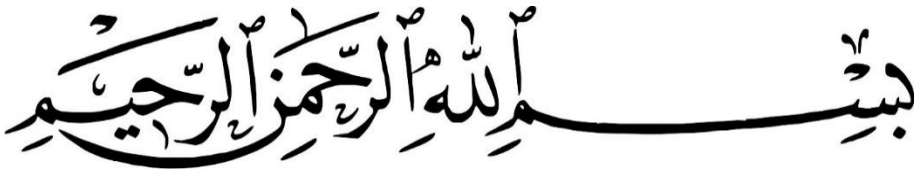


جزوه اصول و مبانی شبکه کامپیوتری

تالَیف :

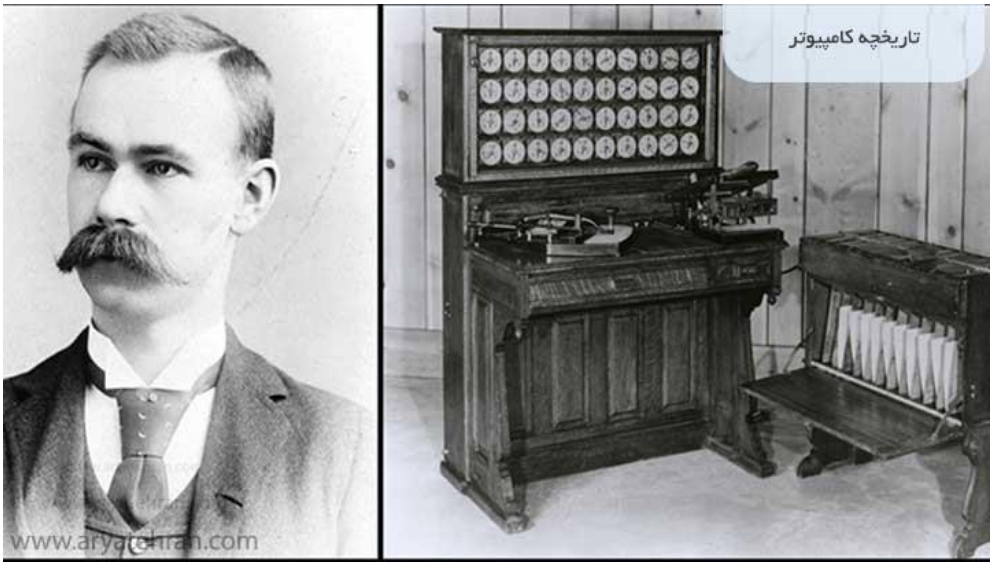
علی صدیقی منش

۱- آشنایی با کامپیوتر

در عصر مدرن امروزی، کامپیوترها بخش مهمی از زندگی روزمره ما را به خودشان اختصاص می دهند. این یعنی رایانه ها تقریبا در هر زمینه و عرصه ای حضور دارند و باعث می شوند کارهای روزمره ما راحت تر و سریعتر انجام بشوند. در حال حاضر کامپیوترها را در هر جایی که فکرش را بکنید مثل بانکها، مغازه ها، مدارس، بیمارستان ها، راه‌آهن ها و بسیاری از مکانهای دیگر از جمله خانه هایمان می‌توان دید.

کامپیوتر چیست

ریشه کلمه کامپیوتر، واژه Compute است که معنی محاسبه کردن می دهد البته محاسبه با ماشین. در واقع کامپیوتر به معنی شمارگر و محاسبه گر است و در ابتدای کار، هدف از اختراع کامپیوتر همین بوده است.
کامپیوتر یک ماشین قابل برنامه ریزی است که زندگی همه ما را از جهت های مختلف تحت تاثیر قرار داده است. این روز ها کم تر کسب و کاری را می توان پیدا کرد که به طور مستقیم یا غیر مستقیم با کامپیوتر مرتبط نباشد.
اگر بخواهیم به زبان ساده بگوییم، کامپیوتر یک وسیله برای پردازش کردن اطلاعات خام است.
کامپیوتر وسیله ای است که اطلاعات خام را گرفته و به اطلاعات پردازش شده و قابل فهم تبدیل می کند. به بیانی ساده مثلا زمانی که شما در حال تایپ کردن یک متن هستید، اطلاعات توسط کیبورد به کامپیوتر فرستاده شده و نتیجه از طریق مانیتور به ما نمایش داده می‌شود. البته فراموش نکنید که کامپیوترها جدید قابلیت پردازش بالایی دارند و می توانند در چند هزارم ثانیه محاسبات ریاضی بسیار بالایی انجام دهند.
بنابراین اگر کسی از شما پرسید **رایانه چیست**؟ باید گفت : رایانِه یا کامپیوترِ دستگاهی الکترونیکی است که برنامه ریزی شده تا دستورهای ریاضیاتی و منطقی را به صورت خودکاره از طریق برنامه نویسی انجام دهد.



تاریخچه کامپیوتر

نخستین بار در سال ۱۶۱۳ از لغت کامپیوتر در کتاب « علم اندوزی مرد جوان »، اثر ریچارد بریثویت نویسنده انگلیسی استفاده شده بود که البته، این کلمه ربطی به کامپیوتر های امروزی نداشت و منظور از کامپیوتر، فردی

محاسبه گر بود. تا مدت ها همچنان به افراد حسابگر کامپیوتر گفته می شد تا این که در اواخر قرن نوزده میلادی کم کم کامپیوتر های ماشینی روی کار آمدند و معنی این کلمه تغییر یافت.
همانطور که در تعریف کامپیوتر آمد، کامپیوتر یعنی دستگاه محاسبه گر. و طبق این تعریف می توان دستگاه ماشین حسابی که پاسکال و یا لایب نیتز و... ساخته بودن را نیز کامپیوتر نامید. البته وسایل مختلفی وجود داشتند که پیش از کامپیوتر و ماشین حساب ها برای محاسبات مورد استفاده قرار می گرفتند. چوب خط ها احتمالا جزو نخستین وسیله هایی بودند که به این منظور استفاده می شدند. اما با پیشرفت علم و نیاز به دانستن و کشف جهان مینی کامپیوتر ها و ابر کامپیوتر ها به به این دنیا گشودند.

اولین کامپیوتر جهان

اولین کامپیوتر را نخستین ماشین حسابی می دانند که توانایی انجام ضرب و تقسیم و جذر گرفتن را نیز داشت. همان طور که گفته شد ماشین حساب قبلی که ساخته شده بود به صورت مکانیکی کار می کرد و تنها می توانست اعمال جمع و تفریق را انجام بدهد.

مخترع کامپیوتر کیست؟

در سال ۱۸۹۰ توسط ریاضی دانی انگلیسی به اسم چارلز بابیج اختراع شد. به همین علت، مخترع کامپیوتر را چارلز بابیج می دانند.
ماشینی که توسط چارلز بابیج ساخته شده بود دارای یک قطعه حافظه بود) که خود چارلز بابیج نام Store را روی آن گذاشته بود (و قطعه ای نیز مشابه با CPU در آن قرار داشت که در زمان خود یکی از پیشرفته ترین ماشین ها محسوب می شد.

همه چیز درباره اختراع رایانه

همان طور که گفته شد، اولین کامپیوتر ها همان ماشین حساب ها بودند و کم کم تحول و تکامل ماشین حساب ها باعث شد که کامپیوتر های امروزی به وجود بیایند. در واقع هدف از اختراع کامپیوتر ساخت ماشینی بود که بتواند محاسبات را ساده تر کند.
در ادامه با نسل های مختلف کامپیوتر ها و تاریخچه تکامل کامپیوتر ها بیش تر آشنا خواهید شد.

نسل های مختلف کامپیوتر ها

کامپیوتر ۵ نسل دارد که می توان آنها را به صورت زیر طبقه بندی کرد:

- **نسل اول (۱۹۴۶ تا ۱۹۵۹) :**کامپیوترهای نسل اول بر اساس دریچه های الکترونیکی (لامپ های خلاء) کار می کردند. از جمله کامپیوترهای معروف نسل اول می توان به انیاک(ENIAC) ، یونیواک(UNIVAC) ، ادواک (EDVAC) و غیره اشاره کرد.

اولین کامپیوتر نسل اول، کامپیوتر ایکن گفته می‌شود. این نام گذاری به افتخار پرفسور ایکن است که اولین کامپیوتری که . در سال ۱۹۳۷ با لامپ های خلاء موفق به ساخت اولین کامپیوتر شد. لامپ‌های

دیودی دارای خاصیت یک سو کنندگی جریان برق هستند و این موضوع سبب می شود که بتوان حافظه ایجاد کرد و به آن دسترسی داشت. همان طور که احتمالا می دانید، وزن اولین کامپیوتر جهان یعنی کامپیوتر ایکن بسیار زیاد بود و علت آن نیز همین استفاده از لامپ های دیودی بود. این موضوع سبب می شد که کامپیوتر ها به سختی قابل جابه جایی باشند و فضای بسیار زیادی را نیز اشغال کنند.
در طرحی که پروفسور ایکن ارائه داده بود از مبنای ده استفاده می شد. در این طرح برای هر کارکتر ده دیود وجود داشت که یکی از آن ها روشن می ماند و بقیه خاموش می شدند. بعد ها این مبنا به مبنای دو تغییر یافت که خود باعث شد وزن و حجم کامپیوتر تا حد خوبی کاهش یابد.

- **نسل دوم (۱۹۵۹ تا ۱۹۶۵) :**در کامپیوترهای نسل دوم ترانزیستورها جای لامپ های خلاء را گرفتند. برخی از معروفترین کامپیوترهای نسل دوم سری های1400 IBM ، 1620 IBM، 7000 IBMو غیره بودند. همان طور که گفته شد، لامپ های دیودی حافظه کم و حجمی بسیار زیاد به کامپیوتر ها می دادند و این موضوع باعث شد که در سال ۱۹۴۸ ترانزیستور ها جایگزین شوند. ترانزیستور ها علاوه بر حجم کم تر، انرژی کم تری نیز نیاز دارند و حرارت کم تری نیز تولید می کننده و به جز این، قیمت کم تری نیز دارند و از هر لحاظ به صرفه تر می باشند. ترانزیستور ها تا ده سال پس از اختراع در کامپیوتر ها به کار برده نشدند اما پس از گذشت ده سال نسل دوم کامپیوتر ها روی کار آمدند. این کامپیوتر ها حافظه بیش تری داشتند، جای کم تری اشغال می کردند، سریع تر بودند و قیمت آن ها نیز کم تر بود. به علاوه زبان برنامه نویسی که در کامپیوتر های نسل دوم مورد استفاده قرار می گرفت نیازی به داشتن اطلاعات مربوط به ماشین ها نداشت.
در نسل اول کامپیوتر ها شما برای برنامه نویسی نیاز به داشتن دانش ماشینی داشتید ولی در نسل دوم، کد های برنامه نویسی برای کامپیوتر ها قابل فهم بودند. این موضوع باعث شد که کامپیوتر ها راحت تر به کار گرفته شوند و استفاده از آن به شکلی گسترده تر رواج پیدا کند.
- **نسل سوم (۱۹۶۵ تا ۱۹۷۱) :** در نسل سوم، از مدارهای مجتمع (IC) در ساخت کامپیوترها استفاده شد. از جمله کامپیوترهای این نسل360 IBM ، 370 IBM، PDPو غیره می توان نام برد.
با وجود این که ترانزیستور ها کارایی بهتری نسبت به لامپ ها و ترانزیستور ها داشتند اما خاصیت اهن ربایی حله ها و میله ها از سال ۱۹۶۴ به جای آن ها به کار گرفته شدند. به جای این که سمت عبور جریان برق را ترانزیستور و لامپ های خلاء تعیین کنند این کار را قطب های آهن ربا انجام می دادند. جنس حلقه و آلیاژی که برای این که مورد استفاده قرار می گرفت دارای اهمیت بسیار زیادی بود.
- **نسل چهارم (۱۹۷۱ تا ۱۹۸۰) :** کامپیوترهای نسل چهارم با استفاده از مدارهای مجتمع در مقیاس بسیار بزرگ (VLSI) ساخته می شدند. برخی از رایانه های معروف این نسل عبارتند از1000 STAR :، CRAY-1، CRAY-X-MP، DEC 10و غیره.
این کامپیوتر ها چندان با کامپیوتر های نسل سوم متفاوت نبودند اما توانایی هایی بیش تر با عمر بالا تری دارند. همچنین در این نسل از کامپیوتر ها از ریز پردازنده ها استفاده شده است.

- **نسل پنجم (۱۹۸۰ –) :** نسل پنجم کامپیوترها هنوز ادامه دارد. کامپیوترهای نسل پنجم بر اساس فناوری های متعددی مثل یکپارچه سازی در مقیاس فوق العاده بزرگ(ULSI) ، هوش مصنوعی (AI) و سخت افزار پردازش موازی ساخته می شوند. کامپیوترهای این نسل شامل رایانه های رومیزی(Desktop)، لپ تاپ(Laptop) ، نوت بوک (Notebook) و ... می شوند.

قیمت سخت افزار های نسل پنجم کامپیوتر ها به شدت کاهش یافت و خرید کامپیوتر برای افراد راحت تر شد. بنابراین برنامه نویسی پیشرفت کرد و بیش تر بین افراد رواج یافت. در نسل پنجم کامپیوتر ها می شد با کمک کامپیوتر ها ارتباط صوتی و تصویری برقرار کرد.

در نسل پنجم کامپیوتر ها از حافظه های نوری کم حجم و با گنجایش زیاد استفاده می شود. از دیگر ویژگی های نسل پنجم کامپیوتر ها می توان به استفاده کردن از هوش مصنوعی و استنتاج کامپیوتری اشاره کرد.

نسل ششم (–) : کامپیوتر های نوع پنتیوم نسل ششم کامپیوتر ها هستند. این کامپیوتر ها از سیستم های چند رسانه‌ای استفاده می کنند و دارای امکانات بسیار زیادی هستند.

اولین کامپیوتر شخصی

کامپیوتر هایی که مورد استفاده قرار می گرفتند همه کاربرد های صنعتی و اداری داشتند. در واقع فروش اولین کامپیوتر شخصی نیز مربوط به یک ماشین حساب بود که در مجله ساینس و توسط شرکت هولت پکارد اتفاق افتاد. پس از آن Altair 800 وارد بازار شد که اولین کامپیوتری بود که نرم افزار مایکروسافت Altair BASIC روی آن نصب می شد.

اولین کامپیوتر های اپل در جولای ۱۹۷۶ به فروش رسیدند. استیو ووزنیاک کامپیوتر Apple 1 را طراحی کرد و ۲۰۰ دستگاه از این کامپیوتر تولید شد.

تاریخچه کامپیوتر در ایران

اولین کامپیوتر ایران سال ۱۳۴۱ وارد شد. این یعنی حدود ده سال پس از این که کامپیوتر وارد کشور های صنعتی شده بود به ایران نیز راه پیدا کرده بود.

از سال ۱۳۵۰ تا ۱۳۶۰، خرید سخت افزار و نصب نرم افزار ها در ایران به شدت حالتی رقابتی پیدا کرده بود. پس از انقلاب و تا سال ۱۳۵۹ یک بازنگری در فعالیت های کامپیوتری اتفاق افتاد و در نهایت پس از باز شدن دانشگاه ها در سال ۱۳۶۲ رشد کامپیوتر در ایران اغاز شد و پیشرفت زیادی در هر دو حوزه سخت افزار و نرم افزار اتفاق افتاد. ضمن این که کامپیوتر ها توانایی پردازش زبان و خط فارسی را پیدا کردند.

آشنایی با نرم افزار و سخت افزار کامپیوتر

نرم افزار(Software)

نرم افزار کامپیوتر به مجموعه ای از دستورالعمل ها یا برنامه هایی گفته می شود که به سیستم کامپیوتری دستور می دهد تا بر اساس آن دستور کار کند. به طور کلی دو نوع نرم افزار وجود دارد:

- **نرم افزار سیستمی (System Software)** کار نرم افزار سیستمی برقراری ارتباط بین اجزای سخت افزاری است تا کاربر بتواند با کامپیوتر تعامل داشته باشد. این نوع نرم افزارها برای عملکرد صحیح کامپیوتر ضروری هستند. نرم افزارهای سیستمی برای اجرای برنامه های جداگانه یا ابزارهای سودمند در کامپیوتر، رابطی فراهم می کنند. سیستم عامل ها(Operating systems) ، درایورها(drivers) ، نرم افزارهای کاربردی (utility software) و فریمورها (firmware) نمونه های رایجی از نرم افزارهای سیستمی هستند.
- **نرم افزار کاربردی (Application Software)** نرم افزار کاربردی برای کمک به کاربران در انجام کارهای خاصی مثل گشت و گذار آنلاین، تنظیم زنگ هشدار، گوش دادن به موسیقی، پخش فیلم، طراحی عکس، ویرایش و غیره طراحی شده است. این نوع نرم افزار اکثرا در فرانت اند (frontend) اجرا می شود و به کاربر امکان می دهد تا روی آنها کار کند. مرورگرهای وب، نرم افزار فتوشاپ، نرم افزارهای چند رسانه ای و واژه پردازها نمونه ای از نرم افزارهای کاربردی هستند.

سخت افزار(Hardware)

قطعات فیزیکی متصل به کامپیوتر که در کنار هم کل یک کامپیوتر را تشکیل می دهند، سخت افزار یا قطعات سخت افزاری نامیده می شوند. سخت افزارها بسته به ساختارشان انواع مختلفی دارند. برخی از رایج ترین سخت افزارها عبارتند از موس(mouse) ، صفحه کلید یا کیبورد(keyboard) ، صفحه نمایش یا مانیتور(monitor) ، چاپگر یا پرینتر (printer) و غیره. در واقع سخت افزارها قطعاتی هستند که با چشم قابل مشاهده و لمس هستند.

بخش های اصلی کامپیوتر

اجزای اصلی کامپیوتر به صورت زیر تعریف می شوند:

واحد ورودی (Input Unit) از واحدها یا دستگاههای ورودی برای ورود داده ها یا دستورالعمل ها به کامپیوتر استفاده می شود. موس و کیبورد جزو رایج ترین دستگاههای ورودی کامپیوتر محسوب می شوند.

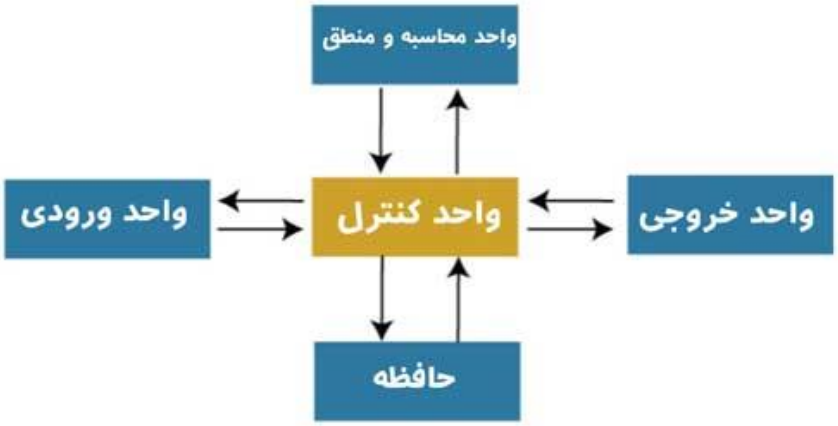
واحد خروجی (Output Unit) واحدها یا دستگاههای خروجی برای ارائه خروجی در فرمت مورد نظر به کاربر، استفاده می شوند. رایج ترین نمونه های دستگاههای خروجی کامپیوتر مانیتور و چاپگر هستند.

واحد کنترل (Control Unit) این واحد همانطور که از اسمش هم پیداست در درجه اول برای کنترل تمام عملکردها و قابلیت های کامپیوتر استفاده می شود. تمام اجزا یا دستگاه های متصل به کامپیوتر از طریق واحد کنترل با یکدیگر تعامل دارند. این واحد به صورت مختصر "CU نامیده می شود.

واحد محاسبه و منطق (Arithmetic Logic Unit) واحد محاسبه و منطق به انجام کلیه عملیات محاسباتی و منطقی در کامپیوتر کمک می کند. این واحد به طور خلاصه "ALU" نامیده می شود.

حافظه (Memory) بخش حافظه کامپیوتر برای ذخیره تمام داده های ورودی، دستورالعمل ها و داده های خروجی استفاده می شود. معمولا دو نوع حافظه وجود دارد: حافظه اولیه (Primary Memory) و حافظه ثانویه (Secondary Memory).حافظه ای که داخل CPU وجود دارد، حافظه اولیه نامیده می شود و به حافظه ای که می تواند از CPU جدا شود هم حافظه ثانویه می گویند.

نکته :واحد کنترل، واحد محاسبه و منطق حافظه به طور همزمان واحد پردازش مرکزی را تشکیل می دهند که به اختصار سی پی یو (CPU) نامیده می شود.



عملکردهای کامپیوتر

کامپیوتر چهار عملکرد اصلی دارد که در ادامه آنها را توضیح می دهیم:

۱- ورودی (Input) : هر چیزی که به کامپیوتر داده می شود ورودی نام دارد. داده های ورودی با استفاده از دستگاه های ورودی به کامپیوتر داده می شوند. کامپیوتر این داده ها را فقط به صورت باینری (binary) یعنی با فرمت خام می گیرد. دستگاههای ورودی کمک می کنند تا داده های ورودی به شکل باینری وارد کامپیوتر شوند تا برای آن قابل درک باشند. این داده ها می توانند در اشکال مختلف مثل حروف، اعداد، تصاویر و غیره وارد کامپیوتر شوند.

۲- پردازش(Processing) : پردازش وظیفه اصلی کامپیوتر است CPU .کار پردازش داده ها طبق دستورالعمل های وارد شده به سیستم رایانه را به عهده دارد. پردازش داده ها یک فرآیند داخلی در سیستم کامپیوتری است

که طی آن داده ها در یک صف اجرا می شوند. پس از تکمیل فرایند پردازش، اکثر داده ها به صورت خروجی منتقل می شوند. پردازنده (CPU) ریز تراشه ایست که مغز کامپیوتر است. سرعت پردازنده در کامپیوترهای مختلف متفاوت است، چون این مساله به عوامل مختلفی مثل نوع سی پی یو، حافظه و مادربُرد (motherboard) بستگی دارد.

۳- خروجی (Output) : هر چیزی که از کامپیوتر خارج می شود خروجی نام دارد. خروجی ها به داده هایی می گویند که برای انسان قابل خواندن هستند و روی صفحه نمایش کامپیوتر (مانیتور) نمایش داده می شوند. در صورت تمایل می توان خروجی را در دستگاه های ذخیره سازی ذخیره کرد. دستگاه های خروجی داده های پردازش شده توسط CPU به شکلی که برای انسان قابل فهم باشد تبدیل می کنند.

۴- ذخیره سازی (Storage) : دستگاهی که از آن برای ذخیره داده های یک سیستم کامپیوتری استفاده می شود، دستگاه ذخیره سازی یا انبارش نام دارد. کار دستگاه های ذخیره سازی، ذخیره داده های دیجیتال است. این دستگاهها می توانند داده ها را در حین کار کامپیوتر و پس از پردازش داده ها ذخیره کنند. دو نوع ذخیره سازی وجود دارد: ذخیره سازی فرار (volatile) و غیر فرار .(non-volatile) ذخیره سازی فرار داده ها را فقط تا زمانی که منبع تغذیه (برق) متصل است ذخیره می کند، اما ذخیره سازی غیر فرار می تواند داده ها را حتی پس از قطع منبع تغذیه نیز به طور دائم ذخیره نماید.

ویژگی های کامپیوتر

این ویژگی های اصلی کامپیوتر است که باعث شده به بخش مهم و جدایی ناپذیر زندگی انسانها تبدیل شود. بیایید با هم ویژگی های اصلی و مهم کامپیوتر را بررسی کنیم:

۱- سرعت (Speed) کامپیوترها ماشین های الکترونیکی پرسرعتی هستند و می توانند در هر ثانیه روی حدود ۳ تا ۴ میلیون دستورالعمل کار کنند. رایانه های پیشرفته حتی می توانند تریلیون‌ها دستورالعمل را در ثانیه انجام بدهند و زمان انجام کارهای دیجیتالی را کاهش بدهند.

۲- دقت (Accuracy) یکی دیگر از ویژگی های مهم کامپیوترها عملکرد دقیق آنهاست. کامپیوترها می توانند وظایف داده شده به آنها را تقریبا با دقت صد در صدی و بدون خطا تکمیل کنند. با اینکه امکان بروز خطا در کامپیوترها هم ممکن است، اما معمولا این خطاها به خاطر ورودی نادرست، دستورالعمل های نادرست یا اشکالات در تراشه ها ایجاد می شوند. در واقع همه این خطاها انسانی هستند و به خاطر کامپیوتر نیستند.

۳- ظرفیت ذخیره سازی (Storage Capacity) کامپیوترها به راحتی می توانند حجم عظیمی از داده ها را ذخیره کنند. رایانه های مدرن در مقایسه با نسخه های قدیمی تر از قابلیت ذخیره سازی بیشتری برخوردارند. داده های اضافی را می توان در دستگاههای جانبی دیگری مثل هارد دیسک های خارجی، فلش مموری ها و یا سایر دستگاهها هم ذخیره کرد. به خاطر سرعت باور نکردنی کامپیوترها، می توان این داده ها را در کمترین زمان ممکن از فضای ذخیره سازی بازیابی کرد.

۴- قابلیت اطمینان (Reliability) کامپیوترها سازگار و قابل اعتماد هستند و می توانند کارها و وظایف تکراری را هر چند بار که بخواهید بدون هیچ خطایی پردازش کنند. کامپیوتر مثل انسان خسته نمی شود و برای همین در انجام کارهای تکراری و مبتنی بر قوانین نسبت به انسانها برتر و بهترند.

۵- تطبیق پذیری (Versatility) تنوع وظایفی که یک کامپیوتر می تواند انجام دهد تقریباً بی نهایت است. این یعنی رایانه ها می توانند پشت سر هم و بدون خطا وظایف مختلفی را انجام بدهند. کامپیوترها الان دیگر فقط یک ماشین محاسباتی نیستند، بلکه می توان از آنها برای انجام کارهای مختلفی از رزرو بلیط گرفته تا وارد کردن اطلاعات مختلف و انجام محاسبات پیچیده ریاضی یا مشاهدات نجومی پیوسته و غیره استفاده کرد.

طبقه بندی کامپیوترها

کامپیوترها با توجه به اندازه فیزیکی شان به انواع زیر طبقه بندی می شوند:

۱- ابر کامپیوتر (Supercomputer) ابر رایانه ها سریع ترین و گران ترین نوع کامپیوتر هستند. این کامپیوترها بسیار بزرگند و برای نصب به فضای بیشتری نیاز دارند. از ابر کامپیوترها عمدتا برای انجام وظایف پیچیده و بزرگ مبتنی بر داده ها استفاده می شود. این نوع کامپیوترها قادرند تریلیون ها دستورالعمل را به طور همزمان مدیریت کنند.

۲- کامپیوتر سیستم اصلی یا کامپیوترهای بزرگ (Mainframe Computer) این نوع کامپیوترها در مقایسه با ابرکامپیوترها کوچکترند ولی هنوز هم ابعاد بزرگی دارند. کامپیوترهای سیستم اصلی برای انجام صدها یا هزاران کار به طور همزمان طراحی شده اند و می توانند کارهای سنگین از جمله محاسبات پیچیده را انجام دهند حجم زیادی از داده را ذخیره کنند. این نوع کامپیوترها برای سازمان های بزرگ مثل سیستم های بانکداری، مخابرات و بخش های آموزشی مناسب هستند.

۳- ریز کامپیوتر (Microcomputer) میکرو کامپیوترها یا ریز رایانه ها از نظر قیمت ارزان هستند و از پلتفرم چند کاربره پشتیبانی می کنند. این نوع کامپیوترها برای انجام کارها و وظایف ضروری و برآورده کردن نیازهای فردی طراحی شده اند. از آنجایی که ریز کامپیوترها نسبت به کامپیوترهای سیستم اصلی کندتر هستند، برای استفاده در سازمانهای کوچک مثل کافی نت ها، مدارس، دانشگاهها، ادارات و غیره مناسبند. میکرو کامپیوترها با نام کامپیوترهای شخصی (PC) هم شناخته می شوند. لپ تاپ و کامپیوترهای دسکتاپ (رومیزی) نمونه هایی از میکروکامپیوترها هستند.

۴- مینی کامپیوتر (Minicomputer) به مینی کامپیوترها مینی فریم (Miniframe) هم گفته می شود. این نوع کامپیوترها در واقع رایانه های چند پردازشی متوسط هستند که به خاطر حمل آسان و سبک بودن طراحی شده اند. مینی کامپیوترها وزن کمی دارند و فضای کمی هم اشغال می کنند. از این نوع کامپیوترها می توان برای انجام کارهای مربوط به صورتحسابها، حسابداری، آموزش و اهداف مرتبط به کسب و کار استفاده کرد. از آنجایی که حمل این کامپیوترها آسان است، بهترین گزینه برای افرادی که در سفر به کامپیوتر نیاز دارند محسوب می شوند. تبلت ها(Tablet) ، نوت بوک ها (Notebooks) و تلفن های همراه نمونه هایی از مینی کامپیوتر هستند.

۵- کامپیوترهای ایستگاه کاری (Workstation) کامپیوتر ایستگاه کاری یک کامپیوتر قدرتمند و تک کاربره است. این نوع کامپیوتر در واقع یک رایانه شخصی با ریزپردازنده سریعتر، حجم حافظه بیشتر، مانیتور با کیفیت بالاتر،حافظه گرافیکی بالا و غیره است. کامپیوترهای ایستگاه کاری برای انجام هر نوع کار خاص به صورت حرفه ای مناسبند. این نوع کامپیوتر بر اساس وظایفی که انجام می دهد به دسته های ایستگاه کاری موسیقی، ایستگاه کاری گرافیکی یا ایستگاه کاری طراحی مهندسی دسته بندی می شود. اکثر مشاغل و افراد حرفه ای از کامپیوترهای ایستگاه کاری برای انجام کارهایی مثل ساخت انیمیشن، موسیقی، ویرایش ویدیو، طراحی پوستر، تجزیه و تحلیل داده ها و موارد دیگر استفاده می کنند.

مزایای استفاده از کامپیوتر

اصلی ترین مزایای استفاده از کامپیوتر شامل موارد زیر می شود:

- کامپیوترها می توانند وظایف داده شده به آنها را با سرعتی باورنکردنی انجام بدهند.
- کامپیوترها می توانند یک یا چند کار را چندین بار با دقت یکسان انجام بدهند.
- کامپیوترها امکان انجام چندین کار را به طور همزمان فراهم می کنند، چون برای عملکرد چند وظیفه ای بسیار مناسبند.
- کامپیوترها داده های ذخیره شده را امن و دور از دسترس کابران غیر مجاز نگه می دارند.
- کامپیوترها وظایف معمول را به طور خودکار و اتوماسیون (بدون نیاز به عامل خارجی یعنی انسان) انجام می دهند و امکان انجام کارهای هوشمندانه تر را برای انسانها فراهم می کنند.

معایب استفاده از کامپیوتر

اصلی ترین معایب استفاده از کامپیوتر شامل موارد زیر می شود:

- کامپیوترها نمی توانند به تنهایی کار کنند و برای انجام وظایفشان به دستورات انسانها نیاز دارند. علاوه بر این، کامپیوترها دستورالعمل های داده شده را کورکورانه و بدون فکر کردن به نتایج دنبال می کنند.
- کامپیوترها برای کار کردن به منبع تغذیه (انرژی) نیاز دارند و بدون منبع تغذیه عملا بی فایده هستند.
- کار کردن مدام با کامپیوتر می تواند باعث بروز مشکلات سلامتی شود.
- ضایعات و قطعات کامپیوتری روی محیط زیست تاثیر منفی می‌گذارند.
- کامپیوترها در بسیاری از بخش های شغلی جای انسان را می‌گیرند. آنها جایگزین کار انسانی می‌شوند و در نتیجه بیکاری را افزایش می‌دهند.

واحدهای اندازه گیری کامپیوتر

در این بخش به بحث **واحدهای اندازه گیری کامپیوتر** یا **واحد حافظه** می‌پردازیم.

بیت (Bit)

به کوچکترین واحد اندازه گیری حافظه که می تواند صفر یا یک دودویی باشد،بیت (Bit)گفته می‌شود. محتوای یک بیت مشابه کلیدی است که می‌تواند باز یا بسته باشد.

بایت (Byte)

به کوچکترین قسمت قابل آدرس دهی حافظه،بایت (Byte)می‌گویند. یک بایت معادل هست بیت است. یک بایت می‌تواند یکی از اعداد صفر تا ۲۵۵ را به صورت دودویی در خود نگهداری کند.

کلمه (Word)

هر کلمه (Word)، بزرگترین واحدی است که ریزپردازنده می تواند در هر عملیات پردازش کند. رایانه های شخصی معمولاً ۱۶ بیتی و ۳۲ بیتی هستند. در رایانه های ۱۶ بیتی طول کلمه ۱۶ بیت است و در رایانه های ۳۲ بیتی طول کلمه ۳ بیت است. نسل جدید رایانه های شخصی،۶۴بیتی هستند یعنی ریزپردازنده این رایانه ها در هرم عملیات ۶۴ بیت را می‌تواند پردازش کند و در نتیجه طول کلمه در آنها ۶۴ بیت است.

کاراکتر(Character)

به هر یک از حروف، ارقام و علائم قابل نمایش در رایانه یک کاراکتر (Character)گفته می‌شود. هر کاراکتر یک بایت حافظه را اشغال می کند. معمولاً تعداد کاراکترهای رایانه ۲۵۶ کاراکتر است. کاراکترها را با کدهای مخصوصی در یک جدول، به نام جدول آسکی (ASCII)نشان می‌دهند. این جدول یک جدول کد بندی است که از ۷ یا ۸ بیت استفاده می‌کند و هر عدد را به یک کاراکتر نسبت می‌دهد.کاراکتر ها شامل حروف، ارقام، علائم و نمادهای دیگر است. به ۱۲۸ کاراکتر اول آسکی استاندارد و به ۱۲۸ کاراکتر بعدی آسکی توسعه یافته می‌گویند. که از اسکی توسعه یافته برای تعریف حروف زبانهای دیگر (نظیر فارسی) استفاده می‌کنند. مثلاً عدد ۶۵ معرف کد آسکی کاراکتر A در اسکی استاندارد است و عدد ۱۴۱ معرف کد اسکی کاراکتر آ در اسکی توسعه یافته پارسی است.

کیلوبایت (KB)

به $۲^{۱۰}$ بایت،یک کیلو بایت (KB)گفته می‌شود. معمولاً برای تعیین اندازه اسناد،مدارک،تصاویر و بطور کلی فایل های رایانه ها از این واحد اندازه گیری استفاده می‌کنند. مثلاً می گویند اندازه این تصویر رایانه‌ای ۲۱۰KBاست

$1 KB = 2^{10} Byte = 1024 Byte$

مگابایت (MB)

به$۲^{۱۰}$بایت،یک مگابایت (MB)گفته می شود. معمولا برای تعیین اندازه قایل های رایانه از این واحد استفاده می کنند. مثلاً می گویند اندازه فایل این کتاب ۲۵MBاست. یک مگابایت حافظ همی‌تواند صدها صفحه متن یا چندین عکس را در خود نگهداری کند.

$1 MB = 2^{10} KB = 1024 = 2^{20} Byte = 1048576 Byte$

گیگابایت(GB)

به $۲^{۱۰}$مگابایت،یک گیگابایت(GB)گفته می‌شود. معمولاً برای تعیین اندازه حافظه های جانبی با ظرفیت بالا نظیر هارددیسک ها از این واحد استفاده می‌کنند. مثلاً می گویند اندازه حافظه هارد این رایانه ۵۰۰GB است.یک گیگابایت حافظه بزرگی است و می‌تواند یک فیلم دو ساعته یا ده‌ها ساعت موسیقی را در خود نگهداری کند.

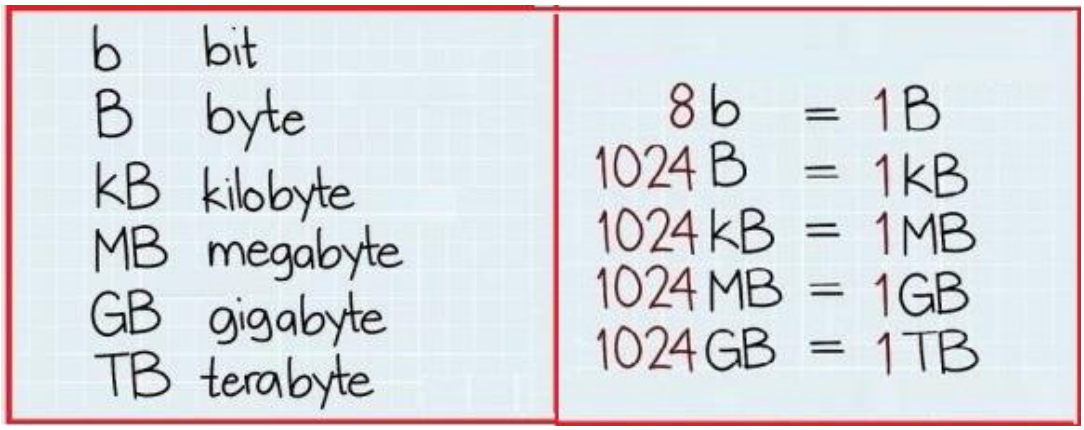
$1 GB = 2^{10} MB = 1024 MB = 2^{20} KB = 2^{30} Byte$

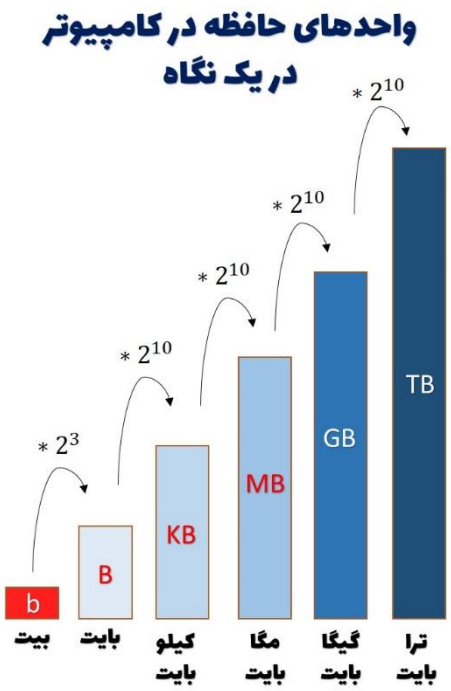
ترابایت (TB)

به $۲^{۱۰}$گیگابایت، یک ترابایت(TB)گفته می‌شود. یک ترابایت حافظه بسیار بالایی است و اطلاعات موجود در یک مرکز داده(Data Center)که تعداد زیادی تجهیزات ذخیره سازی اطلاعات در آن قرار دارد را می‌توان با این واحد حافظه نشان داد. مثلاً می گویند کل اطلاعات موجود در این مرکز داده،۱۶۵TB است.

اگزابایت (EB)

به $۲^{۱۰}$ترابایت،یک اگزابایت (EB)گفته می‌شود. اگزابایت بزرگترین واحد حافظه محسوب می شود. اطلاعات موجود در شبکه جهانی اینترنت را می توان با این واحد از حافظه اندازه گیری کرد.





سیستم اعداد

فلسفه وجودی اعداد به نیاز بشر برای شمارش برمی‌گردد. اعداد در دنیای امروز بخشی جدانشدنی از زندگی روزمره‌ی ما می‌باشند. جالب است بدانید همین کلماتی که در حال خواندن آن‌ها هستید به صورت کدهای صفر و یک برروی کامپیوتر شما ثبت می‌شوند. اعداد دسیمال، باینری، اوکتال و هگزادسیمال همگی نمایش‌های مختلف برای یک چیز یکسان می‌باشند. وقتی از عددی مثل ۶۸ صحبت می‌کنیم، منظورمان یک مقدار عددی است که در مبنای ده (دسیمال) به صورت ۶۸ نمایش داده می‌شود. اما اگر همین عدد را بخواهیم در مبنای دو (باینری) نمایش دهیم، حاصل به‌صورت ۱۰۰۰۱۰۰ می‌شود و اگر همین عدد را در مبنای هشت (اوکتال) نمایش دهیم حاصل به صورت ۱۰۴ بوده و در نهایت اگر همین عدد را در مبنای شانزده (هگزادسیمال) نمایش دهیم حاصل به صورت ۴۴ خواهد شد.

سیستم عددی به سیستمی گفته می‌شود که دارای مجموعه‌ای از اعداد، ارقام و گاهاً کاراکترها می‌باشد و هر کدام از آنها معنی خاصی دارند. بعضی وقت‌ها این اعداد در زندگی روزمره ما به کار برده می‌شوند؛ اما بعضی اوقات این اعداد قابل فهم و درک ما نیستند و فقط کامپیوترها، تراشه‌ها، آیسی‌ها و ... معنی این اعداد و ارقام را متوجه می‌شوند. سیستم‌های عددی به منظور کاربرد خاص و مشخصی طراحی شده‌اند.

برای مثال ساده‌ترین سیستم عددی، سیستم عددی دهدهی می‌باشد که محدوده اعداد آن از عدد ۰ تا ۹ است و مجموعاً شامل ده عدد می‌شود و به همین منظور نام‌گذاری شده است. این سیستم در علم ریاضیات، کامپیوتر و ... کاربرد وسیعی دارد. در زندگی روزمره هم از این سیستم برای "حساب و کتاب" روزانه در همه‌ی امور استفاده خواهد شد.

معروف ترین سیستم عددی در علوم کامپیوتر، سیستم دودویی یا باینری است و مبنای اصلی زبان‌های برنامه نویسی و کامپیوترها بر اساس این سیستم بوده و فقط شامل دو عدد ۰ و ۱ می‌باشد. شاید گاهاً کلی ۰ و ۱ در کنار هم ببینید و معنی آنها را متوجه نشوید؛ اما این بدین معنی نیست که این اعداد کاربردی ندارند.

سیستم های عددی پرکاربرد

در کل ۴ سیستم عددی پرکاربرد داریم که عبارت اند از:

۱) سیستم دهدهی یا اعشاری(Decimal)
۲) سیستم دودویی یا دوتایی(Binary)
۳) سیستم هشت‌تایی یا اکتال(Octal)
۴) سیستم شانزده‌تایی یا هگزادسیمال(Hexadecimal)

در ادامه به بررسی این سیستم‌های عددی و نحوه تبدیل آن‌ها به یکدیگر می‌پردازیم.

سیستم اعداد دهدهی یا اعشاری(Decimal)

این سیستم عددی پر کاربرد ترین سیستم عددی می‌باشد و به نام سیستم عددی روزمره نیز معروف است. در این سیستم ده رقم وجود دارد و به همین علت سیستم دهدهی نامیده می‌شود. این ده رقم شامل عدد ۰ تا ۹ است. در سیستم عددی دهدهی کوچکترین عدد ۰ و بزرگترین عدد ۹ است. به مثال‌های زیر دقت کنید.

- $۵۲۶۳_{۱۰}$.
- $۸۸۴۳_{۱۰}$.
- $۵۷۸_{۱۰}$.

برای نوشتن اعداد در مبنای سیستم دهدهی ابتدا عدد مد نظر را نوشته سپس عدد ۱۰ را به صورت کوچک در کنارش می‌نویسیم.

