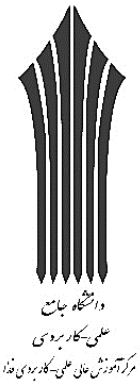


دانشگاه جامع علمی و کاربردی

مرکز آموزش عالی علمی–کاربردی فذا آمل

شبکه های کامپیوتری

دوره کاردانی فنی شبکه های رایانه ای (ناپیوسته)

مدرس

حسین اخوان اسکی

کارشناس ارشد نرم افزار

فهرست مطالب

عنوان **صفحه**

فصل اول

مفاهیم و اصول

شبکه های کامپیوتری

شبکه کامپیوتری چیست ؟

♦یک شبکه کامپیوتری شامل دو یا بیش از دو کامپیوتر و ابزارهای جانبی مثل چاپگرها، اسکنرها و مانند اینها هستند که بطور مستقیم بمنظور استفاده مشترک از سخت افزار، نرم افزار، منابع اطلاعاتی و ابزارهای متصل ایجاده شده است .

♦تمامی تجهیزات سخت افزاری و نرم افزاری موجود در شبکه را 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 و داده ها با کامپیوترهای دیگر همزمان بهره ببرد.

تاریخچه شبکه های کامپیوتری

در سال ۱۹۵۷ نخستین ماهواره، توسط اتحاد جماهیر شوروی سابق به فضا پرتاب شد. در همین دوران رقابت سختی از نظر تسلیحاتی بین دو ابرقدرت آن زمان جریان داشت، وزارت دفاع امریکا در واکنش به این اقدام رقیب نظامی خود، آژانس پروژه های تحقیقاتی پیشرفته یا آرپا (ARPA) را تاسیس کرد. یکی از پروژه های مهم این آژانس تامین ارتباطات در زمان جنگ جهانی احتمالی تعریف شده بود. در همین سال ها در مراکز تحقیقاتی غیر نظامی که بر امتداد دانشگاه ها بودند، تالش برای اتصال کامپیوترها به یکدیگر در جریان بود. در آن زمان کامپیوتر هایMainframe از طریق ترمینال ها به کاربران سرویس می دادند. در اثر اهمیت یافتن این موضوع آژانس آرپا (ARPA) منابع مالی پروژه اتصال دو کامپیوتر از راه دور به یکدیگر را در دانشگاهMIT بر عهده گرفت. در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر راه اندازی شد. این شبکه آرپانت نامگذاری شد. شبکه آرپانت که به امور نظامی اختصاص داشت، اما در سال ۱۹۶۷ به عموم معرفی شد. در این سال شبکه آرپانت مراکز کامپیوتری بسیاری از دانشگاه ها و مراکز تحقیقاتی را به هم متصل کرده بود.

در سال ۱۹۶۷ نخستین نامه الکترونیکی از طریق شبکه منتقل شد. در این سال ها حرکتی غیرانتفاعی به نام MERITکه چندین دانشگاه بنیانگذار آن بوده اند، مشغول توسعه روش های اتصال کاربران ترمینال ها به کامپیوتر مرکزی یا میزبان بود. مهندسان پروژهMERIT در تالش برای ایجاد ارتباط بین کامپیوترها، مجبور شدند تجهیزات الزم را خود طراحی کنند. آنان با طراحی تجهیزات واسطه برای مینی کامپیوتر، نخستین بستر اصلی یا Backdone شبکه کامپیوتری را ساختند. تا سال ها نمونه های اصالح شده این کامپیوتر با نام PCP نقش میزبان را در شبکه ها ایفا می کرد. نخستین شبکه از این نوع که چندین ایالت را به هم متصل می کرد Michnet نام داشت. روش اتصال کاربران به کامپیوتر میزبان در آن زمان به این صورت بود که یک نرم افزار خاص روی کامپیوتر مرکزی اجرا می شد و ارتباط کاربران را برقرار می کرد اما در سال ۱۹۷۶ نرم افزار جدیدی به نامHermes عرضه شد که برای نخستین بار به کاربران اجازه می داد از طریق یک ترمینال به صورت تعاملی مستقیماً به سیستمMERIT متصل شوند. از وقایع مهم تاریخچه شبکه های کامپیوتری، ابداع روش سوئیچینگ بسته ای است. قبل از معرفی شدن این روش از سوئیچینگ مداری برای تعیین مسیر ارتباطی استفاده می شد اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطیIP/TCP این پروتکل جایگزین پروتکل NCP شد و به پروتکل استاندارد برای آرپانت تبدیل شد. با این تغییر و تحول، شبکه های زیادی به بخش تحقیقاتی این شبکه متصل شدند و آرپانت به اینترنت تبدیل.شد

اهداف و مزایای شبکه های کامپیوتری

۱ - استفاده مشترک از منابع : استفاده مشترک از یک منبع اطلاعاتی یا امکانات جانبی رایانه، بدون توجه به محل جغرافیایی هریک از منابع را استفاده از منابع مشترک گویند .

۲ -کاهش هزینه : متمرکز نمودن منابع و استفاده مشترک از آنها و پرهیز از پخش آنها در واحدهای مختلف و استفاده اختصاصی هرکاربر در یک سازمان کاهش هزینه را در پی خواهد داشت.

۳- قابلیت اطمینان : این ویژگی در شبکه ها بوجود سرویس دهنده های پشتیبان در شبکه اشاره می کند، یعنی به این معنا که می توان از منابع گوناگون اطلاعاتی و سیستم ها در شبکه نسخه های دوم و پشتیبان تهیه کرد ودر صورت عدم دسترسی به یکی از منابع اطلاعاتی در شبکه " بعلت از کارافتادن سیستم " از نسخه های پشتیبان استفاده کرد. پشتیبانی از سرویس دهنده ها در شبکه، کارآیی وآمادگی دائمی سیستم را افزایش می دهد.

۴ - کاهش زمان : یکی دیگر از اهداف ایجاد شبکه های رایانه ای، ایجاد ارتباط قوی بین کاربران از راه دور است ؛ یعنی بدون محدودیت جغرافیایی تبادل اطلاعات وجود داشته باشد . به این ترتیب زمان تبادل اطلاعات و استفاده از منابع خود بخود کاهش می یابد .

۵ – قابلیت توسعه : یک شبکه محلی می تواند بدون تغییر در ساختار سیستم توسعه یابد و تبدیل به یک شبکه بزرگتر شود. در اینجا هزینه توسعه سیستم هزینه امکانات وتجهیزات مورد نیاز برای گسترش شبکه مد نظر است .

۶ – ارتباطات : کاربران می توانند از طریق نوآوری های موجود مانند پست الکترونیکی و یا دیگر سیستم های اطلاع رسانی پیغام هایشان را مبادله کنند ؛ حتی امکان انتقال فایل نیز وجود دارد.

ابعاد تقسیم بندی شبکه های کامپیوتری

شبکه های کامپیوتری را بر اساس مولفه های متفاوتی تقسیم بندی می نمایند. در ادامه به برخی از متداولترین تقسیم بندی های موجود اشاره می گردد .

- ♣ تقسیم بندی شبکه از بعد جغرافیایی
- ♣ تقسیم بندی شبکه از بعد نوع سوئیچینگ
- ♣ تقسیم بندی شبکه ها از بعد تکنولوژی انتقال
- ♣ تقسیم بندی شبکه ها از بعد توپولوژی

تقسیم بندی شبکه از بعد جغرافیایی

شبکه های کامپیوتری با توجه به حوزه جغرافیائی تحت پوشش به سه گروه تقسیم می گردد :

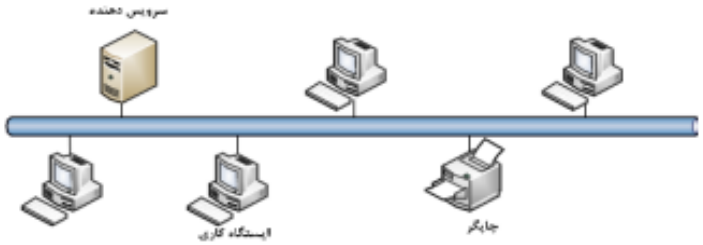
♣شبکه های محلی (LAN)

♣شبکه های متوسط (MAN)

♣شبکه های گسترده(WAN)

شبکه های محلی (LAN)

حوزه جغرافیائی که توسط این نوع از شبکه ها پوشش داده می شود، یک محیط کوچک نظیر یک ساختمان اداری است این نوع از شبکه ها دارای ویژگی های زیر می باشند :



♣ توانائی ارسال اطلاعات با سرعت بالا

♣ محدودیت فاصله

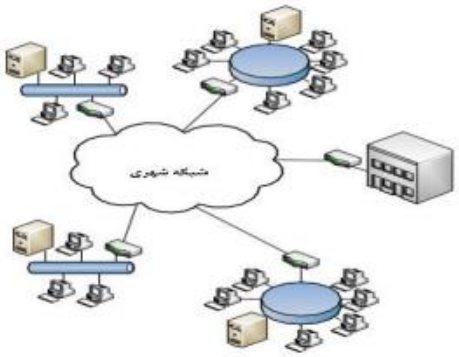
♣ قابلیت استفاده از محیط مخابراتی ارزان نظیر خطوط تلفن بمنظور ارسال اطلاعات

♣ نرخ پایین خطاء در ارسال اطلاعات با توجه به محدود بودن فاصله

شبکه های متوسط (MAN)

حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود، در حد و اندازه یک شهر و یا شهرستان است.

ویژگی های این نوع از شبکه ها بشرح زیر است :



♣پیچیدگی بیشتر نسبت به شبکه های محلی

♣برای اتصال شبکه های کوچکتر محلی به یکدیگر استفاده می شوند

♣به هر دو صورت خصوصی و یا عمومی اداره و مدیریت شوند

شبکه های گسترده (WAN)

حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود ، در حد و اندازه کشور و قاره است .

ویژگی این نوع شبکه ها بشرح زیر است :

- ♣ قابلیت ارسال اطلاعات بین کشورها و قاره ها
- ♣ قابلیت ایجاد ارتباط بین شبکه های LAN
- ♣ سرعت پایین ارسال اطلاعات نسبت به شبکه های LAN
- ♣ نرخ خطای بالا با توجه به گستردگی محدوده تحت پوشش
- ♣ وسعت بسیار زیاد شبکه های ملی هر کشور شبکه جهانی اینترنت شبکه تلفن
- ♣ امکان استفاده از تجهیزات متفاوت

(Wide Area Network)

توپولوژی (Topology) یا همبندی یا ریخت شناسی شبکه

اتصال چندین دستگاه به یکدیگر از طریق رسانه انتقال است .

سوال: به چه اشکال یا روش هایی می توان گره ها را به یکدیگر متصل کرد؟ چگونگی اتصال واقعی گره ها به یکدیگر توسط رسانه انتقال یا کانال را توپولوژی می گویند .

