای port ها و قابلیت بیشتری است. سوئیچ در لایه ۲ کار می کند. برخی از انواع سوئیچ که قادر به مسیردهی پاکت بین شبکه ها هستند در لایه کار می کنند عموما در شبکه های lan با سرعت بالا از switch های پر سرعت به جای Hub، استفاده می شود. قابل ذکر اینکه switch کار repeater و تقویت کنندگی را هم انجام می دهد

مسیریاب یا Router: این دستگاه جهت ارتباط دو شبکه مستقل Lan می باشد روتر در لایه سوم از مدل لایه ای OSI کار می کند و به عبارتی روتر در Network layer فعالیت می کند. لذا جهت توسعه شبکه ها و تشکیل شبکه wan استفاده می گردد. مسیر یاب ها و **Router** ها دو نوع هستند.

- **ایستا یا Static :** ناظر، Administrator یا مدیر شبکه تمام مسیرهای بهینه شبکه را در شروع راه اندازی Router برای آن تنظیم یا config می کند طبیعـتاً با تغییر مسیرها و مشخصات شبکه های پیرامونی این config بایستی اصلاح شود.
- **پویا یا Dynamic** : در این حالت، خود روتر به تدریج اطلاعات جدول مسیریابی خود را به کمک پاکت های دریافتی و ارسالی تکمیل می نماید. لذا در صورت تغییرات شبکه، روتر این اطلاعات را بازسازی می نماید.

نکته: روترها برخلاف Bridge در صورتی که نتوانند packet را شناسایی کنند آن را دور می اندازند. روترها مجهز به الگوریتم های پیچیده و هوشمندی هستند که وظیفه مسیریابی و آدرس دهی پاکت های مختلف را در بین شبکه های متفاوت انجام می دهند. روترها بر اساس حافظه، تعداد پورت های WAN و الگوریتم های دسترسی تقسیم می شوند. آشنایی کامل با روترها و دستورات و نحوه تنظیم آن در قالب دوره های CCNA , CCNP انجام می شود.

Brouter : (Bridge Router) این دستگاه ویژگی های روتر bridge, Router را توأماً دارا می باشد. بطوری که، پروتکل های Routable را Route و پروتکل های non Routable را Bridge می کند. این در حالی است که Router صرفا پروتکل های Routable را می پذیرد و Bridge صرفا non Routable را می پذیرد. لذا وظایف بیشتری نسبت به هر دو آنها دارد. دستگاه روتر می تواند شبکه ethernet با پروتکل TCp/ip را به شبکه Token- Ring با پروتکل Tcp/ip متصل نماید.

دروازه ارتباطی: Gate way

برای ارتباط بین دو یا چند شبکه با معماری و محیط های مختلف به کار می رود. این دستگاه می تواند داده Data را به طور کلی Repackage می نماید یعنی داده را کاملا جدا و تفکیک کرده و سپس آن را بازچینی و اسمبل می نماید. در این دستگاه کلیه اجزای داده مجددا برای شبکه مقصد سرهم می شوند. لذا امکان ارتباط دو شبکه مختلف در فرمت، پروتکل، نحوه نمایش و ..... را داراست. از جمله موارد کاربرد آن اتصال شبکه pc به main frame است. یعنی ارتباط دو شبکه کاملا متفاوت. این دستگاه در تمامی لایه ها عمل می کند یا به عبارت دیگر در لایه Application که لایه های پایین تر را نیز شامل می شود. بنابراین امکان ارسال داده به شبکه با فرمت نمایشی متفاوت، آدرس شبکه ای جداگانه، نرم افزار متفاوت و روش دسترسی مختلف با این شبکه را دارد. طبعاً این دستگاه وظایف بیشتری را نسبت به Router انجام می دهد.

خطوط ارتباطی: Communication line

خط تلفن (dialup line): خط شماره گیری یعنی خطی که با شماره گیری ایجاد و استفاده می شود این خط غیر اختصاصی بوده و برای سرعت های پایین تر شبکه (56kbps) استفاده می شود. خط آنالوگ و مودم مورد استفاده آن Async می باشد.

خط اختصاصی (استیجاری) (Leased line): این خط دیجیتال با کیفیت ارتباطی بهتر نسبت به خط تلفن می باشد. مودم مورد استفاده sync است و برای فعالیت های تجاری، استفاده می گردد. این خط بین دو نقطه دائم وجود دارد و نیازی به شماره گیری نمی باشد لذا هزینه آن بیشتر است.