نکته :برای نشان دادن سیستم عددی، عدد نوشته شده باید در قسمت پایین سمت راست عدد نوشته شود. توجه کنید که مبنای عددی باید بصورت رقم نوشته شود نه چیز دیگری.

سیستم عددی دودویی(Binary)

در سیستم عددی دودویی فقط دو عدد ۰ و ۱ وجود دارد. به همین دلیل به این سیستم، دودویی می‌گویند. برای نشان دادن اعداد بزرگتر از یک، ارقام ۰ و ۱ را با قواعد خاصی کنار یکدیگر قرار می‌دهند. برای مشخص کردن اعداد در این سیستم، عدد ۲ را پایین سمت راست قرار می‌دهیم. به مثال‌های زیر دقت کنید.

- $(01001111)_2$
- $(111011111)_2$
- $(0000011001)_2$

ساختار قرار گرفتن اعداد در سیستم باینری به صورت زیر است.

$(B_N \dots B4\ B3\ B2\ B1)_2$

بجایB ، می‌توان دو عدد ۰ و ۱ را قرار داد. اعداد کنارB ، نشان دهنده تعداد ارقام است (توجه کنید ارزش مکانی نیست بلکه رقم شمارنده است).

به هر رقم یک بیت (Bit) گفته می‌شود. مثلا عدد ۱۱۱ یک عدد سه بیتی است؛ یا عدد ۱۱۰۰۱ یک عدد پنج بیتی می‌باشد. هشت بیت معادل یک بایت (Byte) است. واحد بزرگتر از بایت معادل ۱۰۲۴ بایت است که به آن کیلو بایت ($۲^{۱۰}$) گفته می‌شود.

در تصویر زیر ارزش مکانی سیستم باینری مشخص شده است. بیت اول از سمت راست همان B_0 بوده و کم ارزش ترین بیت می‌باشد که به آن LSB (Least Significant Bit) می‌گویند. به آخرین بیت که در سمت چپ است، B_7گفته و به اصطلاح به آن با ارزش ترین بیت یا MSB (Most Significant Bit) می‌گویند.

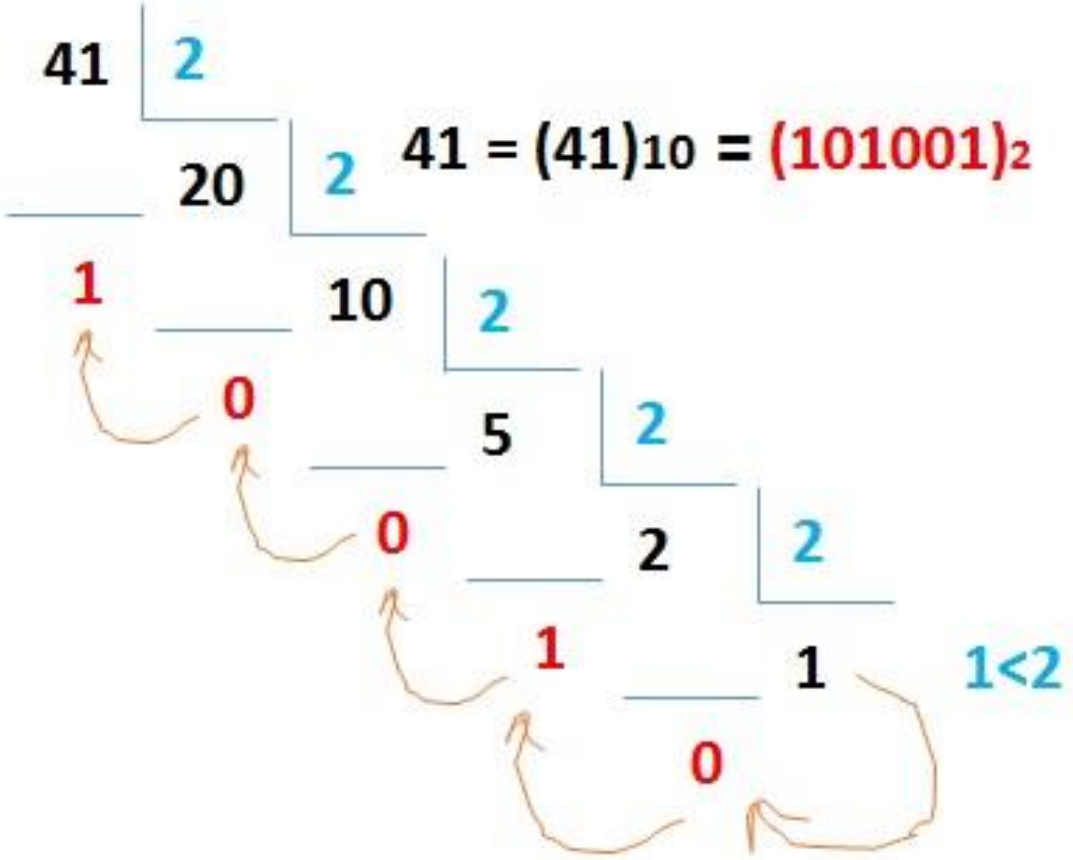
تبدیل اعداد باینری به دهدهی

برای تبدیل اعداد دودویی به دهدهی کافی است ارزش مکانی ارقام را با هم جمع کنیم. برای مثال می‌خواهیم عدد ۱۱۰۱ در مبنای باینری را به عدد دهدهی تبدیل کنیم.

$13 = (\mathbf{1} * 2^3) + (\mathbf{1} * 2^2) + (\mathbf{0} * 2^1) + (\mathbf{1} * 2^0)$ = 1101در مبنای دهدهی (اعشاری)

تبدیل اعداد دهدهی به باینری

برای تبدیل اعداد دهدهی به باینری از روش تقسیم متوالی استفاده می‌کنیم. به شکل زیر دقت کنید.



در این روش باید عدد مدنظر را بصورت متوالی بر عدد ۲ تقسیم کنیم. این تقسیم تا جایی ادامه پیدا می‌کند که آخرین خارج قسمت برابر ۱ باشد. سپس اعداد برحسب مراحل تقسیم در ارزش مکانی باینری جاگذاری می‌شوند. در جدول زیر اعداد ۰ تا ۱۵ در ۴ مبنا آورده شده‌اند.

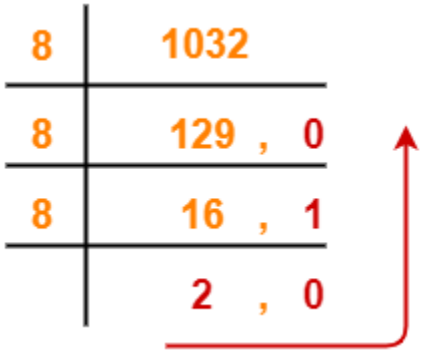
سیستم اعداد هشت تایی یا اکتال(Octal)

در این سیستم مبنا عدد ۸ بوده و از هشت عدد ۰ تا ۷ استفاده می‌کنیم. این سیستم عددی تقریبا منسوخ شده است و امروزه کاربرد کمتری نسبت به دیگر سیستم های عددی دارد؛ اما به عنوان یک مطلب برای یادگیری، مثال های زیر در مبنای ۸ هستند و تبدیل آنها به دهدهی نیز آورده شده است.

- 56_8 = 46 در مبنای دهدهی
- 10_8 = 8 در مبنای دهدهی
- 100_8 = 64 در مبنای دهدهی
- $321_8 = (1 * 8^0) + (2 * 8^1) + (3 * 8^2)$ = 209 در مبنای دهدهی

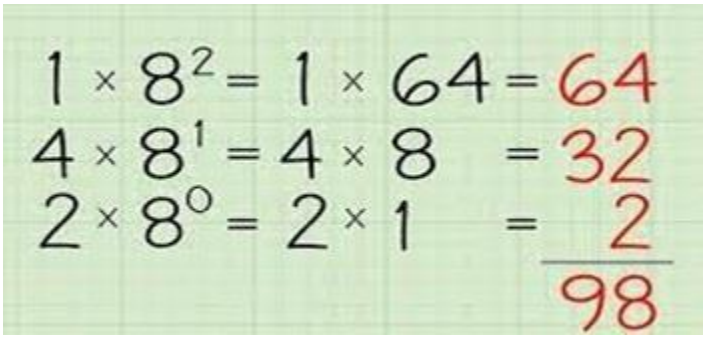
تبدیل اعداد دهدهی به هشت‌تایی

برای تبدیل اعداد در سیستم دهدهی به سیستم هشت‌تایی باید عدد مدنظر(عدد دهدهی) در عدد ۸ تقسیم متوالی شود. این فرآیند تا زمانی که آخرین خارج قسمت کوچکتر از ۸ شود، ادامه پیدا می‌کند.



همان‌طور که در تصویر بالا ملاحضه می‌کنید، عدد $۱۰۳۲_{۱۰}$ را بصورت متوالی در عدد ۸ تقسیم کرده و باقی مانده حاصل از تقسیم را به ترتیب از آخرین باقی مانده به اولین باقی‌مانده چینش می‌کنیم. بنابراین عدد فوق در مبنای ۸ می‌شود $۲۰۱۰_{۸}$.

تبدیل اعداد هشت‌تایی به دهدهی



در مثال بالا عدد $۱۴۲_{۸}$ را به سه عدد ۲ ۴ ۱ تقسیم کردیم؛ سپس به ترتیب در اعداد $۸^{۰}$ و $۸^{۱}$ و $۸^{۲}$ ضرب کردیم و در نهایت حاصل همه موارد را با هم جمع کردیم. توجه شود که توان عدد ۸ برگرفته شده از جدول ارزش مکانی است.

سیستم اعداد شانزده تایی یا هگزا دسیمال(Hexadecimal)

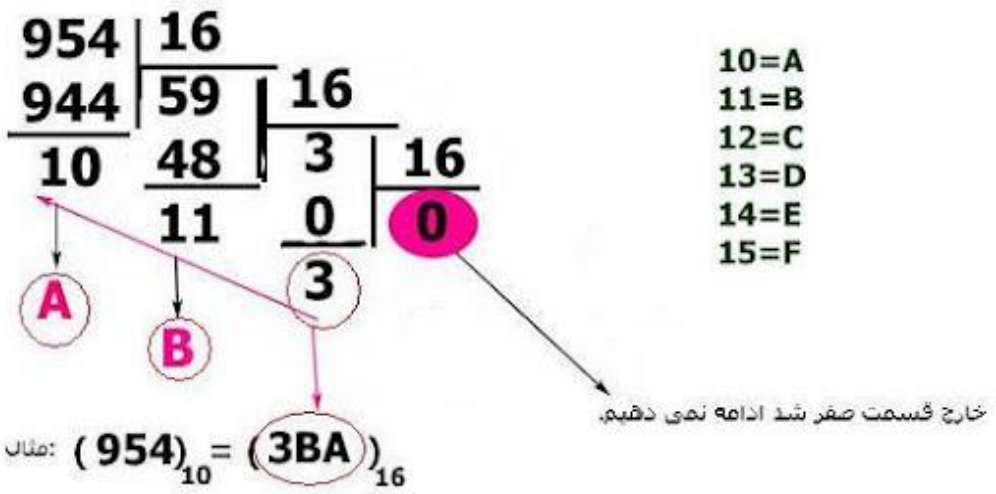
مبنای این سیستم عدد ۱۶ می‌باشد؛ یعنی هر رقم می‌تواند یکی از اعداد ۰ تا ۹ و یا یکی از حروف A تا F باشد. ارزش هر رقم در جدول زیر مشخص است.

Decimal	Hexadecimal
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	A
11	B
12	C
13	D
14	E
15	F

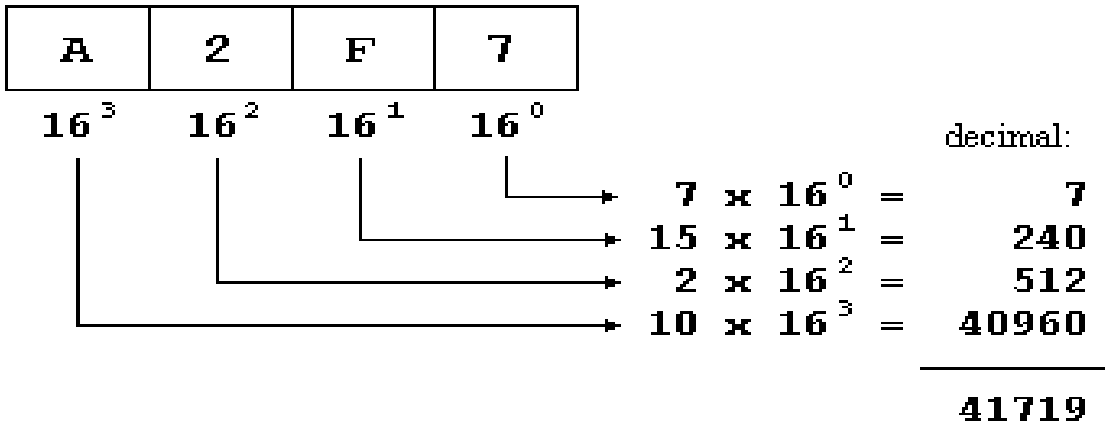
برای نشان دادن اعدادی که ارزش بیشتری از عدد ۱۶دارند، اعداد و حروف مربوطه را طبق قواعد خاصی کنار یکدیگر قرار می‌دهیم.

تبدیل اعداد دهدهی به شانزده‌تایی

برای تبدیل اعداد دهدهی به اعداد شانزده‌تایی همانند روش‌های قبلی، عدد مدنظر را باید بر عدد ۱۶ تقسیم متوالی کنیم.



تبدیل اعداد شانزده‌تایی به دهدهی



برای تبدیل سیستم شانزده‌تایی به سیستم دهدهی همانند سیستم‌های قبلی، طبق ارزش‌دهی موقعیت مکانی بیت‌ها اعداد را از حالت شانزده‌تایی به سیستم دهدهی تبدیل می‌کنیم. در مثال فوق عدد "A2F7" در مبنای شانزده است و ارقام آن به ترتیب در ضرایب ۱۶^۰، ۱۶^۱، ۱۶^۲ و ۱۶^۳ ضرب شده و با هم جمع شده‌اند. حاصل نهایی ۴۱۷۱۹ در مبنای ۱۰ است.

۲- معرفی انواع شبکه های کامپیوتری و موارد استفاده از آنها

وقتی چند کامپیوتر با هدف ارسال داده یا اشتراک منابع به هم وصل می شوند، شبکه کامپیوتری تشکیل می شود که این شبکه ها متناسب با محدوده پوشش، رسانه و نوع ارتباط به انواع مختلف تقسیم شداند که هر کدام کاربرد مخصوص به خود را دارند.

فهرست

- **بررسی مختصر شبکه های کامپیوتری**
- **انواع شبکه کامپیوتری بر اساس ویژگی های مختلف**
- **انواع توپولوژی برای شبکه های کامپیوتری**

۱- ۱- بررسی مختصر شبکه های کامپیوتری

شبکه کامپیوتری، مجموعه ای از کامپیوترهای مستقل است که با هدف اشتراک گذاری منابع و داده ها به همدیگر وصل شده اند. البته، به غیر از کامپیوتر دستگاه های دیگری مثل مودم، روتر، سویچ و هاب هم در این گردهمایی نقش دارند و ارتباط سیمی یا بی سیم بین کاربران را راحت تر می کنند.

شبکه های کامپیوتری از انواع گره ها مثل سرورها، سخت افزارهای شبکه، کامپیوترهای شخصی و لینک های ارتباطی تشکیل شده است. گره های موجود در انواع شبکه های کامپیوتری از مجموعه قوانین و پروتکل های خاصی پیروی می کنند تا نحوه ارسال و دریافت داده ها با اصول خاصی انجام شود.

هدف از ایجاد شبکه

- به دلیل اشتراک منابع و بار، برنامه ها مجبور نیستند روی یک سیستم واحد اجرا شوند.
- استفاده اشتراکی از منابعی مثل چاپگرها، درایوها و لوازم جانبی دیگر باعث کاهش هزینه می شود.
- با خرابی و اختلال در یک سیستم، کل شبکه از کار نمی افتد و با جایگزین کردن سیستم خراب با یک سیستم جدید، مشکل شبکه حل می شود.
- اضافه کردن پردازنده یا کامپیوترهای بیشتر، کار ساده ای است.
- دسترسی به اطلاعات از راه دور، دسترسی به اینترنت، ایمیل و ... با شبکه امکان پذیر است.
- ...

۱- ۲- انواع شبکه کامپیوتری بر اساس ویژگی های مختلف

شبکه های کامپیوتری بر اساس اندازه، نوع ارتباط، رسانه ارتباطی، معماری و توپولوژی تقسیم بندی شده اند که هر کدام متناسب با ویژگی های خود، کاربردهای مخصوصی دارند که در ادامه به بررسی تک تک آنها می پردازیم:

انواع شبکه بر اساس اندازه

۱) Personal Area Network (PAN)

PAN به عنوان کوچک ترین و پایه ترین نوع شبکه، به یک شخص محدود می شود، یعنی ارتباطات بین دستگاه ها فقط در فضای کاری یک فرد متمرکز است. برد شبکه PAN از یک شخص تا دستگاه تقریباً ۱۰ متر است.

لپ تاپ، تلفن همراه، تبلت و پخش کننده رسانه از مهم ترین دستگاه هایی هستند که برای توسعه این نوع شبکه استفاده می شوند. موس های بی سیم، صفحه کلید و بلوتوث از نمونه های PAN هستند. پس دفعه بعد که تلفن خود را به مدیا پلیر ماشین خود وصل می کنید؛ می توانید از شبکه شخصی خود تشکر کنید.

۲) Local Area Network (LAN)

LAN پرکاربردترین نوع شبکه های کامپیوتری است که کامپیوترهای موجود در یک منطقه محلی (خانه، مدرسه، کتابخانه، آزمایشگاه، دانشگاه و اداره) را از طریق یک مسیر ارتباطی مشترک به یکدیگر وصل می کند.

این نوع شبکه برای اتصال دستگاه های موجود در یک یا چند ساختمان (بسته به فاصله آنها) بکار می رود و فرقی می کند که رسانه بین دستگاه ها از نوع سیمی یا بی سیم باشد. ساده ترین نوع شبکهLAN ، اتصال کامپیوترها به یک پرینتر در خانه یا اداره است. البته، تعداد دستگاه های موجود در شبکه محلی نمی تواند بیشتر از ۵۰۰۰ باشد. نیاز دائم به مدیریت، هزینه اولیه نصب نسبتاً بالا و امکان دسترسی کاربران غیرمجاز به داده های حساس از معایب اصلی این نوع شبکه هستند.

۳) Campus Area Network (CAN)

این شبکه از اتصال چند شبکه LAN به وجود می آید و منطقه جغرافیایی خاصی را پوشش می دهد. این شبکه از LAN بزرگتر و از MAN کوچکتر است و معمولاً در مکان هایی مثل مدارس، دانشگاه ها و ... استفاده می شود.

CANها این امکان را به کاربران می دهد که فایل ها و داده های خود را به سرعت در شبکه به اشتراک بگذارند و ماندگاری داده ها در شبکه باعث کاهش تاخیر در ارسال و دریافت داده ها می شود. افزودن امکاناتی مثل **فایروال** های امنیتی، مسدود کردن دستگاه های ناامن، کنترل دسترسی و ... باعث افزایش امنیت این نوع شبکه های کامپیوتری می شود.

۴) Metropolitan Area Network (MAN)

MAN برای اتصال شبکه های کامپیوتری LAN به کار می رود و از لحاظ جغرافیایی قادر به پوشش یک شهر یا شهرک است. معمولاً سازمان های دولتی برای اتصال شهروندان و صنایع خصوصی از این نوع شبکه استفاده می کنند.

البته، بسته به نوع پیکربندی، یک شبکه MAN این امکان را به شما می دهد که منطقه ای با فاصله حداکثری ۵۰ کیلومتر را پوشش دهید. فیبر نوری، رسانه ای است که بیشتر برای این نوع شبکه های کامپیوتری استفاده می شود و همین باعث برقراری سریع تر ارتباطات می شود.

۵) Wide Area Network (WAN)

WAN مهم ترین و گسترده ترین شبکه کامپیوتری است که منطقه بزرگ تری را پوشش می دهد. سیستم شبکه WANمی تواند یک اتصال LAN باشد که با استفاده از خطوط تلفن امواج رادیویی به شبکه های محلی دیگر متصل می شود.

اینترنت بزرگترین شبکه WAN است که نقش مهمی در اتصالات بین المللی با فاصله بسیار زیاد دارد. معمولاً این مدل شبکه ها توسط ارائه دهندگان خدمات ایجاد می شود تا برقراری ارتباط بین مشاغل، مدارس، دولت ها و عموم مردم جهان با محدودیت مکانی روبرو نباشد.
در کل، پوشش گسترده و استفاده از فناوری های سیمی و بی سیم مختلف باعث به وجود آمدن خطا ها، مشکلات و تاخیراتی می شود که می تواند نگران کننده باشد.

۲ – ۲- انواع شبکه بر اساس رسانه ارتباطی

۱) شبکه سیمی

همانطور که از اسم آن مشخص است، در این نوع شبکه های کامپیوتری برای اتصال دستگاه های شبکه از رسانه های فیزیکی مثل سیم مسی، سیم زوج به هم تابیده یا کابل های فیبر نوری استفاده می شود. کابل های فیبر نوری، **پهنای باند** بیشتری دارند و سرعت انتقال آنها بالاتر است.

۲) شبکه بی سیم

در این نوع شبکه ها برای اتصال دستگاه ها و کامپیوترها به جای سیم از اتصالات فرکانس رادیویی استفاده می شود. تلفن های همراه، حسگرهای بی سیم، ریموت کنترل تلویزیون و گیرنده های دیسک ماهواره ای نمونه هایی از دستگاه های بی سیم هستند.

۲- ۳ - انواع شبکه بر اساس نوع ارتباط

۱) شبکه point to point

در این شبکه، بین هر دو گره ارتباط خصوصی و مستقیمی وجود دارد که همین ویژگی باعث می شود به امنیت ارتباطات بالا باشد و نیازی به رمزگذاری نباشد. تماس تلفنی یک نمونه رایج از این نوع شبکه های کامپیوتری است. با این نوع ارتباط، در یک شبکه عمومی امکان انتقال ترافیک خصوصی فراهم می شود. وجود لینک اختصاصی باعث می شود که کل پهنای باند مخصوص دو لینک باشد و امنیت و حریم خصوصی به طور کامل حفظ شود.

۲) شبکهMultipoint

در این نوع شبکه، کانال ارتباطی بین چند دستگاه یا گره به اشتراک گذاشته می شود. استفاده چند گره از ظرفیت کانال ارتباطی باعث می شود که بهره وری پهنای باند به حداکثر برسد. نحوه ارسال داده یا فایل به این صورت است که یک فرستنده وجود دارند و چند گیرنده که همه گیرنده ها به صورت اشتراکی به این داده ها دسترسی دارند و فاصله معیاری برای دریافت داده نیست. مشترک بودن کانال ارتباطی باعث کاهش امنیت و حریم خصوصی می شود.

۳) شبکهBroadcast

در این نوع شبکه های کامپیوتری، یک کانال ارتباطی وجود دارد و یک کامپیوتر نقش ارسال بسته را برعهده دارد و کامپیوترهای دیگر موجود در شبکه آن را دریافت می کنند. البته، بسته دارای آدرس گیرنده است و هر کامپیوتر

موقع دریافت بسته آدرس را بررسی می گیرد و در صورت مطابقت، آن را تحویل می گیرد. این نوع شبکه های کامپیوتری معمولاً کوچک و محلی هستند.

۲- ۴ - انواع شبکه بر اساس معماری

۱) معماری کلاینت – سرور

در این معماری یک کامپیوتر به عنوان سرور عمل می کند که کارایی بالایی دارند و ذخیره داده ها، دسترسی کاربران، درایور دیسک، چاپگرها یا ترافیک شبکه تحت مدیریت سرور است. در این نوع شبکه ها، سرور به عنوان نقطه مرکزی عمل می کند و بقیه کامپیوترها (کلاینت ها) به آن وصل می شوند و با ثبت درخواست، سرویس یا داده های درخواستی خود را از سرور دریافت می کنند.

۲) معماری همتا به همتا(Peer to Peer)

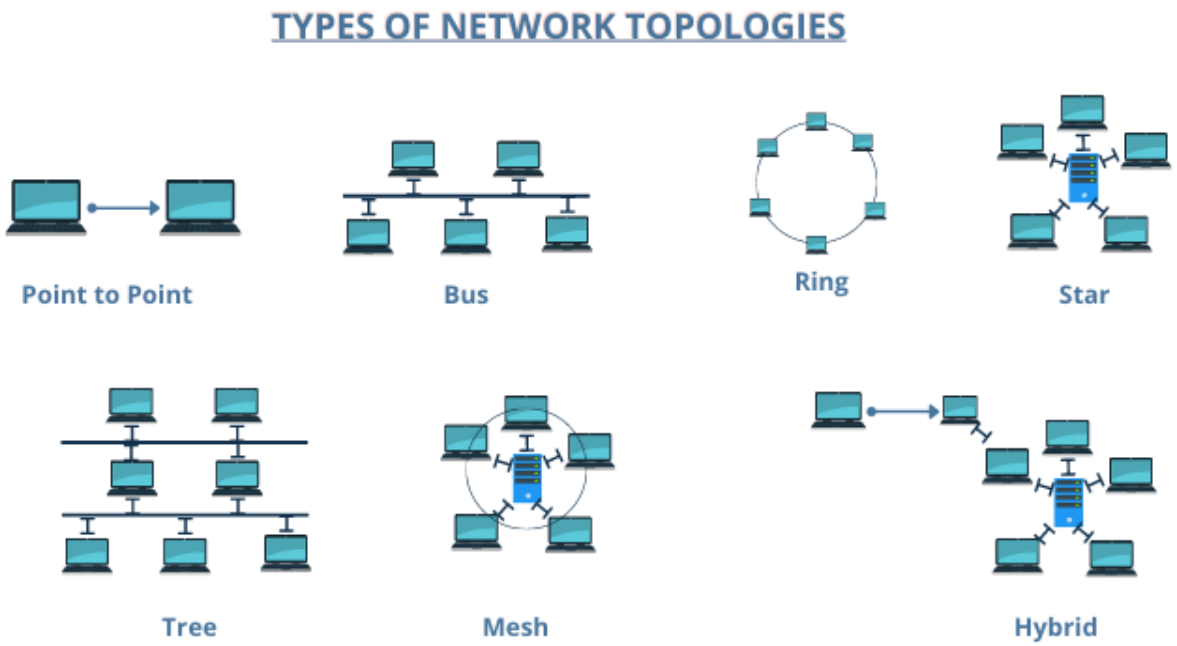
به کامپیوترهای با قابلیت ها و تنظیمات مشابه، همتا گفته می شود. در این نوع معماری، کامپیوترهای همتا از طریق اینترنت به همدیگر وصل می شوند. برای انتقال داده، نیازی نیست که یک کامپیوتر به عنوان سرور عمل کند، هر فایل و داده ای مستقیماً بین سیستم های موجود در شبکه می تواند به اشتراک گذاشته شود یعنی هر کامپیوتری می تواند سرور یا کلاینت باشد.

۳) معماری ترکیبی

همانطور که از اسم آن مشخص است، این معماری ترکیبی از مدل سرور-کلاینت و همتا به همتا است.

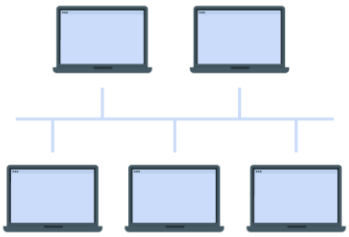
۲ – ۵ - انواع توپولوژی برای شبکه های کامپیوتری

نمایش هندسی نحوهٔ اتصال کامپیوترها یا به عبارتی نحوه قرارگیری کامپیوترها در داخل شبکه و ارتباط آنها با یکدیگر به عنوان توپولوژی شبکه شناخته می‌شود. انواع توپولوژی شبکه در شش دسته وجود دارند:



۱) توپولوژی باس

در توپولوژی خطی شبکه، هر کامپیوتر و هر دستگاه شبکه با یک کابل متصل می‌گردند. یعنی دقیقا دو عدد endpoint دارد. به همین دلیل به آن خطی نیز گفته می‌شود.



کافی است به شکل توجه کنید تا نحوه اتصال کامپیوترها و سایر اجزای شبکه را درک کنید. البته، با این که پیاده سازی این نوع شبکه راحت است ولی خرابی در کابل ارتباطی دستگاه ها باعث قطع تمام ارتباطات می شود و همین باعث می شود که رفع خطاها و پیکربندی مجدد شبکه به مراتب سخت تر است.

مشخصات توپولوژی خطی[۱]

- داده‌ها فقط در یک جهت منتقل می‌شوند.
- هر دستگاه به یک کابل متصل است.

مزایای توپولوژی خطی

- این توپولوژی، مقرون‌به‌صرفه است.
- در مقایسه با سایر توپولوژی‌ها، کابل کمتری نیاز دارد.
- در شبکه‌های کوچک مورد استفاده قرار می‌گیرد.
- اجرا و پیاده‌سازی آن، ساده است.

معایب توپولوژی خطی

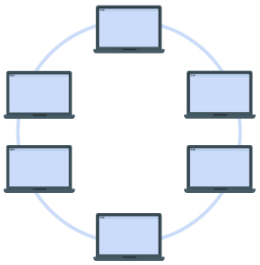
- به این دلیل که در کل سیستم از یک کابل استفاده شده، در صورت قطع شدن یکی از کابل‌ها، کل شبکه از کار می‌افتد.
- در صورت سنگین بودن ترافیک، عملکرد شبکه کاهش می‌یابد.
- طول کابل، محدود است و برای سیستم‌های با فاصله زیاد، قابل استفاده نمی‌باشد.
- در مقایسه با توپولوژی Ring (حلقه‌ای)، کندتر است .انو

[۱] BUS Topology

۲) توپولوژی حلقه‌ای

این روش از آن جهت حلقه‌ای نامیده می‌شود که هر کامپیوتر به کامپیوتر کناری خود، متصل می‌شود. به آن Token Ring نیز گفته می‌شود، زیرا تنها کامپیوترهایی که دارای token (سیگنال‌های ایجاد شده در شبکه) هستند، قادر به انتقال اطلاعات می‌باشند.

به عبارت ساده‌تر می‌توان گفت Token در این کانال در حرکت می‌باشد، و زمانی که به یک کامپیوتر برسد، آن کامپیوتر برای ارسال داده، مجاز است.



در این توپولوژی، کامپیوترها و دستگاه ها به صورت حلقه به همدیگر وصل شده اند، طوری که کامپیوتر آخر به کامپیوتر اول وصل است و دقیقاً دو همسایه برای هر دستگاه وجود دارد. جهت حرکت یکسان دستگاه ها باعث می شد که پروسه انتقال داده نسبتاً راحت باشد. از مهم ترین معایب این توپولوژی می توان به یک جهته بودن و نیاز به روشن بودن دائم کامپیوترها اشاره کرد. یک جهته بودن باعث می شود که یک بسته از همه گره ها عبور کند تا به مقصد برسد و همه کامپیوترها وقتی می توانند به یکدیگر متصل شوند که روشن باشند.

مشخصات توپولوژی حلقه‌ای[۲]

- در این توپولوژی، از تعدادی repeater استفاده می‌شود. چنانچه در شبکه‌های بزرگ، داده‌ای بخواهد از کامپیوتر اول به کامپیوتر آخر یک توپولوژی حلقه‌ای منتقل شود، می‌بایست از کل ۹۹ کامپیوتر دیگر گذر کند تا به آخرین آنها برسد. در نتیجه repeater های به کار برده شده، مانع از بین رفتن داده‌ها در این فرایند انتقال می‌گردند.
- انتقال داده‌ها در این توپولوژی به صورت یک طرفه است، اما می‌توان با ایجاد ارتباط دو طرفه بین هر کامپیوتر، اتصال دو طرفه برقرار نمود که به آن توپولوژی حلقه‌ای دو طرفه نیز گفته می‌شود.
- در توپولوژی حلقه‌ای دو طرفه، دو حلقه‌ی شبکه تشکیل می‌شود و داده‌ها در مسیر مخالف جریان پیدا می‌کنند. همچنین، اگر یکی از حلقه‌ها با شکست روبرو شود، حلقه‌ی دوم به عنوان بکاپ عمل می‌کند تا شبکه را حفظ کند.
- داده‌ها به روش متوالی یعنی بیت به بیت، منتقل می‌شوند. به عبارتی می‌بایست از هر کامپیوتر داخل شبکه، عبور کنند تا به نقطه‌ی آخر برسند.

---

[۲] Ring Topology

مزایا)توپولوژی حلقه‌ای

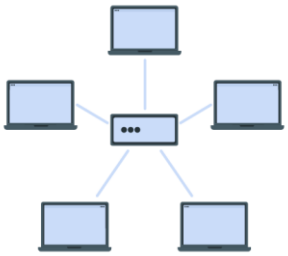
- انتقال داده‌ها در شبکه توسط ترافیک سنگین یا افزودن یک کامپیوتر دیگر به شبکه مورد نظر، تحت تاثیر قرار نمی‌گیرد. زیرا فقط کامپیوترهایی که دارای Token هستند، قادر به انتقال اطلاعات می‌باشند.
- یک توپولوژی ارزان از نظر نصب و گسترش محسوب می‌شود.

معایب توپولوژی حلقه‌ای

- عیب‌یابی در این توپولوژی، بسیار مشکل است.
- افزودن و یا حذف کامپیوتر در این شبکه، باعث بروز اختلال می‌گردد.
- به دلیل متصل شدن متوالی کامپیوترها، در صورت بروز خرابی در یک کامپیوتر، عملکرد کل شبکه مختل می‌شود.

۳) توپولوژی ستاره ای

در توپولوژی ستاره‌ای، تمامی کامپیوترها از طریق کابل به یک هاب (hub) متصل هستند. در این روش، هاب به عنوان یک دستگاه مرکزی می‌باشد و کلیه‌ی دستگاه‌های دیگر شبکه به آن متصل می‌گردند.



در این توپولوژی، یک کنترل کننده مرکزی وجود دارد که همه کامپیوترها به صورت point to point به این کنترل کننده وصل هستند. هیچ ارتباط مستقیمی بین دستگاه ها وجود ندارد و تردد مستقیم داده ها بین دستگاه ها غیر مجاز است. اتصال و جدا کردن دستگاه ها باعث هیچ وقفه ای در شبکه نمی شود و راه اندازی و پیکربندی آن کار ساده ای است. عملکرد همه دستگاه های متصل به کنترل کننده وابسته است و همین باعث می شود که خرابی کنترل کننده، خرابی کل شبکه را به دنبال داشته باشد.

مشخصات توپولوژی ستاره‌ای[۳]

- هر دستگاه در این شبکه، دارای اتصال جداگانه به هاب می‌باشد.
- hubبه عنوان repeater به منظور جریان داده‌ها عمل می‌کند.
- می‌توان با کابل‌هایtwisted pair ، کواکسیال و فیبرنوری راه اندازه نمود.

مزایای توپولوژی ستاره‌ای

- سرعت عملکردی بالای شبکه با تعداد کامپیوترهای کم و ترافیک سبک

[۳] Star Topology

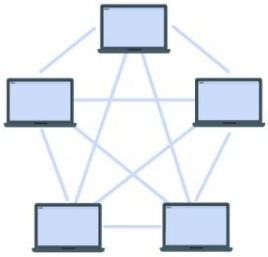
- قابلیت به‌روزرسانی بسیار سادهٔhub
- امکان عیب‌یابی راحت
- ایجاد تنظیمات و اصلاح ساده آن
- در صورت بروز مشکل برای یکی از کامپیوترها، بقیه دستگاه‌ها بدون هیچ مشکلی به کار خود ادامه می‌دهند.

معایب توپولوژی ستاره‌ای

- هزینه بالای نصب و پیاده‌سازی
- از نظر استفاده مقرون‌به‌صرفه نمی‌باشد.
- به دلیل وابستگی تمامی دستگاه‌ها بهhub ، در صورت بروز مشکل برای آن، کل شبکه مختل می‌گردد .انواع توپولوژی شبکه
- عملکرد و سرعت شبکه بستگی به ظرفیت هاب دارد.

۴) توپولوژی مش

در این توپولوژی، همه دستگاه ها به صورت نقطه به نقطه[۴] به یکدیگر وصل هستند و پیوند بین هر دو دستگاه به صورت اختصاصی است یعنی داده ها را فقط بین دو دستگاه منتقل می کند. اتصال n دستگاه به صورت مش کاملاً متصل با n*(n-1)/2 کانال انجام می شود. ارسال داده ها از طریق کانال های ارتباطی مختلف به صورت همزمان به کنترل ترافیک کمک می کند. البته، نیاز به سیم کشی و تعداد پورت ورودی/خروجی زیاد باعث می شود که نصب و پیکربندی آن کار دشواری باشد.



دو روش جهت انتقال داده‌ها در توپولوژی مش وجود دارد :توپولوژی شبکه

- routing
- flooding

MESH Topology: Routing

در این روش، دستگاه‌ها براساس نیاز شبکه، یک منطق مسیریابی (routing) خواهند داشت. به عنوان مثال یکی از منطق‌های مسیریابی می‌تواند انتخاب بر اساس کوتاه‌ترین مسیر باشد. یا این که می‌تواند بر اساس دور شدن از

[۴] point to point

لینک‌های شکسته باشد یا غیره. حتی می‌توان برای مسیریابی مجدد عملیات ناموفق، یک مسیریابی منطقی دیگر داشت.

MESH Topology: Flooding

در این روش، اطلاعات یکسان به تمامی دستگاه‌های شبکه منتقل می‌شود، بنابراین به هیچ مسیریابی منطقی نیاز نیست. به دلیل قدرتمند بودن شبکه، امکان از بین رفتن داده‌ها، بعید به نظر می‌رسد. اما ممکن است به بار ترافیکی ناخواسته‌ی شبکه منجر شود.

انواع MESH Topology چیست؟

- **Partial Mesh Topology** در این روش برخی از سیستم‌ها به همان روش توپولوژی مش، به هم متصل می‌شوند و برخی دیگر فقط به دو یا سه دستگاه متصل می‌گردند.
- **Full Mesh Topology** تمامی کامپیوترها یا دستگاه‌ها در داخل شبکه به هم مرتبط هستند .انواع توپولوژی شبکه

مشخصات توپولوژی مش [۵]

- کانکشن تمامی دستگاه‌ها با یکدیگر
- یک توپولوژی قدرتمند
- غیر قابل انعطاف

مزایای توپولوژی مش

- هر اتصالی فقط داده‌های مربوط به خود را منتقل می‌کند.
- قدرتمند بودن این توپولوژی
- امکان عیب‌یابی بسیار ساده
- برقراری امنیت و حریم خصوصی

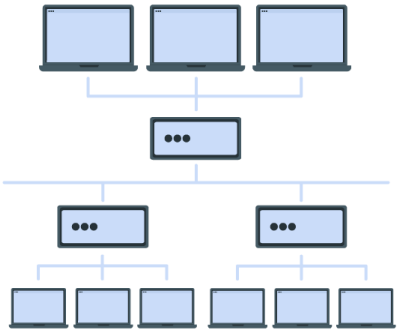
معایب توپولوژی مش

- نصب و پیاده‌سازی مشکل
- نیاز به حجم بالای کابل‌کشی در نتیجه هزینه زیاد آن

[۵] Mesh Topology

۵) توپولوژی درختی

در توپولوژی درختی نیز یک دستگاه مرکزی وجود دارد و تمامی دستگاه‌های دیگر به صورت سلسله مراتبی به آن متصل هستند. به این توپولوژی، سلسله مراتبی نیز گفته می‌شود که حداقل باید سه سطح داشته باشد.



این توپولوژی شبیه توپولوژی ستاره ای است با این تفاوت که گره ها به صورت سلسله مراتبی به ریشه کنترل کننده وصل هستند. آسیب دیدن یک زیردرخت آسیبی به زیردرخت های دیگر نمی رساند و این یکی از مزیت های اصلی این شبکه های کامپیوتری است. متکی بودن گره ها به گره ریشه و چالش برانگیز بودن پروسه نگهداری و تعمیر معایب های مربوط به این توپولوژی هستند.

مشخصات توپولوژی درختی[۶]

- ایده‌آل برای قرارگیری‌های گروهی
- مناسب برای شبکه‌های بزرگ

مزایای توپولوژی درختی

- در مقایسه با توپولوژی‌های خطی و ستاره‌ای، گستردگی بیشتری دارد و دستگاه‌های بیشتری را می‌تواند پوشش دهد.
- گسترش دستگاه‌ها در شبکه امکان‌پذیر و ساده است.
- مدیریت و نگهداری آن ساده می‌باشد.
- عیب‌یابی راحت

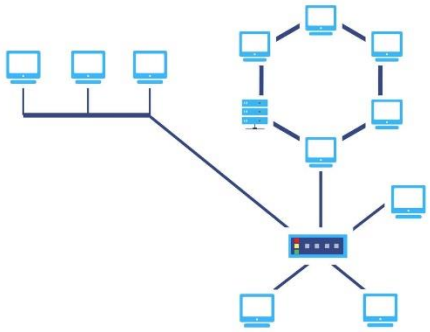
معایب توپولوژی درختی

- استفاده از کابل‌های زیاد
- هزینه بر بودن
- مشکل‌تر شدن نگهداری در صورت افزودن دستگاه به شبکه
- مختل شدن شبکه در صورت بروز اختلال در سیستم مرکزی

[۶] Tree Topology

۶) توپولوژی ترکیبی

این روش یک نوع ترکیبی از دو یا چند توپولوژی مختلف می‌باشد. به عنوان مثال، اگر در قسمتی از یک دفترکار از توپولوژی حلقه‌ای و در قسمت دیگر از توپولوژی ستاره‌ای استفاده شود، ترکیب این دو، توپولوژی ترکیبی را به وجود می‌آورد.



مشخصات توپولوژی ترکیبی [۷]

- ترکیبی از دو توپولوژی مختلف
- این نوع شامل مزایا و معایب توپولوژی‌های مختلف می‌شود.

مزایای توپولوژی ترکیبی

- بسیار قابل اعتماد در تشخیص خطاها و عیب‌یابی ساده
- موثر بودن
- انعطاف‌پذیر بودن و مقیاس‌پذیر بودن به هنگام گسترده‌تر شدن شبکه

معایب توپولوژی ترکیبی

- طراحی پیچیده
- هزینه بر بودن

[۷] HYBRID Topology

۴- انواع پروتکل های ارتباطی

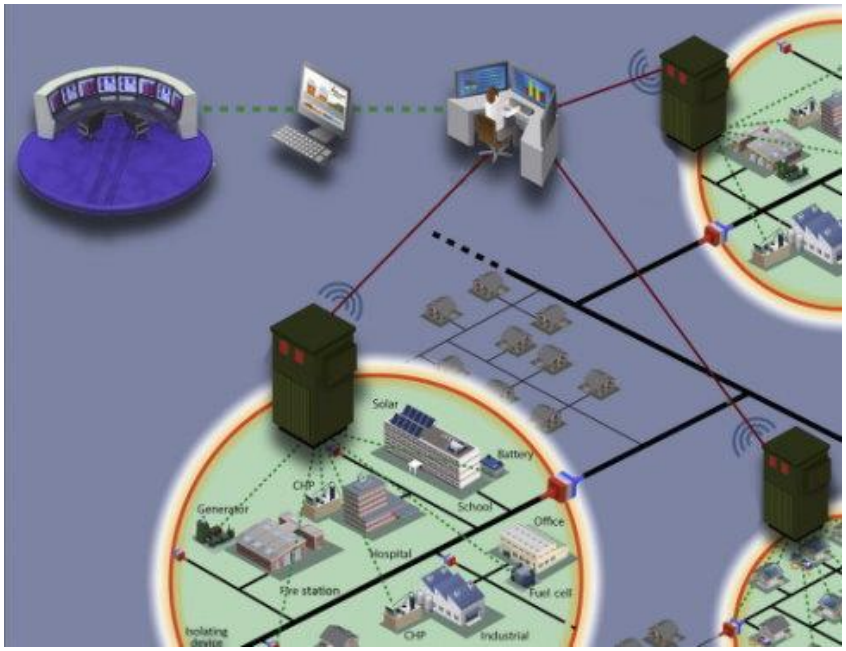
در علوم کامپیوتر یک پروتکل ارتباطی (قرارداد ارتباطی Communication Protocol) به مجموعه قوانینی گفته می‌شود که کامپیوترها برای ارتباط با یکدیگر از آن‌ها استفاده می‌کنند.