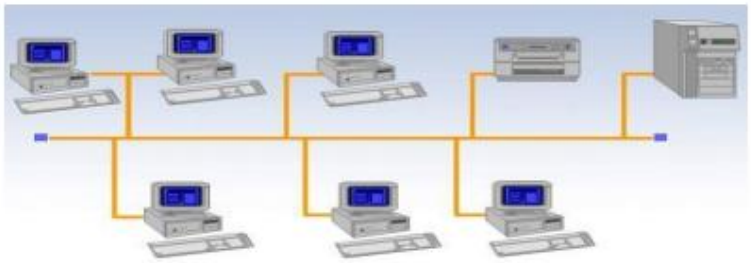
به عبارت دیگر توپولوژی، ساختار یک شبکه را بیان می کند

انواع توپولوژی

Bus	□ گذرگاه مشترک
Star	□ ستار های
Ring	□ حلقه
Tree	□ درخت
Complete	□ کامل
Hybrid	□ ترکیبی

۱- توپولوژی Bus

در این توپولوژی همه کامپیوترها مستقیماً به یک کانال مشترک متصل هستند.



مزایا و معایب bus

♣ برپاسازی ساده و هزینه آن ارزان می باشد .

♣ در صورت قطع شدن یا خرابی کانال مشترک کل شبکه از کار می افتد .

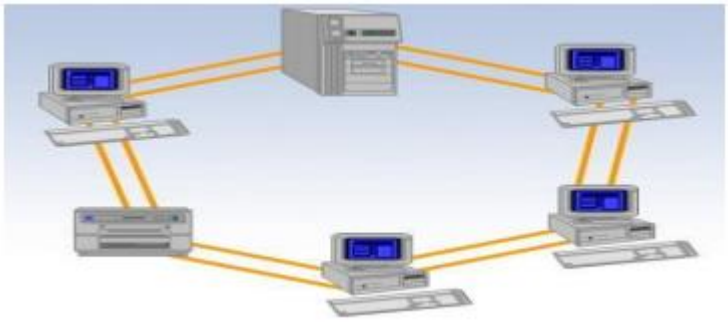
♣ تعداد کامپیوترها و طول کانال مشترک محدود است .

♣ خطایابی و رفع اشکال در این شبکه ها مشکل است .

♦این نوع توپولوژی از توپولوژی های منسوخ شده می باشد.

۲- توپولوژی حلقه (Ring)

♦در این توپولوژی همه کامپیوترها از طریق یک حلقه و به صورت نقطه به نقطه به یکدیگر وصل می شوند



مزایا و معایب Ring

♦مزایا :

♣کم بودن طول کابل

♣ نیاز به فضای خاص جهت انشعابات در کابل کشی نخواهد بود .

♣ مناسب جهت فیبر نوری .

♣ در این توپولوژی به علت این که هر کامپیوتر یک بار اطلاعات را دریافت کرده و دوباره تکرار می کند پدیده تضعیف وجود ندارد .

♦معایب :

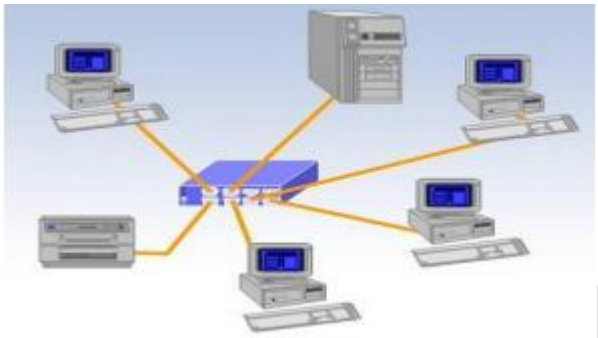
♣ اشکال در یک گره باعث اشکال در تمام شبکه می شود .

♣ اشکال زدایی مشکل .

♣ تغییر در ساختار شبکه مشکل است.

۳- توپولوژی ستاره ای (Star)

در این توپولوژی هر گره از طریق یک کانال اختصاصی نقطه به نقطه مستقیماً به یک ایستگاه مرکزی به نام سوییچ یا هاب متصل می شود.



در توپولوژی ستاره ای (Star)

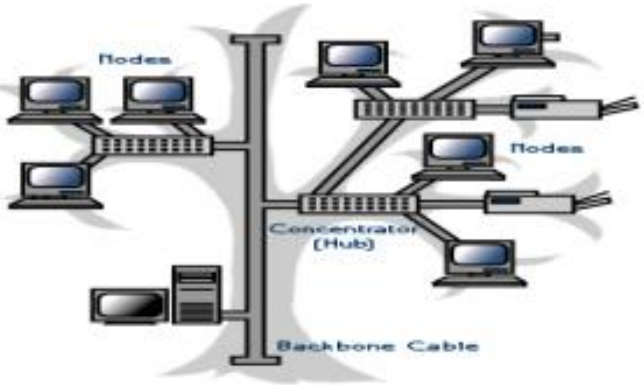
♦ارتباط گره ها با یکدیگر از طریق ایستگاه مرکزی انجام می شود .

♦در صورت خرابی یا قطع شدن هر کانال کل شبکه از کار نمی افتد اما در صورت خرابی ایستگاه مرکزی کل شبکه از کار می افتد .

♦در این توپولوژی تعداد کانال زیادی استفاده می شود.

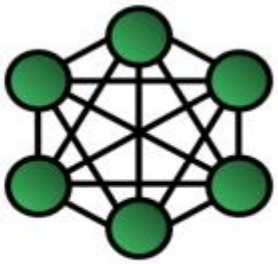
۴- توپولوژی درخت (Tree)

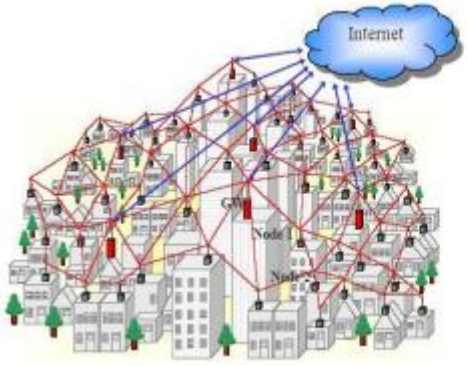
این توپولوژی گسترش یافته شبکه ستاره ای و مبتنی بر کانال نقطه به نقطه است به طوری که تعدادی هاب به یکدیگر اتصال دارند و کامپیوترها به هاب ها متصل هستند.



۵- گراف کامل (Mesh)

در این توپولوژی هر گره مستقیماً از طریق کانال نقطه به نقطه به هر کامپیوتر دیگر در شبکه اتصال دارد.



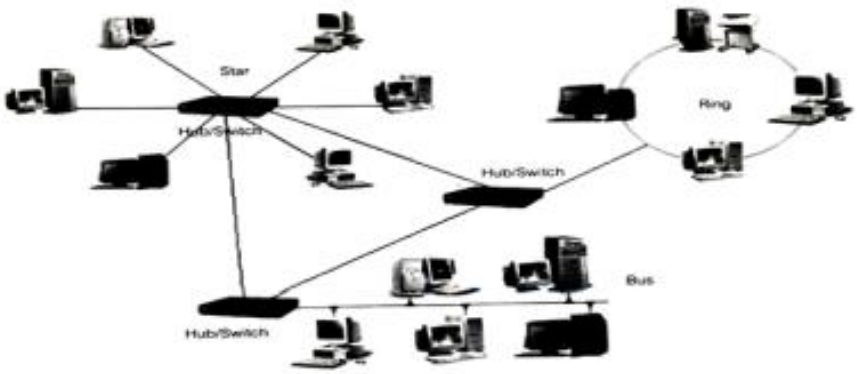


مزایا و معایب Mesh

- سرعت انتقال داده بالا می باشد .
- قابلیت اطمینان بالا (با خرابی چند کانال کل شبکه از کار نمی افتد)
- عدم وجود مشکل ترافیک در شبکه
- برپاسازی شبکه مش مشکل و پیچیده و هزینه بر است .
- قابلیت گسترش و افزودن کامپیوترهای جدید به این شبکه مشکل است.

۶- ترکیبی (Hybrid)

شبکه های بزرگ معمولاً از اتصال چندین توپولوژی مختلف تشکیل شده اند این توپولوژی بزرگ را به نام توپولوژی ترکیبی می شناسند.



ساختار شبکه های کامپیوتری

شبکه های کامپیوتری از لحاظ ساختار منطقی به دو دسته تقسیم میشوند:

۱- Work Group یا شبکه های کاری یا (Peer to Peer)

۲- Server Based یا مبتنی بر دامنه یا (Client – Server – Domain)

Work Groupیا شبکه های کاری یا (Peer to Peer)

اگر در یک شبکه کامپیوتری، سیستم ها همزمان علاوه بر ارائه سرویس از سرویس های سایر سیستم ها نیز استفاده کنند میگوییم مدل سرویس دهی در شبکه به صورت Peer to Peer یا نظیر به نظیر است.

به عبارت دیگر، در صورتی که سیستم ها به طور همزمان هم سرویس دهنده باشند و هم سرویس گیرنده، مدل شبکه اجرا شده نظیر به نظیر یا به اختصار (PtP) است.

در شبکه های نظیر به نظیر، سرویس دهنده اختصاصی وجود ندارد و سلسله مراتبی در رابطه با رایانه ها رعایت نمیشود.

تمام کامپیوترها معادل و همتراز هستند و امنیت به صورت محلی و بر روی هر کامپیوتر ارائه میگردد. به عبارت دیگر هر سیستم مسئول تعیین امنیت و سیاست های کاری خود است.

کاربر هر یک از کامپیوترها مشخص میکند که چه داده ای بر روی سیستم خود را برای اشتراک گذاری قرار دهد.

شبکه های نظیر به نظیر Workgroup نیز نامیده میشوند.

واژه Workgroup نشان دهنده یک گروه کوچک از کامپیوترهای مرتبط با یکدیگر است.

شبکه های Peer to Peer انتخابی مناسب برای محیط هایی با شرایط زیر هستند:

–حداکثر تعداد کابران ۱۰ و یا کمتر (به طور معمول)

–کاربران، منابع (نظیر چاپگر ها و ...) را به اشتراک گذاشته و در این راستا سرویس دهندگان خاصی وجود نداشته باشد.

–امنیت متمرکز مورد نظر نباشد.

–رشد سازمان و شبکه بر اساس آنالیز انجام شده، محدود باشد.

این نوع شبکه ساده ترین و سریعترین روش شبکه سازی به ویژه در محیط های ویندوز می باشد که ابزار خاصی لازم نداشته و دارای مزایای زیر است:

مزایای شبکه: Workgroup

– هزینه راه اندازی و نگهداری پایین تر

– سرعت بیشتر در راه اندازی

– دم نیاز به یک کامپیوتر مجزار به عنوان سرور

به نظر میرسد تنها ویژگی مدل شبکه Peer to Peer نصب و راه اندازی آسان و کم هزینه باشد.

معایب شبکه: Workgroup

– امنیت پایین: (Low Security)

امینت پایین این نوع شبکه که پیشتر نیز به آن اشاره شد به این معنا نیست که هر کامپیوتری با وصل کردن کابل شبکه بتواند وارد چرخه شبکه شده و از منابع سایر سیستم ها استفاده کند.

در اصل هر کامپیوتر بخشی به نام LSD (Local Security Database) دارد که اطلاعات مربوط به کاربران را در خود ثبت میکند . LSD هر رایانه نیز متعلق به خود آن رایانه است.