خط E1 یا خانواده رسانه T1, E1 یا خانواده رسانه T1: این خطوط معروف ترین خطوط دیجیتال هستند که سرعت و دقت آنها به مراتب بیشتر از سایر خطوط می باشد.

معمولا خط دیجیتال سرعت 2/08 Mbps- 1/54 Mbps و ٪۹۰ error free است. با توجه به پهنای باند مناسب و هزینه بالای اینگونه خطوط، صرفاً جهت شرکت های ارائه کننده خدمات ارتباطی و اینترنتی (ICP, ISP ,...) استفاده می شود.

خط فیبر نوری (Fiber optic): خط با امنیت و ظرفیت انتقال داده بالاتر که قابل استفاده در محیط هایی است که از سایر رسانه ها نمی توان استفاده کرد.

روش های wireless ارتباط شبکه :

در این روش به جای استفاده از کابل از امواج مختلف استفاده می شود و انتقال داده از طریق این امواج صورت می گیرد انواع wireless عبارتند از:

- Infra Red transmition
- Laser transmition
- Narrow- band Radio Transmition
- Spread- spectrum Radio transmition

مادون قرمز یا Infra Red transmition : در این نوع انتقال از پرتوهای مادون قرمز برای انتقال اطلاعات استفاده می شود و سرعت آن حداکثر 10 Mbps و جهت مسافت های کوتاه (۳۰m) استفاده می شود. دارای چند نوع مختلف می باشد که هر کدام ویژگی های متفاوتی دارند. در یکی از موارد دستگاه های Transciver (Reciver & Transmiter) بایستی حتماً در مقابل همدیگر باشند یعنی در یک خط مسیر قرار داده شده باشند تا انتقال داده صورت پذیرد. در نوع دیگر دستگاه ها می توانند در یک خط مسیر نباشند (Scatter) ولی موانع منجر به تضعیف می گردد. تولید امواج قوی تر به سبب اینکه نور پنجره یا لامپ تداخل ایجاد نکند برای کنترل از راه دور استفاده می شود.

لیزر یا Laser: مشابه infra red و یک طرفه است . با این تفـــاوت که مـــــوانع آن را قطع می کند. حـــــداکثر سرعت حدود 4 Mbps.

موج رادیویی موج کوتاه یا Narrow- band Radio: در این حالت از امواج رادیویی با طول موج کوتاه استفاده می شود برای مسافت های طولانی تر کاربرد دارد. با توجه به تداخل فرکانس و یا وجود موانع قابلیت اطمینان و سرعت آن کم است.

موج رادیویی وسیع Spread- spectrum Radio: از فرکانس های با طول موج بالاتر و تا مسافت های طولانی تر(۳ کیلومتر) استفاده می شود. سرعت این روش 32 kbps و پایین است.

برای شبکه های بزرگ extended Lan از آن استفاده می ود. در این روش اتصال بین چندین شبکه کامپیوتری Lan از نوع wirless با استفاده از امواج رادیویی صورت می گیرد که در این خصوص دو دستگاه ارتباطی وجود دارد. یکی wireless Bridge که از تکنیک امواج رادیویی استفاده می شود و تا ۳ کیلومتر قابل پیاده سازی است و دوم Long- Distance- wireless Bridge که در این سیستم از spread- spectrum radio استفاده می شود و حداکثر تا ۴۰ کیلومتر می توانیم انتقال اطلاعات داشته باشیم. در هر دو روش انتقال اطلاعات با سرعت کم و حداکثر 4 Mbps و حداقل سرعت ۱۲۵۶kbps امکان پذیر است. پیاده سازی و اجرای شبکه های wirless مستلزم دانش فنی و تخصصی بیشتری است.نکته اینکه در قسمت فرستنده و گیرنده باید تنظیمات لازم برای فرکانس های مربوطه هماهنگ شود.

دستورالعملهای عملی درس طراحی و پیاده سازی زیرساخت شبکه های کامپیوتری

۱ – یک کابل Cat5 یا cat6 به صورت ۳ تا ۵ متری درست کنید.

أ. چند سوکت جدید و مقداری کابل utp یا stp یا ftp تهیه کنید .

ب. از ابزار های پرچ، دم باریک(کاتر) استفاده کنید.