۴- ۱- مفهوم پروتکل چیست ؟

یک پروتکل ارتباطی، ساز و کاری از قوانین به حساب می‌آید که به دو یا بیش از دو موجودیت در یک سیستم ارتباطی اجازه می‌دهد تا اطلاعات را از طریق هر نوعی از انواع یک کمیت فیزیکی انتقال دهد. به بیان ساده‌تر، پروتکل علامت‌ها یا همان سیگنال‌هایی را تعریف می‌کند که کامپیوترها به یکدیگر می‌فرستند. همچنین، پروتکل سایر جزئیاتی مثل نحوه آغاز و پایان ارتباط را نیز تشریح می‌کند. یک پروتکل ارتباطی موارد زیر را برای شبکه‌های ارتباطی تعریف و تعیین می‌کند:

- ✓ قوانین
- ✓ نحو (سینتکس)
- ✓ مفاهیم
- ✓ همگام‌سازی ارتباطات
- ✓ روش‌های ممکن برای جبران خطا
- ✓ سایر موارد

پروتکل‌ها ممکن است به وسیله سخت‌افزار، نرم‌افزار یا ترکیبی از هر دو پیاده‌سازی شوند. سیستم‌های ارتباطی از قالب‌های شفاف و مشخص برای تبادل پیام‌های مختلف استفاده می‌کنند. هر پیام دارای معنای دقیق و مشخصی است. مقصود این پیام، بیرون کشیدن یک پاسخ از تعدادی پاسخ از پیش تعیین شده برای آن شرایط خاص است. رفتار مشخص شده معمولاً از نحوه پیاده‌سازی آن مستقل خواهد بود. باید بر سر پروتکل های ارتباطی در میان طرف‌های ارتباط توافق صوت بگیرد. برای رسیدن به توافق، ممکن است یک پروتکل توسعه پیدا کند و به یک استاندارد تبدیل شود.



۴- ۲- شباهت‌ها و تفاوت‌های پروتکل های ارتباطی با زبان های برنامه نویسی چه هستند؟

یک زبان برنامه نویسی چنین چیزی را برای محاسبات توصیف و تعیین می‌کند. بنابراین، شباهت نزدیکی بین پروتکل‌ها و زبان‌های برنامه نویسی وجود دارد. پروتکل‌ها به منظور ارتباط و زبان‌های برنامه نویسی برای محاسبات مورد استفاده قرار می‌گیرند. در یک ترکیب‌بندی متفاوت، می‌توان گفت پروتکل‌ها برای ارتباطات درست مثل چیزی هستند که الگوریتم‌ها برای محاسبات به حساب می‌آیند. اغلب چندین پروتکل جنبه‌های متفاوتی از یک ارتباط واحد را توصیف و مشخص می‌کنند.

مجموعه پروتکل یا Protocol Suite چیست ؟

به گروه یا دسته‌ای از پروتکل های ارتباطی که به منظور استفاده و عمل کردن به همراه یکدیگر طراحی شده‌اند، «مجموعه پروتکل (Protocol Suite) «گفته می‌شود. همچنین، زمانی که این پروتکل‌ها به صورت نرم‌افزاری پیاده‌سازی می‌شوند به آن‌ها «پُشته پروتکل (Protocol Stack) «می‌گویند.

۴- ۳- پروتکل های ارتباطی توسط چه نهادهایی مدیریت می‌شوند؟

پروتکل های ارتباطی اینترنتی توسط کارگروه مهندسی اینترنت (Internet Engineering Task Force | IETF) منتشر شده‌اند. مؤسسه مهندسان برق و الکترونیک (Institute of Electrical and Electronics Engineers | IEEE)پروتکل های شبکه های کامپیوتری وایرلس و سیمی را مدیریت می‌کند. سازمان بین‌المللی استانداردسازی (International Organization for Standardization | ISO) نیز سایر انواع پروتکل‌ها را تحت کنترل دارد. بخش استانداردسازی مخابرات ITU که به آن ITU-T گفته می‌شود، «پروتکل های ارتباطی و ساختارهای مخابراتی» را برای شبکه تلفن عمومی سوئیچ شده (Public Switched Telephone Network | PSTN) تحت مدیریت دارد. با همگرایی و تلاقی PSTN و اینترنت، استانداردها و پروتکل های مورد استفاده در هر یک از این حوزه‌ها نیز در حال پیوند و ادغام شدن هستند.

۴- ۴- معنی پروتکل ارتباطی چیست؟

پروتکل های ارتباطی توصیف رسمی از قالب‌ها و قوانین پیام‌های دیجیتالی هستند. کارکرد اصلی پروتکل های ارتباطی ، تبادل پیام‌ها از یک سیستم کامپیوتری به سیستم دیگر است. پروتکل های ارتباطی در سیستم‌های مخابراتی اهمیت دارند، چرا که پیام‌ها در این سیستم‌ها به طور دائم در حال ارسال و دریافت شدن هستند. پروتکل های ارتباطی وظایفی را شامل شناسایی و اصلاح خطاها، نشانه‌گذاری (علامت‌دهی)، احراز هویت و سایر موارد بر عهده دارند.

همچنین، پروتکل های ارتباطی می‌توانند مفاهیم، نحو (سینتکس) را تشریح کنند و ارتباط آنالوگ و دیجیتال را به یکدیگر پیوند دهند. پیاده‌سازی این پروتکل‌ها را می‌توان در سخت افزار و نرم افزار انجام داد. بنابراین، انواع پروتکل های ارتباطی که در تمام ارتباط‌های آنالوگ و دیجیتال مورد استفاده قرار می‌گیرند، می‌توانند هزاران نوع مختلف داشته باشند. شبکه‌های کامپیوتری بدون پروتکل های ارتباطی امکان ارائه عملکرد مناسب را نخواهند داشت.

- **پروتکل : (Protocol)** به مجموعه‌ای از قوانین و مقررات، پروتکل گفته می‌شود.
- **ارتباطات : (Communication)** تبادل اطلاعات از یک سیستم به سیستم دیگر با یک وسیله
- **پروتکل ارتباطی : (Communication Protocol)** مجموعه قوانین و مقرراتی که به دستگاه‌های الکترونیکی امکان می‌دهند تا به یکدیگر متصل شوند و داده‌هایی را با هم تبادل کنند.

۴- ۵- چرا انواع پروتکل های ارتباطی مهم هستند؟

پروتکل های ارتباطی دستگاه‌های مختلف تحت شبکه را برای ارتباط با یکدیگر از طریق انتقال سیگنال‌های آنالوگ، سیگنال‌های دیجیتال، فایل‌های مختلف و پردازش داده‌ها از یک دستگاه به سایر دستگاه‌ها هدایت

می‌کنند. انواع پروتکل های ارتباطی در شبکه‌های کامپیوتری و مخابراتی قابل استفاده هستند و قوانین مناسب برای انتقال اطلاعات از منبع به مقصد بر اساس آن‌ها اجرا می‌شوند. پر اهمیت‌ترین انواع پروتکل های ارتباطی در شبکه ، پروتکل کنترل انتقال (TCP | Transmission Control Protocol) و پروتکل بسته داده کاربر (User Datagram Protocol | UDP) را شامل می‌شوند.

۴- ۶- تاریخچه سیستم‌های ارتباطی

اصطلاح «پروتکل» با مضمون ارتباط داده‌ها اولین بار در اساس‌نامه‌ای با عنوان «پروتکلی برای استفاده در شبکه ارتباطات داده «NPL مورد استفاده قرار گرفت. این اساس‌نامه توسط راجر اسکنتل‌بری (Roger Scantlebury) و کیث بارتلت (Keith Bartlett) در سال ۱۳۴۶ (آوریل ۱۹۶۷) نوشته شده است. در شبکه آرپانت (ARPANET) نقطه آغاز برای ارتباط میزبان به میزبان در سال ۱۳۴۸ (۱۹۶۹ میلادی) پروتکل ۱۸۲۲ بود که قواعد انتقال پیام‌ها به یک IMP (پردازنده پیام رابط) را تعریف می‌کرد.

برنامه کنترل شبکه (Network Control Program) برای آرپانت که به اختصار NCP خطاب می‌شود، اولین بار در سال ۱۳۴۹ (۱۹۷۰ میلادی) پیاده‌سازی شد. رابط NCP به برنامه‌های کاربردی اجازه می‌داد تا در شبکه آرپانت با پیاده‌سازی پروتکل‌های ارتباطی سطح بالاتر به یکدیگر متصل شوند که نمونه ابتدایی از مفهوم لایه‌بندی پروتکل (Protocol Layering)به حساب می‌آید.

پژوهش‌های مرتبط با شبکه در اوایل سال ۱۳۴۹ توسط رابرت الیوت کان (Robert E. Kahn) و وینتون گرِی سِرف (Vinton Gray Cerf)به شکل‌گیری برنامه کنترل انتقال (TCP | Transmission Control Program) انجامید. مشخصات RFC 675 پروتکل TCP توسط وینتون سِرف به همراه یوگن دلال (Yogen Dalal) و کارل سانشاین (Carl Sunshine)در دسامبر ۱۳۵۳ (۱۹۷۴ میلادی) نوشته شد که در آن زمان همچنان یک طراحی یکپارچه و یکدست بود.

کارگروه بین‌المللی شبکه‌های کامپیوتری بر سر یک استاندارد داده‌نگار (Datagram) بدون اتصال توافق کردند که در سال ۱۳۵۴ به واحد CCIT ارائه شد اما توسط ITU یا ARPANET به کار گرفته نشد. تحقیقات بین‌المللی، خصوصاً تلاش‌های رِمی دسپرِس (Rémi Després) در توسعه استاندارد X.25 بر اساس مدارهای مجازی (Virtual Circuits) توسط ITU-T در سال ۱۳۵۵ (۱۹۷۶ میلادی) مشارکت داشتند. تولیدکنندگان کامپیوتر پروتکل های اختصاصی را مثل معماری شبکه سیستم‌ها (Systems Network Architecture | SNA) شرکتIBM ، همچنین DECnet مربوط به شرکت تجهیزات دیجیتال و سیستم‌های شبکه زیراکس توسعه دادند.

شکل‌گیری پروتکلTCP

نرم‌افزار پروتکل TCP به عنوان یک پُشته پروتکل ماژولار باز طراحی شد. در ابتدا به آن IP/TCP گفته می‌شد و در سال ۱۳۶۱ (۱۹۸۲ میلادی) روی SATNET نصب و سپس در اوایل سال ۱۳۶۲ (۱۹۸۳ میلادی) روی شبکه ARPANETنصب شد. همان‌طور که در RFC 1122 و RFC 1123 مشخص شده است، توسعه یک مجموعه پروتکل کامل، زیربنایی برای رشد پروتکل TCP/IP را به عنوان یک مجموعه پروتکل جامع و به عنوان جزئی اصلی از اینترنت در حال ظهور بنا نهاد.

تلاش‌های بین‌المللی روی یک مدل مرجع برای استانداردهای ارتباطی به خلق مدل OSI منجر شد که در سال ۱۳۶۳ (۱۹۸۴ میلادی) به انتشار رسیده است. برای مدتی در اواخر سال ۱۳۵۹ (۱۹۸۰ میلادی) تا اوایل دهه ۹۰ میلادی (۱۳۷۰ شمسی) سازمان‌ها و ملت‌ها بر سر این مسئله که از کدام استاندارد یعنی مدل OSI یا مجموعه پروتکل اینترنت استفاده کنند دچار دوقطبی شده بودند و بر سر این موضوع اختلاف داشتند که به کارگیری کدامیک از این استانداردها به ایجاد بهترین و قوی‌ترین شبکه‌های کامپیوتری منجر خواهند شد.

انواع پروتکل های ارتباطی شبکه چه هستند؟

انواع پروتکل های ارتباطی مختلفی وجود دارند که نقشی اساسی و کلیدی در ارتباط میان دستگاه‌های گوناگون در شبکه‌های کامپیوتری ایفا می‌کنند. هر یک از این پروتکل‌های ارتباطی اصلی در ادامه فهرست شده‌اند:

- پروتکل انتقال ابرمتن(Hypertext Transfer Protocol | HTTP)
- قرارداد زبان نشانه‌گذاری ابرمتن(Hyper Text Markup Language | HTML)
- پروتکل ساده نامه‌رسانی(Simple Mail Transfer Protocol | SMTP)
    - قرارداد پاپ(Post Office Protocol | POP)
    - پروتکل دسترسی به پیام اینترنتی) قرارداد پیام‌گزینی Internet Message Access Protocol | | IMAP)
- قرارداد انتقال فایل(File Transfer Protocol | FTP)
- پروتکل هدایت انتقال(Transmission Control Protocol | TCP)
- قرارداد اینترنت(Internet Protocol | IP)
- پروتکل نقطه به نقطه(Point-to-Point Protocol | PPP)

۴- ۷- دسته بندی انواع پروتکل های ارتباطی شبکه

به طور کلی دو نوع پروتکل ارتباطی وجود دارد. این دسته‌بندی بر اساس بازنمایی محتوایی است که باید حمل و انتقال داده شود:

- پروتکل های ارتباطی مبتنی بر متن(Text-Based)
- پروتکل های ارتباطی دودویی(Binary)

پروتکل های ارتباطی مبتنی بر متن چه هستند؟

یک پروتکل ارتباطی مبتنی بر متن یا «پروتکل متن ساده (Plain Text Protocol) «محتوایش را در قالب قابل خواندن توسط انسان اغلب به صورت متن ساده ارائه و نمایش می‌دهد. چنین پروتکلی که قابل خواندن توسط انسان است، در نقطه مقابل پروتکل‌های دودویی قرار می‌گیرد که دارای مزایای ذاتی برای استفاده در محیط‌های کامپیوتری هستند. از جمله این مزایای ذاتی، می‌توان به تجزیه و خوانش مکانیکی و مصرف پهنای باند بهینه اشاره کرد. کاربردهای گوناگون شبکه روش‌های متفاوتی برای کپسوله‌سازی داده‌ها دارند.

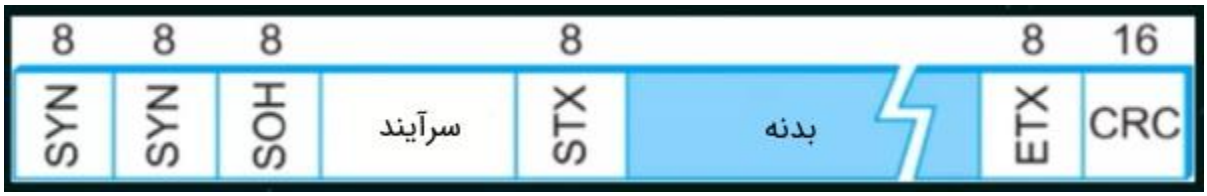
یکی از روش‌هایی که در خصوص پروتکل‌های اینترنت بسیار رایج است، یک نمایش مبتنی بر متن به حساب می‌آید که درخواست‌ها و پاسخ‌ها را به صورت متن با استاندارد اسکی (ASCII) انتقال می‌دهد و با یک کاراکتر خط جدید (و معمولاً با یک کاراکتر تعویض سطر) خاتمه می‌دهد. مثال‌هایی از پروتکل‌هایی که از متن ساده و قابل خواندن توسط انسان در دستورهای آن‌ها استفاده می‌شود، می‌توان به موارد زیر اشاره کرد:

- FTP
- SMTP
- HTTP
- SIP
- Finger Protocol

پروتکل های ارتباطی مبتنی بر متن معمولاً برای تجزیه کردن تحلیل ساختار جملات و تفسیر توسط انسان بهینه‌سازی شده‌اند. بنابراین، این انواع پروتکل های ارتباطی معمولاً برای زمانی مناسب هستند که بررسی محتوای پروتکل به وسیله انسان مورد نیاز باشد. برای مثال در طول عیب‌یابی (دیباگ کردن) و همچنین در طی مراحل

اولیه طراحی پروتکل ممکن است نیاز به بررسی و بازرسی محتوای پروتکل مربوطه توسط انسان وجود داشته باشد.

پروتکل های ارتباطی دودویی چه هستند؟



یک پروتکل ارتباطی دودویی یا همان باینری از تمام مقادیر ممکن برای یک بایت استفاده می‌کند. این برخلاف یک پروتکل ارتباطی مبتنی بر متن است. چرا که در یک پروتکل مبتنی بر متن ، تنها از مقادیری استفاده می‌شود که مربوط به کاراکترهای قابل خواندن توسط انسان در چارچوب کدگذاری آسکی هستند. پروتکل‌های دودویی با این مقصود طراحی شده‌اند که به جای انسان به وسیله ماشین قابل خواندن باشند.

پروتکل های ارتباطی باینری دارای مزیت ایجاز و اختصار هستند که منجر به افزایش سرعت انتقال و تفسیر می‌شود. سیستم باینری در اسناد هنجاری (Normative Documents) برای توصیف استانداردهای مُدرنی مثل HTTP/3، HTTP/2، EbXMLو EDOC مورد استفاده قرار گرفته‌اند. یک رابط در UML نیز ممکن است یک پروتکل دودویی در نظر گرفته شود. مثال‌هایی از پروتکل‌های باینری شامل موارد زیرند:

- RTP
- TCP
- IP

در ادامه این مقاله به شرح و معرفی انواع پروتکل های ارتباطی در محیط‌های تعبیه شده پرداخته شده است. پیش از آن، مجموعه دوره‌های آموزش شبکه‌های کامپیوتری فرادرس به اختصار معرفی شده است.

۴- ۸- مهم ترین انواع پروتکل های ارتباطی در شبکه های کامپیوتری

یک بنیان شبکه قوی، زیربنا و زیرساخت هر حرفه موفقی را در حوزه فناوری اطلاعات تشکیل می‌دهد. یادگیری مفاهیم پایه شبکه‌های کامپیوتری نیازمند یادگیری و به خاطر سپردن اطلاعات بسیاری است. اصطلاحات شبکه خود به تنهایی بسیار گیج‌کننده به نظر می‌رسند. علاوه بر این، در بخش‌های قبلی توضیح داده شد که انواع پروتکل های ارتباطی بسیار زیاد هستند و همچنین می‌توان آن‌ها را به شکل‌های مختلفی دسته‌بندی کرد. بنابراین در این بخش از مقاله انواع پروتکل های ارتباطی به معرفی ۱۲ پروتکل ارتباطی رایج و پرکاربرد در شبکه های کامپیوتری پرداخته شده است. پیش از ارائه شرح مختصری از هر یک از این پروتکل ها، ابتدا فهرستی از این ۱۲ پروتکل ارتباطی رایج در ادامه آمده است:

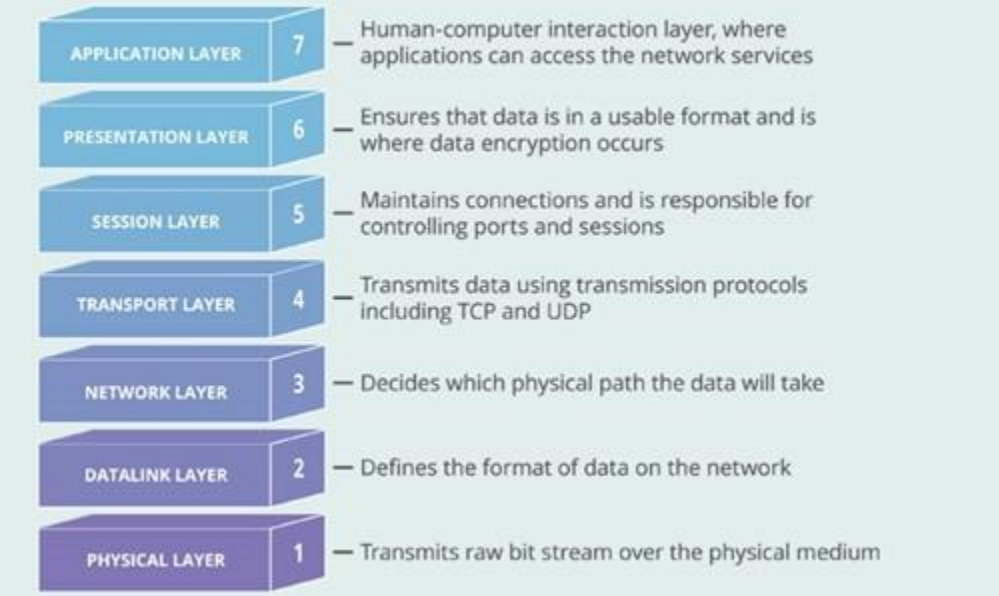
۱. پروتکل تفکیک آدرس(ARP)
۲. پروتکل درخت پوشا(Spanning Tree Protocol | STP)
۳. IEEE 802.1Q
٤. قراردادTCP/IP

۵. پروتکلHTTP
۶. FTP
۷. پروتکل زمان شبکه(Network Time Protocol | NTP)
۸. قرارداد مدیریت گروه اینترنت(Internet Group Management Protocol | IGMP)
۹. قرارداد ساده نامه‌رسانی(SMTP)
۱۰. پوسته ایمن(Secure Shell | SSH)
۱۱. پروتکل دروازه مرزی(Border Gateway Protocol | BGP)
۱۲. پروتکل انتخاب کوتاه‌ترین مسیر(Open Shortest Path First | OSPF)

در علوم کامپیوتر، مفهوم لایه های شبکه به چارچوب یا پلتفرمی گفته می‌شود که که به درک بهتر تعاملات پیچیده شبکه کمک می‌کند. دو مدل لایه شبکه که امروزه به طور گسترده کاربرد دارند مدل OSI و مدل TCP/IP هستند. البته خود لایه‌های این دو مدل با هم متفاوت هستند.

۵- مدل OSIچیست؟

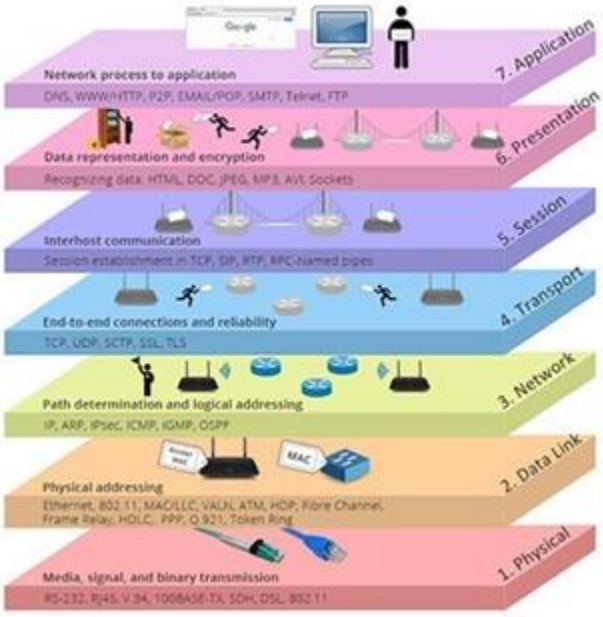
مدلOSI اتصال سیستم‌های باز یا (Open System Interconnection)، یک مدل مفهومی است که توسط سازمان بین‌المللی استاندارد ایجاد شده است و سیستم‌های ارتباطی مختلف را قادر می‌سازد با استفاده از پروتکل‌های استاندارد با هم ارتباط برقرار کنند. به زبان ساده، OSI استانداردی را برای سیستم‌های کامپیوتری مختلف برای ارتباط با یکدیگر فراهم می‌کند.



نمایی از مدل مرجعOSI

سازمان بین‌المللی استاندارد ISO به منظور ترویج بهتر تحقیق و توسعه اینترنت، مدل مرجعی را در چارچوب ۷ لایه اتصال شبکه‌ای تدوین کرده است که به آن مدل مرجع اتصال سیستم باز یا OSI/RM(Open) می‌گویند که به اختصار مدل مرجع اینترنت کار سیستم می‌گویند.

مدل مرجع OSI یک مدل ارتباط متقابل سیستم باز با ساختار پروتکل ۷ لایه است که مجموعه‌ای از مشخصات قابل اجرا جهانی است که توسط سازمان بین‌المللی استاندارد در اوایل دهه ۱۹۸۰ ارتباطات فرموله شده است.



نمایی از لایه‌های هفتگانه OSI و پروتکل‌های مهم هر لایه

با توجه به حالت عملکرد شبکه، لایه های شبکه مدل OSI به ۷ سطح مختلف تقسیم می‌شود و هر سطح با توجه به حالت انتقال شبکه، هنجارها و استانداردهای خود را تعریف می‌کند. از سطح حالت انتقال شبکه خاص تا انتزاعی، این ۷ لایه شبکه عبارتند از:

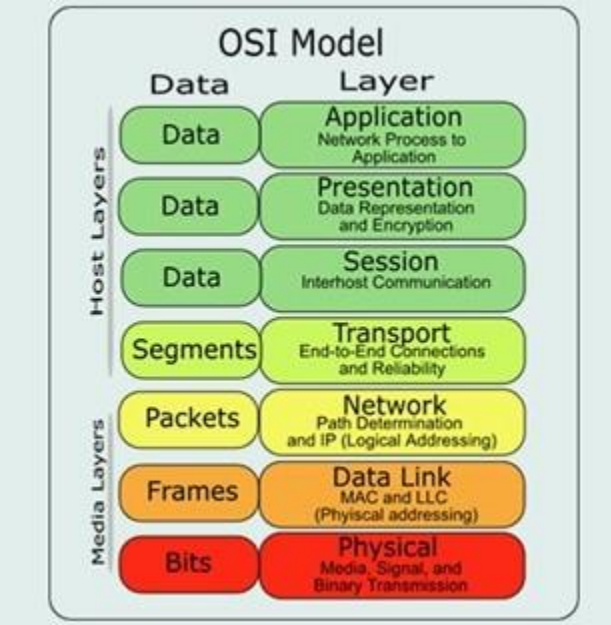
۱. Physical
۲. Data Link
۳. Network
٤. Transport
٥. Session
٦. Presentation
۷. Application

مزیت مدل OSI این است که هر تابع را تقسیم بندی می کند که در توسعه توابع شبکه و آموزش بسیار مفید است.

هنگام توسعه محصولات، فقط باید بر روی توسعه با توجه به مشخصات هر سطح تمرکز کنید. هنگام آموزش، ساختار عملیات شبکه را از طریق مدل OSI توضیح دهید. که درک آن برای مبتدیان نیز آسان‌تر است.

اما با این حال، عملکرد برخی از لایه های شبکه در مدل OSI مانند لایه Presentation و لایه Session هنوز به راحتی قابل درک نیست. در مقایسه با لایه Network یا لایه Application با این حال مدل OSI کار را برای کارشناسان شبکه آسان کرده است.

معمولاً دیتا در لایه اول مدل OSI شامل یک سری صفرها و یک‌هاست که بین دو دستگاه بر روی بستر یا Media مشترک ردوبدل می‌شود، این دیتا در لایه دوم مدل OSI با نام Frame و در لایه سوم با نام Packet شناخته می‌شود. در لایه چهارم این دیتا با ساختار Segment و در لایه ۵ تا ۷ با نام Data شناخته می‌شود.



نمایی از ساختار بسته‌های دیتا در هر لایه شبکه از مدلOSI

لایه ۱ یا Physical Layer

لایه فیزیکی یا physical اولین لایه شبکه در مدل OSI است که برای تعریف انتقال داده بیتی بین دستگاه‌های شبکه، یعنی انتقال سیگنال‌های الکترونیکی ۰ و ۱ سیم‌های فیزیکی دیگر برای تشکیل شبکه استفاده می‌شود. محتوای مشخصات لایه فیزیکی شامل اندازه کابل، سرعت انتقال و مقدار ولتاژ انتقال داده است که برای اطمینان از اینکه سیگنال می‌تواند بر روی انواع رسانه‌های فیزیکی منتقل شود استفاده می‌شود.

نمایی از لایه ۱ یا Physical Layer در مدل مرجعOSI

خطوط شبکه، کارت‌های شبکه وHub ها همگی دستگاه‌های لایه فیزیکی هستند که معمولاً به راحتی قابل دسترسی هستند. خطوط شبکه شامل کابل‌های جفت تابیده RJ-45 UTP که معمولاً در ادارات و اتاق‌های کامپیوتر استفاده می‌شوند، کابل‌های کواکسیال مورد استفاده در تلویزیون کابلی و کابل‌های فیبر نوری مورد استفاده در شبکه‌ها هستند.

Hubبه دستگاهی گفته می‌شود که به سادگی خطوط را بصورت سری به هم متصل می‌کند و داده‌ها را با Broadcast انتقال می‌دهد. دستگاه‌های Hub کامپوزیت که در بازار دیده می‌شوند، مانندSwitching Hub ، محصولاتی هستند که توسط تولید کنندگان مطابق با نیاز بازار توسعه یافته‌اند و معمولاً برخی از عملکردهای لایه پیوند داده) دومین لایه از لایه های شبکه مدل (OSI را شامل می‌شوند.

لایه ۲ یاData Link Layer

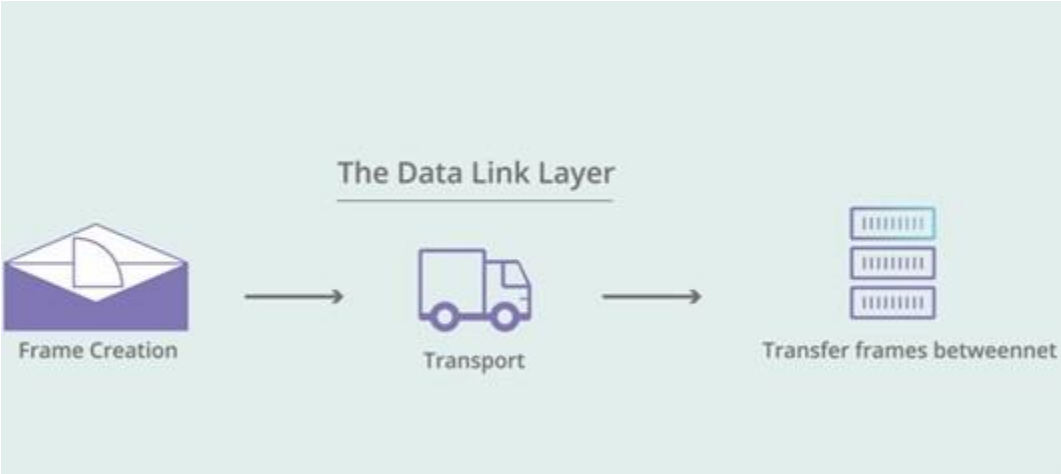
لایه Data Link بین لایه Physical و لایه Network است که عمدتاً یک ارتباط منطقی بین شبکه‌ها برقرار کرده و کنترل جریان و تشخیص خطا را در طول فرآیند انتقال کنترل می‌کند و انتقال و دریافت داده‌ها را پایدارتر می‌کند. لایه Data Link سیگنال‌های دیجیتال لایه فیزیکی را در گروهی از داده‌های منطقی منتقل می‌کند که به این گروه از سیگنال‌ها چارچوب داده یا اصطلاحاً Frame می‌گویند. فریم حاوی آدرس MAC است. هنگامی که داده‌ها در حال انتقال هستند، این اطلاعات آدرس به میزبان دیگر اجازه می‌دهد تا منبع داده‌ها را شناسایی کند.

آدرس MAC مجموعه‌ای ۴۸ بیتی (۶ بایتی) از شماره‌های سریال است MAC .آدرس هر دستگاه شبکه منحصر بفرد است که به دستگاه‌های شبکه اجازه می‌دهد هنگام برقراری ارتباط در شبکه محلی یکدیگر را شناسایی کنند به عنوان مثال کارت‌های شبکه یک مثال بارز هستند.

لایه Data Link خود از دو زیر لایه تشکیل شده است که عبارتند از:

۱. Media Access Control (MAC)

۲. Logical Link Layer (LLC)

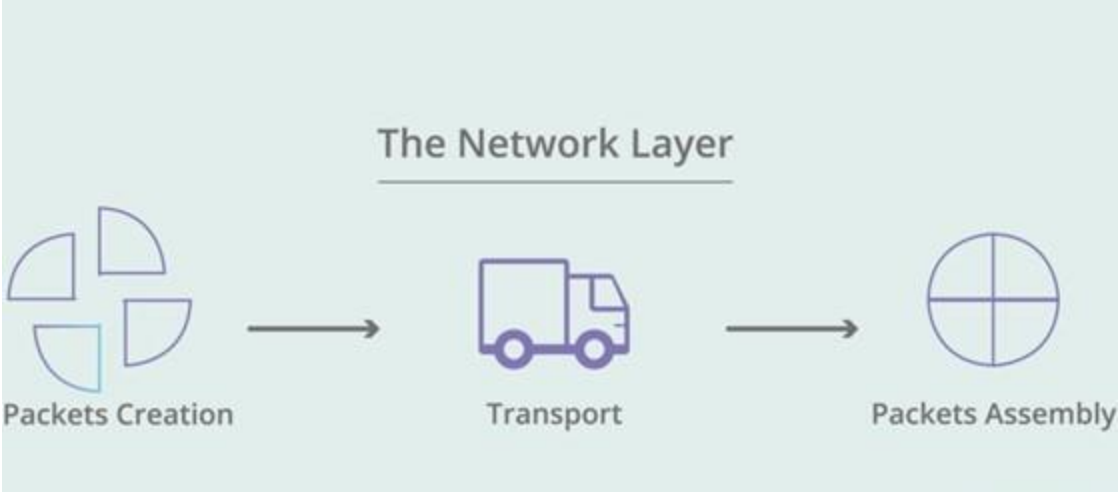


نمایی از لایه دوم مدل OSI یاData Link Layer

بسیاری از پروتکل‌های شبکه بر روی لایه Data Link کار می‌کنند. رایج‌ترین پروتکل‌هایی که می‌شنویم حالت انتقال ناهمزمان (ATM) و پروتکل نقطه به نقطه (PPP) هستند. اولی یک پروتکل ارتباطی است که در روزهای اولیه اینترنت ایجاد شد و به دلیل حجم کم انتقال تک، برای انتقال صدا مناسب است، دومی زمانی است که از ADSLاستفاده می‌کنیم، برای اتصال از طریق این پروتکل به ISP متصل می‌شویم. (اتصال به اینترنت)
سوئیچ شبکه (Switch) یک دستگاه رایج در این لایه است که عمدتاً در شبکه محلی یا Local کار می‌کند و می‌تواند داده‌های شبکه را با توجه به آدرس MAC به میزبان مقصد منتقل کند. سوئیچ‌ها بطور کلی به دو نوع تقسیم می‌شوند: قابل تنظیم و غیرقابل تنظیم و پیکربندی، اولی را می‌توان با کنترل جریان یا تقسیم‌بندی زیرشبکه یا Segmentپیکربندی کرد، در حالیکه دومی فقط داده‌های شبکه را انتقال می‌دهد و عملکردهای پیشرفته دیگری ندارد.

لایه ۳ یا Network Layer

لایه شبکه یا Network توابع مسیریابی و آدرس‌دهی شبکه را تعریف می‌کند که به داده‌ها اجازه می‌دهد بین شبکه‌ها منتقل شوند. مهمترین پروتکل ارتباطی در این لایه، پروتکل اینترنت (IP) است. هنگامیکه داده‌ها منتقل می‌شوند.
پروتکل آدرس IP را به داده‌های انتقال اضافه می‌کند و داده‌ها را بصورت بسته (Packet) تشکیل می‌دهد. هنگام انتقال از طریق شبکه، آدرس IP موجود در بسته، منبع و مقصد داده‌ها را به دستگاه شبکه اضافه می‌کند. از آنجایی که لایه شبکه عمدتاً بر روی IP کار می‌کند، به آن لایه IP نیز می‌گویند. علاوه برIP ، پروتکل‌های فعال در لایه شبکه شامل IPX و X25 می‌باشد. روترها و سوئیچ‌های لایه ۳ از جمله تجهیزاتی هستند که در این لایه کار می‌کنند.



نمایی از لایه ۴ یا Network Layer در مدل مرجعOSI

بطور کلی ۴ وظیفه اصلی این لایه عبارتند از:

Network Control وظیفه اصلی این بخش انجام Network Flow Control یا کنترل جریان شبکه، Network Sequencingیا بررسی توالی بسته‌های دریافتی یا ارسالی و Network Error Checking یا بررسی خطاهای پیش آماده در لایه ۳ است.

Switching وظیفه اصلی این بخش راه‌گزینی و رساندن پکت‌ها یا بسته‌ها از مبدأ به مقصد است. بطور کلی سه روش Switching در این بخش مطرح هستند که عبارتند ازCircuit Switching :، Message Switchingو Packet Switching.

Routing وظیفه اصلی این بخش Route Discovery و Route Selection بین دو نقطه A و B است.

Logical Addressing در واقع این بخش کمک می‌کند تا ارتباطات و آدرس‌دهی منطقی در شبکه بین کلاینت‌ها و سرورها، تجهیزات شبکه‌ای و... صورت بگیرد. بطور کلی سه نوع آدرس‌دهی در شبکه وجود دارد که عبارتند ازPhysical Address :ها، Logical Addressها وService Address ها.

لایه ۴ یا Transport Layer

مورد بعدی از لایه های شبکه مدل OSI لایه Transport است. این لایه به طور عمده مسئول انتقال کلی داده و کنترل کامپیوتر است و نقش کلیدی در مدل OSI دارد .

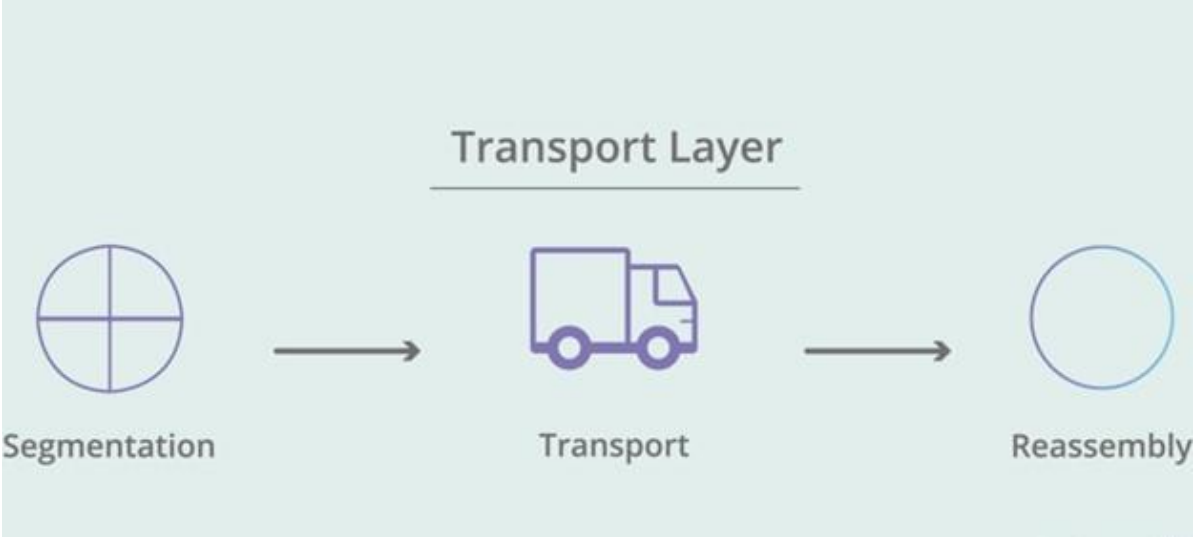
این لایه می‌تواند داده‌های بزرگتر را به چندین داده مناسب برای انتقال برش دهد. مهمترین پروتکل‌های این لایه پروتکل TCP و UDP هستند.

با توجه به اهمیت پروتکل TCP/IP ، ابتدا به معرفی و شرح دقیق‌تر این مجموعه پروتکل‌های مهم پرداخته شده است.

پروتکل TCP از یک دست نشانی سه مرحله‌ای یا اصطلاحاً Three-Way Handshaking برای انتقال اطلاعات بین دو نقطه استفاده می‌کند و براساس بسته‌هایی به نامSyn ، Syn/Ackو Ack کار می‌کند و چنانچه در انتقال یک

پکت به مقصد مشکلی وجود داشته باشد، پروتکل TCP مجدداً اقدام به ارسال آن پکت می‌کند و هیچ دیتایی از دست نمی‌رود.

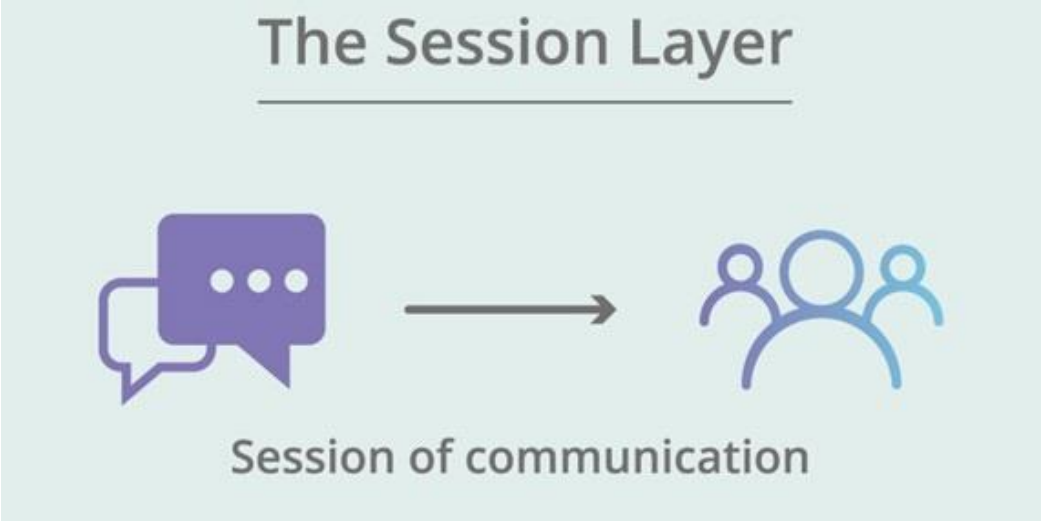
پروتکل UDP برای انتقال Voice و Video استفاده می‌شود و مکانیزم Three-Way Handshaking را برخلاف TCP ندارد. بنابراین اگر در هنگام انتقال صدا و تصویر توسط UDP در شبکه پکتی به هر دلیلی از دست برود، UDPآن را تضمین نکرده و بسته را مجدداً برای مقصد ارسال نمی‌کند.