در این نوع شبکه ها برای اتصال به کامپیوتر دیگر باید یک Username و Password وارد کردن که این دو مورد همان نام کاربری و رمز عبور فرد در ویندوز هستند.پس از وارد کردن این اطلاعات، کامپیوتر میزبان در LSD خود به دنبال این اطلاعات میگردد و اگر اطلاعات ارسالی در آن موجود باشد، اجازه دسترسی را صادر میکند.

– عدم وجود مدیریت مرکزی(No Centralize Manage)

در این نوع شبکه ها هیچ گونه مدیریت مرکزی وجود ندارد. به عنوان مثال در صورت اضافه شدن یک کاربر جدید، باید نام کاربری و رمز عبور آن را در LSD تمام کامپیوتر ها به صورت دستی وارد کرد و این مسئله بسیار وقتگیر و نا مناسب است.

– محدودیت تعداد کاربران: تعداد کاربران در این نوع شبکه ها محدود است و بهترین حالت آن تا ۱۰ کاربر است.

دلیل این محدودیت را با توضیح انواع ارسال Packet در شبکه شرح میدهیم:

در شبکه ها ۳ نوع ارسال(Packet) داده ارسالی داریم:

۱- Uni Cast: اگر آدرس مقصد داده ارسالی یکی باشد.

۲- Multi Cast: اگر آدرس مقصد داده ارسالی چندین مورد باشد.

در این نوع روش فقط کامپیوترهایی داده را دریافت میکنند که داده به سمت آنها ارسال شده باشد.

۳- Broad Cast: آگر آدرس مقصد داده ارسالی یک دسته باشد.

در این روش تمام کامپیوتر ها داده را دریافت میکنند اما فقط کامپیوترهایی از اطلاعات استفاده میکنند که آدرس آنها در داه ارسالی (Packet) قید شده باشد .این مسئله را در نظر داشته باشید که در شبکه ها، در حالت عادی هیچ گاه نمیتوان از طریق نام یک کامپیوتر به آن دسترسی پیدا کرد و لازم است نام رایانه به آدرس IP تبدیل شود.

علت محدودیت در تعداد کاربران این مدل شبکه این است که چون در شبکه های Workgroup هیچ سرویسی برای تبدیل اسم به IP و برعکس وجود ندارد، بنابراین برای اتصال به یک کامپیوتر، باید Packet به صورت Broad Cast به همه رایانه ها ارسال شود تا رایانه مورد نظر شناسایی شود.

در نتیجه با افزایش تعداد کاربران سرعت این نوع شبکه به شدت افت پیدا میکند.

Server Based یا مبتنی بر دامنه یا (Client – Server – Domain)

اگر در یک شبکه کامپیوتری تعدادی از سیستم هال فقط در نقش سرویس دهنده و تعدادی فقط در نقش سرویس گیرنده ظاهر شوند در اینصورت میگوییم مدل سرویس دهی آن شبکه به صورت Server based به اختصار (SB) است.

به موازات رشد شبکه و افزایش کاربران و منابع موجود، یک شبکه نظیر به نظیر قادر به پاسخگویی به حجم بالای تقاضا برای منابع اشتراکی نخواهد بود . به منظور هماهنگی با افزایش تقاضا و ارائه سرویس های مورد نیزا، شبکه های می بایست از سرویس دهندگان اختصاصی استفاده کنند.

یک سرویس دهنده اختصاصی صرفاً به عنوان یک سرویس دهنده در شبکه ایفای نقش میکند. (نه به عنوان سرویس گیرنده)

شبکه های سرویس گیرنده – سرویس دهنده (Client – Server) به عنوان مدلی استاندارد برای برپاسازی شبکه مطرح شده اند.

همگام با رشد یک شبکه (تعدا سیستم های متصل شده، فاصله فیزیکی و ترافیک موجود) میتوان تعداد سرویس دهندگان در شبکه را افزایش داد. با توزیع مناسب فعالیت های شبکه بین چندین سرویس دهنده، کارآیی شبکه به طرز محسوسی افزایش خواهد یافت. سرویس دهی در این مدل شبکه توسط سیستم هایی صورت میگیرد که اصطلاحاً سرویس دهنده یا Serverنامیده میشوند.

سیستم هایی که از این سرویس استفاده میکنند اصطلاحاً سرویس گیرنده یا Client نامیده میشوند. برای سرویس گیرنده ها اصطلاح Workstation نیز به کار میرود.

نکته ای که در مورد **ساختار Server based** بسیار مهم است این است کهServer ها مدیریت کل شبکه را بر عهده دارند وClient ها فقط کارهایی را میتوانند انجام دهند که Server اجازه انجام آن کارها را داده باشند؛ این تعریف به معنی مدیریت متمرکز است.

به عنوان مثال، کاربری مانند User1 که در شبکه حضور دارد، فقط اجازه دارد از کامپیوترهای خاصی استفاده کند یا مثلاً حق دارد ماهیانه فقط ۳۵۰ دستور چاپ و آن هم به چاپگری خاص ارسال کند.

ساختار لایه ای و معماری شبکه

لایه چیست؟

به منظور تفکیک وظایف و عملیات الزم برای انتقال داده، تعدادی لایه در یک سیستم شبکه تعریف می شود که هر لایه وظیفه خاصی را برای انتقال داده بر عهده دارد ومجموعه لایه ها با کمک یکدیگر عمل انتقال داده به صورت صحیح را تضمین می کنند .

هدف ساختار لایه ای :

♣ کاهش پیچیدگی شبکه

♣ افزایش انعطاف پذیری در مقابل تغییرات احتمالی

ساختار لایه ای و معماری شبکه

♦ویژگی ها :

♣ هر لایه برروی لایه دیگری قرار دارد و با آن در ارتباط است

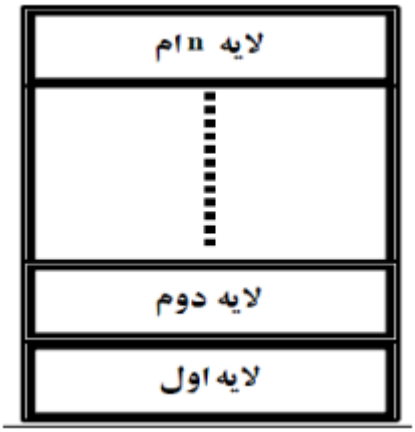
♣ هر لایه شبکه وظایف خاص خود را به عهده دارد و از لایه های دیگر مستقل می باشد

♣ هر لایه ازسرویس لایه پایین تر خود استفاده می نماید و به لایه بالاتر خود سرویس می دهد .

♣ هر لایه شبکه برای انجام وظایف خود از یکسری قواعد و قراردادهای استاندارد استفاده می نماید که به آن پروتکل گفته میشود .

مجموع لایه ها و پروتکل های یک شبکه را معماری شبکه می گویند.

مدل لایه ای



مشکلات مدل لایه ای

♦نیاز به مکانیسمی برای برقراری و قطع ارتبا ط

♦عدم تطابق سرعت لایه های فرستنده و گیرنده

♦محدودیت اندازه بسته ها

♦وقوع خطا در بسته های دریافتی

♦عدم رعایت ترتیب بسته ها

مدل مرجع (OSI (Open System Interconnection

♦مدل OSI در سال ۱۹۸۳ از سوی سازمان جهانی استاندارد ارائه گردید .

♦**سیستم های باز:** مجموعه ای از پروتکل هایی میباشد که امکان اتصال دو سیستم مختلف به یکدیگر را صرف نظراز معماری لایه های پایینی آنها فراهم می آورد .

با استفاده از مدل مرجع OSI امکان اتصال سیستم های مختلف و برقراری ارتباط بین آنها بدون نیاز به اعمال تغییرات در منطق سخت افزار و نرم افزار پایینی آنها وجود دارد.

لایه هایOSI

دو سرویس وجود دارد که توسط لایه ها به لایه های بالاتر داده می‌شود:

۱. **سرویس اتصال گرا (Connection Oriented Service)**

۲. **سرویس بدون اتصال (Connectionless Service)**

سرویس اتصال گرا

دنباله ای از عملیات وجود دارد که توسط کاربران سرویس اتصال گرا دنبال می‌شود:

۱. اتصال برقرار شده است.

۲. اطلاعات ارسال شده اند.

۳. اتصال آزاد شده است.

در این نوع سرویس ما باید قبل از ارتباط، اتصال را برقرار کنیم. هنگامی که اتصال برقرار شده، پیام یا اطلاعات را ارسال می‌کنیم و سپس اتصال را آزاد می‌کنیم.

همچنین در این سرویس اگر خطایی در سمت دریافت کننده ها باشد، می‌توانیم پیام را ارسال کنیم.

TCP (Transmission Control Protocol) یک مثال بارز برای سرویس های اتصال گرا است.

سرویس بدون اتصال

طرز کار این سرویس شبیه به خدمات پستی است. زیرا این سرویس آدرس کامل جایی که پیام باید برود را حمل می‌کند. هر پیام به طور مستقل از مبدا به مقصد ارسال می‌شود. سفارش پیام ارسال شده می‌تواند متفاوت از سفارش پیام دریافت شده باشد.

در این سرویس بدون بررسی اینکه آیا مقصد هنوز وجود دارد یا آماده پذیرش پیام هست یا نه، داده ها در یک سمت از مبدا به سمت مقصد منتقل نمی‌شود. همچنین احراز هویت نیز در این سرویس الزامی نیست. UDP (User Datagram Protocol) یک مثال بارز از این نوع سرویس است.

تفاوت های سرویس های اتصال گرا و بدون اتصال

۱. در سرویس اتصال گرا بر خلاف سرویس بدون اتصال، نیاز به احراز هویت داریم.

۲. سرویس اتصال گرا هنگام ارسال پیام بررسی می‌کند که آیا پیام دریافت شده است یا خیر. اگر خطایی وجود داشت، پیام را دوباره ارسال می‌کند. اما در سرویسس بدون اتصال هیچ ضمانتی مبنی بر رسیدن پیام به مقصد وجود ندارد.

۳. سرویس اتصال گرا قابل اعتماد تر از سرویس بدون اتصال است.

۴. سرویس اتصال گرا بر پایه جریان است و سرویس بدون اتصال بر پایه پیام.

سرویس ها چه هستند؟

سرویس ها در واقع عملیاتی هستند که یک لایه می‌تواند به لایه بالاتر خود در مدل مرجع OSI ارائه دهد. سرویس ها فقط عملیات را تعریف و لایه را اماده می‌کنند اما هیچ چیز در مورد چگونگی اجرای این عملیات مشخص نمی‌کنند.

پروتکل ها چه هستند؟

پروتکل ها (Protocol) مجموعه قوانین و چارچوب هایی هستند که چگونی تبادل پیام بین سرویس دهنده و سرویس گیرنده را مشخص و کنترل می‌کنند.