ج. ترکیب رنگ: سفید نارنجی-نارنجی*سفید سبز-آبی*سفید آبی –سبز* سفید قهوه ای – قهوه ای

د. کابل نارنجی برای ارسال و سبز برای دریافت است.

ه. حداقل طول کابل چقدر باید باشد؟ حداکثر چطور؟ برای چه نوع توپولوژی و شبکه ای است؟

و. آیا سوکت شما به اندازه کافی خوب و محکم هست؟

ز. آیا کابل شما درست کار می کند؟ نتیجه کار خود را بنویسید. چه پیشنهادی برای عملکرد بهتر کابل دارید؟

۲– کارت شبکه رایانه خود را نصب کنید .

أ. یک کارت شبکه آماده کنید . برند های مناسب کارت شبکه کدامند؟

ب. آیا به همراه کارت شبکه تهیه شده دفترچه راهنما و سی دی هم هست؟

ج. کارت شبکه را در یکی از اسلات های رایانه محکم نصب نموده آنرا پیچ کنید.

د. چند کارت شبکه می توان بر روی رایانه نصب نمود؟ کارت های متعدد برای چه هدفی است؟

ه. مدل ها و برند های مختلف کارت شبکه چه تفاوتی با هم دارند؟

و. آیا کارت شبکه بی سیمی هم داریم؟ مزایا و معایب آن چیست؟

۳– نصب نرم افزار و درایور کارت شبکه بر روی رایانه

أ. ایا به طور خودکار سیستم عامل قادر به شناسایی کارت شبکه نصبت شده توسط شما گردید؟ اگر سیستم عامل ویندوز کارت شبکه شما را شناسایی نکرد با استفاده از سی دی مربوطه و یا فایل درایور آن ، درایور کارت شبکه را نصب نمائید.

ب. می توانید از گزینه Update Driver نیز استفاده نمائید.

ج. Windows system-> control panel->system- ->network adaptor

د. از صحت عملکرد کارت شبکه خود اطمینان حاصل کنید.آیا علامت ? یا علامت ! در قسمت مربوطه و آیکون Network Adaptor می بینید؟ این علائم معرف چیست؟

ه. کابل شبکه ای را که درست کرده اید به سوکت مخصوص آن در کارت شبکه متصل کنید.

و. آیا چراق کوچک کارت شبکه روشن شده است؟ روشن شدن چراغ مبین چیست؟

ز. آیا کابل شما به هاب یا سوئیچ وصل است؟ به کدام شماره آن؟

ح. به چند روش می توان درایور کارت شبکه را نصب و راه اندازی نمود؟ کدام مناسب تر است؟ چرا؟

۴ – آدرس Host سیستم خود را بدست آورید.

أ. در قسمت Run یا جستجو (علامت ذره بین)، دستور CMD ر ا تایپ و سپس Enter کنید

ب. دستور Hostname را تایپ نموده و آنرا یادداشت نمایید.

ج. نام هاست رایانه شما چیست ؟

د. نام هاست رایانه در چه مواردی کاربرد دارد؟

ه. واژه CMD مخفف چیست؟

۵ – کارت شبکه یا مودم خود را به لحاظ عملیاتی تست کنید و از صحت آن اطمینان حاصل نمائید.

أ. در قسمت Run دستور CMD ر ا تایپ و سپس Enter کنید

ب. دستور ping 127.0.0.1 را تایپ نموده و نتایج را ببینید.

ج. پاسخ " reply " یا " request time out " است؟ هر کدام به معنی چیست؟

د. چند پاکت ارسال و دریافت می شود؟

ه. چه زمانی طول می کشد تا جوابها دریافت شوند؟ این زمان ها معرف نکته خاصی است؟

و. چه اطلاعات دیگری وجود دارد؟ (مثلا TTL بیانگر چیست؟)

ز. دستور ping چه کاربردهای دیگری به نظر شما دارد؟

ح. کارت شبکه در چه لایه ای از لایه های هفت گانه OSI کار می کند؟ چرا؟

۶ – آدرس اینترنتی (IP) سیستم خود را بدست آورید.