نمایی از لایه ۴ یا Transport Layer در مدل مرجعOSI

لایه ۵ یاSession Layer

این لایه از لایه های شبکه مدل OSI وظیفه برقراری ارتباط شبکه، انتظار تا پایان انتقال داده و سپس قطع اتصال را برعهده دارد. فرآیند عملیات کمی شبیه به تماس با یک جلسه چند نفره (ایجاد اتصال) و سپس تبادل نظر با یکدیگر است. پروتکل‌های VPN از جملهPPTP :، L2TP، SSTPو... همگی از جمله پروتکل‌های مطرح در این لایه به حساب می‌آیند.



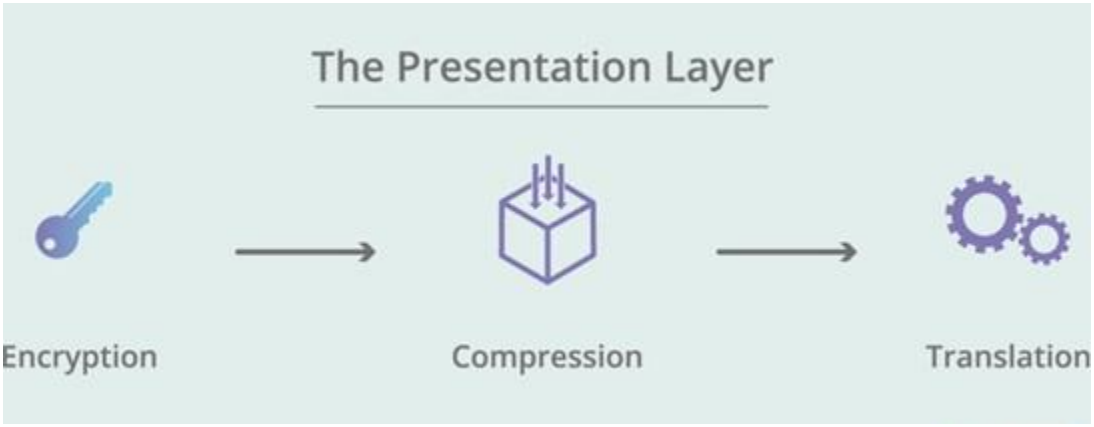
نمایی از لایه ۵ یا Session Layer در مدل مرجعOSI

لایه ۶ یا Presentation Layer

پس از دریافت داده‌ها توسط لایهSession ، عبارت را می‌توان از طریق لایه Presentation تبدیل کرد، مانند تبدیل رمزگذاری ASCII به داده‌هایی که می‌تواند توسط لایه Application استفاده شود، یا پردازش تصاویر و سایر فایل‌های چند رسانه‌ای، مانند فایل‌های تصویری JPGE یا .MIDI فایل‌های صوتی و. ...

علاوه بر تبدیل فایل، گاهی اوقات زمانیکه داده‌ها از طریق شبکه منتقل می‌شوند، محتوا نیاز به رمزگذاری یا رمزگشایی دارد و این کار در لایه ارائه انجام می‌شود.

در واقع وظیفه اصلی لایه Presentation را می‌تواند Encode و Decode کردن و همچنین Encryption و Decryptionکردن داده‌ها دانست. مهمترین پروتکل‌های این لایه عبارتند ازTLS :، SSLو) HTTPS توجه داشته باشید که پروتکل HTTP پروتکل لایه ۷ است نه لایه ۶.(

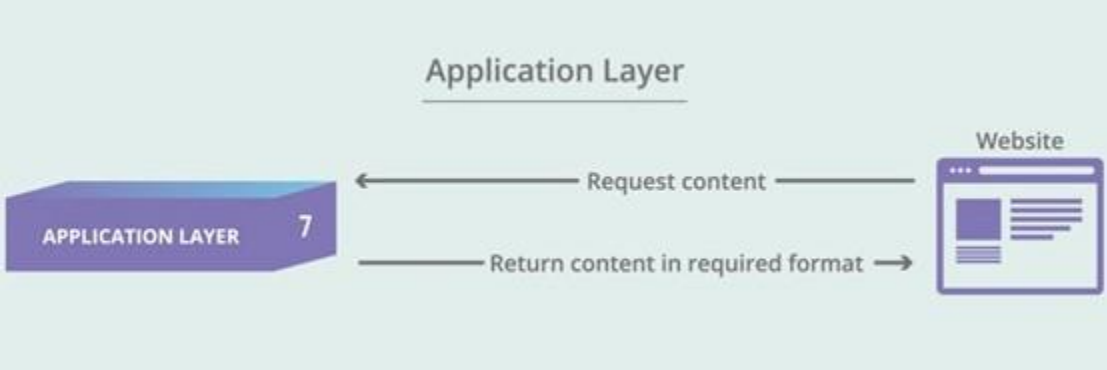


نمایی از لایه ۷ یا Presentation Layer در مدل مرجعOSI

لایه ۷ یا Application Layer

وظیفه اصلی لایه Application پردازش برنامه‌ها و سپس ارائه خدمات برنامه‌های کاربردی شبکه به کاربران است. پروتکل زیادی در این سطح وجود دارند. پروتکل‌های ارتباطی رایج برای کاربران عبارتند از DHCP:،) FTPپروتکل انتقال فایل(، HTTP، POP3و. ...

نرم‌افزارهای کاربردی متعلق به لایه هفتم عبارتند از: مرورگرهای وب، ایمیل، بازی‌های آنلاین، نرم‌افزارهای پیام فوری یاMSN ها از جملهMSN Messenger :،ICQ و غیره.

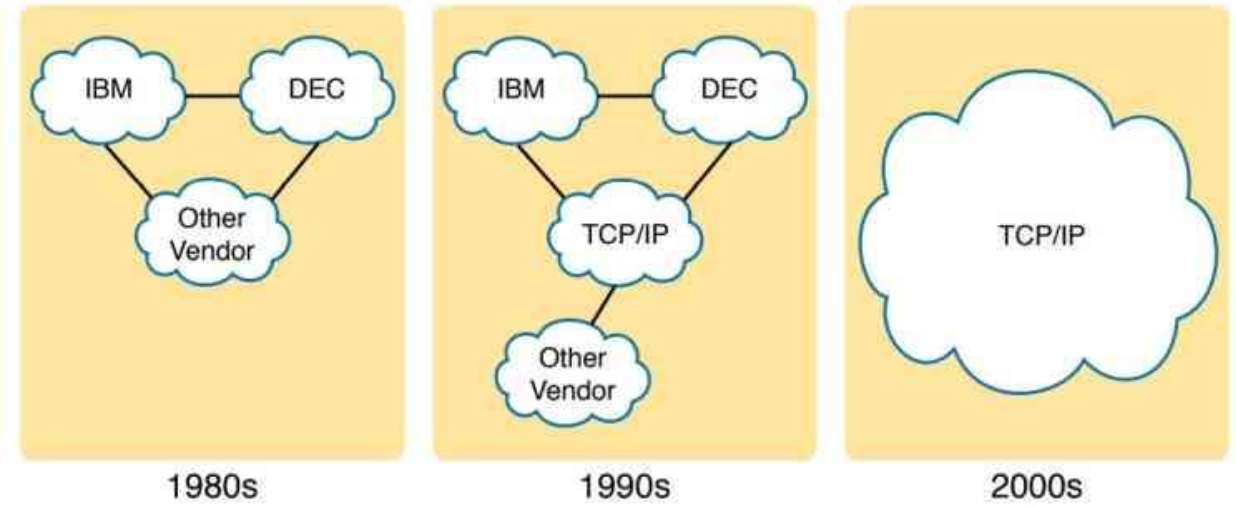


نمایی از لایه ۷ یا Application Layer در مدل مرجعOSI

۶- تاریخچه مدل TCP/IP

امروزه دنیای شبکه های کامپیوتری از مدل شبکه TCP/IP استفاده می کند. با این حال روزی روزگاری ، پروتکل های شبکه از جمله TCP/IP وجود نداشتند . شرکت های سازنده اولین پروتکل های شبکه که تنها با کامپیوتر های آنها سازگاری داشت را ایجاد کردند.

به عنوان مثال ، IBM، شرکت کامپیوتری که بیشترین سهم بازار را در بسیاری از بازارها در دهه ۱۹۷۰ و ۱۹۸۰ داشت ، مدل شبکه Systems Network Architecture(SNA) خود را در سال ۱۹۷۴ منتشر کرد. سایر شرکت های سازنده نیز مدل های شبکه اختصاصی خود را ایجاد کردند. در نتیجه ، اگر شرکت شما کامپیوترها را از سه شرکت سازنده خریداری می کرد ، مهندسان شبکه مجبور بودند سه شبکه مختلف بر اساس مدل های شبکه هر شرکت ایجاد کنند ، و سپس به نحوی آن شبکه ها را به یکدیگر متصل کنند. سمت چپ شکل زیر ایده کلی یک شبکه enterprise یک شرکت در دهه ۱۹۸۰ قبل از اینکه TCP/IP در شبکه های enterprise رایج شود را نشان می‌دهد.



اگرچه مدل های شبکه اختصاصی تعریف شده توسط شرکت های سازنده به خوبی کار می کردند ، اما داشتن یک مدل شبکه باز و مستقل به رقابت و کاهش پیچیدگی کمک می کرد . سازمان استاندارد بین المللی (ISO) وظیفه ایجاد چنین مدلی را بر عهده گرفت ، این سازمان از اواخر دهه ۱۹۷۰ کار بر روی مدل شبکه ای Open Systems Interconnection (OSI)را آغاز کرد ISO .یک هدف عالی (استانداردسازی پروتکل های شبکه داده برای برقراری ارتباط بین همه کامپیوتر ها در سراسر کره زمین) برای مدل OSI داشت ISO .در راستای این هدف خیلی تلاش کرد و شرکت کنندگان بسیاری از کشورهای پیشرفته فن آوری روی زمین در این فرایند شرکت کردند.

دومین تلاش برای ایجاد یک مدل شبکه باز عمومی ، مستقل، از قرارداد وزارت دفاع ایالات متحده Department of Defense (DoD)سرچشمه گرفت. محققان در دانشگاه های مختلف داوطلب شدند تا پروتکل های مربوط به کار اصلی DoD را توسعه دهند. این تلاش ها منجر به ایجاد یک مدل شبکه باز رقیب به نام TCP/IP شد.

در طول دهه ۱۹۹۰ ، شرکت ها شروع به افزودن OSI ، TCP/IPیا هر دو به شبکه های سازمانی خود کردند. با این حال ، در پایان دهه ۱۹۹۰ ، TCP/IPانتخاب شد و OSI از بین رفت. بخش مرکزی شکل بالا ایده کلی شبکه های سازمانی) شبکه هایی که بر اساس چندین مدل شبکه ساخته شده اند وشامل TCP/IP هستند (در آن دهه را نشان می دهد.

در قرن بیست و یکم ، TCP/IPبر بقیه ی مدل ها غالب شد . هر چند هنوز نیز مدل های شبکه اختصاصیوجود دارد ، اما بیشتر آنها به نفع TCP/IP کنار گذاشته شدند. توسعه مدل OSI ، تا حدی به دلیل روند استانداردسازی کند در مقایسه با TCP/IP دچار مشکل شد. و TCP/IP ، مدل شبکه ای که در اصل توسط گروهی از داوطلبان ایجاد شد، به پرکارترین مدل شبکه تبدیل شد.

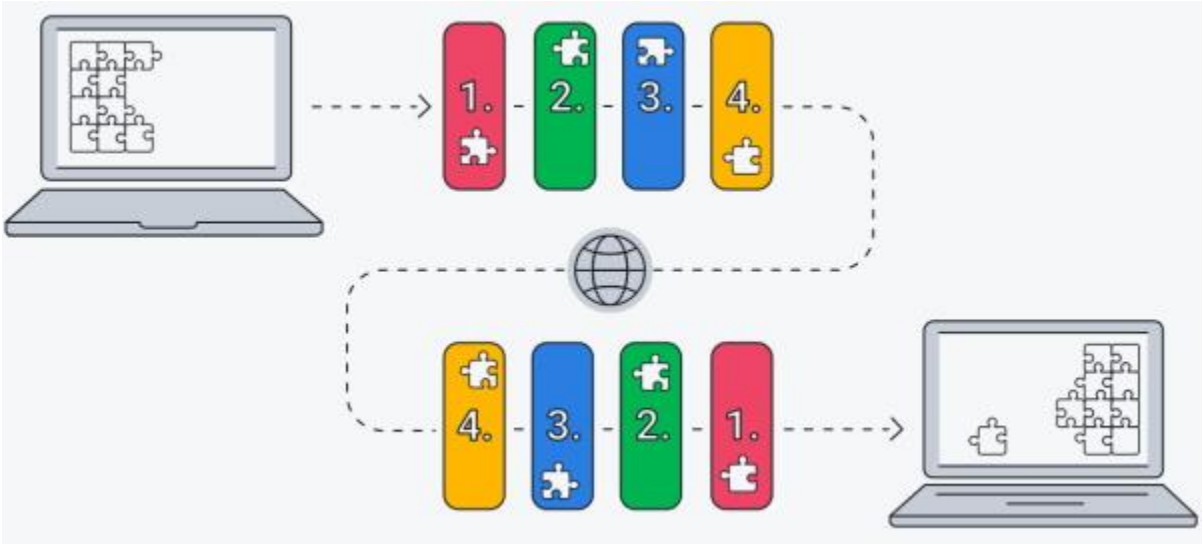
۶- ۱- پروتکلTCP/IP

پروتکل TCP/IP مجموعه‌ای از پروتکل‌های به هم مرتبط است. در لایه سه، پروتکل اینترنت یا همان IP به گونه‌ای عمل می‌کند که امکان مسیریابی فراهم می‌شود. در لایه ۴، پروتکل‌های TCP و UDP فعالیت می‌کنند و دو انتخاب حالت‌مند و بدون حالت را برای انتقال داده‌ها ارائه می‌دهند ICMP .هم جزئی از مجموعه پروتکل‌های TCP/IP به حساب می‌آید، اما داده‌ها را منتقل نمی‌کند و معمولاً برای عیب‌شناسی به کار گرفته می‌شود. اکثر شبکه‌های کامپیوتری از مجموعه یا پُشته TCP/IP استفاده می‌کنند.

آشنایی با پروتکل‌های TCP/IP از این جهت اهمیت دارد که شناخت لازم در خصوص این مسئله حاصل خواهد شد که برای رفع مشکل و عیب‌یابی از چه پروتکل‌هایی باید استفاده کرد. پروتکل ICMP برای سنجش تاخیر (Latency)بسیار مناسب است، اما گاهی وقتی ICMP مسدود باشد، نیاز به استفاده از ابزارهای مبتنی بر UDP وجود خواهد داشت. برای آزمایش پهنای باند و تاخیر، احتمالاً UDP در خصوص تاخیر عملکرد بهتری خواهد داشت. در حالی که، پروتکل TCP برای پهنای باند کلی بسیار مفید خواهد بود. در لایه سه، درک نحوه کارکرد نشانی آی‌پی و زیرشبکه‌ها (Subnet) می‌تواند به عیب‌یابی مشکلات مربوط به رسیدن بسته‌ها به مقصد بسیار مفید باشد.

۶- ۲- نحوه عملکرد پروتکل TCP/IP چگونه است؟

هر گاه کاربر داده‌ای مثل یک پیام، عکس یا فایل را از طریق شبکه انتقال می‌دهد، مدل TCP/IP آن داده‌ها را بر اساس یک روند چهار لایه به بسته‌هایی تقسیم می‌کند. داده‌ها ابتدا به ترتیب از این لایه‌ها عبور می‌کنند و سپس به ترتیب بر عکس با جمع‌آوری داده‌ها در سمت گیرنده مجدداً سر هم می‌شوند.



استفاده از پروتکل TCP/IP در سطح وسیع به این علت است که کل این فرآیند استانداردسازی شده است. بدون استانداردسازی ارتباطات در دنیای شبکه از کنترل خارج خواهند شد و سرعت انتقال نیز به میزان زیادی کاهش پیدا خواهد کرد. به عنوان یک استاندارد جهانی، مدل TCP/IP یکی از کارآمدترین روش‌ها برای انتقال داده از طریق اینترنت به حساب می‌آید.

۶- ۳- پروتکل TCP چیست ؟

TCPمخفف عبارت «Transmission Control Protocol» به معنی «قرارداد هدایت انتقال»، یک استاندارد ارتباطی است که برنامه‌های کاربردی و دستگاه‌های کامپیوتری را قادر می‌سازد تا پیام‌هایی را از طریق شبکه تبادل کنند . TCPبرای ارسال بسته‌ها در طول اینترنت و کسب اطمینان از به مقصد رسیدن موفقیت‌آمیز داده‌ها و پیام‌ها در شبکه طراحی شده است.

۶- ۴- پروتکل IP چیست ؟

پروتکل IP که سرنامی برای «Internet Protocol» به معنی «قرارداد اینترنتی» است، پروتکل ارتباطی لایه شبکه در مجموعه پروتکل اینترنت (Internet Protocol Suite) برای توزیع دیتاگرام (داده‌نگار) در سراسر محدوده‌های شبکه به حساب می‌آید. قابلیت مسیریابی آن امکان ارتباط بین شبکه‌ای را فراهم می‌سازد و اساساً اینترنت را برقرار می‌سازد.

۶- ۵- ویژگی های TCP/IP چه هستند ؟

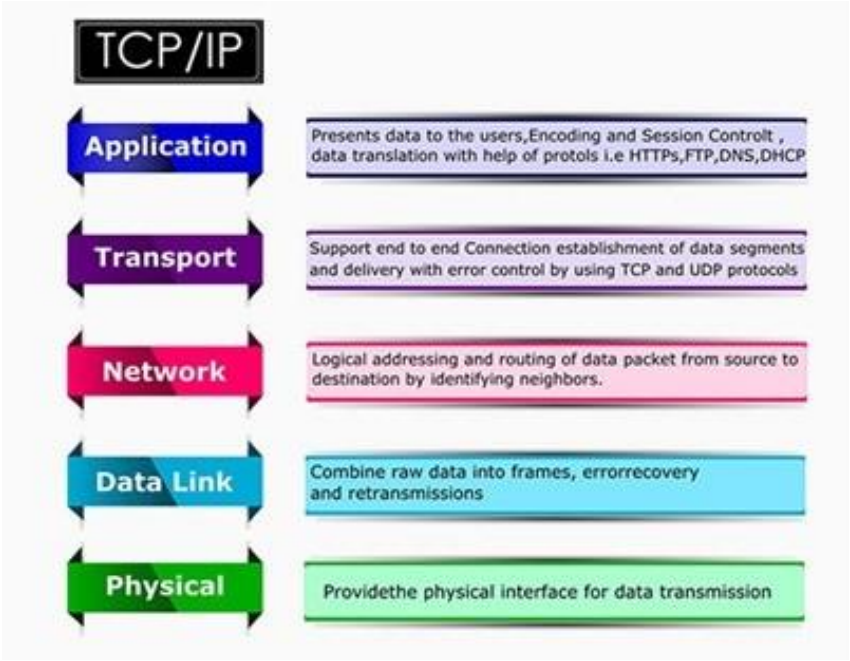
خصوصیات و ویژگی های مهم مجموعه پروتکل های TCP/IP در ادامه فهرست شده‌اند:

- پشتیبانی از همه تولید کنندگان سخت افزار شبکه
- کارکردپذیری مشترک (قابلیت استفاده در انواع دستگاه‌ها، سیستم‌های عامل و نرم‌افزارهای مختلف(
- آدرس‌دهی منطقی (قابلیت زیرشبکه‌سازی قدرتمند)
- قابلیت مسیریابی
- امکان ترجمه نام دامنه(DNS)
- کنترل خطا و کنترل جریان داده‌ها
- امکان پذیرفتن داده‌ها از اپلیکیشن‌های مختلف و هدایت داده‌ها به اپلیکیشن‌های مختلف
- سهولت در اضافه کردن دستگاه‌های بیش‌تر به شبکه
- TCPیک پروتکل اتصال‌گرا به حساب می‌آید.

۶- ۶- مدل لایه‌ای TCP/IP چیست؟

لایه های شبکه مدل TCP/IP به ۵ لایه تقسیم می‌شود، این لایه‌ها عبارتند از:

۱. Physical Layer
۲. Data Link Layer
۳. Network Layer
٤. Transport Layer
٥. Application Layer



مدل TCP/IP

در ادامه به توضیح مختصری از لایه های شبکه مدل TCP/IP خواهیم پرداخت:

لایه ۱ یا Application Layer

لایه Application بخشی است که ما اغلب از آن استفاده می‌کنیم، مانند پروتکل متداولHTTP ، SNMP، FTP، DNS، SMTP، Telnetو... . این بخش عمدتاً برای تعاملات کاربر محور است. در واقع این لایه از مدل TCP/IP همانند لایه‌های ۵، ۶ و ۷ از مدل OSI عمل می‌کند.

لایه ۲ یا Transport Layer

نقش Transport Layer انتقال داده‌ها از لایه برنامه است. به عنوان مثال، پروتکل) TCP پروتکل کنترل انتقال قابل اعتماد(، UDP(پروتکل دیتاگرام کاربر) که وظیفه‌ای انتقال داده‌ها را دارند.

TCP(پروتکل کنترل انتقال) اتصال‌گرا یا اصطلاحاً Connection Oriented بوده (اتصال باید ابتدا از طرف مقابل تأیید شود و اتصال باید در پایان انتقال قطع شود، مشابه برقراری تماس تلفنی)، پیچیده و قابل اعتماد است و دارای یک مکانیسم خوب برای ارسال مجدد و بررسی خطاها هنگام انتقال است.

در حالیکه UDP یک پروتکل Connectionless در ارتباطات محسوب می‌شود. در واقع این لایه از مدل TCP/IP همانند لایه ۴ از مدل مرجع OSI عمل می‌کند.

لایه ۳ یا Network Layer

لایه Network Layer با لایه شبکه مدل مرجع OSI مطابقت دارد و عمدتاً مشکل ارتباط میزبان به میزبان را حل می‌کند. پروتکل‌هایی که حاوی آن است، انتقال منطقی بسته‌های داده در سراسر شبکه را طراحی می‌کنند. تمرکز آن بر تخصیص مجدد یک آدرس IP به میزبان برای تکمیل آدرس‌دهی میزبان است و همچنین مسئولیت مسیریابی بسته‌های داده در شبکه‌های مختلف را برعهده دارد. سه پروتکل اصلی در این لایه وجود دارد:

۱. پروتکل اینترنت(IP)
۲. پروتکل مدیریت گروه اینترنت(IGMP)
۳. پروتکل پیام کنترل اینترنت(ICMP)

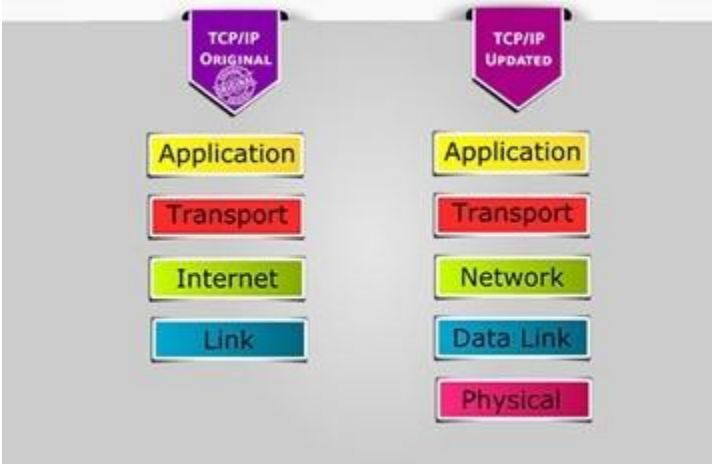
لایه ۴ یا Data Link

لایه Data Link بطور کلی برای مقابله با بخش اتصال سخت‌افزار، از جمله کارت شبکه، درایورهای دستگاه مرتبط با سخت‌افزار و غیره استفاده می‌شود.

لایه ۵ یا Physical Layer

لایه فیزیکی بطور کلی سخت‌افزاری است که مسئول انتقال داده‌ها است، مانند کابل‌های جفت تابیده، سخت‌افزاری‌های که بیسیم انتقال داده انجام می‌دهند و فیبرهای نوری. در این بخش جریان بیت جریان فوتوالکتریک و سیگنال‌های دیگر داده‌ها را ارسال و دریافت می‌کنند. جریان داده‌ها در این لایه همانند لایه ۱ از مدل مرجع OSI شامل یک سری ۰ و ۱ است که بر روی یک بستر فیزیکی منتقل می‌شوند.

مدل‌های متفاوت TCP/IP



نمایی از مدل (۴ لایه و ۵ لایه)

مدل اولیه لایه‌بندی TCP/IP از چهار بخش تشکیل شده بود. لایه های شبکه در مدل اولیه TCP/IP شامل موارد زیر بودند:

۱. Link Layer
۲. Internet Layer
۳. Transport Layer
٤. Application Layer

با گسترش شبکه برای توسعه بهتر زیرساخت‌ها یک لایه به این لایه های شبکه اضافه شده و مدل ۵ لایه TCP/IP عرضه شد. این مدل شامل ۵ لایه است که پیش‌تر و به اختصار به بررسی آن پرداختیم.

TCP/IP ،شامل شش پروتکل اساسی(ARP، TCP,UDP,IP,ICMP,IGMP) و مجموعه ای از برنامه های کاربردی است. پروتکل های فوق، مجموعه ای از استانداردهای لازم بمنظور ارتباط بین کامپیوترها و دستگاهها را در شبکه ، فراهم می نماید. تمامی برنامه ها و سایر پروتکل ها ی موجود در پروتکل TCP/IP ، به پروتکل های شش گانه فوق مرتبط و از خدمات ارائه شده توسط آنان استفاده می نمایند . در ادامه به تشریح عملکرد و جایگاه هر یک از پروتکل های اشاره شده ، خواهیم پرداخت .

۱) پروتکل TCP : لایه Transport

TCP[8] ، یکی از پروتکل های استاندارد TCP/IP است که امکان توزیع و عرضه اطلاعات (سرویس ها) بین صرفا" دو کامپیوتر ، با ضریب اعتماد بالا را فراهم می نماید. چنین ارتباطی (صرفا" بین دو نقطه) ، Unicast نامیده می شود . در ارتباطات با رویکرد اتصال گرا ، می بایست قبل از ارسال داده ، ارتباط بین دو کامپیوتر برقرار گردد . پس از برقراری ارتباط ، امکان ارسال اطلاعات برای صرفا" اتصال ایجاد شده ، فراهم می گردد . ارتباطات از این نوع ، بسیار مطمئن می باشند ، علت این امر به تضمین توزیع اطلاعات برای مقصد مورد نظر برمی گردد . بر روی کامپیوتر مبداء ، TCP داده هائی که می بایست ارسال گردند را در بسته های اطلاعاتی (Packet) سازماندهی می نماید. در کامپیوتر مقصد ، TCP ، بسته های اطلاعاتی را تشخیص و داده های اولیه را مجددا" ایجاد خواهد کرد .

ارسال اطلاعات با استفاده از TCP

TCP ، به‌منظور افزایش کارائی ، بسته های اطلاعاتی را بصورت گروهی ارسال می‌نماید . TCP ، یک عدد سریال (موقعیت یک بسته اطلاعاتی نسبت به تمام بسته اطلاعاتی ارسالی) را به هریک از بسته ها نسبت داده و از Acknowledgment بمنظور اطمینان از دریافت گروهی از بسته های اطلاعاتی ارسال شده ، استفاده می نماید. در صورتیکه کامپیوتر مقصد ، در مدت زمان مشخصی نسبت به اعلام وصول بسته های اطلاعاتی ، اقدام ننماید، کامپیوتر مبداء ، مجددا" اقدام به ارسال اطلاعات می نماید. علاوه برافزودن یک دنباله عددی و Acknowledgment به یک بسته اطلاعاتی ، TCP اطلاعات مربوط به پورت مرتبط با برنامه ها ی مبداء و مقصد را نیز به بسته اطلاعاتی اضافه می نماید. کامپیوتر مبداء ، از پورت کامپیوتر مقصد بمنظور هدایت صحیح بسته های اطلاعاتی به برنامه مناسب بر روی کامپیوتر مقصد ، استفاده می نماید. کامپیوتر مقصد از پورت کامپیوتر مبداء به‌منظور برگرداندن اطلاعات به برنامه ارسال کننده در کامپیوتر مبداء ، استفاده خواهد کرد .

هر یک از کامپیوترهائی که تمایل به استفاده از پروتکل TCP به‌منظور ارسال اطلاعات دارند ، می بایست قبل از مبادله اطلاعات ، یک اتصال بین خود ایجاد نمایند . اتصال فوق ، از نوع مجازی بوده و Session نامیده می شود. دو کامپیوتر درگیر در ارتباط ، با استفاده از TCP و بکمک فرآیندی با نام : Three-Way handshake ، با یکدیگر مرتبط و هر یک پایبند به رعایت اصول مشخص شده در الگوریتم مربوطه خواهند بود. فرآیند فوق ، در سه مرحله صورت می پذیرد :

[8] Transmission Control Protocol

۱) مرحله اول : کامپیوتر مبداء ، اتصال مربوطه را از طریق ارسال اطلاعات مربوط به Session ، مقداردهی اولیه می نماید (عدد مربوط به موقعیت یک بسته اطلاعاتی بین تمام بسته های اطلاعاتی و اندازه مربوط به بسته اطلاعاتی)
۲) مرحله دوم : کامپیوتر مقصد ، به اطلاعات Session ارسال شده ، پاسخ مناسب را خواهد داد .
۳) کامپیوتر مبداء ، از شرح واقعه بکمک Acknowledgment ارسال شده توسط کامپیوتر مقصد ، آگاهی پیدا خواهد کرد .

۲) پروتکل UDP : لایه Transport

UDP[۹] پروتکلی در سطح لایه "حمل" بوده که برنامه مقصد در شبکه را مشخص نموده و از نوع بدون اتصال است . پروتکل فوق، امکان توزیع اطلاعات با سرعت مناسب را ارائه ولی در رابطه با تضمین صحت ارسال اطلاعات ، سطح مطلوبی از اطمینان را بوجود نمی آورد . UDP در رابطه با داده های دریافتی توسط مقصد ، به Acknowledgment نیازی نداشته و در صورت بروز اشکال و یا خرابی در داده های ارسال شده ، تلاش مضاعفی بمنظور ارسال مجدد داده ها ، انجام نخواهد شد . این بدان معنی است که داده هائی کمتر ارسال می گردد ولی هیچیک از داده های دریافتی و صحت تسلسل بسته های اطلاعاتی ، تضمین نمی گردد .از پروتکل فوق ، بمنظور انتقال اطلاعات به چندین کامپیوتر با استفاده از Broadcast و یا Multicast ، استفاده بعمل می آید . پروتکل UDP ، در مواردیکه حجم اندکی از اطلاعات ارسال و یا اطلاعات دارای اهمیت بالائی نمی بانشد ، نیز استفاده می گردد. استفاده از پروتکل UDP در مواردی همچون Multicasting Streaming media ، (نظیر یک ویدئو کنفرانس زنده) و یا انتشار لیستی از اسامی کامپیوترها که بمنظور ارتباطات محلی استفاده می گردند ، متداول است . بمنظور استفاده از UDP ، برنامه مبداء می بایست پورت UDP خود را مشخص نماید دقیقا" مشابه عملیاتی که می بایست کامپیوتر مقصد انجام دهد . لازم به یادآوری است که پورت های UDP از پورت های TCP مجزا و متمایز می باشند (حتی اگر دارای شماره پورت یکسان باشند).

۳) پروتکل IP : لایه Internet

IP[۱۰] ، امکان مشخص نمودن محل کامپیوتر مقصد در یک شبکه ارتباطی را فراهم می نماید. IP ، یک پروتکل بدون اتصال و غیرمطمئن بوده که اولین مسئولیت آن آدرس دهی بسته های اطلاعاتی و روتینگ بین کامپیوترهای موجود در شبکه است. با اینکه IP همواره سعی در توزیع یک بسته اطلاعاتی می نماید ، ممکن است یک بسته اطلاعاتی در زمان ارسال گرفتار مسائل متعددی نظیر : گم شدن، خرابی، عدم توزیع با اولویت مناسب ، تکرار در ارسال و یا تاخیر، گردند.در چنین مواردی ، پروتکل IP تلاشی بمنظور حل مشکلات فوق را انجام نخواهد داد (ارسال مجدد اطلاعات درخواستی). آگاهی از وصول بسته اطلاعاتی در مقصد و بازیافت بسته های اطلاعاتی گم شده ، مسئولیتی است که بر عهده یک لایه بالاتر نظیر TCP و یا برنامه ارسال کننده اطلاعات ، واگذار می‌گردد .

[۹] User Datagram Protocol
[۱۰] Internet Protocol

عملیات انجام شده توسط IP

می توان IP را بعنوان مکانی در نظر گرفت که عملیات مرتب سازی و توزیع بسته های اطلاعاتی در آن محل ، صورت می پذیرد .بسته ها ی اطلاعاتی توسط یکی از پروتکل های لایه حمل (TCP و یا UDP) و یا از طریق لایه " ایترفیس شبکه " ، برای IP ارسال می گردند . اولین وظیفه IP ، روتینگ بسته های اطلاعاتی بمنظور ارسال به مقصد نهائی است . هر بسته اطلاعاتی ، شامل آدرس IP مبداء (فرستنده) و آدرس IP مقصد (گیرنده) می باشد. در صورتیکه IP ، آدرس مقصدی را مشخص نماید که در همان سگمنت موجود باشد ، بسته اطلاعاتی مستقیما" برای کامپیوتر مورد نظر ارسال می گردد . در صورتیکه آدرس مقصد در همان سگمنت نباشد ، IP ، می بایست از یک روتر استفاده و اطلاعات را برای آن ارسال نماید.یکی دیگر از وظایف IP ، ایجاد اطمینان از عدم وجود یک بسته اطلاعاتی (بلاتکلیف !) در شبکه است . بدین منظور محدودیت زمانی خاصی در رابطه با مدت زمان حرکت بسته اطلاعاتی در طول شبکه ، در نظر گرفته می شود .عملیات فوق، توسط نسبت دادن یک مقدار Time To Live(TTL) به هر یک از بسته های اطلاعاتی صورت می پذیرد. TTL ، حداکثر مدت زمانی را که بسته اطلاعاتی قادر به حرکت در طول شبکه است را مشخص می نماید(قبل از اینکه بسته اطلاعاتی کنار گذاشته شود) .

۴) پروتکل ICMP : لایه Internet

ICMP [۱۱] ، امکانات لازم در خصوص اشکال زدائی و گزارش خطاء در رابطه با بسته های اطلاعاتی غیرقابل توزیع را فراهم می نماید. با استفاده از ICMP ، کامپیوترها و روترها که از IP بمنظور ارتباطات استفاده می نمایند ، قادر به گزارش خطاء و مبادله اطلاعاتی محدود در رابطه وضعیت بوجود آمده می باشند. مثلا" در صورتیکه IP ، قادر به توزیع یک بسته اطلاعاتی به مقصد مورد نظر نباشد، ICMP یک پیام مبتنی بر غیرقابل دسترس بودن را برای کامپیوتر مبداء ارسال می‌دارد. با اینکه پروتکل IP بمنظور انتقال داده بین روترهای متعدد استفاده می‌گردد ، ولی ICMP به نمایندگی از TCP/IP ، مسئول ارائه گزارش خطاء و یا پیام های کنترلی است . تلاش ICMP ، در این جهت نیست که پروتکل IP را بعنوان یک پروتکل مطمئن مطرح نماید، چون پیام های ICMP دارای هیچگونه محتویاتی مبنی بر اعلام وصول پیام (Acknowledgment) بسته اطلاعاتی نمی‌باشند. ICMP ، صرفا" سعی در گزارش خطاء و ارائه فیدبک‌های لازم در رابطه با تحقق یک وضعیت خاص را می‌نماید.

۵) پروتکل IGMP : لایه Internet

IGMP [۱۲] ، پروتکلی است که مدیریت لیست اعضاء برای IP Multicasting ، در یک شبکه TCP/IP را بر عهده دارد . IP Multicasting، فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرندگان که گروه multicast نامیده می شوند ؛ ارسال می گردد . IGMP لیست اعضاء را نگهداری می نماید .

مدیریت IP Multicasting

[۱۱] Internet Control Message Protocol

[۱۲] Internet Group Management Protocol

تمامی اعضاء یک گروه multicast ، به ترافیک IP هدایت شده به یک آدرس IP Multicast ، گوش داده و بسته های اطلاعاتی ارسال شده به آن آدرس را دریافت می نمایند. زمانیکه چندین کامپیوتر نیازمند دستیابی به اطلاعاتی نظیر Streaming media باشند، یک آدرس IP رزوشده برای multicasting استفاده می گردد. روترها که بمنظور پردازش multicast پیکربندی می گردند، اطلاعات را انتخاب و آنها را برای تمامی مشترکین گروه multicast ارسال (Forward) می نمایند . بمنظور رسیدن اطلاعات Multicast به گیرندگان مربوطه ، هر یک از روترهای موجود در مسیر ارتباطی می بایست ، قادر به حمایت از Multicasting باشند . کامپیوترهای مبتنی بر سیستم عامل وینوز ۲۰۰۰ ، قادر به ارسال و دریافت IP Multicast ، می باشند .

۶) پروتکل ARP : لایه Internet

ARP [۱۳]، پروتکلی است که مسئولیت مسئله " نام به آدرس" را در رابطه با بسته های اطلاعاتی خروجی (Outgoing) ، برعهده دارد . ماحصل فرآیند فوق ، Mapping آدرس IP به آدرس[14]MAC، مربوطه است . کارت شبکه از آدرس MAC ، بمنظور تشخیص تعلق یک بسته اطلاعاتی به کامپیوتر مربوطه ، استفاده می نمایند . بدون آدرس های MAC ، کارت های شبکه ، دانش لازم در خصوص ارسال بسته های اطلاعاتی به لایه بالاتر بمنظور پردازش های مربوطه را دارا نخواهند بود . همزمان با رسیدن بسته های اطلاعاتی به لایه IP بمنظور ارسال در شبکه ، آدرس های MAC مبداء و مقصد به آن اضافه می گردد .

ARP ، از جدولی خاص بمنظور ذخیره سازی آدرس های IP و MAC مربوطه ، استفاده می نماید. محلی از حافظه که جدول فوق در آنجا ذخیره می گردد ، ARP Cache نامیده می شود. Cache ARP هر کامپیوتر شامل Mapping لازم برای کامپیوترها و روترهائی است که صرفا" بر روی یک سگمنت مشابه قرار دارند.

[۱۳] Address Resolution Protocol

[14] Media Access Control

Physical Address Resolution

پروتکل ARP ، آدرس IP مقصد هر یک از بسته های اطلاعاتی خروجی را با ARP Cache مقایسه تا آدرس MAC مقصد مورد نظر را بدست آورد . در صورتیکه موردی پیدا گردد ، آدرس MAC از Cache بازیابی می گردد . در غیر اینصورت ؛ ARP درخواستی را برای کامپیوتری که مالکیت IP را برعهده دارد ، Broadcast نموده و از وی می خواهد که آدرس MAC خود را اعلام نماید . کامپیوتر مورد نظر (با IP مربوطه) ، در ابتدا آدرس MAC کامپیوتر ارسال کننده درخواست را به Cache خود اضافه نموده و در ادامه پاسخ لازم را از طریق ارسال آدرس MAC خود ، به متقاضی خواهد داد . زمانیکه پاسخ ARP توسط درخواست کننده ، دریافت گردید ، در ابتدا با استناد به اطلاعات جدید دریافتی، Cache مربوطه بهنگام و در ادامه بسته اطلاعاتی به مقصد کامپیوتر مورد نظر ارسال می گردد .

در صورتیکه مقصد یک بسته اطلاعاتی ، سگمنتی دیگر باشد ، ARP ، آدرس MAC را به روتر مسئول در سگمنت مربوطه ، تعمیم خواهد داد (در مقابل آدرس مربوط به کامپیوتر مقصد) . روتر ، در ادامه مسئول یافتن آدرس MAC مقصد و یا Forwarding بسته اطلاعاتی برای روتر دیگر است .

جمع‌بندی

یکی از مدل‌های لایه‌بندی شبکه، استاندارد TCP/IP است که در سال ۱۹۷۰ اختراع شد که مفهوم لایه‌بندی در شبکه را نشان می‌دهد. دیگری OSI است، با نام کامل Open System Interconnection Communication Reference Modelاست که یک استاندارد بین‌المللی است که برای یکسان‌سازی پروتکل‌های مختلف شبکه استفاده می‌شود که در اواخر دهه ۱۹۷۰ طراحی شد.

لایه های شبکه مدل OSI به ۷ لایه تقسیم می‌شود و مدل قدیمی TCP/IP به ۴ لایه و مدل جدید TCP/IP به ۵ لایه تقسیم می‌شوند. رابطه این دو مانند سیستم‌عامل iOS و اندروید است که هر کدام استانداردهایی را توسعه داده‌اند.

استانداردهای بین‌المللی به دلیل گفتمان قوی آنها را هسته اصلی خود می‌دانند و برخی استانداردهای دیگر را مشخص می‌کنند، در میان آنها TCP/IP پیشرو در مدل لایه‌بندی شبکه است OSI .یک نماد و یک استاندارد بین‌المللی است.

۷- تجهیزات فعال و غیرفعال

شبکه های کامپیوتری مجموعه ای از کامپیوترهای متصل شده به هم با یک فناوری است. دو کامپیوتر را متصل به هم می نامند اگر آن ها توانایی تبادل اطلاعات را داشته باشند. اتصال می تواند توسط سیم های مسی, فیبر نوری, مادون قرمز و ماهواره های مخابراتی انجام گیرد. اینترنت شبکه از شبکه ها و وب سیستم های توزیع شده

ای هستند که روی اینترنت اجرا می‌شوند. سیستم های توزیع شده، مجموعه ای ازکامپیوترهای مستقل هستندکه برای کاربران به عنوان یک سیستم منفرد و یکپارچه ظاهرمی‌شود.
اساسا یک شبکه کامپیوتری شامل دو یا بیش از دو کامپیوتر وابزارهای جانبی مثل چاپگرها، اسکنرها ومانند اینها هستند که بطور مستقیم بمنظور استفاده مشترک از سخت افزار ونرم افزار، منابع اطلاعاتی ابزارهای متصل ایجاده شده است توجه داشته باشید که به تمامی تجهیزات سخت افزاری ونرم افزاری موجود در شبکه منبع گویند.
در این تشریک مساعی با توجه به نوع پیکربندی کامپیوتر ، هر کامپیوتر کاربر می تواند در آن واحد منابع خود را اعم از ابزارها وداده ها با کامپیوترهای دیگر به اشتراک بگذراد و تجهیزاتی که در این بین مورد استفاده قرار می‌گیرند به تجهیزات فعال و غیر فعال[۱۵] تقسیم می شوند.

۱) تجهیزات غیر فعال

تجهیزاتی هستند که قابل برنامه ریزی نبوده و نمی‌توانند تغییراتی روی اطلاعات و یا محتوای تبادل شده در شبکه داشته باشند. بخشی از تجهیزاتی هم که بمنظور نصب و پیکر بندی سخت‌افزاری شبکه (از قبیل کابل کشی و نصب دستگاه‌ها) استفاده می‌شود در این دسته جای می‌گیرند.انواع تجهیزات غیر فعال عبارتند از:کابل-پچ پنل-پچ کورد، فیبر نوری، کیستون پریز، سرسوکت، رک، نگهدارنده کابل.