انواع ارتباط میان دو ایستگاه

۱- ارتباط یکطرفه یا Simplex :

یکطرف همیشه گیرنده و یکطرف همیشه فرستنده

مثال: پخش امواج تلویزیونی توسط فرستنده تلویزیون توسط گیرنده ها

۲- ارتباط دوطرفه غیرهمزمان یا Half duplex

هر دو ماشین هم می توانند فرستنده باشند و هم گیرنده ولی نه بصورت همزمان

مثال:کانال ارتباط و انتقال داده توسط دو دستگاه بی سیم

۳- ارتباط دوطرفه همزمان یا Full duplex

مثال:کانال انتقال صوت و داده توسط دو دستگاه تلفن، خطوط ماکروویو

تقسیم بندی شبکه از لحاظ نوع مداری

در شبکه های کامپیوتری دو نوع مختلف سوئیچینگ وجود دارد

۱- سوئیچینگ مداری (Circuit Switching):

۲- سوئیچینگ سلول و بسته(Packet Switching / Cell Switching)

سوئیچینگ مداری (Circuit Switching)

برای ایجاد یک مدار اختصاصی و مسیر فیزیکی بین دستگاه فرستنده و گیرنده از روش سوئیچینگ مداری در لایه فیزیکی استفاده میشود دارای سه مرحله است :

♣ مرحله برقراری ارتباط بین فرستنده و گیرنده

♣ مرحله انتقال داده

♣مرحله قطع ارتباط

این مدار فقط مختص فرستنده و گیرنده است و دیگر کامپیوتر ها نمی توانند از این مدار استفاده کنند .

داده ها بصورت جریانی از بیت(stream) و بدون نیاز به بسته بندی و قرار دادن آدرس مبدأ ومقصد در مدار اختصاصی بین دو کامپیوتر انتقال می یابد .

مثالی از این روش سوئیچینگ، انتقال صدای بلادرنگ مابین دو تلفن است که در شبکه عمومی سوئیچ تلفن بکار می رود.

معایب سوئیچینگ مداری

θ نیاز به زمان قابل توجهی برای برقراری ارتباط بین فرستنده و گیرنده

θ عدم امکان برقراری ارتباط توسط ماشینهای دیگر با دو ماشین فرستنده و گیرنده هنگام اشغال بودن کانال توسط دو ماشین

سوئیچینگ سلول و بسته(Packet Switching / Cell Switching)

شکستن پیام توسط ایستگاه فرستنده به قطعات کوچکتری به نام بسته و ارسال هر بسته به همراه اطلاعات الزم برای بازسازی آن به طور جداگانه به مراکز سوئیچ است .

هر سوئیچ با دریافت کامل بسته می تواند آن را هدایت کند در حالی که می تواند به طور همزمان بسته بعدی را دریافت کند .بسته ها در هر سوئیچ ابتدا ذخیره می شود و سپس با بررسی سر فصل آن و جدول مسیریابی به سمت مناسب هدایت می شوند.

فصل دوم

لایه فیزیکی

لایه فیزیکی

در لایه فیزیکی، انتقال داده‌ها با استفاده از سیگنال‌های الکتریکی انجام می شود . سیگنال‌ها به دو دسته دیجیتال وآنالوگ تقسیم می‌شوند .سیگنال‌های دیجیتال شامل پالس‌های باینری (۰،۱)هستند که در سیستم‌هایکامپیوتری برای انتقال داده‌ها استفاده می‌شوند .این سیگنال‌ها پایداری بالایی دارند و به سادگی قابل تفسیر هستند .در مقابل، سیگنال‌های آنالوگ پیوسته و متغیر هستند و معمولاً برای انتقال داده‌های صوتی و تصویری استفاده می‌شوند . سیگنال‌های آنالوگ می‌توانند مقادیر متفاوتی از ولتاژ یا جریان را نشان دهند، بنابراین اطلاعات بیشتری را در یک دورهزمان ی انتقال می‌دهند .در طول مسیر انتقال، سیگنال‌های الکتریکی ممکن است با نویز و تداخل‌های الکترومغناطیسی روبرو شوند که کیفیت انتقال را کاهش می‌دهد .به همین دلیل، تکنیک‌های مختلفی برای کاهش نویز و تقویت سیگنال به کار گرفته می‌شود .به عنوان مثال، استفاده از تقویت‌کننده‌های سیگنال در طول مسیر انتقال، باعث بهبود کیفیت و فاصله انتقال می‌شود.

روش‌های کدینگ

کدینگ یا رمزنگاری داده‌ها فرآیندی است که در آن داده‌های دیجیتال به فرمتی قابل انتقال تبدیل می شوند .این فرآیند به دو دسته کلی کدینگ خطی (Line Coding)و کدینگ بلوکی (Block Coding)تقسیم می‌شود.

- **کدینگ خطی** :این روش برای تبدیل داده‌های دیجیتال به سیگنال‌های دیجیتال استفاده می‌شود .انواع مختلفی از کدینگ خطی وجود دارد که شامل NRZ (Non-Return-to-Zero)، مانچستر و دیفرانسیل مانچستر است.
  - در کدینگ NRZ، بیت‌ها بدون تغییر ولتاژ بین هر بیت ارسال می‌شوند که باعث کاهش پیچیدگی اما افزایش احتمال خطا می‌شود.
  - در کدینگ مانچستر، هر بیت داده به دو نیم بیت تقسیم می‌شود و تغییر ولتاژ در وسط هر بیت رخ می‌دهد .این روش امکان تشخیص آسان‌تر بیت‌ها و افزایش پایداری سیگنال را فراهم می‌کند.
  - در کدینگ دیفرانسیل مانچستر، تغییر ولتاژ در وسط هر بیت بسته به بیت قبلی رخ می‌دهد که باعث افزایش مقاومت در برابر نویز می‌شود.
- **کدینگ بلوکی** :در این روش، داده‌های دیجیتال به بلوک‌های کوچک‌تر تقسیم و سپس کد می شوند .این روش معمولاً برای تصحیح خطا استفاده می شود .به عنوان مثال، کدینگ هافمن یکی از روش‌های کدینگ بلوکی است که داده‌ها را به صورت بلوک‌های تکراری کد می‌کند و تشخیص و تصحیح خطا را ساده‌تر می‌کند.

تبدیل اطلاعات دیجیتال به دیجیتال

تبدیل دیجیتال به دیجیتال شامل فرآیندهایی نظیر فشرده‌سازی داده‌ها، تصحیح خطا و اصلاح سیگنال است.

- **فشرده سازی داده‌ها** :این فرآیند حجم اطلاعات را کاهش داده و سرعت انتقال را بهبود می‌بخشد .انواع مختلفی از روش‌های فشرده‌سازی وجود دارد که شامل فشرده‌سازی بی‌اتلاف (Lossless)و فشرده‌سازی با اتلاف (Lossy) می‌شود.
  - در فشرده سازی بی‌اتلاف، هیچ گونه اطلاعاتی از بین نمی‌رود و داده‌ها به صورت کامل بازیابی می شوند .به عنوان مثال، الگوریتم ZIPاز روش فشرده‌سازی بی‌اتلاف استفاده می‌کند.
  - اما در فشرده‌سازی با اتلاف، برخی از اطلاعات حذف می‌شوند تا حجم داده‌ها کاهش یابد .این روش بیشتر در فشرده سازی تصاویر و ویدئوها استفاده می شود .به عنوان مثال، فرمت JPEGاز فشرده سازی با اتلاف استفاده می کند.
- **تصحیح خطا** :این فرآیند به کمک کدهای تصحیح خطا انجام می شود که قادر به شناسایی و اصلاح خطاهای احتمالی در سیگنال‌های دیجیتال هستند .به عنوان مثال، کد هامینگ یکی از روش‌های تصحیح خطا است که قادر به تشخیص و اصلاح یک بیت خطا در هر کلمه داده است.
- **اصلاح سیگنال** :این فرآیند شامل تکنیک‌هایی نظیر فیلتر کردن، تقویت و حذف نویز برای بهبود کیفیت سیگنال و افزایش قابلیت اطمینان داده‌ها است.

تبدیل اطلاعات آنالوگ به دیجیتال

تبدیل آنالوگ به دیجیتال (ADC)فرآیندی است که در آن سیگنال‌های آنالوگ به سیگنال‌های دیجیتال تبدیل می شوند . این فرآیند شامل سه مرحله اصلی است:

- **نمونه‌برداری :(Sampling)** سیگنال آنالوگ به فواصل زمانی منظم نمونه‌برداری می شود .فرکانس نمونه‌برداری باید حداقل دو برابر بیشترین فرکانس سیگنال آنالوگ باشد تا از دست دادن اطلاعات جلوگیری شود .به این اصل، تئوری نایکوئیست-شانن می‌گویند.
- **کوانتیزاسیون :(Quantization)**نمونه‌های سیگنال به مقادیر دیجیتال تبدیل می‌شوند .فرآیند کوانتیزاسیون شامل تقسیم دامنه سیگنال به سطوح دیسکریت و نسبت دادن مقادیر دیجیتال به هر سطح است.
- **کدینگ :(Encoding)**مقادیر کوانتیزه شده به کدهای دیجیتال تبدیل می‌شوند .این فرآیند معمولاً با استفاده از روش‌هایی نظیر PCM (Pulse Code Modulation)انجام می‌شود که در آن سیگنال آنالوگ به یک سری پالس‌های دیجیتال تبدیل می‌شود.

تبدیل اطلاعات دیجیتال به آنالوگ

تبدیل دیجیتال به آنالوگ (DAC)فرآیندی است که در آن سیگنال‌های دیجیتال به سیگنال‌های آنالوگ تبدیل می شوند . این فرآیند شامل تبدیل پالس‌های دیجیتال به یک جریان پیوسته از ولتاژ یا جریان‌های آنالوگ است .این فرآیند معمولاً در دستگاه‌هایی نظیر مودم‌ها، کارت‌های صدا و دیگر تجهیزات صوتی و تصویری استفاده می شود .در این فرآیند، داده‌های دیجیتال به یک سیگنال آنالوگ تبدیل می شوند که می‌تواند در طول رسانه‌های انتقال آنالوگ منتقل شود .به عنوان مثال، مودم‌ها برای تبدیل داده‌های دیجیتال کامپیوتر به سیگنال‌های آنالوگ خطوط تلفن استفاده می‌شوند .این تبدیل باعث می‌شود که داده‌ها بتوانند از طریق شبکه‌های تلفنی سنتی منتقل شوند.

تبدیل اطلاعات آنالوگ به سیگنال‌های آنالوگ

این فرآیند شامل تکنیک‌های مختلف برای بهبود کیفیت سیگنال‌های آنالوگ و انتقال بهتر آنها است .تکنیک‌های مورد است فاده شامل فیلتر کردن، تعدیل و تقویت سیگنال می‌باشد.

- **فیلتر کردن :(Filtering)**برای حذف نویز و تداخل از سیگنال استفاده می‌شود .انواع مختلف فیلترها شامل فیلتر های پایین‌گذر، بالاگذر و میان‌گذر است که هر کدام برای حذف نوع خاصی از نویز استفاده می‌شوند.
- **تعدیل :(Modulation)**فرآیندی است که در آن یک سیگنال آنالوگ به سیگنال دیگری تبدیل می شود .انواع مختلف تعدیل شامل AM (Amplitude Modulation)، FM (Frequency Modulation)و PM (Phase Modulation)است.
  - در تعدیل دامنه (AM)، دامنه سیگنال حامل متناسب با سیگنال اطلاعات تغییر می‌کند.
  - در تعدیل فرکانس (FM)، فرکانس سیگنال حامل متناسب با سیگنال اطلاعات تغییر می‌کند.
  - در تعدیل فاز (PM)، فاز سیگنال حامل متناسب با سیگنال اطلاعات تغییر می‌کند.
- **تقویت :(Amplification)**برای افزایش قدرت سیگنال و بهبود فاصله انتقال استفاده می‌شود .تقویت کننده‌های سیگنال در طول مسیر انتقال قرار می‌گیرند و قدرت سیگنال را افزایش می‌دهند تا بتواند فاصله‌های طولانی‌تری را پوشش دهد.