أ. در قسمت Run دستور CMD ر ا تایپ و سپس Enter کنید

ب. دستور ipconfig را تایپ نموده و آدرس IP خود را یادداشت نمایید. IPv4 Address

ج. این آدرس Ip خصوصی یا عمومی است . چرا؟

د. نحوه آدرس دهی به رایانه های شبکه چگونه است؟ static or Dynamic ؟

ه. آدرس IP شما متعلق به چه کلاس آدرسی است؟

و. به نظر شما تعداد IP ها بیشتر است یا تعداد ID ها

۷ – آدرس فیزیکی کارت شبکه سیستم خود را بدست آورید. Mac Address

أ. در قسمت Run دستور CMD را تایپ و سپس Enter کنید

ب. دستور ipconfig/all اطلاعات آدرسی فیزیکی را نمایش می دهد. Physical Address

ج. آیا این آدرس در مبنای Hex یا ۱۶ می باشد؟ چرا؟

د. این آدرس منحصر به فرد و ۴۸ بیتی است یعنی ۱۲ رقم مبنای ۱۶ که هر رقم ان ۴ حرف است.

ه. از ادرس ۲۴ بیت اول آدرس کارخانه سازنده و ۲۴ بیت بعدی آدرس کارت شبکه است.

و. منحصر به فرد بودن آدرس فیزیکی کارت شبکه برای چیست؟

ز. چه اطلاعات دیگری قابل مشاهده است؟

۸– هاب یا سوئیچ خود را بررسی و نصب کنید .

أ. یک هاب یا سوئیچ با تعداد پورت مناسب آماده کنید.

ب. هاب یا سوئیچ شما چند پورت دارد؟ تعداد پورتها معرف چیست؟

ج. ایا هاب را در جای مطمئنی از لحاظ فیزیکی قرارداده اید ؟ چرا باید محل آن مطمئن باشد؟

د. همه رایانه های مجهز به کارت شبکه خود را با کابل به سوئیچ وصل کنید. چه توپولوژی شد؟

ه. چراغ های روشن و خاموش هاب معرف چیست؟ آیا رنگ چراغ ها هم معنی خاصی دارد؟

و. کابل ها از داخل داکت عبور می کنند. چرا؟

ز. مجموعه ای از هاب ها، سوئیچ ها، سرورها، پچ پنل ها، مودم های خارجی به همراه سر کابل ها را در رک قرار می دهند. چرا؟ آیا شما پیشنهاد دیگری دارید؟

ح. هاب و سوئیچ هرکدام در چه لایه ای از لایه های هفت گانه OSI کار می کند؟

۹– تست برقراری ارتباط کامپیوتر با کامپیوتری دیگر

ز. در قسمت Run دستور CMD را تایپ و سپس Enter کنید

ح. دستور ping را با آدرس IP کامپیوتر مورد نظر اجرا می کنیم.

ط. پاسخ " reply " یا " request time out " است؟ هر کدام به معنی چیست؟

ی. آیا ارتباط بین شما و کامپیوتر مورد نظر برقرار است؟

ک. اگر ارتباطی برقرار نباشد. مشکل چه چیزهایی می تواند باشد؟ Troubleshooting

ل. آیتم TTL برای چیست؟

م. Ping Statistics برای آی پی مورد نظر شامل چه اطالاعاتی برای ما است؟

۱۰– به اشتراک گذاری فولدرها و برنامه در شبکه

أ. یک فولدر به نام خودتان بر روی یکی از درایوهای رایانه خود ایجاد کنید .

ب. یک سری فایل و برنامه آزمایشی در فولدر اشتراکی قرار دهید.

ج. فولدر مذکور را به اشتراک گذارید

د. right click->sharing and security->share this folder آیا این شیوه در سیستم های عامل مختلف مشابه است؟

ه. نام share شده و نام اصلی فولدر چه فرقی با هم دارند؟

و. ایا فولدر شما را سایر رایانه های متصل به شبکه می بینند؟ رایانه های غیر متصل چطور؟

ز. ایا بقیه می توانند فولدر اشتراکی شما را پاک کنند؟ چرا؟

ح. ایا شما نیز فولدرهای اشتراکی بقیه را می بینید؟

ط. ایا یکی از اهداف شبکه به اشتراک گذاری منابع موجود است؟ منابع دیگر کدامند؟

ی. چگونه امنیت فایل ها و فولدر های موجود بر روی سیستم خود را تامین می کنید؟

۱۱– تعیین و تخصیص مجوزهای دسترسی به کاربران جهت نحوه استفاده از فولدر های اشتراکی

أ. یک فولدر دیگر به نام special folder بر روی یکی از درایوهای رایانه خود ایجاد کنید

ب. سعی کنید که فولدر ایجاد شده را به اشتراک گذارید :

ج. right click->sharing and security->share this folder

د. از قسمت security کاربران خاص group or username را انتخاب کنید.