۲) تجهیزات فعال

تجهیزاتی هستند که فعالیت الکترونیکی در درون آنها صورت می‌گیرد و اطلاعات وارد شده به انها بسته به شرایط برنامه ریزی شده برای دستگاه، پردازش و رد و بدل می‌گردد. انواع تجهیزات فعال عبارتند از: مسیریاب روتر، مودم، دیواره‌های آتش سخت‌افزاری ، کارت شبکه، سوئیچ، اکسس پوینت و ... .
در ادامه به لیستی از تجهیزات فعال اشاره می‌شود و مواردی از آن مورد بررسی قرار می‌گیرند.

تعریف شبکه:

شبکه مجموعه ای از سرویس دهنده ها و سرویس گیرنده های متعدد می باشد که به یکدیگرمتصل اند و با هم تبادل اطلاعات می کنند. به مجموع دو یا چند کامپیوتر که با هم ارتباط داشته باشند نیز شبکه گویند و معمولا در شبکه هم سرویس دهنده وجود دارد و هم سرویس گیرنده بنابراین شبکه شامل مجموعه ای از سرویس دهنده ها و سرویس گیرنده ها می باشد.
تمام شبکه‌های بزرگ و کوچک، متشکل از تجهیزات سخت‌افزاری و نرم‌افزاری مختلفی هستند که بر مبنای توپولوژی‌های مختلف به یکدیگر متصل شده‌اند و به تبادل اطلاعات می‌پردازند. برای نیل به این هدف، سرپرستان شبکه باید تجهیزات اکتیو و پسیو را به‌گونه‌ای پیکربندی کنند که در نهایت بتواند بدون افت کیفیت و حفظ سرعت و رعایت موازین امنیتی به کلاینت‌ها اجازه تبادل اطلاعات را بدهد.

هدف های برقراری شبکه کامپیوتری

هدف از ایجاد شبکه ی کامپیوتری عبارت است از :

[۱۵] Passive & Active

- ✓ اشتراک منابع
- ✓ تبادل پیغام
- ✓ مدیریت از راه دور

مجموعه ای از کامپیوتر ها، نرم افزار ها و سخت افزار های متصل به هم است که باعث میشوند کاربران بتوانند با هم ارتباط داشته باشند.

مزایای شبکه

- ✓ استفاده از منابع مشترک (اطلاعات، سخت افزار و نرم افزار)
- ✓ حذف محدودیت های جغرافیایی
- ✓ تبادل سریع تر و دقیق تر اطلاعات
- ✓ صرفه جویی در هزینه ها
- ✓ افزایش امنیت

تجهیزات شبکه یا سخت افزار شبکه، دستگاه‌های فیزیکی هستند که برای ارتباط و تعامل بین سخت‌افزارها در یک شبکه کامپیوتری مورد نیاز هستند. در ادامه به بررسی تجهیزات مورد نیاز برای راه اندازی شبکه و تجهیزات پسیو و اکتیو می‌پردازیم.

تجهیزات فعال

تجهیزات فعال به تجهیزاتی گفته می‌شود که سیگنال‌های الکترونیکی را تولید، بازتولید، هدایت و مسیریابی می‌کنند. تجهیزات اکتیو یا فعال، در شبکه سیگنال‌ها را تولید می‌کند و از طریق تجهیزات پسیو سیگنال‌ها را در شبکه جابه جا می‌کنند. تجهیزات اکتیو شبکه برای انتقال، مدیریت یا نظارت بر بسته‌هایی که توسط شبکه‌ها ارسال می‌شوند نیز به کار گرفته می‌شوند. نبود هر یک از تجهیزات اکتیو باعث می‌شود عملکرد شبکه با مشکل روبرو شود. وجود برخی از آن‌ها ضروری است و برخی تنها برای دسترسی ساده‌تر به اطلاعات استفاده می‌شود.
در یک شبکه کامپیوتری به قطعاتی که معمولاً به برق متصل شده و در تولید، هدایت و یا تقویت سیگنال‌ها نقش دارند و در اصطلاح به خودی خود فعالیت دارند، قطعات « فعال » گفته می‌شود. مثل سوئیچ و مودم و...

لیستی از تجهیزات فعال:

۱) دوربین های مداربسته – دیجیتال و آنالوگ (IP Camera)
۲) انواع تجهیزات ویدئو کنفرانس (IP Surveillance/ Internet Video Conferencing)
۳) سیستم های تلفن اینترنتی (Internet – Telephony Gateway)
۴) انباره های ذخیره سازی (Network Attached Storage) – NAS
۵) انواع Print Server
۶) انواع تجهیزات شبکه های بی سیم (Wireless) و Bluetooth
۷) انواع تجهیزات فیبر نوری (Fiber Optic Media Converter)

۸) انواع مودم دیجیتال و ADSL
۹) انواع کارت شبکه (۱۰/۱۰۰/۱۰۰۰)
۱۰) انواع درگاه و روتر پیشرفته (Advanced Router / Multi-Homing Security Gateway)
۱۱) تجهیزات Power Line Communication – PLC
۱۲) تجهیزات L4-L7 Ethernet Devices
۱۳) انواع سوئیچ های KVM
۱۴) تجهیزات IP Power Management
۱۵) انواع سوئیچ های خانگی و صنعتی

دیدیم که تجهیزات اکتیو چیست در ادامه به معرفی تجهیزات اکتیو می‌پردازیم:

سرور

قلب تپنده شبکه‌های ارتباطی است. اصلی‌ترین وظیفه سرور خدمت‌رسانی به کاربران است. در محیط‌های بزرگ و پیچیده سرور وظیفه تامین منابع پردازشی موردنیاز کلاینت‌ها را دارد. به‌طور مثال، در محیط‌های ابری یا مبتنی بر فناوری‌های مجازی‌ساز، کاری که سرور انجام می‌دهد تخصیص منابع موردنیاز به کلاینت‌ها است. این فرایند می‌تواند امکان دسترسی به ماشین‌های مجازی میزبانی شده روی سرور، دسترسی به دسکتاپ‌های مجازی‌ساز یا دسترسی ساده به اطلاعاتی باشد که روی بانک‌های اطلاعاتی ذخیره‌سازی شده‌اند.

سرورها در انواع مختلفی به بازار عرضه می‌شوند که سرورهای تیغه‌ای، رک‌مونت، ایستاده، ابری و.... از مهم‌ترین آن‌ها هستند. در میان برندهایی که اقدام به تولید سرور می‌کنند محصولات اچ پی و به ویژه سرورهای پرولیانت به دلیل کیفیت و طول عمر بالا مورد توجه سازمان‌ها قرار دارند. سرورهای پرولیانت نسل نهم و دهم از گزینه‌های اصلی سازمان‌ها هستند.

هاب شبکه

hubدستگاهی است که امکان اتصال تجهیزات مختلف به شبکه را می‌دهد. امکان استفاده از هاب به عنوان یک تکرارکننده وجود دارد زیرا سیگنال‌هایی که پس از طی مسافت‌های طولانی روی کابل‌ها ضعیف می‌شوند را تقویت می‌کند. هاب ساده‌ترین عضو دنیای شبکه است، زیرا مولفه‌های یک شبکه محلی را بر مبنای پروتکل‌های یکسانی به یکدیگر متصل می‌کند. در مقایسه با سوئیچ سرعت و کارایی پایین‌تری دارد و تقریبا منسوخ شده است.

یک هاب می‌تواند با داده‌های دیجیتالی و آنالوگ مورد استفاده قرار گیرد، به شرطی که تنظیمات آن برای آماده‌سازی قالب‌بندی داده‌های ورودی پیکربندی شده باشد. به عنوان مثال، اگر داده‌های ورودی به صورت دیجیتال باشد، هاب باید آن‌را به عنوان بسته منتقل کند، اما اگر داده‌های ورودی آنالوگ باشند، هاب آن‌را به شکل سیگنال منتقل می‌کند. هاب‌ها عملکردهای فیلترینگ یا آدرس‌دهی بسته‌ها را انجام نمی‌دهند. آن‌ها فقط بسته‌های داده را برای همه دستگاه‌های متصل ارسال می‌کنند. هاب‌ها در لایه فیزیکی مدل Open Systems Interconnection (OSI)کار می‌کنند. هاب‌ها به دو نوع پورت ساده و چندگانه تقسیم می‌شوند.

هاب فاقد هرگونه مولفه هوشمندی است به همین دلیل مشکل بزرگی که ایجاد می‌کند تداخل و مصرف بیش از اندازه پهنای باند است، زیرا هنگامی که گره‌ای قصد دارد یک بسته اطلاعاتی را برای گره دیگری ارسال کند از رویکرد همه پخشی استفاده می‌کند که باعث می‌شود یک بسته اطلاعاتی برای همه گره‌های متصل به هاب ارسال شود.

سوئیچ شبکه

عملکرد سوئیچ شبیه به هاب است با این تفاوت که هوشمند است. سوییچ هنگامی که بسته‌ای را دریافت می‌کند بر مبنای مک‌آدرس یا آدرس آی‌پی دستگاه بسته را برای گره درست ارسال می‌کند و در نتیجه بسته برای همه پورت‌ها ارسال نمی‌شود. با توجه به این‌که بسته برای پورت مشخصی ارسال می‌شود مشکل تصادم، ازدحام و مصرف بیش از اندازه ترافیک به وجود نمی‌آید.

سوئیچ یک دستگاه چند پورتی است که کارایی شبکه را بهبود می‌بخشد. سوئیچ اطلاعات مسیریابی محدود در مورد گره‌های شبکه داخلی را حفظ می‌کند و به سیستم‌ها امکان اتصال به روتر را می‌دهد. به‌طور کلی، سوئیچ‌ها می‌توانند آدرس سخت‌افزاری بسته‌های ورودی را بخوانند و بسته‌ها را به مقصد مناسب انتقال دهند.

سوئیچ‌ها به دلیل قابلیت مدار مجازی و هوشمندی که دارند، کارایی شبکه را بهبود می‌بخشند. سوئیچ‌ها امنیت شبکه را افزایش می‌دهند، زیرا از طریق الگوریتم‌های مسیریابی، بهترین مسیر را انتخاب می‌کنند و قابلیت دفع حملات سایبری شناخته شده را دارند. شما می‌توانید یک سوئیچ را به عنوان دستگاهی در نظر بگیرید که بهترین قابلیت‌های روترها و هاب‌ها را دارد، البته بدون وجود روتر قادر به اتصال به اینترنت نیست.

یک سوئیچ می‌تواند در لایه پیوند داده یا لایه شبکه مدل OSI کار کند. سوئیچ چند لایه سوئیچی است که می‌تواند در هر دو لایه کار کند یعنی می‌تواند به عنوان سوئیچ و روتر عمل کند. پس سوئیچ چند لایه یک دستگاه با کارایی بالا است که از پروتکل‌های مسیریابی مشابه روترها پشتیبانی می‌کند.

سوئیچ‌ها می‌توانند در معرض حملات انکار سرویس توزیع شده (DDoS) قرار بگیرند. البته سوییچ‌های امروزی راهکارهایی برای محافظت از شبکه در برابر حمله‌های سیلابی دارند. امنیت پورت سوئیچ یکی از مهم‌ترین نکاتی است که باید به آن دقت کنید، بنابراین مطمئن شوید که پورت‌های بلااستفاده غیرفعال هستند و از جستجوی DHCP، بازرسی ARP و فیلتر آدرس مک استفاده می‌کنید.

از مهم‌ترین نکاتی که در زمان خرید سوییچ باید به آن دقت کنید مدیریتی، غیر مدیریتی، نیمه هوشمند بودن، تعداد پورت‌ها، توانایی پشتیبانی از فناوری PoE و... است. علاوه بر این باید به نوع سوییچ نیز دقت کنید که قابل استفاده در کدام لایه است. همان طور که گفتیم برخی از سوییچ‌ها در لایه ۲ و برخی دیگر در لایه ۳ کار می‌کنند.

بریج

برای اتصال دو شبکه مجزا از هم یک پل ارتباطی ایجاد می‌شود که به آن پل (bridge) می‌گویند. در این حالت شبکه محلی A می‌تواند از طریق دستگاه بریج به شبکه محلی B متصل شود. از پل‌ها می‌توان برای اتصال دو lan فیزیکی به یک lan منطقی بزرگ‌تر نیز می توان استفاده کرد. همچنین پل‌ها برای تقسیم شبکه‌های بزرگ‌تر به

بخش‌های کوچک‌تر با قرار گرفتن بین دو بخش فیزیکی شبکه و مدیریت جریان داده بین هر دو نیز استفاده می‌شوند.

bridgeفقط در لایه‌های فیزیکی (physical) و پیوند داده (data link) مدل osi کار می‌کند. نقش اساسی پل‌ها در معماری شبکه، ذخیره و ارسال فریم‌ها بین بخش‌های مختلف است. آن‌ها از مک آدرس‌ها برای انتقال فریم استفاده می‌کنند. با مشاهده مک آدرس پل‌ها می‌توانند داده‌ها را به سمت دستگاه‌های متصل به هر بخش هدایت کنند.

پل‌ها از بسیاری جهات مانند هاب‌ها هستند، از جمله این که مولفه‌های lan را با پروتکل‌های یکسان به یکدیگر متصل می‌کنند، با این تفاوت که پل‌ها بسته‌های داده ورودی را به عنوان فریم می‌شناسند و قبل از ارسال آدرس، آن‌ها را فیلتر و بسته‌بندی می‌کنند. از آن‌جایی که بسته‌های داده را فیلتر می‌کنند، پل هیچ تغییری در قالب یا محتوای داده‌های ورودی ایجاد نمی‌کند. جدول بریج در ابتدا خالی است، اما به مرور زمان آدرس هر کامپیوتر متعلق به شبکه محلی و آدرس‌های هر رابطی که شبکه محلی به سایر شبکه‌ها را متصل می‌کند نگه‌داری می‌کند. پل‌ها، مانند هاب‌ها می‌توانند چند پورته باشند. پل‌ها در سال‌های اخیر به ندرت استفاده می‌شوند و سوئیچ‌ها جایگزین آن‌ها شده‌اند که عملکرد بهتری دارند. در واقع، سوئیچ‌ها به‌علت نحوه عملکرد خود به‌عنوان پل چند پورته (multiport bridges) نامیده می‌شوند.

روتر

هنگامی که قصد اتصال دو شبکه محلی به یکدیگر را دارید به ابزاری برای اتصال شبکه‌ها به یکدیگر نیاز دارید. برای این منظور باید از مودم‌روتر استفاده کنید. مودم‌روتر وسیله‌ای است که برای برقراری ارتباط سامانه‌ها به یکدیگر از طریق کابل یا شبکه وای‌فای استفاده می‌شود.

روترها در انواع مختلفی به بازار عرضه می‌شوند و در زمان خرید روتر باید به استانداردهای مخابراتی که پشتیبانی می‌کند، فرکانس‌ها و تعداد آنتن‌ها دقت کنید. به‌عنوان یک قاعده کلی، پیشنهاد می‌شود به سراغ خرید روترهایی بروید که از استاندارد ۸۰۲.۱۱ acپشتیبانی می‌کنند. علاوه بر این، اگر در نظر دارید در آینده از اینترنت سیار استفاده کنید باید به توانایی روتر در پشتیبانی از سیم‌کارت دقت کنید.

روترها با ترسیم مسیری برای دستگاه‌های متصل به شبکه و از طریق توپولوژی‌های مختلف شبکه به انتقال بسته‌ها به مقاصد کمک می‌کنند. روترها دستگاه‌های هوشمندی هستند و اطلاعات مربوط به شبکه‌هایی که به آن‌ها متصل هستند را ذخیره می‌کنند. اکثر روترها را می‌توان طوری پیکربندی کرد که به عنوان فایروال فیلتر بسته‌ها عمل کند و از فهرست کنترل دسترسی (ACL) نیز پشتیبانی می‌کنند.

روترها، همراه با واحد سرویس کانال/واحد سرویس داده (CSU/DSU) توانایی ترجمه فریم LAN به فریم WAN را دارند، این فرایند ضروری است، زیرا شبکه‌های محلی و شبکه‌های گسترده از پروتکل‌های مختلف شبکه استفاده می‌کنند. این روترها به‌نام روترهای مرزی نیز شناخته می‌شوند. این روترها توانایی برقراری ارتباط شبکه‌های LAN به WAN را دارند.

روتر برای تقسیم شبکه‌های داخلی به دو یا چند زیر شبکه استفاده می‌شود. روترها می‌توانند به‌صورت داخلی به سایر روترها متصل شوند و مناطقی را ایجاد کنند که مستقل عمل می‌کنند. روترها با حفظ جداول در مورد مقاصد

قابلیت برقراری ارتباطات محلی را فراهم می‌کنند. برای این منظور روتر حاوی اطلاعاتی در مورد سیستم‌های متصل به آن است و در صورت عدم تشخیص مقصد، محل ارسال درخواست‌ها را حدس می‌زند.
روترها معمولاً مسیریابی را با استفاده از یکی از سه پروتکل استاندارد پروتکل اطلاعات مسیریابی(RIP) ، پروتکل دروازه مرزی (BGP) یا ابتدا کوتاهترین مسیر (OSPF) را انتخاب کن انجام می‌دهند.

مودم

مودم‌ها برای انتقال سیگنال‌های دیجیتال از طریق خطوط تلفن آنالوگ استفاده می‌شوند. بنابراین، سیگنال‌های دیجیتال توسط مودم به سیگنال‌های آنالوگ با فرکانس‌های مختلف تبدیل شده و به مودم مقصد انتقال داده می‌شوند. مودم دریافت‌کننده سیگنال آنالوگ را به دیجیتال تبدیل کرده و خروجی دیجیتال را به دستگاهی متصل به مودم که معمولاً کامپیوتر است تحویل می‌دهد. داده‌های دیجیتالی معمولاً از طریق رابط کاربری استاندارد-RS 232به مودم یا از طریق خط سریال انتقال داده می‌شوند. مودم‌ها روی هر دو لایه فیزیکی و پیونده داده کار می‌کنند.
به زبان ساده مودم، ارتباط شما را با مراکز ارائه دهنده اینترنت برقرار می کند.

اکسس پوینت

به‌طور معمول در شبکه کابلی برای برقراری ارتباط تجهیزات با شبکه به یک سوئیچ نیاز داریم، اما در شبکه‌های وایرلس به اکسس پوینت نیاز داریم تا به کلاینت‌هایی که دورتر از روتر قرار دارند اجازه اتصال به شبکه وای‌فای را بدهد. پس اکسس پوینت در شبکه‌های وایرلس همان کاری را انجام می‌دهد که سوئیچ در شبکه‌های کابلی انجام می‌دهد.
اکسس پوینت می‌تواند از نظر فنی شامل اتصال سیمی یا بی سیم باشد اما معمولاً به دستگاه بی سیم اشاره دارد. یک Access Point در لایه دوم مدل OSI کار می‌کند و می‌تواند یا به عنوان پلی که یک شبکه سیمی استاندارد را به دستگاه‌های بی سیم متصل می‌کند یا به عنوان یک روتر انتقال داده‌ها از یک نقطه به نقطه دیگر استفاده شود. اکسس پوینت‌های بی‌سیم (WAP) شامل یک دستگاه فرستنده و گیرنده هستند که برای ساخت شبکه محلی بی‌سیم (WLAN) استفاده می‌شود. اکسس‌پوینت‌ها دستگاه‌های مجهز به آنتن، فرستنده و آداپتور داخلی هستند. آن‌ها دارای چند پورت هستند که به شما این امکان را می‌دهند تا شبکه را برای پشتیبانی از کلاینت‌های بیشتر گسترش دهید. بسته به اندازه شبکه، ممکن است یک یا چند اکسس پوینت برای پوشش کامل مورد نیاز باشد.
اکسس پوینت‌ها ممکن است پورت‌های زیادی را برای افزایش وسعت شبکه، قابلیت‌های دیوار آتش و سرویس DHCPارائه دهند. بنابراین، ما اکسس‌پوینت‌هایی در بازار داریم که یک سوئیچ، سرورdhcp ، روتر و فایروال هستند.

ریپیتر

تکرار کننده یک دستگاه الکترونیکی است که سیگنال دریافتی را تقویت می‌کند. شما می‌توانید تکرار کننده را دستگاهی تصور کنید که یک سیگنال دریافت می‌کند و آن‌را با قدرت بیشتری ارسال می‌کند تا سیگنال بتواند مسافت‌های طولانی‌تری را پوشش دهد. تکرارگرها روی لایه فیزیکی کار می‌کنند.

اگر دو ساختمان بزرگ از طریق شبکه به هم وصل شوند و فاصله بین کاربران زیاد باشد، ممکن است هنگام انتقال، داده‌ها از بین برود یا سیگنال‌ها ضعیف شود. در چنین شرایطی سرپرستان شبکه برای حل مشکل از repeater استفاده می‌کنند. ریپیتر وظیفه تقویت و بازسازی داده‌های انتقالی را در شبکه وایرلس بر عهده دارد، به‌گونه‌ای که سیگنال‌ها به خوبی و بدون دست خوردگی به مقصد برسند.

Gateway

گیت‌وی‌ها معمولاً در لایه‌های انتقال و نشست (Transport and Session) مدل OSI کار می‌کنند. در لایه انتقال (Transport)و بالاتر، پروتکل‌ها و استانداردهای متعددی از سوی فروشندگان ارایه شده است. گیت‌وی‌ها را باید همانند مترجمی میان توپولوژی‌های شبکه مانند اتصال سیستم باز (OSI) و پروتکل کنترل انتقال/پروتکل اینترنت (TCP/IP)هستند. به همین دلیل، گیت‌وی‌ها دو یا چند شبکه مستقل را متصل می‌کنند که هریک دارای الگوریتم‌های مسیریابی، پروتکل‌ها، توپولوژی، خدمات نام دامنه و رویه‌ها و خط‌مشی‌های مدیریت شبکه هستند. gatewayبیشترِ عملکردهای روترها را دارند. در حقیقت، یک روتر با قابلیت ترجمه اضافی عملکردی یکسان با یک گیت‌وی دارد. به فرایند ترجمه فناوری‌های مختلف شبکه به شکلی که دستگاه‌ها قادر به درک زبان یکدیگر باشند، مبدل پروتکل (protocol converter) گفته می‌شود.

پرینت سرور

در برخی سازمان‌ها لازم است بدون نیاز به کامپیوتر، چاپگری به اشتراک قرار گیرد تا کاربران از طریق شبکه به آن متصل شوند و پرینت‌های خود را ارسال کنند. در چنین سناریویی پرینتر را با کابل یواس‌بی پرینت سرور وصل می‌کنید و پرینت سرور را با یک کابل شبکه به سوئیچ شبکه متصل می‌کنید. این کار باعث می‌شود که پرینت سرور آی‌پی موردنیاز را دریافت کند و در شبکه شناسایی شود. از این به بعد کاربران درخواست‌های چاپ را مستقیما برای پرینتر ارسال می‌کنند.

کارت شبکه

مکانیزم برقراری ارتباط کامپیوتر با شبکه و سایر دستگاه‌های متصل به شبکه است. به‌طور کلی، تمامی تجهیزات برای برقراری ارتباط با شبکه محلی یا اینترنت به کارت شبکه نیاز دارند. بدون کارت شبکه هیچ دستگاهی قادر به برقراری ارتباط با اینترنت نیست. هر کارت شبکه دارای یک مک‌آدرس است که با استفاده از آن در شبکه شناسائی شده و توانائی برقراری ارتباط با سایر دستگاه‌ها را دارد. کارت‌های شبکه در سرعت‌های مختلفی وجود دارند و می‌توانند از استانداردها و پروتکل‌های مختلفی پشتیبانی کنند. نکته مهم در زمان خرید کارت شبکه توانایی پشتیبانی از دو فرکانس کاری و استانداردهای روز است.

فایروال یا دیوارآتش

وظیفه اصلی دیوارهای آتش نظارت بر بسته‌های ورودی و خروجی به شبکه سازمانی است. دیوارهای آتش با بررسی و بازبینی بسته‌ها مانع از آن می‌شوند برنامه‌های کاربردی بدون اطلاع کاربر به اینترنت متصل شده و تبادل اطلاعات بپردازند یا هکرها بتوانند به راحتی اقدام به سرقت یا شنود اطلاعات کنند.

فایروال‌ها نقش مهمی در پیشگیری از بروز حمله‌های رایج اینترنتی دارند. به‌طور معمول کاربران، دیوارهای آتش را به شکل نرم‌افزاری می‌شناسند، در حالی که دیوارهای آتش سخت‌افزاری نقش مهمی در تامین امنیت شبکه‌های سازمانی دارند. یکی از شناخته‌شده‌ترین دیوارهای آتش سخت‌افزاری که تقریبا همه کاربران از آن استفاده می‌کنند روترها هستند. فایروال روتر مانع از بروز حمله‌های سیلابی یا حمله‌های بدافزاری می‌شود اما در مقیاس وسیع‌تر، فایروال‌ها در تعامل با سامانه‌های پیشگیری و تشخیص نفوذ در شبکه‌ها نصب می‌شوند تا سرآیندهای مربوط به مبدا و مقصد بسته‌ها را بررسی کنند و اگر محتویات بسته‌ها مغایر با قواعد از پیش تعریف شده برای دیوارآتش بود مانع ارسال یا دریافت بسته‌ها شوند.

سامانه‌های پیشگیری و تشخیص نفوذ

این سامانه‌ها همانند دیوارهای آتش به شکل نرم‌افزاری و سخت‌افزاری وجود دارند و با ارزیابی بسته‌ها و بر مبنای اطلاعاتی که از قبل دارند حمله‌های سایبری رایج را شناسایی کرده و هشداری برای سرپرستان شبکه ارسال می‌کنند. این سامانه‌ها به انواع مختلفی مثل مبتنی بر میزبان، مبتنی بر شبکه و نمونه‌های مشابه تقسیم می‌شوند که هر یک بسته به نوع شبکه عملکرد خاص خود را دارند. مهم‌ترین نکته‌ای که باید در مورد این سامانه‌ها مکان درست قرارگیری آن‌ها در شبکه است که پهنای باند شبکه را بیهوده مصرف نکنند و از طرفی به شکل درستی قادر به تشخیص موارد مشکوک باشند.

تجهیزات IDS و IPS از جمله تجهیزات امنیتی در شبکه هستند IDS :برای یافتن تهدیدها استفاده می‌شود و IPSبرای از بین بردن و قطع دسترسی تهدیدها در شبکه.

تجهیزات غیرفعال

تجهیزاتی هستند که قابل برنامه ریزی نمی باشند و نمی توانند تغییراتی روی اطلاعات یا محتوای تبادل داده شده در شبکه داشته باشند.اغلب تجهیزاتی که به منظور نصب و پیکربندی سخت افزار شبکه از قبیل کابل کشی و نصب دستگاهها استفاده می شود در این دسته جا می گیرند.

تجهیزات یا وسایل غیرفعال یا منفعل، تجهیزاتی هستند که در مقابل سیگنال الکترونیکی(یا نوری)، رفتاری غیرفعال دارند .به عبارت دیگر، این تجهیزات به برق متصل نمی‌شوند و توانایی تقویت سیگنال را ندارند و تنها نظاره گر عبور آن ها هستند که ممکن است منجر به تضعیف سیگنال نیز بشود.

۲-۴-لیستی از تجهیزات غیر فعال (Passive):

- پریز شبکه
- انواع Keystone
- انواع کابل
- انواع Patch Cable
- انواع Patch Panel (برای کابلهای Cat 5, Cat6 و Fiber Optic)
- انواع Cable Management و Rack Panel

- انواع رک
- داکت و ترانکینگ(Duct &Trunk)(کانال پلاستیکی)
- انواع Power Module برای Rack
- انواع Connector
- انواع FLB - FLOOR BOXES FOR RAISED FLOORS
- انواع FACE PLATE
- انواع سوکت دیواری
- انواع Inline Coupler
- انواع ابزار نظیر Crimping، Striper، Punch Down و...
- انواع USB HUB
- انواع تستر

مهم‌ترین بخش راه اندازی شبکه، تجهیزات مستقر در زیرساخت است. پسیو به معنای غیرفعال است و به تجهیزاتی اشاره دارد که تاثیری روی انتقال داده‌ها ندارند. پسیو به خدمات نصب و راه اندازی تجهیزات شبکه که وارد مرحله پیکربندی نمی‌شوند گفته می‌شود.

تجهیزات پسیو شبکه های کامپیوتری تجهیزاتی هستند که بدون جریان برق کار می‌کنند و نیازی به جریان الکتریسیته ندارند. تجهیزات پسیو شبکه فاقد برنامه‌ریزی هستند و به لحاظ اندازه قابل تغییر نبوده و ثابت هستند. منظور از ثابت و غیر قابل تغییر بودن این است که هنگامی که یکی از ملزومات پسیو شبکه مثل رک را خریداری می‌کنید، امکان تغییر اندازه آن وجود ندارد.

تجهیزات پسیو در تعامل با تجهیزات اکتیو قابل استفاده هستند، زیرا مادامی که تجهیزات اکتیو آماده نباشند، هیچ‌گونه اطلاعاتی انتقال نمی‌یابد و در واقع شبکه قابل استفاده نیست. اولین قدم در عملیات پسیو شبکه، طراحی استاندارد، پیاده‌سازی نقشه طراحی و به‌کارگیری تجهیزات با کیفیت است.

معرفی تجهیزات پسیو شبکه

تجهیزات پسیو شبکه‌های کامپیوتری گسترده هستند و بسته به نوع شبکه‌ای که قصد پیاده‌سازی آن‌را دارید و بزرگی و کوچکی می‌توان از تجهیزات مختلفی استفاده کرد. اما برخی تجهیزات کاربرد کلی دارند و جزو تجهیزات لازم برای راه اندازی شبکه هستند.

دیدیم که پسیو چیست حال به معرفی تجهیزات پسیو شبکه می‌پردازیم:

کابل‌ها

کابل و سوکت های شبکه نقشی اساسی و مهم در شبکه دارند و به سیستم ها کمک می کنند تا بتوانند به شبکه متصل شوند.
کابل‌ها همانند رگ در بدن انسان هستند، برخی از رگ‌ها قطور و بزرگ هستند در حالی که برخی دیگر نازک و باریک هستند. کابل‌های دنیای شبکه نیز چنین قاعده‌ای دارند: برخی ضخیم و مقاوم در برابر نویزها و ضد آب و مناسب برای نصب در محیط‌های خارجی هستند، در حالی که برخی دیگر ظریف و مناسب برای مکان‌هایی هستند که اطلاعات حساس را انتقال نمی‌دهند یا در یک محیط ایزوله شده استفاده می‌شوند.
کابل‌ها انواع مختلفی دارند که زوج به هم تابیده، کواکسیال، فیبر نوری، مستقیم و کراس از جمله آن‌ها هستند. نکته مهمی که در زمان خرید کابل‌های Cat باید به آن‌ها دقت کنید ظرفیت و پهنای باند آن‌ها و نوع روکش آن‌ها است. به‌طور معمول در بیشتر کابل‌کشی‌ها cat 5e و cat6 جوابگوی نیازهای روزمره هستند. اما در محیط‌های مرکز داده بهتر است از کابل‌های cat7 یا cat8 استفاده شود. هرچند در بیشتر موارد سازمان‌های بزرگ در مراکز داده از فیبرنوری استفاده می‌کنند.
دستگاه‌ها و ابزارهایی وجود دارند که با استفاده آن‌ها می‌توان امور مربوط به کابل کشی و نصب تجهیزات را انجام داد.

پچ کورد

کابل‌های کوچکی هستند که برای اتصال تجهیزات نزدیک به هم استفاده می‌شوند. به‌طور معمول طول این کابل‌ها کمتر از ۵ متر است و در دو نوع مسی و فیبر نوری در بازار وجود دارند. از پچ کوردها می‌توان برای اتصال یک سوئیچ شبکه به کامپیوتر یا یک سوئیچ شبکه به روتر استفاده کرد.

داکت/ترانک

داکت و ترانک محفظه‌ای از جنس مادهPVC ، LSZHیا PEهستند که برای عبور دسته‌ای از کابل‌های برق یا شبکه در خدمات پسیو استفاده می‌شوند. تفاوت داکت و ترانک چیست؟ ترانک به دلیل ابعاد بزرگ برای عبور دسته کابل‌های بیشتر استفاده می‌شود و از داکت برای مسیرهایی که حجم کابل‌ها کم است استفاده می‌شود.

سوکت‌های دیواری

سوکت‌های دیواری دسترسی سامانه‌ها به شبکه را برقرار می‌کنند و به کاربر امکان می‌دهند با استفاده از کابل شبکه به شبکه متصل شوند. پس سوکت های دیواری دسترسی سیستم کاربران را به شبکه برقرار می کنند و به کاربر این امکان را می دهند تا با استفاده از کابل شبکه، به شبکه اصلی متصل شود.

کیستون شبکه چیست

برای استفاده از کابل‌های شبکه مسی باید از یک کانکشن استفاده کرد. به این کانکشن‌ها، کیستون (پریز) گفته می‌شود. کیستون برای اتصال کابل شبکه به تجهیزاتی مانند سوئیچ، روتر و موارد این چنینی استفاده می‌شود. کیستون یکی از مهم‌ترین تجهیزات شبکه است که نقش مهمی در سرعت شبکه دارد. در مکان‌های مختلفی مثل پچ پنل، ترانک، باکس‌ها از کیستون‌ها استفاده می‌شود.

باید با توجه به نوع کاربری از کیستون مناسب استفاده کنید، در غیر این صورت راه اندازی شبکه با مشکل روبرو می‌شود. کیستون ها بر اساس category به یکی از دسته‌های cat5 و cat5e و cat6 و cat6a و cat7 و cat7a و cat8 تعلق دارند و بر اساس جنس بدنه در ۲ نوع فلزی و پلاستیکی موجود هستند.

پچ پنل

کابل‌های شبکه گره‌های شبکه را به سوییچ متصل می‌کنند. پچ پنل یکی از ملزومات مهمی است که پیشنهاد می‌شود در کابل کشی ساخت‌یافته به آن دقت کنید. این قطعه دارای پورت‌های شماره‌گذاری شده است که تمامی کابل‌های شبکه به آن‌ها وصل می‌شوند.

پچ پنل نقش مهمی در منظم کردن کابل‌ها و مدیریت آن‌ها دارد و باعث می‌شود مدیریت و عیب‌یابی شبکه سریع‌تر انجام شود و پچ‌پنل با ارایه یک مکانیزم مدیریتی متمرکز به سرپرستان شبکه اجازه می‌دهد کابل‌هایی که از اتاق‌ها و مکان‌های مختلف به سمت رک‌سرور و سوییچ وارد می‌شوند را در یک مکان، متمرکز و مدیریت کنند. علاوه بر این، پچ پنل‌ها در زمان عیب‌یابی یا قطع و وصل دسترسی یک کلاینت به شبکه کار سرپرستان شبکه را راحت‌تر می‌کنند.

رک

یک محفظه مستطیلی شکل است که برای قرارگیری سرور، سوئیچ، روتر، فایروال سخت‌افزاری، پچ پنل‌ها، upsها و سایر تجهیزات شبکه استفاده می‌شوند. به‌طور کلی رک‌ها به دو گروه رک‌های دیواری و رک‌های ایستاده تقسیم می‌شوند. هنگام خرید رک باید به اندازه رک که بر مبنای واحد یونیت محاسبه می‌شود، عمق رک (به‌طور معمول ۳۰، ۳۴، ۴۰، ۴۶ هستند)، فن (برخی رک‌ها یک یا چند فن برای خنک کردن تجهیزات داخلی دارند) و پچ پنل یا پریز برق اشاره کرد.

با استفاده از رک می توان تمام دستگاه ها را به صورت منظم و با ترتیبی خاص در یک جا جمع کرد که هم از آن ها محافظت شود و هم استفاده از آن دستگاه ها آسان تر شود.

فیس پلیت(Face Plate)

صفحه پریز توکار شبکه است که کیستون‌های شبکه و تلفن روی آن نصب می‌شوند. فیس پلیت‌ها به دو گروه تک و دو پورتی تقسیم می‌شوند. فیس پلیت‌ها روی جعبه‌ها (قوطی‌های) استاندارد نصب می‌شوند. با استفاده از برچسبی که روی برخی از آن‌ها وجود دارد، می‌توانید شماره آن پریز در شبکه را مشخص کنید. فیس پلیت با توجه به کاربرد دارای عمق‌های مختلفی است و داخل دیوار یا روی سطح دیوار نصب می‌شوند.

PDU چیست؟

PDUیا Power Distribution Unit دستگاهی برای مدیریت توزیع برق است که یک ورودی و خروجی های متعدد برق دارد و اغلب در داخل Rack و برای تغذیه برق سرورها و تجهیزات شبکه و دیتاسنتر مورد استفاده قرار می‌گیرد PDU .ها به صورت تک فاز و سه فاز با ولت آمپر های مختلف در بازار وجود دارند.
با توجه به افزایش سرورها و تعدد تجهیزات شبکه در مراکز داده و اتاق های سرور استفاده از PDU ها امری ضروری درجهت مدیریت ظرفیت برق مصرفی تجهیزات شبکه است.
قابلیت های PDU عبارتند از:

۱) اداره و بهره وری بهتر از توان برق در جهت مراکز داده
۲) تعیین برنامه‌ای برای روشن و خاموش کردن تجهیزات متصل بهPDU ها
۳) اطلاع از افزایش بار مصرفی برق در دستگاه های متصل به PDU قبل از Fail شدن دستگاه و امکان جلوگیری از Fail شدن
۴) برخی از PDU ها دارای یک صفحه نمایش برای نمایش مقدار برق و شاخص‌های آن هستند و از طریق ابزارهای مدیریتی بوسیله پروتکل SNMP قابل مدیریت هستند.

تفاوت تجهیزات فعال و غیرفعال

همان‌گونه از معنای لغوی مشخص است تجهیزات اکتیو (فعال) به ملزوماتی از شبکه اشاره دارند که نبود آن‌ها به معنای از دست رفتن قابلیتی در شبکه می‌شود. به‌طور مثال، نبود یک سوییچ مانع از آن می‌شود تا طیف گسترده‌ای از تجهیزات را به شبکه متصل کرد. در حالی که تجهیزات پسیو (غیر فعال) به ملزوماتی اشاره دارند که ماهیت کارکردی آن‌ها منوط به وجود ملزومات اکتیو است. به‌طور مثال، یک کابل شبکه، مادامی که سوییچ یا سروری در شبکه نباشد کاربردی ندارد.

شبکه فعال و غیرفعال چیست؟

شبکه فعال نوعی شبکه کامپیوتری است که در آن هر گره روی یک عملکرد یا فرآیند از پیش تعریف شده کار می‌کند. شبکه غیرفعال هیچ کد یا دستورالعمل تخصصی را در هیچ گره‌ای اجرا نمی‌کند و رفتار خود را به صورت پویا تغییر نمی‌دهد. به‌طور معمول، این رفتار مربوط به هر گره روتر شبکه است. شبکه غیرفعال یکی از متداول‌ترین نوع شبکه‌بندی تجهیزات است. البته این امر مستلزم آن است که کل زیرساخت‌های شبکه قبل از بهره برداری از پیش تعیین و تنظیم شوند.
شبکه فعال ، شبکه‌ای است که انواع مختلفی از تجهیزات الکترونیکی در آن‌ها وجود دارد. این دستگاه‌ها ممکن است در سمت کاربر نهایی، در مرکز شبکه برای پشتیبانی از پروتکل اترنت به منظور بهبود سرعت بارگذاری و بارگیری بسته‌های اطلاعاتی باشند.
امروزه انواع مختلفی از شبکه‌های مسی پسیو وجود دارد. شبکه‌ای که تقریباً همه با آن آشنا هستیم، شبکه تلویزیون کابلی خانگی[16] است. در شبکهCATV مسی، ارائه‌دهنده خدمات کابلی، سیگنال را از طریق کابل کواکسیال

[16] CATV

به خانه مشترکان تحویل می‌دهد. در ابتدایی‌ترین حالت، کابل وارد خانه و به یک تلویزیون می‌رسد. برای خانه‌هایی که چند تلویزیون دارند، سیگنال باید میان تلویزیون‌ها تقسیم شود. تقسیم معمولاً با یک دستگاه ارزان قیمت انجام می‌شود که معمولاً به آن تقسیم‌کننده می‌گویند. اسپلیتر نیازی به برق ندارد. معمولاً یک ورودی واحد دارد و ممکن است دو، سه، چهار یا بیشتر خروجی داشته باشد.

یکی از مشکلات این نوع شبکه غیرفعال از دست دادن قدرت سیگنال است. وقتی سیگنال ارائه‌دهنده کابل تقسیم می‌شود و به چند تلویزیون منتقل می‌شود، قدرت سیگنال هر تلویزیون کاهش می‌یابد. افزودن بیش از حد تلویزیون‌ها می‌تواند قدرت سیگنال را کاهش دهد.

در چنین شرایطی کاربران مجبور هستند از شبکه فعال catv استفاده کنند. شبکه فعال مسی نیز انواع مختلفی دارد. همان‌گونه که در مثال قبل به آن اشاره کردیم در مدل یک شبکه غیرفعال catv خانگی، وقتی تعداد تجهیزات زیاد می‌شود و قدرت سیگنال کاهش پیدا می‌کند کاربران به سراغ شبکه فعال می‌روند. در این حالت یک کابل وارد خانه می‌شود و به آمپلی‌فایر (تقویت‌کننده) هدایت می‌شود. تقویت‌کننده، سیگنال کابل را تقویت و سپس تقسیم می‌کند. قدرت سیگنال در هر خروجی آمپلی‌فایر تقریباً با قدرت سیگنال کابل ورودی یکسان است.

بدین ترتیب مشکل قدرت سیگنال در شبکه غیرفعال حل می‌شود، اما پیچیدگی را افزایش می‌دهد. علاوه بر این، اگر آمپلی‌فایر توزیع‌کننده خراب شود، همه تجهیزات سیگنال‌های خود را از دست می‌دهند. شبکه فعال و غیرفعال هر کدام مزایای خود را دارند.

تفاوت شبکه فعال و غیرفعال

در قسمت قبل دیدیم شبکه فعال و غیرفعال چیست حال به بیان تفاوت این دو شبکه می‌پردازیم. نوع شبکه در بررسی تفاوت شبکه فعال و غیرفعال نقش مهمی دارد. شبکه اکتیو مسی یکی از انواع اصلی است که دسته‌بندی‌های مختلفی دارد. تفاوتی که میان شبکه فعال مسی و غیرفعال مسی وجود دارد این است که برخی تجهیزات، همچون آمپلی‌فایر به منظور تقویت سیگنال‌های آسیب دیده استفاده می‌شود و این اطمینان را می‌دهد که سیگنال‌ها می‌توانند تا مسافت‌های طولانی منتقل شود.

ساختار شبکه‌های فعال مسی پیچیده‌تر از شبکه‌های غیرفعال است و بدون استفاده از تجهیزات فعال غیر قابل استفاده است. شبکه غیرفعال نوری یکی دیگر از انواع غیرفعال شبکه‌ها است و شباهت زیادی با شبکه غیرفعال مسی دارد، با این تفاوت که در این شبکه‌ها، به جای کابل‌های شبکه مثل کواکسیال از کابل‌های نوری استفاده می‌شود. در این نوع شبکه، کوپلر نقش کلیدی دارد و وظیفه آن، توزیع و جفت سیگنال‌های نوری است. البته در شبکه‌های غیرفعال نوری می‌توان از اسپلیتر نوری برای توزیع سیگنال‌های نوری استفاده کرد.