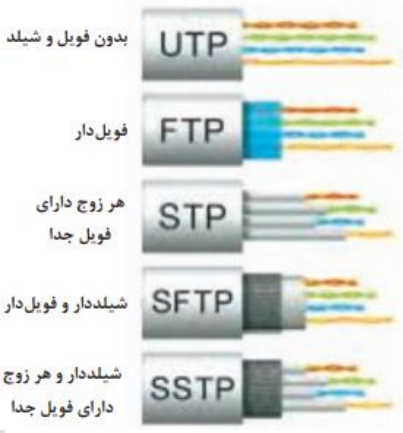
معرفی رسانه‌های انتقال

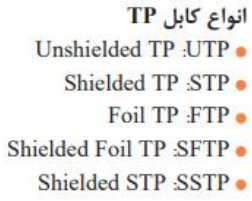
رسانه‌های انتقال نقش حیاتی در لایه فیزیکی ایفا می‌کنند و شامل انواع مختلفی از کابل‌ها و تکنولوژی‌های بی‌سیم می‌شوند .هر یک از این رسانه‌ها ویژگی‌های خاص خود را دارند که بر اساس نیاز شبکه و محیط کاربری انتخاب می‌شوند.

۱ .کابل‌های مسی

کابل‌های مسی به دلیل هزینه پایین و راحتی نصب، یکی از رایج‌ترین رسانه‌های انتقال هستند .انواع مختلفی از کابل‌های مسی وجود دارد:

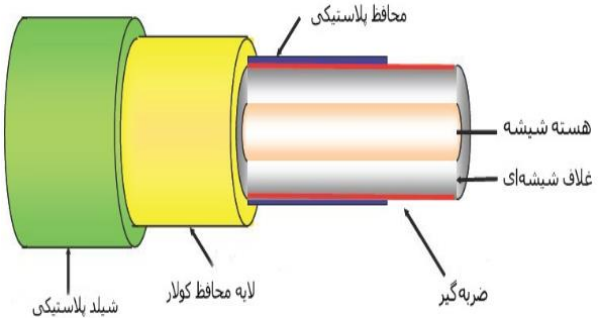
- **کابل‌های زوج به هم تابیده :(Twisted Pair)**این نوع کابل‌ها از جفت سیم‌های مسی تشکیل شده‌اند که به صورت مارپیچ به هم تابیده شده‌اند .این طراحی باعث کاهش تداخل الکترومغناطیسی می‌شود .دو نوع اصلی از ک ابل‌های زوج به هم تابیده وجود دارد:
  - **UTP (Unshielded Twisted Pair)**: این کابل‌ها بدون شیلد هستند و بیشتر در شبکه‌های محلی (LAN)استفاده می‌شوند.
  - **STP (Shielded Twisted Pair)**: این کابل‌ها دارای شیلد هستند که تداخل الکترومغناطیسی را بیشتر کاهش می‌دهد و در محیط‌های با تداخل بالا استفاده می‌شوند.





- **کابل‌های هم‌محور :(Coaxial)**این نوع کابل‌ها شامل یک هادی مرکزی، یک لایه عایق، یک شیلد فلزی و یک پو شش خارجی ه ستند .کابل‌های هم‌محور برای انتقال سیگنال‌های تلویزیونی و اینترنت ا ستفاده می شوند .این کابل‌ها به دلیل پایداری بالا و قابلیت انتقال داده‌های با سرعت بالا، همچنان در برخی کاربردها محبوب هستند.

۲ .فیبر نوری



فیبر نوری یک رسانه انتقال پیشرفته است که از نور برای انتقال داده‌ها استفاده می‌کند .فیبر نوری از هسته‌ای شیشه‌ای یا پلاستیکی تشکیل شده که نور در آن جریان می‌یابد .مزایای فیبر نوری شامل:

- **پهنای باند بالا** :فیبر نوری می‌تواند حجم زیادی از داده‌ها را با سرعت بالا انتقال دهد.
- **امنیت** :فیبر نوری در برابر تداخل الکترومغناطیسی مقاوم است و امکان استراق سمع کمتر است.
- **فاصله انتقال طولانی** :فیبر نوری قادر است داده‌ها را بدون کاهش کیفیت در فواصل طولانی انتقال دهد .

فیبر نوری به دو دسته اصلی تقسیم می‌شود:

- **فیبر نوری تک حالته (Single Mode Fiber - SMF)**: این نوع فیبر نوری برای انتقال داده ها در فواصل طولانی با پهنای باند بالا استفاده می‌شود.
- **فیبر نوری چند حالته (Multi Mode Fiber - MMF)**: این نوع فیبر نوری برای انتقال داده ها در فواصل کوتاه‌تر و با هزینه کمتر استفاده می‌شود.

۳ .رسانه‌های بی‌سیم

رسانه‌های بی‌سیم از امواج الکترومغناطیسی برای انتقال داده‌ها استفاده می‌کنند و نیاز به کابل ندارند .انواع مختلفی از رسانه‌های بی‌سیم وجود دارد که شامل:

- **امواج رادیویی (Radio Waves)**: این امواج برای انتقال داده‌ها در فواصل طولانی استفاده می‌شوند و در شبکه‌های Wi-Fi و تلفن‌های همراه استفاده می‌شوند.
- **مایکروویو (Microwaves)**: این امواج برای انتقال داده ها در فواصل کوتاه‌تر و با پهنای باند بالا استفاده می‌شوند .مایکروویوها به دو دسته زمینی و ماهواره‌ای تقسیم می‌شوند.
- **مادون قرمز (Infrared)**: این امواج برای ارتباطات کوتاه برد مانند کنترل های از راه دور استفاده می‌شوند .ارتباطات مادون قرمز نیاز به خط دید مستقیم دارند و نمی‌توانند از موانع عبور کنند.

فصل سوم

لایه پیوند داده

لایه پیوند داده

کنترل جریان

کنترل جریان یکی از مهم‌ترین وظایف لایه پیوند داده در مدل مرجع OSIاســت .این فرآیند به منظور جلوگیری از ازدحام شبکه و اطمینان از تحویل صحیح داده‌ها انجام می‌شود .تصور کنید یک فرستنده با سرعت بالا داده‌ها را ارسال کند، ولی گی رنده نتواند به همان سرعت داده‌ها را پردازش کند؛ در این صورت، داده‌ها در بافر گیرنده انباشته می‌شوند و ممکن است بسته هـا از دســـت برونـد .روش‌هـای مختلفی برای کنترل جریـان وجود دارد کـه می‌توان بـه روش‌هـای توقف و انتظـار (Stop-and-Wait)، پـنـجـره لـغـزان (Sliding Window)و کـنـتـرل جـریـان بـر اســـاس اعـتـبـار (Credit-Based Flow Control)اشاره کرد.

روش توقف و انتظار (Stop-and-Wait)

در این روش، فرســـتنده پس از ارســـال هر بســـته داده منتظر دریافت تأییدیه از گیرنده می‌شـــود .پس از دریافت تأییدیه، فرستنده بسته بعدی را ارسال می‌کند .این روش ساده است ولی کارایی کمی دارد زیرا فرستنده باید بعد از ارسال هر بسته منتظر بماند.

روش پنجره لغزان (Sliding Window)

این روش پیچیده‌تر است و به فرستنده اجازه می‌دهد چندین بسته داده را بدون منتظر ماندن برای تأییدیه هر بسته ارسال کند .هر بسـته دارای یک شـماره ترتیب اسـت و گیرنده نیز با اسـتفاده از این شـماره‌ها می‌تواند ترتیب درسـت بسـته‌ها را تشخیص دهد .این روش باعث افزایش کارایی و سرعت انتقال داده‌ها می‌شود ولی مدیریت آن نیاز به پیچیدگی‌های بیشتری دارد.

کنترل جریان بر اساس اعتبار (Credit-Based Flow Control)

در این روش، گیرنده به فرستنده اطلاع می‌دهد که چه تعداد بسته داده می‌تواند دریافت کند .این اعتبارها به فرستنده اجازه می‌دهد که داده‌ها را تا زمانی که اعتبارها تمام شـود، ارسـال کند .وقتی اعتبارها تمام شـود، فرسـتنده باید منتظر دریافت اعتبارهای جدید از گیرنده باشد.

کنترل جریان باعث می‌شود که ازدحام در شبکه کاهش یابد و داده‌ها به صورت صحیح و کامل به گیرنده تحویل داده شوند . این مکانیزم‌ها در پروتکل‌های مختلف شبکه مانند TCPنیز استفاده می‌شوند تا ارتباطات شبکه با کارایی بالا انجام شود.

لایه پیوند داده در شبکه‌های محلی

لایه پیوند داده یکی از لایه‌های مهم در مدل مرجع OSIاســـت که وظایف مختلفی را در شـــبکه‌های محلی (LAN)انجام می‌دهد .این لایه به دو زیرلایه تقسیم می‌شود :

۱- زیرلایه کنترل دسترسی به رسانه (MAC)

۲- زیرلایه کنترل منطقی پیوند داده .(LLC)

زیرلایه MAC

زیرلایه MACمسئولیت کنترل دسترسی به رسانه فیزیکی را بر عهده دارد .در شبکه‌های اترنت، MACآدرس‌های فیزیکی دستگاه‌ها را مدیریت می‌کند و تصمیم می‌گیرد که چه زمانی هر دستگاه می‌تواند داده‌ها را ارسال کند .این فرآیند با استفاده از پروتکل (CSMA/CD (Carrier Sense Multiple Access with Collision Detectionانجام می شود .در این پروتکل، د ستگاه‌ها قبل از ار سال داده‌ها به ر سانه گوش می‌دهند و اگر ر سانه آزاد با شد، داده‌ها را ار سال می‌کنند .اگر دو دســـتگاه به طور همزمان داده‌ها را ارســـال کنند، برخورد (Collision)رخ می‌دهد و هر دو دســـتگاه باید پس از یک زمان تصادفی مجدداً تلاش کنند .این مکانیزم باعث کاهش احتمال برخورد و افزایش کارایی انتقال داده‌ها می‌شود.

زیرلایه LLC

زیرلایه LLCیک رابط بین لایه شـــبکه و زیرلایه MACفراهم می‌کند LLC .وظایفی مانند فریم‌بندی داده‌ها و مدیریت ارتباطات منطقی بین دستگاه‌ها را انجام می‌دهد .این زیرلایه اطمینان حاصل می‌کند که داده‌ها به درستی فریم‌بندی شده و به مقصد صحیح ارسال می‌شوند .همچنین، LLCوظیفه تشخیص و تصحیح خطاهای احتمالی در داده‌ها را نیز بر عهده دارد .این زیرلایه از تکنیک‌هایی مانند (CRC (Cyclic Redundancy Checkبرای تشـــخیص خطاهای داده‌ها اســـتفاده می کند.