ه. چه کاربرانی موجود هستند؟ کدام ناظر است؟ کدام مهمان است؟

و. تفاوت کاربران مختلف در چیست؟

ز. سپس مجوزهای کاربر مورد نظر permission را نیز انتخاب کنید.

ح. چه مجوز هایی موجود است؟ اختصاص کدام مجوز به کاربر ریسک بیشتری دارد؟ چرا؟

ط. آیا shareکردن فولدرهای رایانه منجر به افزایش آسیب پذیری آن می شود؟ چرا؟

ی. فولدر مربوطه را از حالت share خارج سازید.

ک. میزان فوادرهای share شده چه تاثیری بر آسیب پذیری سیستم شما دارد؟

۱۲ – برقراری ارتباط شبکه ای خود با سایت فرضی یاهو را چک کنید.

أ. در قسمت Run دستور www.yahoo.com ping را تایپ کنید

ب. چه پاسخی دریافت کردید؟

ج. اگر نتیجه پاسخ پاکت های رسالی را برگرداند پس ارتباط هست.

د. آیا بدست آوردن آدرس IP سایتها به این روش مقدور است؟

ه. آیا صرفا با زدن آدرس آی پی سایت یاهو بجای آدرس حرفی آن، باز هم سایت مشاهده می شود؟

۱۳- مسیر ارتباطی خود تا سایت گوگل را شناسایی کنید.

أ. در قسمت Run دستور www.google.com tracert را تایپ کنید

ب. نتایج نشان داده شده مبین چیست؟ از چه آدرس Ip هایی عبور کردید؟

ج. پرش یا Hop چیست ؟ زیاد بودن یا کم بودن ان معرف چیست؟

د. آیا می توان کشورهایی که از آنها جهت رسیدن به سایت طی می کنید را مشخص کرد؟

۱۴ – مشاهده سایت با آدرس IP

أ. در قسمت Run دستور www.yahoo.com ping را تایپ کنید

ب. چه پاسخی دریافت کردید؟ ایا ipمشاهده شده ip سایت یاهو است؟

ج. بجای نام سایت در نرم افزار internet Explorer آدرس آی پی آنرا وارد کنید.

د. چه فرقی با حالت استفاده از نام اینترنتی دارد؟ کدام ساده تر است؟

۱۵- آدرس IP رایانه خود را تنظیم کنید.

أ. وارد control Panel شوید.

ب. سپس وارد network Connection یا network and sharing center شوید.

ج. روی Local Area Connection یا Properties کلید کنید.

د. به قسمت properties و سپس Internet protocol (TCP/IP) بروید.

ه. با استفاده از use the following ip address آدرس را تنظیم کنید. مثلا ۱۹۲,۱۶۸,۰,۵

و. آیا subnet mask اتوماتیک تایپ می شود؟ چرا؟

ز. آدرس ip شما از چه کلاسی است؟ چرا؟

ح. آدرسی Gateway و DNS چیست؟ چه کاربردی دارد؟

ط. آیا شیوه دیگری هم برای تنظیم و مشاهده آدرس IP سیستم وجود دارد؟

۱۶- دستور ARP و نمایش آدرس Mac متناظر با آدرس IP :

أ. وارد محیط CMD می شویم و یا از منوی اصلی Start وارد Windows system می شویم و Run را اجراء می کنیم.

ب. دستور ARP با پارامتر a– را اجراء می کنیم.

ج. این دستور چه کاری انجام می دهد؟

د. کدام آدرس فیزیکی و کدام منطقی است؟ چرا؟

۱۷- دستور Net و نمایش مشخصات شبکه :

أ. وارد محیط CMD می شویم و یا از منوی اصلی Start وارد Windows system می شویم و Run را اجراء می کنیم

ب. دستور Net را اجراء می کنیم.

ج. این دستور چه پارامترهایی دارد؟ هر پارامتر چه کاری انجام می دهد؟

د. دستور Net time , net user را اجراء کنید. چه نمایش داده می شود؟

ه. آیا پارامتر دیگری برای دستور Net وجود دارد؟

آیا دستورات شبکه ای دیگری سراغ دارید؟ نحوه استفاده از آنها را با نحوه عملکرد و کاربرد هریک مشابه دستور العمل های فوق بنویسید.