نحوه نظارت بر شبکه جنبه دیگری از تفاوت شبکه فعال و غیرفعال را مشخص می‌کند. مانیتورینگ شبکه فعال synthetic monitoring نام دارد. در روش مذکور ترافیک آزمایشی به شبکه تزریق می‌شود تا خطاها یا مشکلات

درون شبکه شناسایی شوند. این روش در یافتن و گزارش داده‌های بلادرنگ مثل از دست دادن بسته، جیتر[۱۷]، زمان پاسخ پروتکل‌های http و https و غیره کمک می‌کند.
فرایند نظارت غیرفعال شبکه شامل ثبت و تجزیه و تحلیل ترافیک واقعی کاربران برای درک روندهای استفاده از شبکه است. در این حالت ابزار نظارتی می‌تواند به ردیابی این موضوع بپردازد که کدام عناصر شبکه پهنای باند موجود را مصرف می‌کنند. در این روش به جای تزریق داده‌های آزمایشی برای تجزیه و تحلیل ترافیک از داده‌های واقعی کاربران استفاده می‌شوند.

۸- فـــــایـــروال

مقدمه

اتصال به اینترنت بدون استفاده از یک فایروال همانند گذاشتن سوئیچ در اتومبیل، قفل نکردن درب های آن و رفتن به یک فروشگاه برای تهیه لوازم مورد نیاز است.با اینکه ممکن است بتوانید در صورت سرقت اتومبیل سریعا

[۱۷] jitter

واکنش مناسبی را انجام دهید، ولی فرصت ارزشمندی را برای سارقین ایجاد نموده اید تا آنان بتوانند در سریع ترین زمان ممکن به اهداف مخرب خود دست یابند.چنین وضعیتی در اینترنت نیز وجود دارد و مهاجمان در ابتدا با استفاده از کدهای مخربی نظیر ویروس ها، کرم ها و تروجان ها اقدام به شناسائی قربانیان خود می‌نمایند و در مرحله بعد، اهداف شناسایی شده را مورد تهاجم قرار می دهند. برنامه های فایروال یک سطح حفاظتی و امنیتی مناسب در مقابل این نوع حملات را ارائه می نمایند.

در حقیقت فایروال، دیواری بین کامپیوتر شما و اینترنت است. فایروال به شما اجازه می‌دهد صفحات وب را ببینید و به آنها دسترسی داشته باشید، فایل دانلود کنید، چت کنید و..... در حالیکه مطمئن هستید افراد دیگری که در اینترنت مشغول هستند نمی‌توانند به کامپیوتر شما دست درازی کنند. بعضی از فایروال ها نرم ا فزارهایی هستند که روی کامپیوتر اجرا می شوند اما فایروال های دیگر به صورت سخت افزاری ساخته شده اند و کل شبکه را از حمله مصون می کنند.

فایروال یا دیوارآتش نام عمومی برنامه هایی است که از دستیابی غیر مجاز به یک سیستم رایانه جلوگیری می‌کنند. دربرخی از این نرم افزارها ، برنامه ها بدون اخذ مجوز قادر نخواهند بود از یک رایانه برای سایر رایانه ها داده ارسال کنند. به این گونه نرم افزارها ،دیوار آتش دو طرفه گویند، زیرا علاوه بر درگاه ورود ،درگاه های خروجی هم کنترل می شوند. بسته های اطلاعاتی که حاوی اطلاعات بدون مجوز هستند، به وسیله دیوار آتش متوقف می شوند.

تاریخچه فایروال

هنگام بررسی تاریخچه فایروال با یکدیگر تکنولوژی‌ها، پی می‌بریم که تکتولوژی نوجوان و تازه وارد است. اولین نسل معماری فایروال ها که فایروال فیلتر شده بسته ای نامیده می شد در سال۱۹۸۵ توسط شبکه ی عظیم سیسکو به وجود آمد.

سه سال بعد اولین صفحه ی فایروال با موفقیت ایجاد شد که مؤسس آن جف موگل از شرکت تجهیزات دیجیتالیDEC بود. با این وجود در طول این سه سال دیو پرستو و هاوارد تری کی ار شرکت AT&T Bell Laboratories در حال توسعه ی نسل دوم فایروال ها یعنی فایروال های دوره ای بودند. کار آنها یک دهه طول کشید، در سال ۱۹۸۰ شروع و در سال ۱۹۹۰ به سرانجام رسید.

در سال های ۱۹۹۰ و ۱۹۹۱، بیل چسویک و مارکوس رانوم ژن اسپافورد صفحاتی را که نسل سوم فایروال ها یعنی فایروال‌های لایه ای را توصیف می‌کرد، منتشر کردند این نوع فایروال ، فایروال مبتنی بر پروکسی نیز نامیده می‌شد. این گروه سه نفری هر یک به تنهایی نسل سوم را توسعه دادند و در پایان رانوم موفقیت بیشتری بدست بیاورد.

در سال ۱۹۹۱ شرکتDEC اولین فایروال تجاری را منتشر کرد و نام محصول را "SEAL" گذاشت SEAL بر اساس کار های مارکوس رانوم ساخته شده بود. در سال بعد از باب باردن و آنت دشولان از دانشگاه کالیفرنیای جنوبی شروع به توسعه نسل چهارم فایروال ها کردند که ویزاس نامیده می شد. این سیستم دارای اولین یکپارچگی مجازی و دارای رنگ ها و آیکون هایی بود . ویزاس اولین نوع فایروال های تجاری بود که در سال ۱۹۹۴ توسط شرکت اسرائیلی چک پینت منتشر شد. در سال ۱۹۹۶ اسکات ویگل از شرکت نرم افزار های جهانی اینترنت شروع به کار بر روی نسل پنجم فایروال ها کرد که معماری با کرنل پروکسی نامیده می شد. شرکت سیسکو اولین فایروال بر مبنای این تکنولوژی را ایجاد کرد و سپس منتشر کرد . در حال حاضر این صنعت در حال دیدن یک همگرایی در تکنولوژی فایروال ها و ضد نفوذگر ها است.

فایروال چیست؟

تصویری از دیوار آتش

" اساساً یک فایروال سدی است برای دور نگهداشتن نیروهای مخرب از دارائی شما. در حقیقت علت اینکه فایروال نامیده می شود همین است. کار آن مشابه فایروال فیزیکی است که از گسترش آتش از یک ناحیه به ناحیه دیگر است ممانعت به عمل می آورد.

تعریف فوق، تعریف ساده و عامیانه ای از فایروال است. در حقیقت تا چند سال پیش فقط کسانی که در بانک ها، مشاغل تجاری بزرگ و دوایر دولتی کار می کردن، از فایروال ها استفاده می نمودند. اما زمانه به کلی تغییر کرده است. امروزه داشتن یک فایروال خوب به اندازه داشتن ضد ویروس قوی، مسئله امنیتی مهمی حساب می شود. فایروال یک معیار امنیتی است که یک کامپیوتر تنها و یا کامپیوتر های موجود در یک شبکه را از دسترسی غیر مجاز حفظ می کند. متاسفانه در دنیای امروز کامپیوتری،تعداد زیادی هکر وجود دارد که با نفوذ به داخل کامپیوتر ها سعی در ربودن اطلاعات مهم می کنند. هر چند که تا دیروز هدف هکر ها حمله به شرکت های بزرگ بود اما هکر های امروزی علاقمند به دزدیدن اطلاعات از کامپیوترهای کوچک هم هستند..

فایر وال می تواند یک دستگاه سخت افزاری و یا یک برنامه نرم افزای و یا ترکیبی از هر دو باشد که در ادامه هر یک از آن ها توضیح داده می شود.

در حقیقت یک فایروال خوب می تواند جلوی دسترسی هکر ها بداخل کامپیوتر را بگیرد..در ضمن نمی گذارد هیچ گونه اطلاعاتی بدون اجازه کاربر از کامپیوترتان خارج شود. فایروال نمی تواند مستقیماً جلوی حمله ویروس ها را بگیرد اما گاهی جلوی ویروس ها را برای ارسال ایمیل از یک کامپیوتر آلوده می گیرد.

در نتیجه در یک تعریف کلی، می توان فایروال را این چنین تعریف کرد:

فایروال وسیله ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف می کند. علاوه بر آن از آنجایی که معمولا یک فایروال بر سر راه ورودی یک شبکه می نشیند لذا برای ترجمه آدرس شبکه نیز بکار گرفته می شود.

امکانات:

یکی از استفاده های معمول فایروال واگذاری اختیار ویژه به گروهی خاص از کاربران جهت استفاده از یک منبع بوده، وهمچنین بازداشتن کسانی که از خارج از گروه خواهان دسترسی به منبع هستند می باشد. استفاده دیگر فایروال جلوگیری از ارتباط مستقیم یک سری از رایانه ها با دنیای خارج می باشد .هرچند فایروال بخش مهمی از سیستم امنیتی را تشکیل می دهد ولی طراحان به این نکته نیز توجه میورزند که اکثر حملات از درون شبکه می آیند و نه از بیرون آن نمایش شماتیک یک سرویس دهنده پروکسی ،در اینجا کامپیوتر وسط مثل پروکسی بین دو رایانه دیگر عمل می کند.

نحوه عملکرد بسیاری از سیستم های فایروال اینگونه است تمامی ارتباطات از طریق یک سرویس دهنده پروکسی به سمت فایروال هدایت شده و همین سرویس دهنده درباره امن بودن یا نبودن عبور یک پیام یا یک فایل از طریق شبکه تصمیم گیری می کنداین سیستم امنیتی معمولا ترکیبی از سخت افزار و نرم افزار است. با توجه به ضرورتهای استاندارد فایروالها جزء لاینفک شبکه های کامپیوتری قرار گرفته اند و یکی از دغدغه های اصلی مسئولین شبکه شده اند ، دراین میان با توجه به حساسیت هر سازمان لایه بندی و قدرت فایروال‌ها در نظر گرفته می شود.

مثلا در بانک‌ها همواره دقت بسیاری را در این ارتباط به خرج می دهند. برخی از شرکتهای بزرگ که در این ارتباط با مهمترین بانک‌های بین المللی همکاری دارند عبارتند از : cisco، juniper،secure point و...

فایروال چه کار می کند ؟

فایروال ها حفاظت لازم در مقابل مهاجمان خارجی را ایجاد و یک لایه و یا پوسته حفاظتی پیرامون کامپیوتر و یا شبکه را در مقابل کدهای مخرب و یا ترافیک غیرضروری اینترنت ، ارائه می نمایند . با بکارگیری فایروال ها ، امکان بلاک نمودن داده از مکانی خاص فراهم می گردد . امکانات ارائه شده توسط یک فایروال برای کاربرانی که همواره به اینترنت متصل و از امکاناتی نظیر DSL و یا مودم های کابلی استفاده می نمایند ، بسیار حیاتی و مهم می باشد.حال که فهمیدیم فایر وال چه کاری می‌کند، بهتر است به نحوه کار آن بپردازیم. داده‌ها در یک ارتباط شبکه‌ای (چه اینترنت باشد چه یک شبکه محلی) در رفت و برگشت از محلی به نام دروازه (Gateway) عبور می‌کنند. فایروال‌ها برای بالاترین امنیت ممکن، در این قسمت قرار می‌گیرند. اگر مقیاس را کوچک تر کرده و یک کامپیوتر مستقل را در نظر بگیرید، فایروال درست بعد از درایور کارت شبکه قرار می‌گیرد بنابراین در هر دو حالت، همه داده‌های ورودی و خروجی از فایروال باید بگذرند. فایروال‌ها طبق معیارهایی (که به آن‌ها Rule گفته می‌شود) که برای آن تعیین می‌شود داده‌ها را فیلتر می‌کنند. برای درک بهتر یک دربان کنفرانسی را در نظر بگیرید. این دربان طبق لیستی که دارد (همان معیارهای فایروال) به اشخاص دارای مجوز امکان ورود را می‌دهد و از ورود سایر افراد غیرمجاز به کنفرانس جلوگیری می‌کند. فایروال نیز مانند همین دربان کار می‌کند یعنی داده‌های ورودی و خروجی را با لیست Rule های خود مطابقت داده و آن‌هایی که اجازه گذشتن از فایروال را دارند، عبور می‌دهد (Allow کند) یا آن‌ها را عبور ندهد (Deny کند).از جمله Rule های فایروال می‌توان به باز بودن یا بسته بودن یک درگاه (پورت – Port)، اجازه داشتن یک برنامه خاص برای ارتباط با شبکه، محدود کردن یا آزاد کردن پروتکل‌ها (مانند HTTP یا FTP)، مقایسه کردن بسته‌های داده با محتوای مشخص و . . . .

تصویری نمادین از دیوار آتش

اگر شما یک کاربر اینترنت هستید یا در خانه و محل کار خود در وب ، گشت و گذار می کنید احتمالا بارها و بارها کلمه firewall یا دیواره آتش را شنیده اید؛ البته بحث فایروال به ارتباط تلفنی Dial-up مربوط نیست و کسانی که احتمالا مودم های کابلی و ارتباط از نوع DSL دارند، از فایروال استفاده بیشتری می برند. در حقیقت این برنامه ، شبکه های کوچک خانگی و شبکه های بزرگ شرکتی را از حملات احتمالی هکرها و وب سایت های نامناسب و خطرناک حفظ می کند و مانع و سدی است که متعلقات و دارایی های شما را از دسترس نیروهای نفوذی دور نگاه می دارد و به همین دلیل است که فایروال دیوار آتش خوانده می شود. چون فایروال های فیزیکی هم حوزه آتش را محدود می کنند و مانع گسترش آن به نواحی دیگر می شوند. به طور کلی فایروال یک برنامه یا وسیله سخت افزاری است که اطلاعات ورودی به سیستم رایانه و شبکه های اختصاصی را تصفیه یا به اصطلاح فیلتر می کند. اگر یک بسته اطلاعاتی ورودی به وسیله فیلترها نشان دار شود، اجازه ورود به شبکه و رایانه کاربر را نخواهد داشت.

به عنوان مثال در یک شرکت بزرگ ، بیش از ۱۰۰ رایانه وجود دارد که با کارت شبکه به یکدیگر متصل هستند. این شبکه داخلی به وسیله یک یا چند خط ویژه به اینترنت متصل است.بدون استفاده از یک فایروال تمام رایانه ها و اطلاعات موجود در این شبکه برای شخص خارج از شبکه قابل دسترس است و اگر این شخص راه خود را بشناسد می تواند تک تک رایانه ها را بررسی و با آنها ارتباط هوشمند برقرار کند. در این حالت اگر یک کارمند خطایی انجام دهد و یک سوراخ امنیتی ایجاد شود، هکرها می توانند وارد سیستم شوند و از این سوراخ سوئاستفاده کنند؛ اما با داشتن یک فایروال همه چیز متفاوت خواهد بود.

فایروال ها روی خطوطی که ارتباط اینترنتی برقرار می کنند، نصب می شوند و از یک سری قانون های امنیتی پیروی می کنند. به عنوان مثال یکی از قانون های امنیتی شرکت می تواند به این ترتیب باشد، از تمام ۵۰۰ رایانه موجود در شرکت فقط یکی اجازه دریافت صفحات FTP را دارد و فایروال باید مانع ارتباط دیگر رایانه ها از طریق FTP شود. این شرکت می تواند برای وب سرورها و سرورهای هوشمند و... همچنین قوانینی در نظر بگیرد. علاوه بر این شرکت می تواند شیوه اتصال کاربران و کارمندان به شبکه اینترنت را هم کنترل کند؛ به عنوان مثال اجازه

ارسال فایل از شبکه به خارج را ندهد. درحقیقت با استفاده از فایروال یک شرکت می تواند شیوه استفاده از اینترنت را تعیین کند.

فایروال ها برای کنترل جریان عبوری در شبکه ها از ۳ روش استفاده می کنند:

۱) Packet Filtering: تک تک بسته های اطلاعاتی با توجه به فیلترهای تعیین شده مورد تحلیل و ارزیابی قرار می گیرند. بسته هایی که از تمام فیلترها عبور می کنند به سیستم های مورد نیاز فرستاده و بقیه بسته رد می شوند.

۲) Proxy Service: اطلاعات موجود در اینترنت به وسیله فایروال اصلاح و سپس به سیستم فرستاده می شود و بلعکس.

۳) Stateful inspection: در این روش جدید محتوای هر بسته با بسته های اطلاعاتی ویژه ای از اطلاعات مورد اطمینان مقایسه می شوند، اطلاعاتی که باید از اردل فایروال به بیرون فرستاده شوند، با اطلاعاتی که از بیرون به اردل ارسال می شود از لحاظ داشتن خصوصیات ویژه مقایسه می شوند و در صورتی که با یکدیگر ارتباط منطقی داشتند. اجازه عبور به آنها داده می شود، در غیر این صورت امکان مبادله اطلاعات فراهم نمی شود.

مشخصه های مهم یک فایروال:

همانطور که گفته شد، فایروال سیستمی است که در بین کاربران یک شبکه محلی و شبکه جهانی قرار می گیرد و ضمن نظارت بر دسترسی ها در تمام سطوح ورود و خروج اطلاعات را تحت نظر دارد. در این ساختار هر سازمان یا نهادی که بخواهد ورود و خروج اطلاعات را کنترل کند موظف است تمام ارتباطات مستقیم شبکه داخلی خود را با دنیای خارج قطع کرده و هرگونه ارتباط خارجی از طریق یک دروازه که دیوار آتش یا فیلتر نام دارد انجام شود. بدیهی است هرچه این فیلتر قوی تر باشد حفاظت کامپیوتر بهتر خواهد بود. مشخصه های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

۱) توانایی ثبت و اخطار

ثبت وقایع یکی از مشخصه های بسیار مهم یک فایروال به شمار می رود و به مدیروان شبکه این امکان را می دهد که انجام حملات را کنترل کنند. هم چنین مدیر شبکه می تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می تواند به راحتی به بخش های مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

۲) بازدید حجم بالایی از بسته های اطلاعات

یکی از تست های فایروال، توانایی آن در بازدید حجم بالایی از بسته های اطلاعاتی بدون کاهش چشم گیر کارایی شبکه است. حجم داده ای که یک فایروال می تواند کنترل کند برای شبکه های مختلف متفاوت است اما یک

فایروال قطعاً نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود. عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیت ها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر کارایی فایروال تحمیل می شوند. عامل محدود کننده دیگر می تواند کارت های واسطی باشد که بر روی فایروال نصب می شوند. فایروالی که بعضی کارها مانند صدور اخطار، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم افزار های دیگر می سپارد از سرعت و کارایی بیشتر و بهتر برخوردار است.

۳) سادگی پیکربندی

سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها مشکلات است.در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه ها می شود به پیکربندی غلط فایروال بر می گردد. لذا پیکربندی سریع و ساده یک فایروال، امکان بروز خطا را کم می کند. برای مثال امکان نمایش گرافیکی معماری شبکه و بپیا ابزاری که بتواند سیاست های امنیتی را به پیکربندی ترجمه کند ، برای یک فایروال بسیار مهم است.

۴) امنیت و افزونگی فایروال

امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است. فایروالی که نتواند امنیت خود را تامین کند، قطعاً اجازه ورود هکرها و مهاجمان را به سایر بخش های شبکه نیز خواهد داد. **امنیت در دو بخش از فایروال،** تامین کننده امنیت فایروال و شبکه است:

a) امنیت سیستم عامل فایروال:

اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار می کند، نقاط ضعف امنیتی سیستم عامل،می تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابر این امنیت و استحکام سیستم عامل فایروال و بروز رسانی آن از نکات مهم در امنیت فایروال است.

b) دسترسی امن به فایروال جهت مقاصد مدیریتی:

یک فایروال باید مکانیزم های امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روش ها می تواند رمزنگاری را همراه با روش های مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذ گران تاب بیاورد.

انواع فایروال

فایروال یکی از اولین خطوط دفاع در یک شبکه است . انواع مختلف فایروال وجود دارند و این موارد می توانند به صورت سیستم های مستقل باشند یا به صورت تعبیه شده در دیگر دیوایس ها باشند مثلا داخل روترها یا سرورها. شما می توانید فایروال هایی را پیدا کنید که فقط سخت افزاری باشند و یا فقط نرم افزاری باشند. گرچه اکثر فایروال ها شامل نرم افزارهای افزونه‌ای هستند که برای سرورها و ورک استیشن ها در دسترس‌اند. هرچند در فایروال هایی که به عنوان فقط سخت افزاری شناخته می شوند کماکان بخش کوچکی از نرم افزار وجود دارد و این نرم افزار در حافظه Rom تعبیه شده تا از دستکاری حفظ شود .

هدف اولیه و اصلی یک فایروال ایزوله کردن و جداسازی یک شبکه از شبکه دیگر است. فایروال ها به عنوان (Appliances) تجهیزات اختصاصی در دسترس هستند به این معنی که به منظور جداسازی شبکه به

عنوان دیوایس اولیه نصب و راه اندازی می شوند. Appliances دیوایس های ساده ای هستند که به طور وسیع به تنهایی و مستقل عمل می کنند و نگهداری و پشتیبانی کمتری نسبت به محصولات شبکه محور دارند.
به منظور درک مفهوم یک فایروال بایستی بدانید که این واژه از کجا منشا گرفته است. در دوران قدیم خانه ها بسیار نزدیک به هم ساخته می شد به نحوی که اگر آتش در یک خانه شعله ور می شد , به راحتی بلوک بین دو خانه تخریب می شد . به منظور کاهش ریسک این اتفاق دیوارآتش یا همان فایروال بین دو ساختمان ساخته شد. فایروال دیوار خشتی بزرگی بود که دو ساختمان را از هم جدا می کرد و آتش را بین دو ساختمان جدا می کرد. همان مفهوم منع و محدود کردن در شبکه هم حقیقت پیدا می کند . ترافیکی که از دنیای خارج وارد می شود به فایروال برخورد می کند و فایروال اجازه ورود این ترافیک را به شبکه نمی دهد.
فایروال بطور واحد کار حفاظت از کامپیوتر و اطلاعات شخصی از نفوذگران را دارد، اما روش انجام کارتوسط انواع مختلف، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می شود. بر این اساس ۲ نوع دسته بندی را برای فایروال ها در نظر میگیریم.
در دسته بندی نخست، فایروال را به ۲ دسته نرم افزاری و سخت افزاری تقسیم می نماییم که در ذیل توضیح داده شده است. و در تقسیم بندی دیگر فایروال ها را به ۵ گروه تقسیم می کنیم. در ابتدا در مورد انواع نرم/ سخت افزاری این فیلتر صحبت می کنیم:

فایروال های سخت افزاری

این نوع از فایروال ها که به آنان فایروال های شبکه نیز گفته می شود ، بین کامپیوتر کاربر (و یا شبکه) و کابل و یا خطDSL قرار خواهند گرفت. فایروال های سخت افزاری در مواردی نظیر حفاظت چندین کامپیوتر مفید بوده و یک سطح مناسب حفاظتی را ارائه می نمایند در صورتی که شما صرفاً دارای یک کامپیوتر پشت فایروال می باشید و یا این اطمینان را دارید که سایر کامپیوترهای موجود بر روی شبکه نسبت به تمامیPatch ها، به هنگام بوده و عاری از ویروس ها و یا کرم ها می باشند ضرورتی به استفاده از یک سطح اضافه حفاظتی نخواهید داشت.
فایروال های سخت افزاری عموما ترافیک بین شبکه و اینترنت را کنترل کرده و نظارت خاصی ب روی ترافیک بین کامپیوتر های موجود در شبکه را انجام نخواهند داد. این نوع فایروال ها را می توان به صورت محصول جداگانه خریداری کرد اما معمولا ، به صورت تعبیه شده بر روی روتر های شبکه هستند.

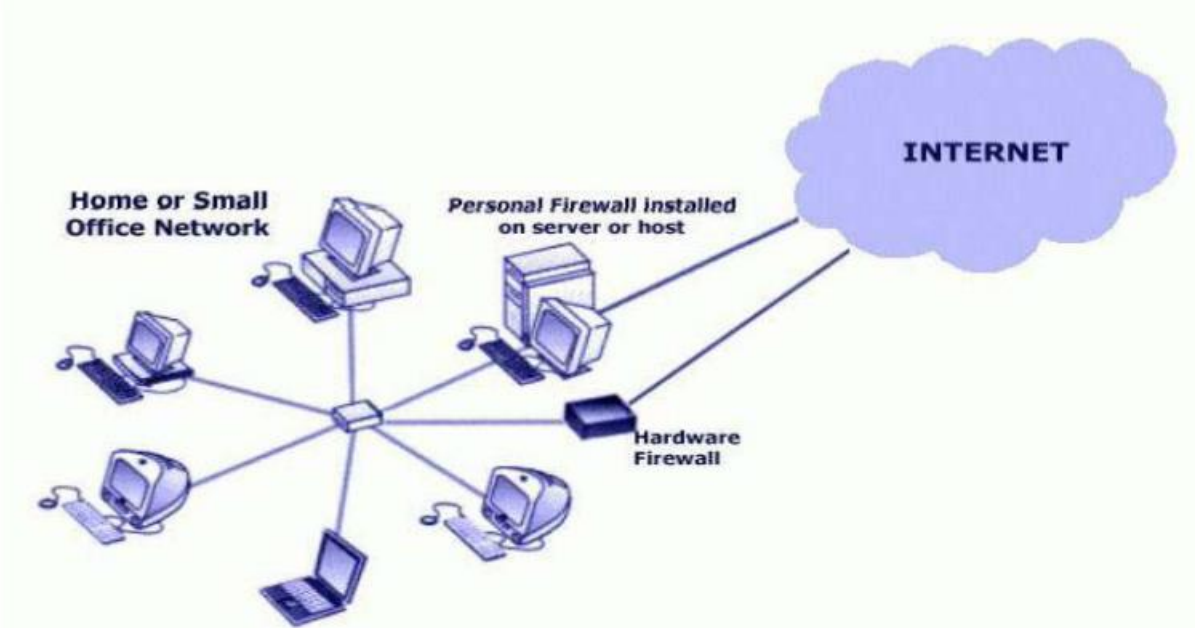
مزایای روترهای فایروال:

- ✓ معمولا دارای حداقل چهار پورت برای اتصال سایر کامپیوتر ها می باشند.
- ✓ امکان حفاظت چندین کامپیوتر را ارائه می نمایند.

معایب روتر های فایروال:

- ✓ کابل کشی اضافه که مسلماً هزینه ای اضافی را نیز در بردارد.

فایروال های سخت افزاری ، از تکنیک فیلتر کردن بسته ها برای تست هدر بسته ، جهت تعیین مقصد و مبدا استفاده می کنند. اطلاعات به دست آمده از این تست، با تنظیمات پیش فرض یا تنظیماتی که کاربر انجام داده است مقایسه و تصمیم گیری می شود که آیا بسته ارسال یا متوقف شود.



شکل۵-۱- محل قرارگیری فایروال سخت افزاری در شبکه

معمولا این نوع فایروال ها به علت داشتن سیستم عامل جدایی که دارند، در معرض خطر کمتری از طرف شبکه قرار می گیرند و می توان مانند یک نود در شبکه یا یکmini Computer به آن ها نگاه کرد.

۵ نکته کلیدی در مورد فایروال های سخت افزاری

۱) فایروال‌های سخت افزاری می‌توانند در روتر نیز گنجانده شوند. در صورت خرید چنین دستگاه‌هایی، بطور همزمان از قابلیت روتر و فایروال سخت افزاری بهره‌مند می‌شوید.

۲) از نظر فنی، یک سیستم کامپیوتری قابل حمل با نرم افزار فایروال نصب شده بر روی آن، می‌تواند به عنوان یک فایروال سخت افزاری عمل کند.

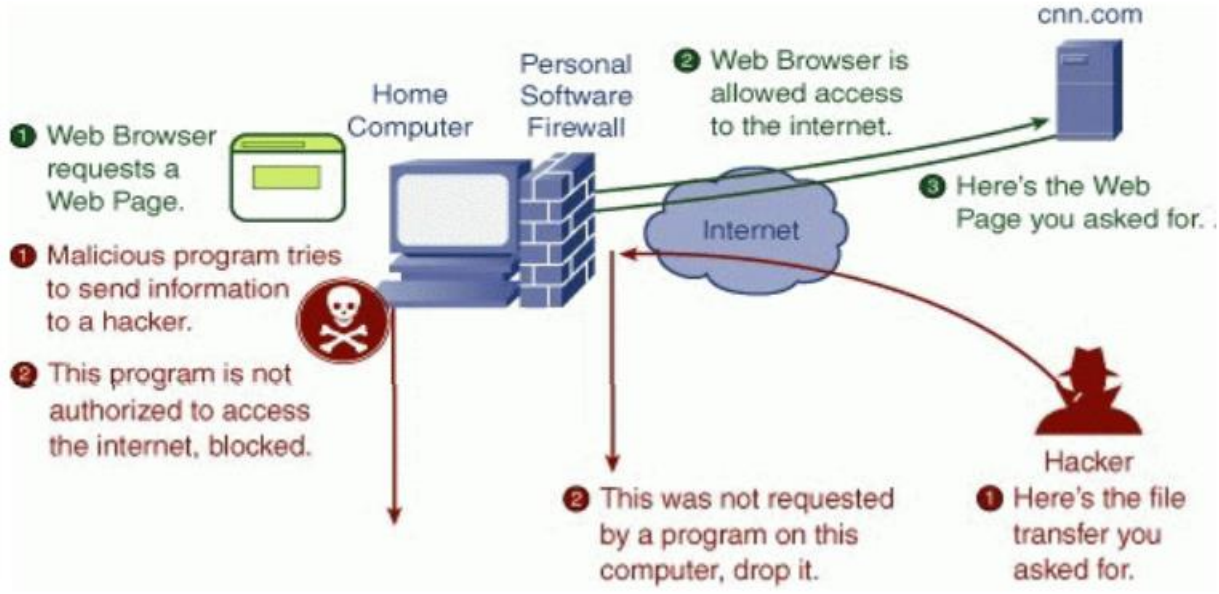
۳) فایروال‌های سخت افزاری اغلب برای ذخیره تنظیمات امنیتی، سازوکارهای اختصاصی و مسیریابی ترافیک با حافظه داخلی عرضه می‌شوند.

۴) بسته به اندازه شبکه، طیف گسترده‌ای از دستگاه‌های فایروال سخت افزاری وجود دارد. از دستگاه‌های کوچک رومیزی گرفته تا تجهیزات بزرگی که در اتاق‌های سرور قرار می‌گیرند.

۵) دو نوع فایروال وجود دارد، مستقل از وضعیت[۱۸] و وابسته به حالت سیستم[۱۹]. نوع دوم پیچیده‌تر بوده و برای اعمال تنظیمات بیشتر و سفارشی‌سازی شبکه مناسب‌تر است.

فایروال های نرم افزاری

برخی از سیستم های عامل دارای یک فایروال تعبیه شده درون خود می باشند. در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای ویژگی فوق می باشد، پیشنهاد می گردد که آن را فعال نموده تا یک سطح حفاظتی اضافی در خصوص ایمن سازی کامپیوتر و اطلاعات ایجاد گردد.(حتی اگر از یک فایروال خارجی یا سخت افزاری استفاده می نمایند.) در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال تعبیه شده نمی باشد، می توان اقدام به تهیه یک فایروال نرم افزاری کرد. با توجه به عدم اطمینان لازم در خصوص دریافت نرم افزار از اینترنت با استفاده از یک کامپیوتر محافظت شده، پیشنهاد می گردد. برای نصب فایروال از CD و یا DVD مربوطه استفاده گردد. در شکل زیر چگونگی کارکرد یک فایروال نرم افزاری را به صورت ساده بیان شده است.



شکل۶-۱- چگونگی کار یک فایروال نرم افزاری

این نوع فایروال ها، اغلب توسط کاربران خانگی که به صورت جدا از شبکه خاصی، به شبکه جهانی اینترنت متصل می شوند استفاده می شود. فایروال های نرم افزاری، ماند هر نرم افزار دیگری بر روی سیستم نصب و تنظیمات و

[۱۸] Stateless
[۱۹] Stateful

تعاریفی برای آن انجام می شود. این نوع فایروال ها، از هرگونه حمله به کامپیوتر شخصی جلوگیری می کنند و حتی با تنظیمات خاص این نرم افزار می توان جلوی حملات Trojan و کرم های E-mail را نیز گرفت و اجازه اجرای دوباره این برنامه ها را نمی دهد.

بعضی از بسته های فایروال های نرم افزاری،حاوی آنتی ویروس و آنتی اسپم نیز هستند. سوالی در اینجا مطرح است این است که چرا با وجود یک فایروال سخت افزاری باز هم نیاز به فایروال های نرم افزاری است!

در جواب این سوال E-mail Worms را مثال می زنیم. برای ارسال ایمیل، همانطور که می دانیم از پورت۲۵ یعنی SMTP استفاده می شود. زمانی که این ایمیل حاوی Worm نیز می باشد به فایروال سخت افزاری که معمولا در روتر شبکه تعبیه شده است می رسد به عنوان یک پورت صحیح عبور می کند. در ثانی فایروال های سخت افزاری تنها ترافیک کلی شبکه را در نظر دارند و به کاربر هشدار یا پیغامی مبتنی بر نفوذ و حمله به کامپیوتر شخصی وی را نمی دهند. در نتیجه پیشنهاد می شود از هر دو نوع فایروال استفاده شود.

در ادامه، مزایا و معایب استفاده از هر نوع فایروال مطرح می شود و سپس به مقایسه این دو می پردازیم.

مزایای استفاده از فایروال سخت افزای

- حفاظت بیشتر و کلی تری نسبت به فایروال های نرم افزاری دارند.
- کل شبکه را محافظت می کنند.
- تا زمانی که در سیستم اجرا نشده اند، هیچ تاثیری بر روی عملکرد سیستم ندارند.
- این نوع فایروال ها، به صورت مستقل از سیستم عامل و نرم افزار های سیستم عامل عمل می کند و دارای سیستم عامل جدایی هستند.

معایب استفاده از فایروال سخت افزاری

- ✓ هزینه بیشتری نسبت به فایروال های نرم افزاری دارند. حتی با وجود اینکه به نظر خرید یک فایروال سخت افزاری کم هزینه تر از خرید چند فایروال نرم افزاری در یک شبکه بزرگ است.
- ✓ جاگیر و کابل کشی پیچیده دارد.
- ✓ فایروال های سخت افزاری، با مودم های Dial up کار نمی کنند.
- ✓ نصب و upgrade کردن آن دشوار است.

مزایای استفاده از فایروال نرم افزاری

- ✓ این نوع فایروال ها،برای کامپیوترهای شخصی استفاده می شوند و در نتیجه بر روی هر سیستم عاملی کار می کنند.
- ✓ به صورت مستقل و جداگانه و کامل قابل نصب هستند و نیاز به بسته یا دستور خاصی ندارند.
- ✓ معمولا همراه بسته نرم افزاری آن، آنتی ویروس و آنتی اسپم هم هست.
- ✓ به راحتی upgrade می شوند.

معایب استفاده از فایروال نرم افزاری

- ✓ برای هر کامپیوتر موجود در شبکه،نیاز به نصب جداگانه ای دارد در نتیجه زمان بر است.
- ✓ گاهیun-install کردن کامل آن دشوار است.
- ✓ در زمانی که زمان پاسخ گویی سیستم بحرانی و مهم است،مناسب نیستند.
- ✓ اشغال کردن فضایCPU و Memory

برتری فایروال سخت افزاری به فایروال نرم افزاری

- ✓ **سرعت**: فایروال های سخت افزاری برای پاسخ گویی سریعتر طراحی شده اند و از این رو در کنترل بار ترافیکی شبکه و جایی که زمان پاسخ گویی اهمیت دارد استفاده می شوند.
- ✓ **امنیت**: فایروال های سخت افزاری به دلیل داشتن سیستم عامل جدا، کمتر از فایروال های نرم افزاری در معرض توجه نفوذگران قرار می گیرند. از طرفی دارای کنترل کننده های بسیار قوی است.
- ✓ **بدون مداخله**: این فایروال، به دلیل جدا بودن از نودهای شبکه مدیریت بهتر و آسان تری دارد و تاثیری بر کند یا تند کردن بقیه قسمت ها ندارد. به راحتی و جدا از سیستم می تواند خاموش، یا دوباره نصب شود بدون هیچ تداخلی در شبکه.

برتری فایروال های نرم افزاری به فایروال سخت افزاری

- ✓ **هزینه:** هزینه کمتری نسبت به فایروال های سخت افزاری دارد.
- ✓ جاگیر نیست و هیچ گونه کابل کشی ندارد.
- ✓ با مودم های dialup نیز کار می کند.
- ✓ نصب و راه اندازی آن نیاز به دانش خاصی ندارد.

تفاوت فایروال های سخت افزاری و نرم افزاری

نرم افزارهای فایروال معمولا رایج‌تر از فایروال‌های سخت افزاری هستند. زیرا این نرم افزارها رابط کاربری جذاب‌تری داشته و در عین حال کار با آن‌ها آسان‌تر است.

برخی از سازمان‌ها نیز اقدام به ایجاد نرم افزارهای فایروال تخصصی بر اساس نیازهای خود می‌کنند تا کنترل بیشتری روی ترافیک داده‌های ورودی داشته باشند. قطعا این کار پیچیدگی کمتری نسبت به ساخت یک دستگاه فایروال سخت افزاری سفارشی خواهد داشت.

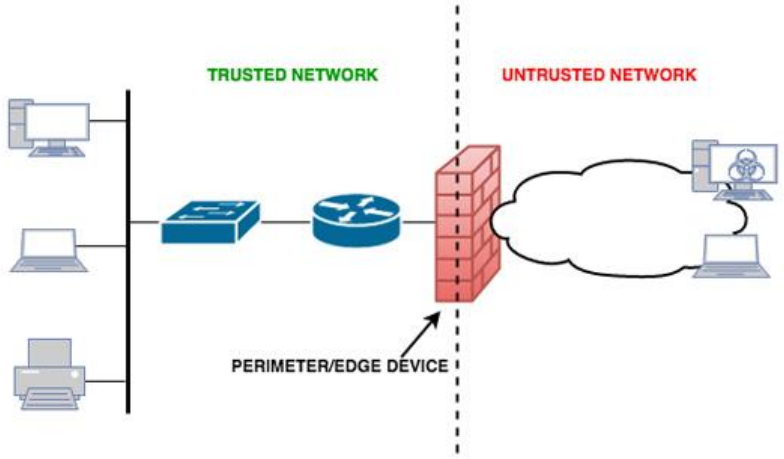
نکته جالب اینجاست که نرم افزار فایروال نمی‌تواند جایگزین مستقیمی برای فایروال‌های سخت افزاری باشد. این دو با هم تفاوت‌هایی دارند:

	فایروال سخت افزاری	نرم افزار فایروال
چه چیزی را فیلتر می‌کند؟	جریان ترافیک را از آپ‌لینک به سمت آخرین تجهیزات شبکه (معمولا سیستم کامپیوتری)	ترافیکی را که قبلا از آپ‌لینک به آخرین تجهیزات در شبکه (معمولا سیستم

	هدایت کرده و همزمان آن را طبق تنظیمات اعمال شده فیلتر می‌کند.	کامپیوتری) منتقل شده، اما هنوز توسط کاربر قابل دسترسی نیست را فیلتر می‌کند.
چگونه منابع محاسباتی خود را بدست می‌آورد؟	دارای حافظه رم و ذخیره سازی داخلی است تا تنظیمات مورد نظر را ذخیره و اعمال کند.	قدرت محاسباتی خود را از سیستم کامپیوتری کاربر دریافت می‌کند.
ادغام آن با دیگر تجهیزات شبکه آسان است؟	بله، می‌توانید فایروال سخت افزاری را با سایر تجهیزات زیرساخت شبکه مانند SEIM یا مرکز عملیات امنیتی شبکه (SOC) یکپارچه کنید.	بله، پلتفرم‌های نرم افزاری فایروال بطور پیش‌فرض، به صورت یکپارچه با برخی از برنامه‌های رایج، به بازار عرضه می‌شوند.
پوشش دهی آن چگونه است؟	بسته به نوع فایروال سخت افزاری، می‌توانید از هر شبکه‌ای محافظت کنید) از سرورهای سازمانی گرفته تا دستگاه‌های IoT خانگی.(	بطور مستقیم تنها از سیستمی که روی آن نصب شده محافظت کرده و بطور غیرمستقیم از سایر سیستم‌های موجود در همان شبکه نیز محافظت می‌کند.
هزینه آن چقدر است؟	فایروال‌های سخت افزاری می‌توانند از چند صد هزار تومان برای دستگاه‌های خانگی تا چندین میلیون تومان برای دستگاه‌های سازمانی را شامل شوند.	نرم افزارهای فایروال از ابزارهای رایگان و متن باز تا اپلیکیشن‌های پولی حرفه‌ای را شامل می‌شوند.
برای چه شرایطی مناسب‌تر است؟	در وهله اول از ورود ترافیک مخرب یا ناخواسته به سیستم جلوگیری کرده و در صورت نیاز جریان داده را در آپ‌لینک متوقف می‌کند. این دستگاه‌های برای سرورهای سازمانی، اینترنت اشیاء (IoT) و سایر سیستم‌هایی که نمی‌توانید ترافیک اینترنت یا تاثیرات آن را در لحظه بررسی کنید، حیاتی است.	به عنوان خط دوم دفاعی در امنیت شبکه عمل کرده و از ایجاد خرابی بیش از حد توسط ترافیک مخرب جلوگیری می‌کند. استفاده از آن در هوش مصنوعی، Machine Learningو دیگر راهکارهای پیچیده تحلیل داده جهت کشف تهدیدات مناسب است.

همانطور که می‌بینید، هم فایروال‌های سخت افزاری و هم نرم افزارهای فایروال، نقش مهمی در تضمین امنیت سازمانی دارند.

همانطور که اشاره کردیم نوع دیگری تقسیم بندی فایروال ها را نیز داریم که در این تقسیم بندی، فایروال به ۵ دسته تقسیم می شوند. این تقسیم بندی براساس کارکرد و سطح امنیتی فایروال در نظر گرفته شده است:

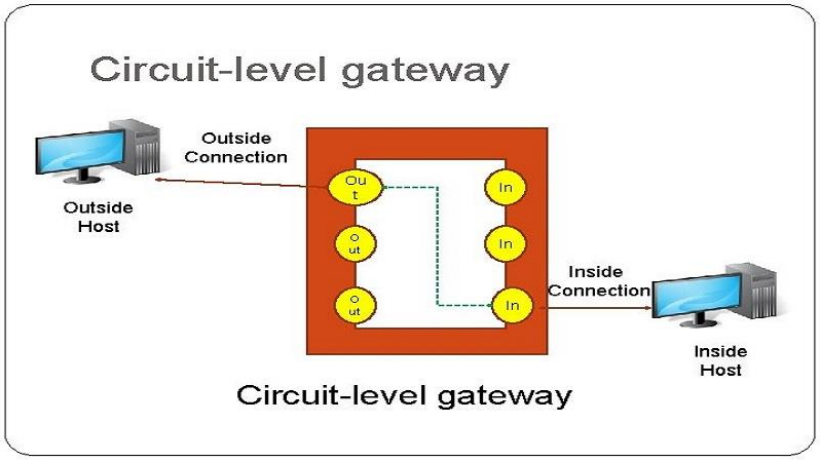


۱) فایروال‌های سطح مدار[۲۰]
۲) فایروال‌های پروکسی سرور
۳) فیلترهایNosstateful packet
۴) فیلترهایStateful Packet
۵) فایروال‌های شخصی

فایروال های سطح مدار

این فایروال ها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند. تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از فایروال ها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی‌دهند و لذا سرعت خوبی دارند. ضمناً امکان ایجاد محدودیت بر روی سایر پروتکل ها (غیر از TCP) را نیز نمی‌دهند.