استانداردهای IEEE برای شبکه‌های محلی

IEEE (Institute of Electrical and Electronics Engineers)مجموعه‌ای از استانداردهای مهم را برای شبکه‌های محلی تعریف کرده است .این استانداردها تضمین می‌کنند که دستگاه‌ها و پروتکل‌های مختلف بتوانند با همدیگر به درستی کار کنند و سازگاری داشته باشند .برخی از استانداردهای معروف IEEEبرای شبکه‌های محلی عبارتند از:

IEEE 802.3 (اترنت)

استاندارد IEEE 802.3برای شبکه‌های اترنت تعریف شده است .این استاندارد از پروتکل CSMA/CD (Carrier Sense Multiple Access with Collision Detection) برای کنترل دسترسی به رسانه استفاده می‌کند .اترنت یکی از پرکاربردترین استانداردهای شبکه‌های محلی است و از انواع مختلف کابل‌ها و اتصالات استفاده می‌کند .اترنت از سرعت‌های مختلفی پشتیبانی می‌کند که شامل ۱۰مگابیت بر ثانیه، ۱۰۰مگابیت بر ثانیه (Fast Ethernet)، ۱گیگابیت بر ثانیه (Gigabit Ethernet)و حتی بالاتر است.

IEEE 802.11 (Wi-Fi)

استاندارد IEEE 802.11برای شبکه‌های محلی بی‌سیم تعریف شده است و شامل پروتکل‌های مختلفی برای کنترل دسترسی به رسانه و امنیت ارتباطات بی‌سیم است .استانداردهای مختلف IEEE 802.11شامل ۸۰۲٫۱۱، ۸۰۲٫۱۱ب، ۸۰۲٫۱۱ا، ۸۰۲٫۱۱گ، ۸۰۲٫۱۱نو ۸۰۲٫۱۱اچ هستند که هر کدام ویژگی‌ها و سرعت‌های مختلفی دارند .این استانداردها تضمین می‌کنند که دستگاه‌های بی سیم مختلف بتوانند با همدیگر سازگار باشند و ارتباطات بی سیم با کیفیت و قابلیت اطمینان بالا انجام شود.

IEEE 802.1Q (VLAN)

استاندارد IEEE 802.1Qامکان ایجاد شبکه‌های مجازی (VLAN)بر روی شبکه‌های فیزیکی را فراهم می‌کند .با استفاده از VLAN، می‌توان دستگاه‌ها را به صورت منطقی گروه‌بندی کرد و ترافیک شبکه را جدا کرد، حتی اگر دستگاه‌ها به یک شبکه فیزیکی متصل باشند .این استاندارد باعث افزایش امنیت و کارایی شبکه می شود و امکان مدیریت بهتری را فراهم می‌کند.

IEEE 802.15

این استاندارد برای شبکه‌های بی‌سیم شخصی (Wireless Personal Area Networks - WPAN)تعریف شده است و شامل تکنولوژی‌هایی مانند بلوتوث است .بلوتوث امکان ارتباط بی‌سیم بین دستگاه‌های نزدیک به هم را فراهم می‌کند و در بسیاری از دستگاه‌های مدرن استفاده می‌شود.

این استانداردها باعث می‌شوند که شبکه‌های محلی با کارایی بالا و سازگاری کامل ایجاد شوند و دستگاه‌های مختلف بتوانند به درستی با یکدیگر ارتباط برقرار کنند.

پروتکل‌های لایه پیوند داده

پروتکل‌های لایه پیوند داده وظایف مختلفی را بر عهده دارند که شامل فریم‌بندی داده‌ها، کنترل جریان، تشخیص و تصحیح خطاها و مدیریت آدرس‌دهی فیزیکی می‌باشد .برخی از پروتکل‌های معروف لایه پیوند داده عبارتند از:

اترنت (Ethernet)

اترنت یکی از پرکاربردترین پروتکل‌های لایه پیوند داده است که در شبکه‌های محلی استفاده می شود .اترنت از پروتکل CS MA/CD (Carrier Sense Multiple Access with Collision Detection)برای کنترل دسترسی به رسانه استفاده می‌کند .در این پروتکل، دستگاه‌ها قبل از ارسال داده‌ها به رسانه گوش می‌دهند و اگر رسانه آزاد باشد، داده‌ها را ارسال می‌کنند .اگر دو دستگاه به طور همزمان داده‌ها را ارسال کنند، برخورد (Collision)رخ می‌دهد و هر دو دستگاه باید پس از یک زمان تصادفی مجدداً تلاش کنند .اترنت قابلیت اطمینان بالایی دارد و در بسیاری از شبکه‌های مدرن استفاده می‌شود.

Wi-Fi

Wi-Fiیک پروتکل بی‌سیم است که در شبکه‌های محلی بی‌سیم استفاده می‌شود. از پروتکل CSMA/CA (Collision Avoidance)برای کنترل دسترسی به رسانه استفاده می‌کند .این پروتکل با استفاده از مکانیزم‌های مختلف، سعی در جلوگیری از برخوردهای داده‌ها دارد .

فصل چهارم

لایه شبکه

مسیریابی

مسیریابی فرآیندی است که داده‌ها از طریق شبکه از منبع به مقصد هدایت می‌شوند .این فرآیند توسط روترها و سوئیچ‌ها انجام می‌شود که وظیفه آن‌ها هدایت بسته‌های داده از طریق مسیرهای مختلف در شبکه است تا به مقصد نهایی برسند.

مسیریابی ایستا (Static Routing)

در مسیریابی ایستا، مسیرها به صورت دستی توسط مدیر شبکه پیکربندی می‌شوند و تغییرات در مسیرها نیازمند دخالت انسانی است .این نوع مسیریابی برای شبکه‌های کوچک با توپولوژی ثابت مناسب است .از مزایای آن می‌توان به سادگی و پایداری اشاره کرد؛ اما معایب آن شامل انعطاف‌پذیری کم و نیاز به مدیریت دستی برای تغییرات در توپولوژی شبکه است.

مسیریابی پویا (Dynamic Routing)

در مسیریابی پویا، روترها از پروتکل‌های مسیریابی استفاده می‌کنند تا به صورت خودکار بهترین مسیرها را پیدا کنند .این پروتکل‌ها اطلاعات شبکه را به صورت دوره‌ای به روز می‌کنند و تغییرات توپولوژی شبکه را مدیریت می‌کنند .مسیریابی پویا برای شبکه‌های بزرگ و پیچیده مناسب است .از مزایای آن می‌توان به انعطاف‌پذیری بالا و مدیریت خودکار اشاره کرد.

وظایف مسیریابی

- **هدایت بسته‌ها** :روترها بسته‌های داده را از ورودی به خروجی هدایت می‌کنند.
- **انتخاب بهترین مسیر** :انتخاب بهترین مسیر بر اساس معیارهایی مانند تعداد هاپ‌ها، پهنای باند و تاخیر.
- **مدیریت جدول م سیریابی** :نگهداری و به‌روزرسانی جدول مسیریابی که شامل اطلاعات مسیرها و روترهای همسایه است.

الگوریتم‌های مسیریابی

الگوریتم‌های مسیریابی فاصله–برداری (Distance-Vector)

در این نوع الگوریتم‌ها، هر روتر جدولی شامل اطلاعات فاصله تا مقصدهای مختلف را نگهداری می‌کند و این جداول را با هم سایگان خود مبادله می‌کند تا بهترین مسیرها را تعیین کنند.

- **RIP (Routing Information Protocol)**:در این الگوریتم، هر روتر جدول مسیریابی خود را به صورت دوره ای با همسایگان خود به اشتراک می‌گذارد .این پروتکل ساده و قدیمی است و برای شبکه‌های کوچک تا متوسط مناسب است.

الگوریتم‌های مسیریابی پیوند–حالت (Link-State)

در این نوع الگوریتم‌ها، هر روتر اطلاعات کامل توپولوژی شبکه را نگهداری می‌کند و با استفاده از این اطلاعات، بهترین مسیر ها را محاسبه می‌کند.

- **OSPF (Open Shortest Path First)**: در این الگوریتم، هر روتر اطلاعات توپولوژی را به صورت دوره‌ای به همسایگان خود ارسال می‌کند و از الگوریتم Dijkstra برای محاسبه کوتاه‌ترین مسیرها استفاده می‌کند .این پروتکل برای شبکه‌های بزرگ و پیچیده مناسب است.

الگوریتم‌های مسیریابی پیشرفته

- **EIGRP (Enhanced Interior Gateway Routing Protocol)**: یک پروتکل مسیریابی هیبریدی که ویژگی‌های مسیریابی فاصله-برداری و پیوند-حالت را ترکیب می‌کند .این پروتکل توسط شرکت سیسکو توسعه داده شده است و به دلیل کارایی و سرعت بالا در شبکه‌های بزرگ مورد استفاده قرار می‌گیرد.
- **BGP (Border Gateway Protocol)**: این پروتکل برای مسیریابی بین سیستم‌های خودمختار (AS) استفاده می‌شود و نقشی حیاتی در اینترنت ایفا می‌کند BGP .به روترها امکان تبادل اطلاعات مسیرها را می‌دهد و از سیاست‌های مختلف مسیریابی پشتیبانی می‌کند.

کنترل ازدحام در لایه شبکه

ازدحام در شبکه زمانی رخ می‌دهد که تعداد بسته‌های داده‌ای که وارد شبکه می شوند، بیش از ظرفیت پردازش و انتقال شبکه باشد .این موضوع می‌تواند باعث کاهش کارایی شبکه، افزایش تأخیر و از دست رفتن بسته‌های داده شود.

تکنیک‌های کنترل ازدحام

- **مدیریت صف (Queue Management)**: این تکنیک شامل ایجاد صف‌های مختلف برای بسته‌های داده و او لویت‌بندی ترافیک است .الگوریتم RED (Random Early Detection) یکی از تکنیک‌های مدیریت صف است که بسته‌های داده را بر اساس احتمال از دست می‌دهد تا از ازدحام جلوگیری کند.
- **کنترل جریان (Flow Control)**: این تکنیک شامل محدود کردن سرعت ارسال داده‌ها توسط فرستنده‌ها است. الگوریتم‌هایی مانند TCP Congestion Control از این تکنیک‌ها برای مدیریت ترافیک شبکه استفاده می‌کنند
- **تفکیک ترافیک (Traffic Shaping)**: این تکنیک شامل تغییر شکل ترافیک شبکه به گونه‌ای است که ترافیک در طول زمان یکنواخت‌تر شود .به عنوان مثال، الگوریتم Leaky Bucket برای شکل‌دهی ترافیک استفاده می‌شود.

الگوریتم‌های کنترل ازدحام

- **الگوریتم AIMD (Additive Increase Multiplicative Decrease)**: این الگوریتم در پروتکل TCP استفاده می‌شود و شامل افزایش تدریجی سرعت ارسال داده‌ها تا زمانی که نشانه‌ای از ازدحام مشاهده شود. پس از مشاهده ازدحام، سرعت ارسال به صورت ضریبی کاهش می‌یابد.
- **الگوریتم TCP Tahoe و TCP Reno**: این الگوریتم‌ها از تکنیک‌های مختلفی برای شناسایی و مدیریت ازدحام استفاده می‌کنند. TCP Tahoe از الگوریتم AIMD و الگوریتم Fast Retransmit برای مدیریت ازدحام استفاده می‌کند، در حالی که TCP Reno علاوه بر این‌ها از الگوریتم Fast Recovery نیز استفاده می‌کند.

کنترل ازدحام در شبکه‌های بی‌سیم

در شبکه‌های بی‌سیم، کنترل ازدحام به دلیل محدودیت‌های پهنای باند و تداخل‌های محیطی بسیار چالش‌برانگیزتر است. تکنیک‌های کنترل ازدحام در این شبکه‌ها شامل تنظیم توان ارسال، مدیریت دسترسی به کانال‌ها و استفاده از الگوریتم‌های تطبیقی است.

شبکه‌های خصوصی مجازی (VPN)

شبکه‌های خصوصی مجازی یا VPNها ابزاری هستند که امکان ایجاد اتصالات امن و خصوصی از طریق اینترنت را فراهم می‌کنند. VPN از تکنیک‌های رمزنگاری و تونل‌زنی استفاده می‌کند تا داده‌ها به صورت امن از یک نقطه به نقطه دیگر منتقل شوند. این تکنیک‌ها به کاربران این امکان را می‌دهد که به منابع شبکه‌ای که به صورت فیزیکی در دسترس نیستند، دسترسی پیدا کنند.

مزایا و کاربردها

- **امنیت** VPN: ها با رمزنگاری داده‌ها، امنیت ارتباطات را تضمین می‌کنند و از نظارت و دسترسی غیرمجاز جلوگیری می‌کنند.
- **حریم خصوصی**: با استفاده از VPN، فعالیت‌های آنلاین کاربران پنهان می‌ماند و از ردیابی توسط دیگران جلوگیری می‌شود.
- **دسترسی از راه دور**: کارکنان شرکت‌ها می‌توانند از هر نقطه‌ای به شبکه شرکت دسترسی داشته باشند.
- **دور زدن محدودیت‌ها**: کاربران می‌توانند به محتواهایی که به صورت جغرافیایی محدود شده‌اند دسترسی پیدا کنند.

انواع VPN

- **VPNهای د ستر سی از راه دور** :این نوع VPNبه کاربران اجازه می‌دهد تا از طریق اینترنت به شبکه سازمانی خود متصل شوند .این نوع VPNبرای کارکنانی که به صورت دورکاری فعالیت می‌کنند، بسیار مفید است.
- **VPNهای سایت به سایت** :این نوع VPNبه سازمان‌ها امکان می‌دهد تا شعبات مختلف خود را به یکدیگر متصل کنند .این نوع VPNمعمولاً بین روترهای سایت‌های مختلف پیکربندی می‌شود و به سازمان‌ها اجازه می‌دهد تا شبکه‌های محلی خود را به صورت امن به یکدیگر متصل کنند.

پروتکل‌های VPN

- **PTP (Point-to-Point Tunneling Protocol)**:
یکی از پروتکل‌های قدیمی VPNکه از رمزنگاری پایه‌ای برای ایجاد اتصال امن استفاده می‌کند.
- **L2TP (Layer 2 Tunneling Protocol)**:این پروتکل معمولاً با پروتکل IPsecترکیب می‌شود تا امنیت بیشتری فراهم کند L2TP .به تنهایی رمزنگاری را فراهم نمی‌کند، اما وقتی با IPsecترکیب می‌شود، اتصالات امن و مطمئنی را ایجاد می‌کند.
- **IPsec (Internet Protocol Security)**:یک مجموعه پروتکل برای امنیت لایه شبکه که امکان ایجاد ارتباطات امن بین دو نقطه را فراهم می‌کند IPsec .برای ایجاد تونل‌های امن و رمزنگاری داده‌ها استفاده می‌شود.
- **OpenVPN**:یک پروتکل منبع باز که از SSL/TLSبرای ایجاد اتصالات امن استفاده می‌کند OpenVPN .بسیار انعطاف‌پذیر است و در بسیاری از سیستم‌ها و دستگاه‌ها پشتیبانی می‌شود.

ا ستفاده از VPNها به کاربران و سازمان‌ها این امکان را می‌دهد تا ارتباطات خود را از طریق اینترنت به صورت امن انجام دهند و از نظارت و دسترسی غیرمجاز جلوگیری کنند VPN .ها علاوه بر امنیت، امکان دسترسی به منابع شبکه از راه دور را نیز فراهم می‌کنند و به کاربران اجازه می‌دهند تا به راحتی به شبکه‌های سازمانی متصل شوند.

آدرس‌دهی IP و نحوه کارکرد زیرشبکه‌ها

آدرس‌دهی IP (Internet Protocol)نقش حیاتی در ارتباطات شبکه دارد .هر دستگاه در شبکه یک آدرس IPمنحصر به فرد دارد که به آن اجازه می‌دهد داده‌ها را ارسال و دریافت کند .آدرس‌های IPبه دو نسخه IPv4و IPv6تقسیم می‌شوند.

آدرس‌دهی IPv4

- **فرمت** :آدرس‌های IPv4شامل چهار بخش عددی (octet)است که با نقطه از هم جدا می‌شوند
  مثل ۱۹۲,۱۶۸,۱,۱
- **زیر شبکه‌ها** :زیرشبکه‌ها به تقسیم‌بندی‌های منطقی از یک شبکه بزرگتر می‌گویند که با استفاده از ماسک زیرشبکه (subnet mask)تعریف می‌شوند .ماسک زیرشبکه تعداد بیت‌های شبکه و میزبان را مشخص می‌کند . مثلاً ماسک زیرشبکه ۲۵۵,۲۵۵,۲۵۵,۰به این معنی است که اولین ۲۴بیت آدرس به شبکه و ۸بیت آخر به میزبان اختصاص دارد.

آدرس‌دهی IPv6

- **فرمت** :آدرس‌های IPv6شامل هشت بخش هگزادسیمال است که با کولون از هم جدا می‌شوند.
  مثل ۲۰۰۱:۰□□۸:۸۵□۳:۰۰۰۰:۰۰۰۰:۸□۲□:۰۳۷۰:۷۳۳۴
- **فضای بیشتر** IPv6 :فضای آدرس‌دهی بسیار بزرگتری نسبت به IPv4دارد و برای آینده‌ای با تعداد بیشتر دستگاه های متصل به اینترنت طراحی شده است.

آدرس های IP چگونه کار می کنند؟

پروتکل اینترنت با برقراری ارتباط با استفاده از دستورالعمل های تنظیم شده با هدف انتقال اطلاعات کار می کند، همه دستگاه‌ها با استفاده از این پروتکل اطلاعات را با سایر دستگاه‌های متصل پیدا، ارسال و تبادل می‌کنند، با صحبت کردن به یک زبان، هر رایانه ای در هر مکانی می تواند با یکدیگر صحبت کند؛

آدرس IP شما قابلیت تغییر را دارند، برای مثال، خاموش یا روشن کردن مودم یا روتر می تواند سبب تغییر آن شود؛ یا می توانید با ISP خود تماس بگیرید و آنها می توانند IP را برای شما تغییر دهند.

وقتی خارج از منزل هستید – مثلاً در سفر – و دستگاه خود را با خود می برید، آدرس IP منزل شما همراه شما نخواهد بود؛ دلیل آن این است که شما از شبکه دیگری Wi-Fi) در هتل، فرودگاه، یا کافی شاپ و غیره (برای دسترسی به اینترنت استفاده می کنید و از یک آدرس IP متفاوت (و موقت) استفاده می کنید که توسط ISP به شما اختصاص داده شده است؛ هتل، فرودگاه یا کافی شاپ؛ همانطور که از فرآیند پیداست، انواع مختلفی از آدرس های IP وجود دارد

انواع آدرس هایIP

گروه های مختلفی از آدرس های IP وجود دارد و در هر مجموعه، انواع متفاوتی وجود دارد.

هر فرد یا کسب و کاری با طرح خدمات اینترنتی دو نوع آدرس IP خواهد داشت: آدرس IP خصوصی و آدرس IP عمومی. اصطلاحات خصوصی و عمومی مربوط به مکان شبکه می شود؛ یعنی منظور از آدرس IP خصوصی، استفاده از آن در داخل شبکه صورت میگیرد در حالی که یک آدرس عمومی در خارج از شبکه استفاده می شود.

۱. آدرس های IP خصوصی

هر دستگاهی که به شبکه اینترنت شما متصل می شود یک نشانی آیپی خصوصی دارد. این شامل رایانه‌ها، تلفن‌های هوشمند و تبلت‌ها می‌شود اما هر دستگاه دارای بلوتوث مانند بلندگوها، چاپگرها یا تلویزیون‌های هوشمند را نیز شامل می‌شود. با رشد روزافزون اینترنت اشیا، تعداد آدرس های IP خصوصی که در خانه دارید در حال افزایش است.

روتر شما به راهی برای شناسایی این موارد به طور جداگانه نیاز دارد و بسیاری از موارد نیاز به راهی برای شناسایی یکدیگر دارند؛ بنابراین روتر شما برای تمایز در شبکه، آدرس‌های IP خصوصی با شناسه‌های خاص و مشخصی برای هر دستگاه را تولید می‌کند.

۲. آدرس های IP عمومی

آدرس IP عمومی آدرس اصلی مرتبط با کل شبکه شما است، در حالی که هر دستگاه متصل آدرس IP مخصوص به خود را دارد. همانطور که در بخش قبل به آن اشاره شد، آدرس IP عمومی شما به واسطه ISP به روتر ارائه می شود؛ معمولاً ISP ها دارای گروهی از آدرس های IP می باشند که آن ها را بین مشتریان خود تقسیم می کنند، آدرس IP عمومی شما آدرسی است که برای شناسایی شبکه شما توسط دستگاه های خارج از شبکه اینترنتی شما از آن استفاده می کنند.

لازم به ذکر است؛ آدرس های IP عمومی نیز به دو صورت پویا و استاتیک هستند که در مبحث بعدی نیز به این موضوع خواهیم پرداخت:

- **آدرس های IP پویا**

آدرس های IP پویا به طور خودکار و منظم تغییر می کنند، ISPها مجموعه بزرگی از آدرس های IP را خریداری می کنند و آنها را به طور خودکار به مشتریان خود اختصاص می دهند و آدرس‌های IP قدیمی‌تر را دوباره در اختیار مشتریان دیگر قرار می‌دهند هدف و منطق این رویکرد ایجاد صرفه جویی در هزینه برای ISP است.

خودکار کردن حرکت منظم آدرس‌های IP به این معنی است که برای مثال، در صورت نقل مکان به خانه، سرویس های ISPمجبور نیستند اقدامات خاصی را برای ایجاد مجدد آدرس IP مشتری انجام دهند، دز این زمینه مزایای امنیتی نیز وجود دارد، زیرا تغییر آدرس IP هک کردن رابط شبکه شما را برای مجرمان دشوارتر می کند.