[۲۰] Circuit-Level

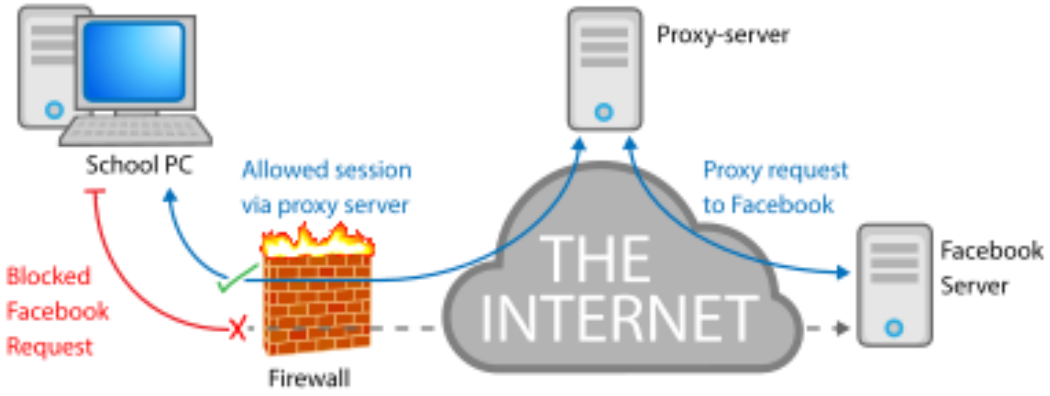


شکل۷-۱- نحوه کار فایروال های سطح مدار

فایروالی که در شکل زیر نمایش داده شده است به طور موثر دسترسی از دنیای خارج به شبکه ها را محدود می کند . در عین حال کاربران داخل شبکه می توانند به منابع خارج از شبکه دسترسی داشته باشند . همچنین در این شکل فایروال نقش یک پروکسی را ایفا می کند.

فایروال های پروکسی سرور

شاید تا کنون بارها در هنگام استفاده از اینترنت با کلمه پراکسی برخورد داشته‌اید اما مفهوم کاملی از آن در ذهن نداشته باشید. برخی از کاربران عادی پراکسی سرور را فقط به معنای سیستم [[فیلترینگ]] می‌شناسند در صورتی‌که چنین دیدگاهی اشتباه است و پراکسی سرور قابلیت‌های فراوانی دارد که در ادامه به آن اشاره خواهد شد. فلسفه ایجاد پراکسی سرور قرار دادن یک خط اینترنت در اختیار تعداد بیش از یک نفر استفاده‌کننده در یک شبکه بوده‌است اما بعدها قابلیت‌هایی به پراکسی سرور اضافه شد به طوری‌که هم اکنون استفاده از این قابلیت‌ها در شبکه سازمان‌های مختلف اجتناب ناپذیر است.!



شکل۸-۱- شکل فایروال در نقش یک پروکسی

فایروال های پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند. نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروال ها پروتکل های سطح کاربرد را می شناسند، لذا می توانند بر مبنای این پروتکل ها محدودیت هایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیت های لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروال ها بی انجامد. همچنین از آنجایی که این فایروال ها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرور ها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتواند این فایروال ها را به کار بگیرد. هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

پراکسی یا پراکسی سرور برنامه واسطه‌ای بین کاربر داخلی شبکه و اینترنت است که قابلیت‌های فراوانی در راستای حفظ امنیت، نظارت مدیریتی، کنترل کاربران و سرویس‌های ذخیره‌سازی دارد. پراکسی سرور امکان ایجاد فیلترهایی خاص را برای امنیت بیشتر در شبکه فراهم می‌کند، قابلیت ذخیره‌سازی، سرعت دستیابی به اطلاعات را بالا می‌برد و با سیستم‌های تصدیق هویت و تغییر هویت، ضامن امنیت در شبکه داخلی سازمان است و نیز امکان ثبت گزارش کامل کارکردش را دارد. همچنین قابلیت مسدود کردن محتویات آسیب‌رسان و بررسی تبعیت از قوانین برقرار شده در شبکه را دارا می‌باشد. پراکسی سرور امکان استفاده از اکثر پروتکل‌های محلی را فراهم می‌آورد و امکان رمز کردن داده‌ها را نیز دارد. پراکسی‌ها انواع مختلفی دارند که هر یک کار خاصی را انجام می‌دهد، که از آن جمله می‌توان FTP، HTTP، SMTP و DNS را نام برد.

پراکسی چیست؟

پراکسی سرور واسطه‌ای بین کاربر داخلی و اینترنت است. در حقیقت پراکسی در خواست کلاینت (client)را به پراکسی سرور فرستاده، پراکسی سرور محتویات بسته را بررسی می‌کند و در صورت لزوم پردازش‌های مورد نظر را روی بسته دیتا انجام می‌دهد و بسته را می‌سنجد، در صورت عدم مغایرت با سیاست‌های امنیتی تنظیم شده برای شبکه به آن‌ها اجازه عبور از فایروال را می‌دهد و این درخواست روی شبکه ارسال می‌شود و جواب آن توسط پراکسی سرور از اینترنت دریافت و برای کلاینت ارسال می‌شود.

مزایای استفاده از پراکسی

همانطور که اشاره شد پراکسی سرور دارای قابلیت‌های فراوانی است که از آن جمله می‌توان به موارد زیر اشاره کرد:

۱) ذخیره‌سازی

با توجه به گران بودن هزینه استفاده از اینترنت (بسته به اندازه پهنای باند مصرفی) و محدودیت پهنای باند معمولاً اطلاعات مورد نظر در زمان کم و با سرعت مطلوب به دست نمی‌آید. برای کمک به رفع این مشکل، پراکسی سرور

منابعی مانند فایل‌ها و صفحات وبی که مورد دسترسی قرار می‌گیرند در یک حافظه جداگانه ذخیره می‌کند و تقاضای مجدد این منابع با محتویات کش پاسخ داده می‌شود، در نتیجه از یک سو زمان دستیابی کاهش می‌یابد و از سوی دیگر چون اطلاعات از اینترنت دریافت نمی‌شود باعث کاهش ترافیک شبکه می‌شود و پهنای باند محدود با اطلاعات تکراری اشغال نمی‌شود.

۲) دیوار آتش (fire wall)

پراکسی سرور می‌تواند تقاضای کاربران را به فایروال بدهد که به انها اجازه ورود یا خروج به شبکه داخلی داده شود.

۳) فیلتر کردن

پراکسی سرور می‌تواند تمام محتویات ترافیک وارد شونده یا خارج شونده از شبکهٔ داخلی سازمان را باز بینی کند و طبق تنظیمات انجام شده هر چیزی که به معیارهای تعیین شده برای امنیت یا سیاست‌های آن سازمان، مغایرت دارد مسدود کند (مانند سیستم فیلترینگ مخابرات ایران).

۴) تصدیق هویت

بیشتر منابع الکترونیکی سازمان‌ها برای حفظ امنیت محدود می‌شوند. این محدودیت می‌تواند با ایجاد کلمهرمز یا محدود کردن دامنه آی پی اعمال شود در اینصورت اگر کاربری از یک سرویس‌دهنده اینترنت دیگر، در جایی غیر از سازمان استفاده کند آی پی کامپیوتر کاربر غیر معتبر تشخیص داده می‌شود و نیز برای کاربرانی که در داخل سازمان باشند ولی به صورت فیزیکی به شبکه داخلی متصل نشده باشند پراکسی می‌تواند به کاربران دور اجازه عبور موقت دهد و یا به آنها به طور موقت یک آی پی سازمان تخصیص داده می‌شود (مانند استفاده از لپ تاپ شخصی در شبکه داخلی سازمانی مثل دانشگاه) تا بتوانند از منابع محدود شده استفاده کنند.

۵) تغییر هویت

برای جلوگیری از برخی حمله‌های نفوذ گران و محافظت از شبکهٔ داخلی سازمان سرور پراکسی قادر به تغییر هویت کلاینت‌های داخلی می‌باشد. بدین صورت که اگر منبع تقاضا شده در کش موجود نباشد، سرور پراکسی برای آن کاربر به عنوان کلاینت عمل می‌کند و از یکی از آدرس‌های آی پی خودش، برای ارسال تقاضا به سرور موجود در اینترنت استفاده می‌کند و سپس پاسخ به وسیلهٔ پراکسی سرور برای کاربر ارسال می‌شود. این پروسه تغییر آی پی باعث می‌شود تقاضا دهندهٔ اولیه قابل ردیابی نباشد و معماری شبکهٔ سازمان از دید بیرونی مخفی بماند.

۶) ثبت کردن

پراکسی سرور امکان ثبت گزارش کامل کارکردش را دارد تا در هر زمان امکان پیگیری اعمال کاربران داخل سازمان را فراهم آورد. اینکه کلاینت در چه ساعت و و دقیقه‌ای چه درخواستی ارسال کرده و حجم اطلاعات مبادله شده، نوع اطلاعات و ... از این جمله‌اند.

برخی از انواع پراکسی

در واقع، انواع مختلف پراکسی وجود دارد که هرکدام با نوع متفاوتی از ترافیک اینترنت سروکار دارند. در بخش بعد به چند نوع آن اشاره می‌کنیم و شرح می‌دهیم که هرکدام در مقابل چه نوع حمله‌ای مقاومت می‌کند. البته پراکسی‌ها تنظیمات و ویژگی‌های زیادی دارند. ترکیب پراکسی‌ها و سایر ابزار مدیریت فایروال‌ها به مدیران شبکه شما قدرت کنترل امنیت شبکه تا بیشترین جزئیات را می‌دهد. در ادامه به پراکسی‌های زیر اشاره خواهیم کرد:

۱) SMTP Proxy
۲) HTTP Proxy
۳) FTP Proxy
۴) DNS Proxy
۵) SMTP Proxy

SMTP Proxy

پراکسی SMTP محتویات ایمیل‌های واردشونده و خارج‌شونده را برای محافظت از شبکه شما در مقابل خطر بررسی می‌کند. بعضی از توانایی‌های آن این‌ها هستند:

- ✓ مشخص کردن بیشترین تعداد دریافت‌کنندگان پیام:

این اولین سطح دفاع علیه اسپم (هرزنامه) است که اغلب به صدها یا حتی هزاران دریافت‌کننده ارسال می‌شود.

- ✓ مشخص کردن بزرگترین اندازه پیام:

این به سرور ایمیل کمک می‌کند تا از بار اضافی و حملات بمباران توسط ایمیل جلوگیری کند و با این ترتیب می‌توانید به درستی از پهنای باند و منابع سرور استفاده کنید.

- ✓ اجازه دادن به کاراکترهای مشخص در آدرس‌های ایمیل آنطور که در استانداردهای اینترنت پذیرفته شده‌است:

چنانچه قبلاً اشاره شد، بعضی حمله‌ها بستگی به ارسال کاراکترهای غیرقانونی در آدرس‌ها دارد. پراکسی می‌تواند طوری تنظیم شود که بجز به کاراکترهای مناسب به بقیه اجازه عبور ندهد.

- ✓ فیلترکردن محتوی برای جلوگیری از انواع محتویات اجرایی

معمول‌ترین روش ارسال ویروس، کرم و اسب تروا فرستادن آنها در پیوست‌های به ظاهر بی‌ضرر ایمیل است. پراکسی SMTP می‌تواند این حمله‌ها را در یک ایمیل از طریق نام و نوع، مشخص و جلوگیری کند، تا آنها هرگز به شبکه شما وارد نشوند.

- ✓ فیلترکردن الگوهای آدرس برای ایمیل‌های مقبول\مردود:

هر ایمیل شامل آدرسی است که نشان‌دهنده منبع آن است. اگر یک آدرس مشخص شبکه شما را با تعداد بیشماری از ایمیل مورد حمله قرار دهد، پراکسی می‌تواند هر چیزی از آن آدرس اینترنتی را محدود کند. در بسیاری موارد، پراکسی می‌تواند تشخیص دهد چه موقع یک هکر آدرس خود را جعل کرده‌است. از آنجا که پنهان کردن آدرس بازگشت تنها دلایل خصمانه دارد، پراکسی می‌تواند طوری تنظیم شود که بطور خودکار ایمیل جعلی را مسدود کند.

✓ فیلترکردن هدرهای ایمیل:

هِدرها شامل دیتای انتقال مانند اینکه ایمیل از طرف کیست، برای کیست و غیره هستند. هکرها راه‌های زیادی برای دستکاری اطلاعات هِـــدر برای حمله به سرورهای ایمیل یافته‌اند. پراکسی مطمئن می‌شود که هِـــدرها با پروتکل‌های اینترنتی صحیح تناسب دارند و ایمیل‌های دربردارنده هِدرهای تغییر شکل داده را مردود می‌کنند. پراکسی با اعمال سختگیرانه استانداردهای ایمیل نرمال، می‌تواند برخی حمله‌های آتی را نیز مسدود کند.

تغییردادن یا پنهان‌کردن نامهای دامنه و شناسه‌های پیام‌ها:

ایمیل‌هایی که شما می‌فرستید نیز مانند آنهایی که دریافت می‌کنید، دربردارنده دیتای هِـــدر هستند. این دیتا بیش از آنچه شما می‌خواهید دیگران درباره امور داخلی شبکه شما بدانند، اطلاعات دربردارند. پراکسی SMTP می‌تواند بعضی از این اطلاعات را پنهان کند یا تغییر دهد تا شبکه شما اطلاعات کمی در اختیار هکرهایی قرار دهد که برای وارد شدن به شبکه شما دنبال سرنخ می‌گردند.

HTTP Proxy

پراکسی HTTP بر ترافیک داخل شونده و خارج شونده از شبکه شما که توسط کاربرانتان برای دسترسی به اینترنت ایجاد شده، نظارت می‌کند. این پراکسی برای مراقبت از کلاینت‌های وب شما و سایر برنامه‌ها که به دسترسی به وب از طریق اینترنت متکی هستند و نیز حملات برپایه HTML، محتوا را فیلتر می‌کند. بعضی از قابلیت‌های آن این‌ها هستند:

✓ برداشتن اطلاعات اتصال کلاینت:

این پراکسی می‌تواند آن قسمت از دیتای هِـــدر را که نسخه سیستم‌عامل، نام و نسخه مرورگر، حتی آخرین صفحه وب دیده شده را فاش می‌کند، بردارد. در بعضی موارد، این اطلاعات حساس است، بنابراین چرا فاش شوند؟

تحمیل تابعیت کامل از استانداردهای مقررشده برای ترافیک وب

در بسیاری از حمله‌ها، هکرها بسته‌های تغییرشکل داده شده را ارسال می‌کنند که باعث دستکاری عناصر دیگر صفحه وب می‌شوند، یا بصورتی دیگر با استفاده از رویکردی که ایجادکنندگان مرورگر پیش بینی نمی‌کردند، وارد می‌شوند. پراکسی HTTP این اطلاعات بی معنی را نمی‌پذیرد. ترافیک وب باید از استانداردهای وب رسمی پیروی کند، وگرنه پراکسی ارتباط را قطع می‌کند.

✓ برداشتن کوکی‌ها:

پراکسی HTTP می‌تواند جلوی ورود تمام کوکی‌ها را بگیرد تا اطلاعات خصوصی شبکه شما را حفظ کند.

✓ برداشتن هِدرهای ناشناس:

پراکسی HTTP، ازهِـــدرهای HTTP که از استاندارد پیروی نمی‌کنند، ممانعت بعمل می‌آورد. یعنی که، بجای مجبور بودن به تشخیص حمله‌های برپایه علائمشان، پراکسی براحتی ترافیکی را که خارج از قاعده باشد، دور می‌ریزد. این رویکرد ساده از شما در مقابل تکنیک‌های حمله‌های ناشناس دفاع می‌کند.

✓ فیلترکردن محتوا:

دادگاه‌ها مقررکرده‌اند که تمام کارمندان حق برخورداری از یک محیط کاری غیر خصمانه را دارند. بعضی عملیات تجاری نشان می‌دهد که بعضی موارد روی وب جایگاهی در شبکه‌های شرکت‌ها ندارند.
پراکسی HTTP سیاست امنیتی شرکت شما را وادار می‌کند که توجه کند چه محتویاتی مورد پذیرش در محیط کاریتان است و چه هنگام استفاده نامناسب از اینترنت در یک محیط کاری باعث کاستن از بازده کاری می‌شود. بعلاوه، پراکسی HTTP می‌تواند سستی ناشی از فضای سایبر را کم کند. گروه‌های مشخصی از وب سایت‌ها که باعث کم کردن تمرکز کارمندان از کارشان می‌شود، می‌توانند غیرقابل دسترس شوند.

FTP Proxy

بسیاری از سازمان‌ها از اینترنت برای انتقال فایل‌های دیتای بزرگ از جایی به جایی دیگر استفاده می‌کنند. در حالیکه فایل‌های کوچک تر می‌توانند بعنوان پیوست‌های ایمیل منتقل شوند، فایل‌های بزرگ تر توسط FTP فرستاده می‌شوند. بدلیل اینکه سرورهای FTP فضایی را برای ذخیره فایل‌ها آماده می‌کنند، هکرها علاقه زیادی به دسترسی به این سرورها دارند. پراکسی FTP معمولاً این امکانات را دارد:

- ✓ محدودکردن ارتباطات از بیرون به فقط خواندنی:

این عمل به شما اجازه می‌دهد که فایل‌ها را در دسترس عموم قرار دهید، بدون اینکه توانایی نوشتن فایل روی سرورتان را بدهید. یعنی یک ارتباط یک طرفه

- ✓ محدود کردن ارتباطات به بیرون به فقط خواندنی:

این عمل از نوشتن فایل‌های محرمانه شرکت به سرورهای FTP خارج از شبکه داخلی توسط کاربران جلوگیری می‌کند.

DNS Proxy

DNS شاید به اندازه HTTP یا SMTP شناخته شده نیست، اما چیزی است که به شما این امکان را می‌دهد که نامی را مانند http://www.ABC.com در مرورگر وب خود تایپ کنید و وارد این سایت شوید. بدون توجه به اینکه از کجای دنیا به اینترنت متصل شده‌اید. بمنظور تعیین موقعیت و نمایش منابعی که شما از اینترنت درخواست می‌کنید، DNS نام‌های دامنه‌هایی را که می‌توانیم براحتی بخاطر بسپاریم به آدرس آی پی هایی که کامپیوترها قادر به درک آن هستند، تبدیل می‌کند. در اصل این یک پایگاه داده‌است که در تمام اینترنت توزیع شده‌است و توسط نام دامنه‌ها فهرست شده‌است. بهرحال، این حقیقت که این سرورها در تمام دنیا با مشغولیت زیاد در حال پاسخ دادن به تقاضاها برای صفحات وب هستند، به هکرها امکان تعامل و ارسال دیتا به این سرورها را برای درگیرکردن آنها می‌دهد. حمله‌های برپایه DNS هنوز خیلی شناخته شده نیستند، زیرا به سطحی از پیچیدگی فنی نیاز دارند که بیشتر هکرها نمی‌توانند به آن برسند. بهرحال، بعضی تکنیک‌های هک که می‌شناسیم باعث می‌شوند هکرها کنترل کامل را بدست گیرند. بعضی قابلیت‌های پراکسی DNS می‌تواند موارد زیر باشد:

- ✓ تضمین انطباق پروتکلی

یک کلاس تکنیکی بالای اکسپلویت می‌تواند لایه حامل را که تقاضاها و پاسخ‌های DNS را انتقال می‌دهد به یک ابزار خطرناک تبدیل کند. این نوع از حمله‌ها بسته‌هایی تغییرشکل داده شده بمنظور انتقال کد آسیب رسان ایجاد

می‌کنند. پراکسی DNS، هِـــدرهای بسته‌های DNS را بررسی می‌کند و بسته‌هایی را که بصورت ناصحیح ساخته شده‌اند دور می‌ریزد و به این ترتیب جلوی بسیاری از انواع سوء استفاده را می‌گیرد.

- ✓ فیلترکردن محتوای هِدرها بصورت گزینشی

DNS در سال ۱۹۸۴ ایجاد شده و از آن موقع بهبود یافته‌است. بعضی از حمله‌های DNS بر ویژگی‌هایی تکیه می‌کنند که هنوز تایید نشده‌اند. پراکسی DNS می‌تواند محتوای هِـــدر تقاضاهای DNS را بررسی کند و تقاضاهایی را که کلاس، نوع یا طول هِـــدر غیرعادی دارند، مسدود کند.

فیلترهای Nosstateful packet

این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه ای از قواعد، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلاک می کنند. این تصمیم ها با توجه به اطلاعات ادرس دهی موجود در پروتکل های لایه شبکه مانند IP . این فیلترها زمانی می توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویس های مورد نیار شبکه جهت محافظت داشته باشند. همچنین این فیلترها سریع باشند چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکل های لایه کاربرد ندارند.

فیلترهای Stateful packet

این فیلتر ها بسیار باهوش تر از فیلترهای ساده هستند.آنها تقزیبا تمامی ترافیک ورودی را بلاک می کنند اما می توانند به ماشین های پشتیبان اجازه بدهند تا به پاسخ گویی بپردازند. انها این کار را با نگهداری رکورد اتصالاتی که ماشین های پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند. این فیلترها، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند. این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ثبت کنند.

برای مثال شماره پورت های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچم هایTCP .

بسیاری فیلتر های جدید Stateful می توانند پروتکل های لایه کاربرد مانند FTP و HTTP را تشخیص می دهند و لذا می توانند اعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکل ها انجام دهند.

فایروال های شخصی

فایروال های شخصی ، فایروال هایی هستند که بر روی رایانه های شخصی نصب می شوند. آنها برای مقابله با حملات شبکه ای طراحی شده اند. معمولا از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات ایجاد شده توسط این برنامه ها اجازه می دهند که به کاربر بپردازند نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می شوند، فایروال شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده(همانند پروکسی) نیست.

موقعیت یابی برای فایروال

محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت **عبارتند از:**

۱) موقعیت و محل نصب از لحاظ توپولوژیکی

معمولا مناسب به نظر می رسد که فایروال را در درگاه ورودی/خروجی شبکه خصوصی نصب می کنیم. این امر به ایجاد بهترین پوشش امنیتی برای شبکه خصوصی با کمک فایروال از یک طرف و جداسازی شبکه خصوصی از شبکه عمومی از طرف دیگر کمک می کند.

۲) قابلیت دسترسی و نواحی امنیتی

اگر سرورهایی وجود دارند که باید برای شبکه عمومی در دسترس باشند، بهتر است آنها را بعد از فایروال و در ناحیه DMZ قرار دهید. قرار دادن این سرورها در شبکه خصوصی و تنظیم فایروال جهت صدور اجازه به کاربران خارجی برای دسترسی به این سرورها برابر خواهد بود با هک شدن شبکه داخلی.چون شما خود مسیر هکرها را در فایروال باز کرده اید. در حالی که با استفاده از ناحیهDMZ ، سرورهای قابل دسترسی برای شبکه عمومی از شبکه خصوصی شما بطور فیزیکی جدا هستند، لذا اگر هکرها بتوانند به نحوی به این سرورها نفوذ کنند باز هم فایروال را پیش روی خود دارند.

انواع فایروال را با توجه به ساختار کلی و روش کار می‌توان به چندین دسته مختلف دسته‌بندی کرد که در اینجا به هشت نمونه از آن‌ها خواهیم پرداخت:

۱) فایروال های فیلترینگ بسته(Packet-Filtering Firewalls)
۲) فایروال های مداری(Circuit-level gateways)
۳) فایروال های بررسی کننده وضعیت(Stateful inspection firewalls)
۴) فایروال های پروکسی(proxy firewalls)
۵) فایروال های نسل بعدی(Next-gen firewalls)
۶) فایروال های نرم افزاری(Software firewalls)
۷) فایروال های سخت افزاری(Hardware firewalls)
۸) فایروال ابری(Cloud firewall)

۱) فایروال های فیلترینگ بسته(Packet-Filtering Firewalls)

فایروال فیلترینگ بسته از ابتدایی‌ترین و قدیمی‌ترین انواع فایروال است که استفاده از آن مانند یک ایست بازرسی در روتر و سوئیچ ایجاد می‌کند. این فایروال از طریق روتر بررسی ساده‌ای روی داده‌ها انجام می‌دهد که با این بررسی می‌تواند به جزئیات بسیاری مانند مبدا و مقصد داده، آدرسIP ، شماره پورت و اطلاعاتی از قبیل بدون باز کردن کردن داده‌ها دست پیدا کند. در صورتی که داده در این قسمت امکان بررسی را برای فایروال به وجود نیاورد، از بین خواهد رفت. نکته مهم درباره فایروال های فیلترینگ بسته آن است که این نوع فایروال به انرژی

زیادی برای کار نیاز ندارد و به همین دلیل بهره‌مندی از آن روی عملکرد سیستم تاثیری نخواهد داشت ولی باید گفت که این فایروال عملکرد قوی دارد و کار با آن نیز ساده است.

۲) فایروال های مداری(Circuit-level gateways)

فایروال های مداری از دیگر انواع فایروال های ساده‌ای هستند که به آسانی و بدون استفاده از منابع محاسباتی کار می‌کنند. این به طور کلی TPC نامیده می‌شود که از قانونی بودن داده‌ها اطمینان حاصل می‌کند. هرچند این فایروال بسیار کاربردی است ولی خود بسته داده را بررسی نمی‌کند، بنابراین اگر خو بسته حاوی نرم افزارهای مخرب باشد، وارد شبکه خواهد شد. با توجه به ضعفی که فایروال های مداری دارند، توصیه می‌شود این محصول در کنار یکی دیگر از انواع فایروال ها مورد استفاده قرار گیرد.

۳) فایروال های بررسی کننده وضعیت(Stateful inspection firewalls)

فایروال‌های بررسی کننده وضعیت از بهترین سطح امنیت برخوردار هستند. عملکرد این فایروال به این ترتیب است که بسته‌ای اطلاعاتی را در لایه سه و لایه IP مانیتور می‌کند و در صورت معتبر بودن بسته اطلاعاتی محتوای این بسته را مورد ارزیابی قرار می‌دهد.

۴) فایروال های پروکسی(proxy firewalls)

فایروال‌های پروکسی، فایروال‌هایی هستند که از آن‌ها به عنوان یک میانجی بین شکبه‌ها استفاده می‌شود. پروکسی فایروال به منظور پردازش درخواست‌های رسیده از خارج شبکه مورد استفاده قرار می‌گیرد. این پروکسی داده را تست می‌کند و با توجه به قوانین تعیین شده تصمیم‌گیری می‌کند که آیا درخواست مورد قبول است یا خیر. همچنین این پروکسی تمامی بسته را پیگیری می‌کند و آن‌ها را داخل شبکه باز فرآوری خواهد کرد.

۵) فایروال های نسل بعدی(Next-gen firewalls)

از جدیدترین نوع از انواع فایروال های ارائه شده به بازار فایروال های نسل بعدی (Next-gen firewalls) هستند که بررسی عمیق بسته‌ها و محتواهای آن‌ها و بررسی بسته‌های TCP می‌پردازند. همچنین این فایروال نسل بعدی از فناوری‌های دیگری مانند سیستم‌های پیشگیری از نفوذ حمله علیه شبکه نیز برخوردار است.

۶) فایروال های نرم افزاری(Software firewalls)

فایروال های نرم افزاری هر نوع فایروالی هستند که به جای استفاده از یک قطعه سخت افزاری بر روی دستگاه نصب می‌شوند. از مزیت‌های اصلی فایروال‌های نرم افزاری آن است که از آن می‌توان برای جدا کردن نقاط انتهایی شبکه استفاده می‌شود. هرچند این نوع فایروال بسیار کاربرد دارد ولی نصب آن بر روی دستگاه دشوار و زمان‌بر است و در مواردی دستگاه با آن سازگار نیست.

۷) فایروال های سخت افزاری(Hardware firewalls)

فایروال‌های ساخت افزاری دستگاه‌های فیزیکی مانند روتر هستند که از ورود بسته‌ها و محتواهای نامعتبر جلوگیری می‌کنند. از مزیت‌های این فایروال‌ها آن است که از آن‌ها می‌توان برای ایجاد سطح بالایی از امنیت استفاده کرد. قابلیت‌های فایروال‌های سخت افزاری با توجه به شرکت‌های سازنده آن متفاوت است و برخی از آن‌ها بیشتری برای بررسی همزمان چندین اتصال را خواهند داشت.

۸) فایروال ابری(Cloud firewall)

هرگاه که از یک راه حل ابری برای ارائه فایروال استفاده شود، به آن می‌توان فایروال ابری گفت. در بسیاری از موارد فایروال‌های پروکسی به جای فایروال‌های ابری مورد استفاده قرار می‌گیرند زیرا معمولا از سرور ابری برای نصب فایروال های پروکسی استفاده می‌شود. مزیت اصلی فایروال های ابری آن است که به آسانی در سازمان‌های مختلف قابل استفاده هستند و با افزایش نیاز می‌توان ظرفیت آن را اضافه کرد تا بارهای ترافیکی بیشتری فیلتر شوند. این نوع از فایروال مانند فایروال‌های سخت افزاری از سطح بالایی از امنیت برخوردار هستند.

متناسب ساختن فایروال

فایروال ها قابل تنظیم متناسب با نیازهای کاربران می باشند. این بدان معنی است که کاربر می توانید فیلترهایی را بر اساس شرایط مختلف اضافه یا حذف نمائید. برخی از این ها عبارتند از :

۱) آدرس های IP

به هر دستگاه در اینترنت یک آدرس منحصر به فرد به نام آدرس IP تخصیص داده می شود. آدرس های IP اعداد ۳۲ بیتی هستندکه معمولا بصورت چهار بایت به شکل اعداد ده دهی نقطه دار بیان می گردد.یک آدرس IP نمونه شبیه به این می باشد.۶۴،۲۳۶،۱۶،۵۲ :

به عنوان مثال اگر یک آدرس IP معین خارج از شرکت در حال خواندن فایل های بسیار زیادی از یک سرور باشد، فایروال می تواند تمام ترافیک را از/یا به آن آدرس**IP** مسدود نماید.

۲) نام های دامنه

از آنجا که به یادآوری رشته ای از اعداد که آدرس IP را درست می کنند، سخت می باشد و آدرس های IP گاهی نیاز به تغییر دارند، تمامی سرورها در اینترنت همچنین دارای نام هایقابل خواندن توسط بشر به نام های دامنه می باشند.

به عنوان مثال برای اغلب ما یادآوری www.google.com راحت تر از ۶۹،۲۵۴،۱۵،۲۵ می باشد. یک شرکت ممکن است تمام دسترسی ها به نام های دامنه خاصی را ببندد یا فقط دسترسی به نام های دامنه حاصی را اجازه دهد.

۳) پروتکل ها

پروتکل روش از پیش تایین شده است که کسی که میخواهد از سرویسی استفاده نماید، به وسیله ان با آن صحبت می نماید. این کس می تواند یک شخص باشد اما در اغلب اوقات یک برنامه کامپیوتری شبیه یک browser وب است. پروتکل ها غالبا متن هستند و به سادگی توصیف می کنند که سرویس گیرنده و سرویس دهنده مکالماتشان را چگونه خواهند داشت، http پروتکل وب می باشد. برخی از پروتکل های متداول را که می توانید فیلترهای فایروال را جهت آنها تنظیم نمائید در زیر نام برده شده است:

- ✓ **IP** پروتکل اینترنت_سیستم اصلی تحویل اطلاعات روی اینترنت.

- ✓ **TCP** پروتکل کنترل ارسال_جهت شکستن و بازسازی اطلاعاتی که روی اینترنت در حال گردش هستند، استفاده می گردد.
- ✓ **PTTP** پروتکل انتقال ابر متن_جهت صفحات وب استفاده می شود.
- ✓ **UDP** پروتکل ثبت داده های کاربر
- ✓ **FTP** پروتکل انتقال فایل
- ✓ **ICMP** پروتکل کنترل پیام اینترنت_ بوسیله یک روتر جهت تبادل اطلاعات با روتر های دیگر استفاده می گردد.
- ✓ **SMTP** پروتکل حمل پست ساده _برای ارسال اطلاعات متنی
- ✓ **SNMP** پروتکل مدیریت شبکه ساده

۴) پورت ها

هر دستگاه سرور ، سرویس هایش را در اینترنت با استفاده از پورت های شماره گذاری شده، یک پورت برای هر سرویس که در سرور موجود است، فراهم می سازد. به عنوان مثال،اگر یک سرور در حال اجرا یک سرور وب (HTTP) و یک سرور (FTP) باشد، سرور وب نوعا در پورت ۸۰ و سرور FTP در پورت ۲۱ در دسترس خواهد بود. یک شرکت ممکن است دسترسی به پورت۲۱ را در تمام دستگاه های داخل شرکت به جز یکی ببندد.

۵) کلمات و عبارات خاص

این می تواند هر چیزی باشد. فایروال هر بسته از اطلاعات را برای مطابقت دقیق متنی که در فیلتر لیست شده، جستجو می کند مثلا می توانید به فایروال بگ.ئید هر بسته ای که در آن کلمه "x-rated";"x rated" را نخواهید فهمید . اما شما می توانید کلمات، عبارات و گونه های مختلف آنها را تا حدی که نیاز دارید بگنجانید

نحوه انتخاب یک فایروال

فایروال ها اطلاعات دریافتی از اینترنت و یا ارسالی بر روی اینترنت را بررسی نموده و در صورتی که اطلاعات دریافتی از منابع غیر ایمن و خطرناک باشد، آنان را شناسایی و حذف می نمایند. در صورتی که یک فایروال به درستی پیکربندی گردد، مهاجمانی که تلاشی مستمر به منظور شناسایی کامپیوترهای حفاظت نشده و آسیب پذیر را انجام می دهند در ماموریت خود با شرکست مواجهه خواهند شد.

فایروال های موجود را می توان به سه گروه اساسی تقسیم نمود که هر یک دارای مزایا و معایب مختص به خود می باشند.

اولین مرحله برای انتخاب یک فایروال، بررسی و تشخیص فایروالی است که با اهداف و خواسته شما به درستی مطابقت می نماید. در این رابطه از سه گزینه متفاوت می توان استفاده نمود:

۱) فایروال های نرم ا فزاری
۲) روتر های سخت افزاری
۳) روتر های بدون کابل

در زمان انتخاب یک فایروال سوالات متعددی مطرح می گردد که پاسخ به برخی از آنان دارایی اولویت بیشتری است:

- ✓ چه تعداد کامپیوتر می بایست از فایروال استفاده نمایند؟
- ✓ از چه نوع سیستم عاملی استفاده می گردد؟(ویندوز ،یونیکس،لینوکس...)

چگونگی کارکرد فایروال در یک نگاه کلی

فایروال سیستمی سخت افزاری یا نرم افزاری است که بین کامپیوتر شما یا یک شبکه LAN و شبکه بیرونی(مثلا اینترنت) قرار گرفته و ضمن نظارت بر دسترسی به منابع resource سیستم، در تمام سطوح ورود و خروج اطلاعات را تحت نظر دارد. هر زمان یا نهادی که بخواهد ورود و خروج اطلاعات شبکه خود را کنترل کند موظف است تمام ارتباطات مستقیم شبکه خود را با دنیای خارج قطع نموده و هر گونه ارتباط خارجی از طریق یک دروازه که **فایروال یا فیلتر** نام دارد، انجام شود.

قبل از تحلیل اجزای فایروال عملکرد کلی و مشکلات استفاده از فایروال را بررسی می کنیم.

بسته های TCP وIP قبل از ورود یا خروج به شبکه ابتدا وارد فایروال می شوند و منتظر می مانند تا طبق معیارهای حفاظتی و امنیتی پردازش شوند. پس از پردازش و تحلیل بسته سه حالت ممکن اتفاق بیفتد:

۱) اجازه عبور بسته صادر می شود.
۲) بسته حذف می شود.
۳) بسته حذف شده و پاسخ مناسب به مبدا آن بسته داده شود.

غیر از حذف بسته می توان عملیاتی نظیر ثبت، اخطار ، ردگیری، جلوگیری از ادامه استفاده از شبکه و توبیخ هم در نظر گرفت.

به مجموعه ای قواعد فایروال سیاست های امنیتی نیز گفته می شود. همانطور که همه جا عملیات ایست و بازرسی وقت گیر و اعصاب خرد کن است فایروال هم به عنوان یک گلوگاه می تواند منجر به بالا رفتن ترافیک، تاخیر ، ازدحام و نهایتاً بن بست در شبکه شود. یعنی بسته ها آنقدر در پشت فایروال معطل می مانند تا زمان طول عمرشان به اتمام رسیده و فرستنده مجبور می شود مجدداً اقدام به ارسال آنها کند و این کار متناوباً تکرار می گردد. به همین دلیل فایروال نیاز به طراحی صحیح و دقیق دارد تا کمترین تأخیر را در اطلاعات امن و صحیح ایجاد نماید. تأخیر در فایروال اجتناب ناپذیر است و فقط باید به گونه ای باشد که بحران ایجاد نکند. از آنجایی که معماری شبکه به صورت لایه لایه است، در مدل TCP/IP برای انتقال یک واحد اطلاعات از لایه چهرم بر روی شبکه باید تمام لایه ها را بگذارند ، هر لایه برای انجام وظیفه خود تعدادی فیلد مشخص به ابتدای بسته اطلاعاتی اضافه کرده و آنرا تحویل لایه پایین تر می دهد.

قسمت اعظم کار یک فایروال ، تحلیل فیلدهای اضافه شده در هر لایه و header هر بسته می‌باشد. سیاست امنیتی یک شبکه مجموعه ای متناهی از قواعد امنیتی است که بنابر ماهیتشان در یکی از لایه های فایروال تعریف می شود:

۱) قواعد تعیین بسته های ممنوع (بسته های سیاه) در اولین لایه از دیوار آتش

۲) قواعد بسته برخی از پورت های متعلق به سرویس هایی مثل Telnet یا FTP در لایه دوم
۳) قواعد تحلیل header متن یک نامه الکترونیکی یا صفحه وب در لایه سوم

لایه اول فایروال

لایه اول فایروال براساس تحلیل بستهIP و فیلدهای HEADER این بسته کار می کند و در این بسته فیلدهای زیر قابل نظارت و بررسی هستند:

۱) آدرس های مبدا: برخی از ماشین های داخل و یا خارج شبکه با آدرس IP خاص حق ارسال بسته نداشته باشند و بسته های آنها به محض ورود به فایروال حذف شود.
۲) آدرس مقصد: برخی از ماشین های داخل و یا خارج شبکه با آدرس IP خاص حق دریافت بسته نداشته باشند و بسته های آنها به محض ورود به فایروال حذف شود.(آدرس های IP غیر مجاز توسط مسئول فایروال تعریف می شود.)
۳) شماره شناسایی یک دیتاگرام قطعه قطعه شده: بسته هایی که قطعه قطعه شده اند یا متعلق به یک دیتاگرام خاص هستند باید حذف شوند.
۴) شماره پروتکل: بسته هایی که متعلق به پروتکل خاصی در لایه بالاتر هستند می توانند حذف شوند. یعنی بررسی اینکه بسته متعلق به چه پروتکلی است و آیا تحویل به آن پروتکل مجاز است یا خیر؟
۵) زمان حیات بسته : بسته هایی که ربیش از تعداد مشخصی مسیریاب را طی کرده اند مشکوک هستند و باید حذف شوند.
۶) بقیه فیلدها بنابر صلاح دید و قواعد امنیتی مسئول فایروال قابل بررسی هستند. مهم ترین خصوصیت لایه اول از فایروال آن است که در این لایه بسته ها بطور مجزا و مستقل از هم بررسی می شوند . هیچ نیازی به نگه داشتن بسته های قبلی یا بعدی یک بسته نیست. به همین دلیل ساده ترین و سریع ترین تصمیم گیری در این لایه انجام می شود. امروزه برخی مسیریاب ها با امکان لایه اول فایروال به بازار عرضه می شوند یعنی به غیر از مسیر یابی وظیفه لایه اول یک فایروال را هم انجام می دهند که به آنها مسیر یاب های فیلتر کننده بسته گفته می شود. بنابراین مسیر یاب قبل از اقدام به مسیر یابی براساس جدولی بسته های IP را غربال می کند و تنطیم این جدول براساس نظر مسئول شبکه و برخی قواعد امنیتی انجام می گیرد.
۷) با توجه به سریع بودن این لایه هرچه درصد قواعد امنیتی در این لایه دقیق تر و سخت گیرانه تر باشند حجم پردازش در لایه های بالاتر کمتر و در عین حال احتمال نفوذ پایین تر خواهد بود ولی در مجموع بخاطر تنوع میلیاردی آدرس های IP نفوذ از این لایه با آدرس های جعلی یا قرضی امکان پذیر خواهد بود و این ضعف در لایه های بالاتر باید جبران شود.

لایه دوم فایروال

در این لایه از فیلدهای header لایه انتقال برای تحلیل بسته استفاده می شود عمومی ترین فیلدهای بسته های لایه انتقال جهت بازرسی در فایروال عبارتند از:

۱) شماره پورت پروسه مبدا و مقصد : باتوجه به آنکه پورت های استاندارد شناخته شده هستند ممکن است مسئول یک فایروال بخواهد سرویس ftp فقط در محیط شبکه محلی امکان پذیر باشد و برای تمام ماشین های خارجی این امکان وجود نداشته باشد. بنابراین فایروال می تواند بسته های TCP با شماره پورت های۲۰ و۲۱ مربوط به FTP که قصد ورود و خروج از شبکه را دارند، حذف کند. یکی دیگر از سرویس های خطرناک که ممکن است مورد سو استفاده قرار گیرد Telnet است که می توان به راحتی پورت ۲۳ را مسدود کرد . یعنی بسته هایی که مقصدشان شماره پورت ۲۳ است حذف شوند.

۲) فیلد شماره ترتیب و فیلد : این دو فیلد بنا بر قواعد تعریف شده توسط مسئول شبکه قابل استفاده هستند.

۳) کدهای کنترلی: فایروال با بررسی این کدها، به ماهیت آن بسته پی برده و سیاست های لازم را بر روی آن اعمال می کند. بعنوان مثال یک دیوار آتش ممکن است بگونه ای تنظیم شود که تمام بسته هایی که از بیرون به شبکه وارد می شوند و دارای بیت SYN=1 هستند را حذف کند. بدین ترتیب هیچ ارتباط TCP از بیرون به درون شبکه برقرار نخواهد شد.

از مهم ترین خصوصیات این لایه آن است که تمام تقاضا های برقراری ارتباط TCP بایستی از این لایه بگذرد و چون در ارتباط TCP ، تا مراحل" سه گانه اش" به اتمام نرسد انتقال داده امکان پذیر نیست. لذا قبل از هرگونه مبادله داده فایروال می تواند مانع برقراری هرر ارتباط غیر مجاز شود. یعنی فایروال می تواند تقاضاهای برقراری ارتباط TCP را قبل از ارائه به ماشین مقصد بررسی نموده و در صورت قابل اطمینان نبودن مانع از برقراری ارتباط گردد. فایروال این لایه نیاز به جدولی از شماره پورت های غیر مجاز را دارد.

لایه سوم فایروال

در این لایه حفاظت براساس نوع سرویس و برنامه کاربردی انجام می شود. یعنی با در نظر گرفتن پروتکل در لایه چهارم به تحلیل داده ها می پردازد. تعداد header ها در این لایه بسته به نوع سرویس بسیار متنوع و فراوان است. بنابراین در لایه سوم فایروال برای هر سرویس مجزا (مانند وب ، پست الکترونیک و...) باید یک سلسه پردازش و قواعد امنیتی مجزا تعریف شود و به همین دلیل حجم و پیچیدگی پردازش ها در لایه سوم زیاد است. توصیه موکد آن است که تمام سرویس های غیر ضروری و شماره پورت هایی که مورد استفاده نیستند در لایه دوم مسدود شوند تا کار لایه سوم کمتر باشد.

آنچه فایروال ها سیستم را از آن محافظت می نمایند:

شاید این سوال مطرح باشد که یک مهاجم قادر به انجام چه کاری خواهد بود و یا اصطلاحا شعاع میدان تخریب وی به چه میزان است و چه اطلاعاتی در معرض تهدید و یا آسیب قرار خواهند گرفت؟ پاسخ به سوال فوق به نوع و ماهیت تهاجم بستگی دارد. با این که برخی از حملات صرفا در حد و اندازه یک مزاحمت و یا شوخی ساده می باشد ولی برخی دیگر با اهداف کاملا مخرب طراحی و پیاده سازی می گردند. در چنین مواردی، مهاجمان سعی

می نمایند که به اطلاعات، آسیب رسانده و آنان را حذف نموده و حتی قادر به سرقت اطلاعات شخصی و حساس نظیر رمزهای عبور و یا شماره کارت های اعتباری نمایند.
برای برخی از مهاجمان، نفوذ به کامپیوتر شیرین ترین و فراموش نشدنی ترین لحظات زندگی شان است! چرا که آنان ماحصل تلاش خود را عملا مشاهده نموده و از این بابت لذت می برند. با استفاده از یک فایروال می توان میزان مقاومت سیستم خود را در مقابل این نوع حملات افزایش دهید.
روش های زیادی وجود دارد که افراد جهت دسترسی یا سوء استفاده از کامپیوترهای محافظت نشده بکار می‌برند که در زیر اشاره شده است:

۱) **ورود به سیستم از راه دور**

هنگامی که افراد قادر به اتصال کامپیوتر و کنترل آن در برخی از اشکال باشند. این مورد می تواند از قادر بودن به مشاهده یا دسترسی فایل هایتان تا عملا اجرای برنامه ها روی کامپیوترتان متغیر باشد.

۲) **درهای مخفی برنامه کاربردی**

برخی از برنامه ها خصوصبات خاصی دارند که اجازه دسترسی از راه دور را از سطوح کنترل برنامه را فراهم می سازد.

۳) **دزدیدن ارتباط**

متداول ترین شیوه ارسال e-mail در اینترنت می باشد با استفاده از دسترسی به لیستی از آدرس های e-mail ، یک فرد می تواند e-mail های آشغال ناخواسته را برای هزاران کاربر ارسال نماید.
این کار اغلب اوقات با تغییر دادن مسیر e-mail ها از طریق سرورSMTP بر روی یک میزبان که مورد ظن نمی باشد صورت گرفته، رد یابی فرستنده اصلی هرزنامه را مشکل می سازد.

۴) **اشکال سیستم عامل**

برخی از سیستم عامل ها نیز مشابه با برنامه های کاربردی دارایbackdoor هستند. انواع دیگر دسترسی از راه دور با کنترل های امنیتی ناکافی را فراهم می سازد. یا اشکالاتی دارد که یک هکر با تجربه می تواند از آنها بهره برداری نماید.

۵) **رد سرویس**

شما احتمالا این اصطلاح را در گزارشات خبری در حملات وب سایت های بزرگ شنیده اید مقابله با این نوع حمله تقریبا غیر ممکن است. آنچه اتفاق می افتد این است که یک هکر یک تقاضا به سرور جهت اتصال به آن می فرستد. وقتی سرور با یک تاییدیه پاسخ می دهد و سعی می کند ارتباط را برقرار سازد، نمی تواند سیستمی که این تقاضا را داده است پیدا کند.با مواجه کردن سرور با سیلی از تقاضاهای غیرقابل پاسخ برای ازتباط، هکر باعث می شود سرور تا حد خزیدن کند شده یا سرانجام از کار بی افتد.

۶) **بمب های e-mail**

یک بمب e-mail معمولا یک حمله شخصی می باشد. در این حمله، فرد e-mail های یکسان راصدها و هزاران بار برایتان می فرستد تا آنکه سیستم e-mail تان دیگر نتواندe-mail بیشتری را بپذیرد.

۷) ماکروها

برای آسان تر نمودن رویه های پیچیده ، بسیاری از برنامه های کاربردی به شما اجازه ایجاد اسکریپی از فرامین که آن برنامه می تواند اجرا کند را می دهند. این اسکریپت تحت عنوان ماکرو معروف می باشد. هکرها از این ویژگی برای ایجاد ماکروهای خودشان سود می جویند که بسته به آن برنامه کاربردی، می تواند داده های شما را از بین برده یا کامپیوتر شما را از کار بیاندازد.

۸) ویروس ها

احتمالا شناخته ترین تهدید ، ویروس های کامپیوتری می باشند . یک ویروس برنامه ای است که می تواند خودش را به کامپیوتر های دیگر کپی کند. با این روش ویروس می تواند به سرعت از یک سیستم به سیستم دیگر گسترش یابد. خط ویروس ها از پیغام های بی ضرر تا پاک کردن تمام فایل هایتان، متغیر می باشند.

۹) هرزنامه

نوعا بی ضرر اما همواره رنجش آور است؛ هرزنامه معادل الکترونیکی نامه آشغال می باشد. اغلب اوقات هرزنامه شامل لینک هایی به سایت های وب است. باید مراقب بود که بر روی این هرزنامه ها کلیک نکرد چون ممکن است تصادفا یک cookie که یک backdoor را به کامپیوترتان فراهم می سازد،باشد.

۱۰)تغییر دادن مسیر بمب ها

هکرها می توانند از ICMP برای تغییر دادن مسیر اطلاعات با ارسال به یک روتر متفاوت استفاده کنند. این یکی از شیوه های است که با آن حمله رد سرویس صورت می گیرد

۱۱)مسیر یاب مبدأ

در بیشتر موارد مسیری که یک بسته در اینترنت(یا هر شبکه دیگر) گردش می کند، به وسیله زوتر ها طول آن مسیر مشخص می شود. اما مبدأ فراهم کننده بسته می تواند به دلخواه مسیری که بسته باید گردش کند را مشخص نماید. گاهی اوقات هکر ها از این امر جهت نشان دادن اینکه اطلاعات در ظاهر از یک منبع مطمئن یا حتیاز داخل شبکه می آیند، سود می جویند. اغلب محصولات فایروال بصورت پیش فرض، مسیریابی مبدأ را غیرفعال می سازد. برخی از موارد در لیست فوق برای فیلتر کردن بوسیله فایروال. اگر نگوییم غیر ممکن، مشکل می باشند. باتوجه به اینکه بعضی از فایروال ها محافظت در مقابل ویروس را ارائه می‌دهند. نرم افزار ضد ویروس روی کامپیوتر ارزش سرمایه گذاری را دارد. باید توجه داشت برخی از هرزنامه ها، مادامیکه پذیرای e-mail هستید قصد رسیدن از طریق فایروال را دارند.

سطح امنیتی که برقرار می سازید، تعیین خواهد نمود چه تعداد از این تهدیدات می تواند با استفاده از فایروال متوقف گردد.بالاترین سطح امنیت، بطور ساده مسدود نمودن همه چیز خواهد بود. واضح است این کار هدف از داشتن یک اتصال اینترنت را خنثی می نماید. اما یک قائده سرانگشتی موسوم ، مسدود نمودن هرچیز ، سپس

انتخاب انواع ترافیک هایی که می خواهید اجاره دهید، می باشد. همچنین می توان ترافیکی که از طریق فایروال گردش می کند را محدود نمائید بطوریکه فقط انواع معینی از اطلاعات از قبیل e-mail بتوانند از این طریق برسند. این قاعده خوبی برای بنگاه های تجاری می باشد که مدیر شبکه با تجربه ای که دارد بفهمد چه نیازهایی وجود دارد و دقیقا بداند چه ترافیکی را اجازه عبور بدهد. احتمالا برای اغلب کاربران عادی بهتر است با پیش فرض های فراهم شده توسط توسعه دهنده فایروال کار کنیم. مگر آنکه دلیل خاصی برای تغییر آنها وجود داشته باشد.

یکی از بهترین راه ها برای فایروال ها از نقطه نظر امنیتی این است که هر کسی را در بیرون، از متصل شدن به کامپیوتر در شبکه خصوصی متوقف می سازد. در حالی که این موضوع برای بنگاه های تجاری مهم می باشد. احتمالا اغلب شبکه های خانگی از این طریق مورد تهدید نخواهند بود. با این وجود قرار دادن یک فایروال در محل، قدری آرامش فکر را فراهم می آورد.

مزایا و معایب استفاده از فایروال

مزایا

۱) ایجاد یک دریچه متمرکز بر روی شبکه که از ورود کاربران غیر مجاز جلوگیری می کند.
۲) فایروال برای کامپیوتر ها، حفاظتی را جهت جلوگیری از ایجاد ترافیک و اخطار به کاربران ایجاد می کند اما در صورتی که کاربر به این پیغام ها توجهی نکند،این کار فایده ای ندارد.
۳) فضای منطقی برای گسترش آدرس های شبکه_NAT_ایجاد می کند . این آدرس ها به کم کردن فضای آدرس کمک می کنند.
۴) به مدیر شبکه اجازه می دهد که از پهنای باند هر یک از کاربران آگاهی داشته باشد و در صورت لزوم به آنها اخطار دهد.

معایب

۱) بسته ها و نرم افزار های ویروسی توسط فایروال سخت افزاری تشخیص داده نمی شوند.
۲) برای فایروال های سخت افزاری مسئله هزینه و کابل کشی و برای فایروال نرم افزاری مسئله زمان بر بودن و کمبود حافظه مطرح است.
۳) فایروال ها نمی تواند ویروس هایی که در میزبان کپی شده را تشخیص و در نتیجه در کل شبکه پخش می شود.
۴) فایر وال های نرم افزاری سرعت را پایین می آورند.

DNS –۹

دی‌ان‌اس یا همان پروتکل DNS[21]، کاری اصلی این پروتکل اتصال دامنه سایت به هاست و سرور های مربوطه آن برای نمایش صحیح وب سایت است. یک سیستم پایگاه داده است که نام کامل دامنه یک کامپیوتر را به یک آدرس IP ترجمه میکند.

بطور کلی دی ان اس، فهرست توزیع شده ای است که نام دامنه قابل خواندن توسط انسان مانند www.AAA.com را به اعداد خوانا برای کامپیوترها یعنی همان IP آدرس (مثلا ۱۹۲،۱۶۲،۱،۱) تبدیل می کند تا اطلاعات به درستی در مرورگر ها نمایش داده شوند. خوب است بدانید عمل ترجمه نام دامنه به آدرس IP را اصطلاحا Resolve کردن نام دامنه می نامند. و بطور کلی هدف سیستم نام دامنه یا همان DNS این است که هر کاربری از هر نقطه از دنیا با وارد کردن نام دامنه مورد نظر، به آدرس IP مربوطه ارجاع داده شود.

کامپیوترهای موجود در یک شبکه برای اتصال به یکدیگر از آدرس‌های **IP** استفاده می کنند، ولی به یاد داشتن آدرس های IP کامپیوترهای یک شبکه برای افرادی که قصد اتصال به آنان را دارند بسیار دشوار است. مثلا به خاطر سپردن نام دامنه Google.com بسیار ساده تر از به خاطر سپردن آدرس IP نظیر آن (۲۰۷.۱۷۱.۱۶۶.۴۸) است. به همین علت اغلب ما برای اتصال به سایت ها، نام دامنه آن را وارد می کنیم. لذا DNS به شما امکان می دهد تا به جای استفاده از آدرس های عددی IP برای اتصال به یک کامپیوتر خاص در شبکه ای دیگر (یا برای دسترسی به یک سرویس راه دور)، با به کارگیری نام دامنه ای که به خاطر آوردن آن برای شما راحت تر است به آن کامپیوتر متصل شده یا از آن سرویس بهره بگیرید.

برعکس عکس این مسئله، Reverse DNSیا RDNS نام دارد که آدرس IP را به نام دامنه متناظر ترجمه می‌کند.

Reverse DNS

در واقع عمل تبدیل یک IP به نام دامنه را عمل Reverse DNS می‌گویند، این عمل دقیقا بر عکس کار DNS است، همانگونه که همه می‌دانیم در عمل DNS ما نام دامنه را وارد کرده و با استفاده از این سرویس به شماره IP آن دسترسی پیدا می‌کنیم ، اما در Reverse DNS دقیقا کر بر عکس است. مثلا : سیستمی با IP ۱۹۲.۲.۴.۸۶ برابر می‌شود با www.exmaple.com و البته شاید چندین نام را به ما باز گرداند که در اکثر مواقع اینگونه است.

کاربرد

کاملا واضح است اما ، این عمل بیشتر هنگامی مورد استفاده واقع می‌شود که ما بخواهیم ببینیم روی یک Host چند سایت وجود دارد و نام آن ها چیست، و اطلاعاتی از این قبیل را بدست بیاوریم . برای بدست آوردن اطلاعات بیشتر می‌توانید به اینجا مراجعه کنید.

در DNS ، کل آدرس های اینترنت درون بانک های اطلاعاتی توزیع شده‌ای هستند که هیچ تمرکزی روی نقطه ای خاص از شبکه ندارند . روش ترجمه نام بدین ترتیب است که وقتی یک برنامه کاربردی مجبور است برای برقراری یک ارتباط ، معادل آدرس IP از یک ماشین با نامی مثل CS.ucsb.edu را بدست بیاورد ، قبل از هر کاری

[21] Domain Name System

یک تابع کتابخانه ای (Library Function) را صدا می زند ، به این تابع کتابخانه ای تابع تحلیلگر نام[۲۲] گفته می شود .تابع تحلیلگر نام ، یک آدرس نمادین را که بایستی ترجمه شود ، بعنوان پارامتر ورودی پذیرفته و سپس یک بسته‌ی درخواست (Query Packet) به روش UDP تولید کرده و به آدرس یک سرویس دهنده ی DNS (که به صورت پیش فرض مشخص می باشد) ارسال می کند . همه ی ماشین های میزبان ، حداقل باید آدرس IP از یک سرویس دهنده ی DNS را در اختیار داشته باشند . این «سرویس دهنده ی محلی» پس از جستجو ، آدرس IP معادل با یک نام نمادین را بر می گرداند . (تابع تحلیلگر نام) نیز آن آدرس IP را به برنامه ی کاربردی تحویل می دهد با پیدا شدن آدرس IP ، برنامه ی کاربردی می تواند عملیات مورد نظرش را ادامه بدهد . روش های جستجو در سیستم DNS برای تحلیل یک نام حوزه ، سطوح از سمت راست به چپ تفکیک می شوند و در یک روند سلسله مراتبی ، سرویس دهنده ی متناظر با آن سطح پیدا می شود . نام های حوزه به هفت منطقه ی عمومی و حدود صد و اندی منطقه‌ی کشوری تقسیم بندی شده است. حوزه بدین معناست که شما با یک نگاه ساده به انتهای آدرس نمادین، می‌توانید ماهیت آن نام و سرویس دهنده ی متناظر با آن را حدس بزنید . یعنی اگر انتهای نام های حوزه متفاوت باشد منطقه ی جستجو برای یافتن آدرس IP معادل نیز متفاوت خواهد بود.

هفت حوزه عمومی که همه آنها سه حرفی هستند عبارتند از:

۱) Com: صاحب این نام جزو موسسات اقتصادی و تجاری به شمار می آیدwww.sony.com .
۲) Edu: صاحب این نام جزو موسسات علمی یا دانشگاهی به شمار می آیدwww.sharif.edu .
۳) Gov: این نام برای آژانس های دولتی آمریکا اختصاص داده شده استwww.whitehouse.gov .
۴) Int: صاحب این نام یکی از سازمان های بین المللی (مثل یونسکو ، فائو ،...) محسوب می‌شود . www.unicef.int
۵) Mil: این نام ویژه مراکز نظامی آمریکا می باشد.
۶) Net: صاحب این نام از ارائه دهندگان خدمات شبکه به شمار می‌رود www.pegah.net .
۷) Org: صاحب این نام از سازمان های عام المنفعه و غیر انتفاعی محسوب می شوند www.ieee.org .

نام حوزه های بسیار زیادی در اینترنت تعریف شده اند که هیچیک از حوزه های سه حرفی هفتگانه را در انتهای آنها نمی‌بینید. معمولا در انتهای این آدرس ها یک رشته دو حرفی مخفف نام کشوری است که آن آدرس و ماشین صاحب آن ، در آن کشور واقع است.

هر حوزه می‌تواند به زیر حوزه های کوچکتری تقسیم شود که به آن دامنه سطح دوم نیز گفته می‌شود . به عنوان مثال نام های مربوط به حوزه ایران که با .irمشخص می شود به ۷ زیرحوزه به شرح زیر تقسیم می شود:

۱) ac.ir.: فقط برای دانشگاه‌ها یا موسسه های آموزشی
۲) co.ir.: فقط برای شرکت های سهامی خاص، سهامی عام، مسوولیت محدود و تضامنی
۳) gov.ir.: فقط برای موسسه ها یا سازمان های دولتی
۴) id.ir.: فقط برای افراد دارای ملیت ایرانی

[۲۲] Name Resolver

۵) net.ir.: فقط برای سرویس دهندگان رسمی اینترنت
۶) org.ir.: فقط برای موسسه ها و سازمان های خصوصی
۷) sch.ir.: فقط برای مدارس

مثلا" برای دامین http://eng.ut.ac.ir اطلاعات زیر را داریم:

- کشور: ایران
- هویت: دانشگاه
- نام دانشگاه: سرواژه ای برای نام دانشگاه تهران (ut)
- نام دانشکده: سرواژه ای برای بخش فنی مهندسی (eng)

حوزه‌ها (Zone) با دامنه‌ها (Domain) یکسان نبوده و یک حوزه می‌تواند شامل مقادیری در رابطه با چندین دامنه باشد. به عنوان مثال دامنه www.google.com دارای زیردامنه ای به نام news است , (news.google.com) درصورتیکه زیردامنه mail آن (mail.google.com) از دامنه اختصاصی www.gmail.com نیز قابل دسترسی می باشد.

روش‌های جستجو در سرویس دهنده های نام

اسامی نمادین در شبکه اینترنت که خود در قالب حوزه ها و زیر حوزه ها سازماندهی شده اند در یک فایل متمرکز ذخیره نمی شوند بلکه روی کل شبکه اینترنت توزیع شده اند ، به همین دلیل برای ترجمه یک نام به آدرس IP ممکن است چندین مرحله "پرس و جو" صورت بگیرد تا یک آدرس پیدا شود. طبیعی است که یک پرس و جو برای تبدیل یک نام حوزه همیشه موفقیت آمیز نباشد و ممکن است به پرس و جوهای بیشتری نیاز شود یا حتی ممکن است یک آدرس نمادین اشتباه باشد و هیچ معادل IP نداشته باشد.

سه روش برای پرس و جوی نام در سرویس دهنده های نام وجود دارد:

۱) پرس و جوی تکراری(Iterative Query)
۲) پرس و جوی بازگشتی(Recursive Query)
۳) پرس و جوی معکوس(Reverse Query)

۱) پرس و جوی تکراری: در پرس و جوی تکراری قسمت اعظم تلاش برای تبدیل یک نام بر عهده سرویس دهنده محلی است؛ این DNS حداقل به آدرس ماشین Root ، به عنوان نقطه شروع نیاز دارد . وقتی یک تقاضای ترجمه آدرس به سرویس دهنده محلی ارسال می شود در صورتی که قادر به ترجمه نام به معادل IP آن باشد ، معادل آدرس IP نام مورد نظر را به تقاضا کننده برمی گرداند. (این حالت وقتی است که سرویس دهنده محلی قبلاً آن نام را ترجمه و در یک فایل ذخیره کرده باشد.) در غیر این صورت سرویس دهنده محلی خودش یک تقاضا برای DNS سطح بالا ارسال می کند. این سرویس دهنده ، آدرس ماشینی را که می تواند برای ترجمه نام مورد نظر مفید باشد ، به سرویس دهنده محلی معرفی می کند؛ سرویس دهنده محلی مجدداً یک تقاضا به ماشین معرفی شده در مرحله قبل ارسال می کند. در این حالت هم سرویس دهنده نام می تواند در صورت یافتن آدرس

IPبا آن نام حوزه ، آنرا ترجمه کند و یا آنکه آدرس سرویس دهنده سطح پایینتری را به او برگرداند .این روند ادامه می یابد تا DNS نهایی نام مورد نظر را به آدرس IP ترجمه نماید. برای درک بهتر از روند کار به شکل زیر دقت کنید. در این مثال فرض شده است که یک برنامه کاربردی با فراخوانی "تابع تحلیلگر نام"، تقاضای ترجمه نام www.microsoft.com را می نماید.

مراحلی که انجام می شود به شرح زیر است:

I. در مرحله اول برنامه کاربردی با فراخوانی "تابع تحلیل نام" ، تقاضای ترجمه آدرس www.microsoft.comرا برای سرویس دهنده محلی ارسال کرده و منتظر می ماند.
II. در مرحله دوم ، سرویس دهنده محلی از سرویس دهنده Root (که حوزه های متفاوت را تفکیک می کند) آدرس ماشین یک DNS که متولی حوزه com. است را سؤال می کند.
III. در مرحله سوم ، آدرس سرویس دهنده مربوط به حوزه com. بر می گردد.
IV. در مرحله چهارم ، سرویس دهنده محلی ، از ماشین معرفی شده در مرحله قبلی ، آدرس سرویس دهنده مربوط به حوزه Microsoft.com را سؤال می نماید.
V. در مرحله پنجم فهرستی از سرویس دهنده های DNS مربوط به Microsoft.com بر می گردد.
VI. در مرحله ششم، سرویس دهنده محلی تقاضای ترجمه آدرس نمادین www.microsoft.com را از DNS متعلق به حوزه Microsoft.com می کند.
VII. در مرحله هفتم ، معادل آدرس IP نام www.microsoft.com برمی گردد.
VIII. در مرحله هشتم ، آدرس IP خواسته شده در اختیار برنامه کاربردی قرار می گیرد.

۲) **پرس و جوی بازگشتی:** در این روش هر گاه برنامه ای بخواهد آدرس IP معادل یک نام مثل cs.yale.edu را بدست آورد بگونه ای که قبلاً اشاره شد ، "تابع سیستمی تحلیل نام" را فراخوانی می کند. این تابع یک ماشین را بعنوان سرویس دهنده محلی از قبل می شناسد و بنابراین تقاضای تبدیل نام را به روش UDP برای آن ارسال کرده و منتظر جواب می ماند. (پاسخ نهایی DNS طبیعتاً باید یک آدرس ۳۲ بیتی معادل آدرس IP یک ماشین باشد) دو حالت ممکن است اتفاق بیفتد:

I. ممکن است در بانک اطلاعاتی مربوط به سرویس دهنده محلی ، آدرس IP معادل با آن نام از قبل وجود داشته و بالطبع به سرعت مقدار معادل IP آن بر می گردد.
II. ممکن است در بانک اطلاعاتی سرویس دهنده محلی ، معادل IP آن نام وجود نداشته باشد.مثلاً سرویس دهنده محلی در بانک اطلاعاتی خودش معادل IP نامcs.mit.eduرا نداشته و طبیعتاً نمی تواند آن را ترجمه کند. در چنین حالتی سرویس دهنده محلی موظف است بدون آنکه به تقاضا دهنده خبر بدهد، خودش رأساً به سرویس دهنده سطح بالاتر تقاضای ترجمه آدرس بدهد. در این حالت هم DNS سطح بالاتر به همین نحو ترجمه آدرس را پیگیری می کند یعنی اگر معادل IP آن نام را داشته باشد آنرا برمی گرداند و در غیر اینصورت خودش از سرویس دهنده سطح پایینتر تقاضای ترجمه آن نام را می نماید و این مراحل تکرار می شود. در روش پرس و جوی بازگشتی ماشین سرویس دهنده محلی این مراحل

متوالی را نمی بیند و هیچ کاری جز ارسال تقاضای ترجمه یک آدرس بر عهده ندارد و پس از ارسال تقاضا برای سرویس دهنده سطح بالا منتظر خواهد ماند. بازهم تکرار می کنیم ، روشی که DNS برای ترجمه آدرس بکار می برد می تواند بدون اتصال (UDP) باشد که این کار به سرعت عمل ترجمه آدرس می افزاید. دقت کنید که در روش پرس و جوی تکراری نسبت به روش پرس و جوی بازگشتی ، حجم عمده عملیات بر عهده سرویس دهنده DNS محلی است و مدیریت خطاها و پیگیری روند کار ساده تر خواهد بود و روش منطقی تری برای بکارگیری در شبکه اینترنت محسوب می شود. روش پرس و جوی بازگشتی برای شبکه های کوچک کاربرد دارد .

۳) پرس و جوی معکوس: فرض کنید حالتی بوجود بیاید که یک سرویس دهنده DNS ، آدرس IP یک ماشین را بداند ولی نام نمادین معادل با آن را نداند. بعنوان مثال DNS مایل است بداند که چه نامی در شبکه اینترنت معادل با ۱۹۵.۱۳.۴۲.۷ می باشد. در چنین حالتی مسئله کمی حادتر به نظر می رسد ، چرا که برای ترجمه نامهای نمادین ، چون این نامها دارای حوزه و زیرحوزه هستند ، تحلیل آدرسها ساده است ولی ترجمه آدرس IP به معادل نام حوزه ، از چنین روابطی تبعیت نمی کند ؛ بعبارت بهتر هیچ ارتباط مستقیم و متناظری بین آدرسهای IPو اسامی انتخاب شده در اینترنت وجود ندارد. برای یافتن نامهای متناظر با یک آدرس IP باید یک جستجوی کامل و در عین حال وقتگیر انجام بشود. روش کار بدین صورت است که سرویس دهنده محلی یک تقاضا برای DNSمتناظر با شبکه ای که مشخصه آن در آدرس IP ، مشخص شده ، ارسال می کند. بعنوان مثال آدرس IP شبکه ای را ۱۳۸.۱۴.۷.۱۳ در نظر بگیرید ، آدرس کلاس B و مشخصه آن ۱۳۸.۱۴.۰.۰ است . زمانی که مؤسسه ای یک کلاس IP ثبت می دهد یک سرویس دهنده DNS ، متناظر با شبکه خود ایجاد کرده و آنرا نیز معرفی می کند. سرویس دهنده محلی بایستی آدرس DNS متناظر با شبکه ۱۳۸.۱۴.۰.۰ را پیدا کرده و سپس برای آن یک تقاضا ارسال کند DNS .مربوط به این شبکه ، براساس زیر شبکه هایی که دارد این سؤال را از طریق سرویس دهنده های متناظر با هر زیر شبکه پیگیری می کند) .چون هر زیر شبکه یک سرویس دهنده DNS مخصوص به خود دارد (نهایتاً یک نام نمادین حوزه معادل با آن آدرس IP بر خواهد گشت.

:Queries&Resolution

یک سرویس گیرنده به منظور استفاده از DNS و اخذ پاسخ لازم از دو روش متفاوت استفاده می نماید :

۱) **non Recursive query** : در روش اول، سرویس گیرنده با سرویس دهندگان نام ارتباط برقرار می نماید . فرآیند فوق مادامیکه سرویس دهنده مجاز شامل اطلاعات مورد نیاز پیدا نشود ، ادامه خواهد یافت.

۲) **Recursive query** : در روش دوم ، ماموریت ترجمه نام به آدرس به DNS واگذار می‌شود . در این روش سرویس گیرنده اقدام به ارسال درخواست خود برای DNS نموده و DNS پس از انجام عملیاتی خاص و یافتن آدرس IP سایت درخواستی ، آن را برای سرویس گیرنده ارسال می نماید.

به منظور آشنائی با نحوه انجام عملیات فوق به بررسی یک نمونه مثال می‌پردازیم . زمانی که شما قصد مشاهده یک وب سایت نظیر وب سایت شرکت سیسکو (www.cisco.com) را داشته باشید ، پس از فعال نمودن مرورگر

وب و تایپ آدرس http://www.cisco.com و یا www.cisco.com ، پس از مدت زمان کوتاهی ! صفحه اصلی وب سایت در مرورگر شما نمایش داده می‌شود. برای یافتن آدرس IP وب سایت درخواستی مراحل زیر دنبال می شود :

مرحله اول: فعال نمودن مرورگر و درج آدرس www.cisco.com در بخش آدرس آن . در این مقطع کامپیوتر شما دارای آگاهی لازم در خصوص آدرس IP وب سایت سیسکو نمی باشد. بنابراین یک درخواست DNS را برای سرویس دهنده DNS مربوط به مرکز ارائه دهنده سرویس های اینترنت (ISP) ارسال می نماید . حتما" این سوال برای شما مطرح شده است که کامپیوتر به چه صورت از آدرس IP سرویس دهنده DNS آگاهی می یابد تا درخواست خود را برای وی ارسال نماید ؟ در صورتی که شما از طریق Dial-up به اینترنت متصل شده اید ، این موضوع با استفاده از تنظیمات انجام شده (ایستا و پویا) پروتکل TCP/IP مرتبط با آداپتور مجازی Dial-up انجام خواهد شد . در صورتی که دارای یک اتصال دائم به اینترنت و از طریق یک شبکه محلی می باشید ، این موضوع با استفاده از تنظیمات انجام شده (ایستا و پویا) پروتکل TCP/IP مرتبط با آداپتور کارت شبکه انجام خواهد شد.

مرحله دوم: سرویس دهنده DNS مرکز ارائه دهنده خدمات اینترنت (ISP) شما ، آدرس IP مربوط به سایت سیسکو را نمی داند و بدین دلیل، آدرس سایت فوق را از یکی از سرویس دهندگان نام ریشه درخواست می نماید.

مرحله سوم: سرویس دهنده DNS ریشه ، بانک اطلاعاتی خود را بررسی نموده و از سرویس دهنده DNS اولیه Cisco.com آگاهی می یابد (:IP ۱۹۸.۱۳۳.۲۱۹.۲۵) . پس از آگاهی از آدرس IP سرویس دهنده DNS مربوط به cisco.com ، پاسخ لازم برای سرویس دهنده ISP شما ارسال می گردد.

مرحله چهارم: در این مرحله سرویس دهنده DNS مرکز ISP شما دانش لازم به منظور ارتباط با سرویس دهنده DNS سیسکو را پیدا نموده و پس از برقراری ارتباط از وی آدرس IP وب سایت سیسکو (www.cisco.com) را جویا می شود. بدین منظور سرویس دهنده شما یک درخواست Recursive را برای سرویس دهنده DNS مربوط به Cisco.com ارسال می نماید.

مرحله پنجم: سرویس دهنده DNS سیسکو، بانک اطلاعاتی خود را بررسی نموده و از وجود رکورد www.cisco.com در بانک آگاه می گردد. رکورد فوق دارای یک آدرس IP معادل :IP۱۹۸.۱۳۳.۲۱۹.۲۵ است . در این حالت خاص ، سرویس دهنده وب بر روی ماشین مشابهی است که سرویس دهنده DNS نصب شده است. در صورتی که سرویس دهنده وب و سرویس دهنده DNS بر روی یک ماشین مشابه نصب نشده باشند ، آدرس IP آنان متفاوت بوده و این موضوع از طریق رکوردهای منبع موجود در بانک اطلاعاتی سرویس دهنده DNS مشخص می گردد .

مرحله ششم: سرویس دهنده DNS مربوط به ISP شما از آدرس IP مربوط به www.cisco.com آگاهی پیدا نموده و نتایج را برای کامپیوتر شما ارسال می نماید .

مرحله هفتم: کامپیوتر شما در این مقطع دارای آگاهی لازم در خصوص آدرس IP وب سایت سیسکو بوده و می تواند با آن ارتباط برقرار نماید . بنابراین کامپیوتر شما یک درخواست http را مستقیما" برای سرویس دهنده وب سیسکو ارسال نموده و از وی درخواست یک صفحه وب را می‌نماید .

۱۰- آی پی و زیر ساخت های آن

دنیای تکنولوژی پر از ناشناخته‌هایی است که هر کدام از ما نهایتا توانسته‌ایم بخش کوچکی از آن را درک یا تجربه کنیم، هر روز با عبارات و پدیده های جدیدی روبرو می شویم که ناخودآگاه ذهن جستجوگرمان را به کاوش وا می‌دارند، عرصه وب نیز به عنوان زیر مجموعه ای از این دنیای پهناور، ناگفته ها و ناشناخته های زیادی می تواند در خود به صورت بالقوه و نهفته داشته باشد که البته دانستن تمام آنها نه لازم است و نه مقدور.

IP

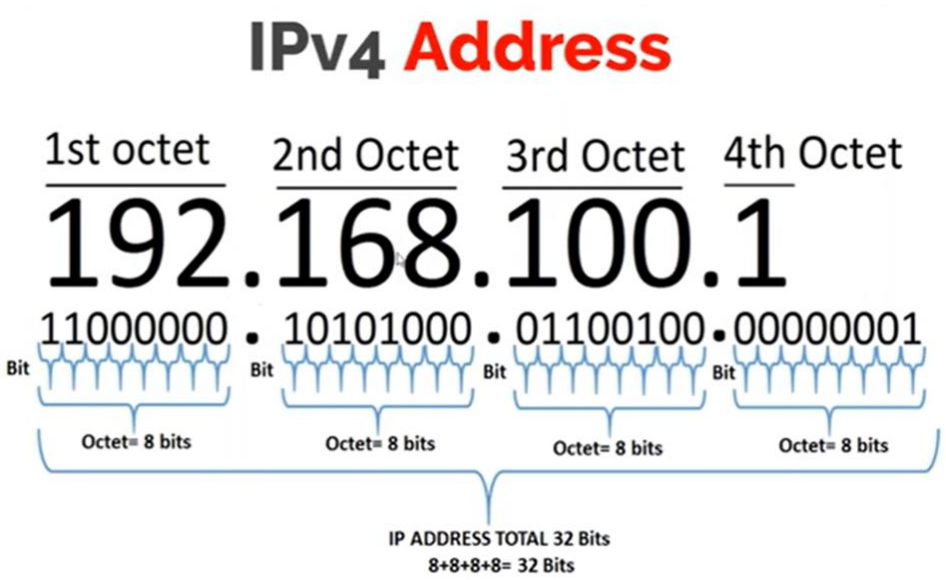
(IP آی پی) که آن را IP address هم می گویند در واقع مخفف عبارت Internet Protocol address یا آدرس های پروتکل اینترنت (شبکه جهانی) است که به صورت یک سری اعداد با قاعده، به هر وسیله ای (اعم از کامپیوتر، تلفن همراه، چاپگر و...)که به شبکه وب متصل شود، اختصاص داده می شود، IPدر واقع یک شماره شناسایی یکتا برای یک ارتباط تحت وب است که با آن کامپیوترهای مختلف (یا سرورهای مختلف) در شبکه گسترده وب از هم بازشناخته می شوند، بدین ترتیب موقعیت جغرافیایی کاربر، اطلاعات اتصال به شبکه و... قابل شناسایی و پیگیری است، البته باید توجه نمود که بیشتر کاربران خانگی از IP اختصاص داده شده توسط سرویس دهنده خود (ISP) یا Internet service provider استفاده می کنند، لذا IP آنان در واقع شماره اختصاص داده شده توسط شرکت خدمات دهنده اینترنت است که معمولا تعداد و سری خاصی از IP ها را برای اتصال در اختیار دارد، از این رو IP شما در هر بار اتصال به اینترنت ممکن است تغییر کند، منتها کشور، نام و موقعیت جغرافیایی سرویس دهنده شما همان اطلاعات ISP خواهد بود، چون شما از یکی از کانال ها و شماره های اتصال آن شرکت استفاده می‌کنید.

کامپیوترها برای حضور در شبکه نیاز به آدرس شناسایی دارند. این آدرس IP یا Internet Protocol نامیده می‌شود یک آدرس IP ممکن است به شکل (216.27.61.137) باشد. این صورت از مقادیر در مبنای ۱۰ نوشته می‌شود و همانطور که می‌بینید دارای سه نقطه و چهار ناحیه مختلف است.

البته آدرس‌های IP به این صورت برای کامپیوترها قابل درک نیستند.کامپیوترها هر کدام از قسمت‌های بین دو نقطه را در مبنای دو می‌بینند. برای مثال آدرس IP که در بالا مشاهده کردید برای کامپیوترها به شکل زیر ترجمه می‌شود:

(11011000.00011011.00111101.10001001)

هر کدام از قسمت‌های آدرس یک هشت‌تایی یا یکOctet نامیده می‌شود. دلیل این نامگذاری نیز این است که هر کدام از این قسمت‌ها ۸ حالت متفاوت دارد. وقتی همه حالات را با هم جمع کنیم ۳۲ ترکیب مختلف ایجاد می‌شود. به همین دلیل هم آدرس‌های IP با چنین فرمتی را آدرس‌های ۳۲ بیتی می‌نامند. در مبنای دو نیز هر عدد دو حالت(۱ یا ۰) و هر قسمت از آدرس ۸ ترکیب مختلف دارد. به این ترتیب تمام ترکیب‌های هر قسمت ۲۸ یا ۲۵۶ است.



چطور بیت و بایت کار می‌کند؟

حدود ۴.۳ میلیارد ترکیب مختلف از اکتت‌ها می‌توان بدست آورد. البته تمام حالات این ترکیب‌ها قابل استفاده نیستند. برای مثال ۰.۰.۰.۰به صورت قراردادی برای پیش‌فرض شبکه و آدرس ۲۵۵.۲۵۵.۲۵۵.۲۵۵ نیز برای انتشار در شبکه (Broadcast) مورد استفاده قرار می‌گیرد.

هر آدرس IP به دو قسمت Net و Host تقسیم می‌شود. قسمت Net بیانگر آدرس شبکه‌ای است که آدرس به آن تعلق دارد و Host هر آدرس در شبکه Net را مشخص می‌کند. ترتیب مورد استفاده برای تخصیص Net و Host به یک آدرسIP ، بستگی به کلاس (Class) آن آدرس دارد.

در کل ۵ کلاس و تعدادی آدرس IP ثابت وجود دارد:

پیش‌فرض شبکه 0.0.0.0 :

کلاس A: این نوع کلاس بیشتر برای تخصیص IP در شبکه‌های بزرگ مورد استفاده قرار می‌گیرد. اکتت اول این کلاس‌ها از ۱ تا ۱۲۶ متفاوت می‌باشد. از باقی اکتت‌ها برای Host استفاده می‌شود. به این ترتیب ۱۲۶ شبکه، ۱۶۷۷۷۲۱۴ هاست و ۲۱۴۷۴۸۳.۶۴۸ آدرس در کلاس Aتعریف می‌شود. حدود نیمی از ترکیب‌های موجود برای تمام آدرس‌هایIP ، در این کلاس قرار می‌گیرند. اولین رقم این آدرس‌ها در مبنای دو نیز با ۰ شروع می‌شود. برای مثال یک آدرس در این کلاس می‌تواند به صورت زیر باشد:

Net	Host
24.53.107	.115

Loopback : آدرس ۱۲۷.۰.۰.۱ برای عملیاتی به نام Loopback استفاده می‌شود Loopback .زمانی انجام می‌شود که یکی از کامپیوترهای میزبان بسته‌ای را برای خودش می‌فرستد. کاربرد این متد در رفع مشکل و تست اتصالات شبکه است.

کلاس B: معمولاً شبکه‌های متوسط از این نوع کلاس بهره می‌برند. آدرس‌هایی که اولین اکتت آن‌ها از ۱۲۸ تا 191تغییر می‌کند عضو این کلاس هستند. اکتت دوم این آدرس‌ها نیز برای تعیین Net، و دو اکتت دیگر برای

مشخص کردن آدرس Host مورد استفاده قرار می‌گیرد .به این ترتیب ۱۶۳۴۸ شبکه با ۶۵۵۳۴ هاست و ۱۰۷۳۷۴۱۸۲۴ آدرس IP مختلف در این کلاس قابل تخصیص است. اولین رقم اولین اکتت این آدرس‌ها در مبنای دو ۱ و رقم دوم ۰ است.

Net	Host
145.24.	53.107

کلاس :C شبکه‌های کوچک می‌توانند از این کلاس استفاده کنند. آدرس‌های که اکتت اول آن‌ها از ۱۹۲ تا 223 است در این کلاس قرار می‌گیرند. اکتت‌های اول تا سوم برای معین کردن آدرس Net و باقی برای تخصیص آدرس به Host مورد استفاده قرار می‌گیرد .می‌توان ۲۰۹۷۱۵۲ شبکه با ۲۵۴ Host و ۵۳۶۸۷۰۹۱۲ آدرس IP در کلاس C ایجاد کرد. این آدرس‌ها در مبنای دو دارای اولین رقم ۱ دومین رقم ۱ و سومین رقم ۰ است.

Net	Host
195.24.53.	107

کلاس :D از این کلاس برای Multicast استفاده می‌شود و کمی با کلاس‌ها و آدرس‌ها قبلی تفاوت دارد .اولین، دومین و سومین بیت این آدرس‌ها با ۱ و چهارمین بیت با صفر شروع می‌شود. ۲۸ بیت بعدی برای مشخص کردن آدرس مقصد پیغام‌های Multicast مورد استفاده قرار می‌گیرد. یک شانزدهم ترکیب‌های آدرس IP 268435456 آدرس بخشی از این کلاس هستند.

Net	Host
224.	24.53.107

کلاس :E این کلاس شباهتی زیادی به کلاس D دارد و بیشتر در موارد آزمایشی مورد استفاده قرار می‌گیرد. تنها تفاوت آن با کلاس D این است که بیت چهارم آن از ۱ شروع می‌شود.

Net	Host
240.	24.53.107

Broadcast: پیغام‌هایی که همواره برای تمام اعضای شبکه فرستاده می‌شود با نام Broadcast شناخته و با روش Broadcastارسال می‌شوند. این پیغام‌ها از آدرس ۲۵۵.۲۵۵.۲۵۵.۲۵۵ استفاده می‌کنند.

آدرس‌هایی که بررسی کردیم دارای ۳۲ ($۲^۴$) بیت رقم بودند به همین دلیل آن‌ها را بیشتر به آدرس‌های IPv4 می‌شناسند.

Class	HOB	NET ID Bits	Host ID Bits	No of Networks	Host Per Network	Start Address	End Address
Class A	0	8	24	2^7=128	2^{24}=16,777,216	0.0.0.0	127.255.255.255
Class B	10	16	16	2^{14}=16,384	2^{16}=65,536	128.0.0.0	191.255.255.255
Class C	110	24	8	2^{21}=2,097,152	2^8=256	192.0.0.0	223.255.255.255
Class D	1110	-	-	-	-	224.0.0.0	239.255.255.255
Class E	1111	-	-	-	-	240.0.0.0	255.255.255.255