- **آدرس های IP استاتیک**

برعکس آدرس‌های IP پویا، آدرس‌های استاتیک ثابت می‌مانند،با اختصاص دادن شبکه به یک آدرسIP ، همان آدرس باقی می ماند؛ اکثر افراد و مشاغل نیازی به آدرس IP ثابت ندارند، اما برای مشاغلی که قصد دارند سرور خود را میزبانی کنند، داشتن یک آدرس بسیار مهم است، به این دلیل است که تضمین می کند وب سایت ها و آدرس های ایمیل متصل به آن دارای یک آدرس IP ثابت هستند؛ در پیدا کردن آن ها به طور مداوم در وب توسط دستگاه های دیگر حائز اهمیت است.

نحوه کارکرد زیر شبکه‌ها

- **تقسیم‌بندی شبکه** :زیرشبکه‌ها به مدیران شبکه اجازه می‌دهند تا شبکه‌های بزرگتر را به بخش‌های کوچکتر و مدیریتی‌تر تقسیم کنند.
- **کاهش ترافیک** :با استفاده از زیرشبکه‌ها، ترافیک شبکه داخلی کمتر می‌شود و کارایی شبکه افزایش می‌یابد.
- **امنیت** :زیرشبکه‌ها امکان اعمال سیاست‌های امنیتی مختلف برای بخش‌های مختلف شبکه را فراهم می‌کنند.

مزایای زیرشبکه‌بندی

- **استفاده بهینه از آدرس‌ها** :زیرشبکه‌بندی به تخصیص بهینه‌تر آدرس‌های IPکمک می‌کند.
- **کاهش برخورد آدرس‌ها** :با تقسیم‌بندی شبکه به زیرشبکه‌های کوچکتر، برخورد آدرس‌ها کمتر می‌شود.
- **مدیریت بهتر** :زیرشبکه‌بندی امکان مدیریت بهتر و اعمال سیاست‌های شبکه‌ای مختلف را فراهم می‌کند.

چگونگی کارکرد کپسوله‌سازی

کپسوله‌سازی (Encapsulation)فرآیندی است که در آن داده‌ها در هر لایه از مدل مرجع OSIبسته‌بندی شده و به لایه پایین‌تر منتقل می‌شوند .این فرآیند به هر لایه اجازه می‌دهد تا وظایف خود را به صورت مستقل انجام دهد و داده‌ها را به در ستی منتقل کند .کپسوله‌سازی از بالا به پایین مدل OSIبه شرح زیر است:

مراحل کپسوله‌سازی

۱. **لایه کاربرد :(Application Layer)**

- داده‌ها به شکل پیام‌ها یا داده‌های کاربردی تولید می‌شوند.
- مثال :یک ایمیل که توسط کاربر نوشته می‌شود.

۲. **لایه نمایش :(Presentation Layer)**

- داده‌ها ممکن است فشرده‌سازی یا رمزنگاری شوند تا فرمت مناسبی برای انتقال پیدا کنند.
- مثال :فشرده‌سازی یک فایل یا رمزنگاری پیام.

۳. **لایه نشست :(Session Layer)**

- نشست‌های ارتباطی برقرار می‌شوند و مدیریت می‌شوند.
- مثال :برقراری ارتباط برای انتقال داده‌ها بین دو دستگاه.

۴. **لایه انتقال :(Transport Layer)**

- داده‌ها به قطعات کوچکتر تقسیم می‌شوند و هدر لایه انتقال به آن‌ها اضافه می‌شود.
- هدر شامل اطلاعاتی مانند پورت‌های مبدأ و مقصد است.
- داده‌ها در این مرحله به سگمنت (segment)تبدیل می‌شوند.
- مثال :پروتکل‌های TCPیا .UDP

۵. **لایه شبکه :(Network Layer)**

- سگمنت‌ها به بسته‌های (packets)تبدیل می‌شوند.
- هدر شبکه که شامل آدرس‌های IPمبدأ و مقصد است به داده‌ها اضافه می‌شود.
- مثال :پروتکل .IP

۶. **لایه پیوند داده :(Data Link Layer)**

- بسته‌ها به فریم‌ها (frames)تبدیل می‌شوند.
- هدر و تریلر پیوند داده که شامل آدرس‌های MACو اطلاعات کنترل خطا است به داده‌ها اضافه می‌شود.
- مثال :پروتکل‌های اترنت یا .Wi-Fi

۷. **لایه فیزیکی :(Physical Layer)**

- فریم‌ها به بیت‌های سیگنال الکتریکی یا نوری تبدیل می‌شوند و از طریق رسانه انتقال ارسال می‌شوند.
- مثال :کابل‌های مسی، فیبر نوری، امواج رادیویی.

مزایای کپسوله‌سازی

- **انعطاف‌پذیری** :هر لایه می‌تواند به صورت مستقل عمل کند و تغییری در یک لایه نیاز به تغییر در سایر لایه‌ها ندارد.
- **امنیت** :داده‌ها می‌توانند در لایه‌های مختلف رمزنگاری شوند تا امنیت بیشتری فراهم شود.
- **قابلیت مدیریت** :داده‌ها می‌توانند به سادگی از طریق شبکه‌های مختلف منتقل شوند و هر لایه نقش خاص خود را ایفا کند.

پروتکل های لایه شبکه

پروتکل ARP (Address Resolution Protocol)

وظیفه:

پروتکل ARPوظیفه تبدیل آدرس‌های IPبه آدرس‌های MACرا بر عهده دارد .این تبدیل برای ارتباطات در شـــبکه‌های محلی (LAN)ضـــروری اســـت زیرا پروتکل IPاز آدرس‌های IPاســـتفاده می‌کند در حالی که لایه پیوند داده از آدرس‌های MACبرای تحویل بسته‌ها استفاده می‌کند.

نحوه کارکرد:

۱. **درخواست :ARP**وقتی دستگاهی می‌خواهد به دستگاه دیگری در همان شبکه محلی پیام ارسال کند، یک بسته ARP Requestبه شبکه ارسال می‌کند که شامل آدرس IPمقصد است .این بسته به صورت برودکست (Broadcast)ارسال می‌شود.

۲. **پاسخ :ARP**دستگاهی که آدرس IPمورد نظر را دارد، یک بسته ARP Replyارسال می‌کند که شامل آدرس MACخود است .این پاسخ به صورت یونی‌کست (Unicast)به فرستنده ارسال می‌شود.

۳. **نگهداری در کش :ARP**دستگاه فرستنده، آدرس MACرا در کش (cache)خود ذخیره می‌کند تا در ارتباطات بعدی نیازی به ارسال مجدد درخواست ARPنباشد .اطلاعات موجود در کش ARPدارای زمان محدودیت (TTL) است و پس از گذشت این مدت زمان، اطلاعات حذف می‌شوند.

کاربرد:

ARPبرای تسهیل ارتباطات در شبکه‌های محلی استفاده می‌شود و به دستگاه‌ها اجازه می‌دهد تا آدرس‌های فیزیکی MA) (Cیکدیگر را پیدا کنند .این پروتکل یکی از پروتکل‌های پایه‌ای در شـــبکه‌های اترنت اســـت و بدون آن، ارســـال داده‌ها در شبکه‌های محلی امکان‌پذیر نخواهد بود.

پروتکل RARP (Reverse Address Resolution Protocol)

وظیفه:

پروتکل RARPوظیفه تبدیل آدرس‌های MACبه آدرس‌های IPرا بر عهده دارد .این پروتکل بیشـــتر در دســـتگاه‌هایی استفاده می‌شود که آدرس IPثابت ندارند و باید آدرس IPخود را از طریق آدرس MACدرخواست کنند.

نحوه کارکرد:

۱. **درخواست RARP**: دستگاهی که به آدرس IP نیاز دارد، یک بسته RARP Request به شبکه ارسال می‌کند که شامل آدرس MAC خود است. این درخواست به سرورهای RARP موجود در شبکه ارسال می‌شود.

۲. **پاسخ RARP**: یک سرور RARP که اطلاعات مربوط به آدرس‌های MAC و IP را نگهداری می‌کند، یک بسته RARP Reply ارسال می‌کند که شامل آدرس IP مربوط به آدرس MAC درخواست‌کننده است.

کاربرد:

RARP برای دستگاه‌هایی که هنگام راه‌اندازی به آدرس IP نیاز دارند و از آدرس IP ثابتی برخوردار نیستند، استفاده می‌شود. این پروتکل جای خود را به پروتکل‌های DHCP و BOOTP داده است که قابلیت‌های بیشتری دارند. DHCP (Dynamic Host Configuration Protocol) یکی از پروتکل‌های پیشرفته‌تر است که علاوه بر تخصیص آدرس IP، اطلاعات دیگری مانند ماسک زیرشبکه، دروازه پیش‌فرض و سرورهای DNS را نیز فراهم می‌کند.

پروتکل IP (Internet Protocol)

وظیفه:

پروتکل IP مسئول ارسال بسته‌های داده از منبع به مقصد است. این پروتکل بسته‌ها را از لایه بالاتر دریافت کرده، آنها را به بسته‌های کوچکتر تقسیم می‌کند و به هر بسته هدر IP اضافه می‌کند که شامل اطلاعاتی مانند آدرس‌های مبدا و مقصد، طول بسته و غیره است.

ویژگی‌ها:

- **اتصال‌گرا نیست IP**: یک پروتکل اتصال‌گرا نیست، به این معنا که قبل از ارسال داده‌ها نیازی به برقراری ارتباط بین دستگاه‌ها ندارد.
- **تحویل غیر قابل اعتماد IP**: تحویل غیر قابل اعتماد را فراهم می‌کند، به این معنا که تضمینی برای تحویل صحیح و بدون خطای بسته‌ها وجود ندارد.
- **مسیریابی IP**: از روترها برای مسیریابی بسته‌ها استفاده می‌کند و به این ترتیب بسته‌ها را از طریق شبکه‌های مختلف هدایت می‌کند.

پروتکل ICMP (Internet Control Message Protocol)

وظیفه:

پروتکل ICMPبرای ارسال پیام‌های کنترل و خطا در شبکه استفاده می‌شود .این پروتکل به دستگاه‌ها اجازه می‌دهد تا اطلاعات مربوط به وضعیت شبکه و مشکلات ارتباطی را به یکدیگر ارسال کنند.

کاربرد:

- **پیام‌های خطا** :وقتی بسته‌ای به مقصد نمی‌رسد یا مشکلی در ارتباطات وجود دارد، ICMPپیام خطایی به فرستنده ارسال می‌کند .مثلاً اگر یک بسته به دلیل نبود مسیر مناسب به مقصد نرسد، یک پیام ICMP Destination Unreachableبه فرستنده ارسال می‌شود.
- **دستور Ping**: دستور Pingکه برای بررسی قابلیت دسترسی و تأخیر شبکه استفاده می‌شود، از ICMPاستفاده می‌کند .این دستور بسته‌های ICMP Echo Requestرا ارسال می‌کند و منتظر دریافت ICMP Echo Reply می‌ماند .با استفاده از زمان برگشت این بسته‌ها، می‌توان کیفیت ارتباط را ارزیابی کرد.
- **ردیابی مسیر (Traceroute)**: ابزار Tracerouteکه برای ردیابی مسیر بسته‌ها از منبع به مقصد استفاده می‌شود، از پیام‌های ICMP Time Exceededبهره می‌برد تا هر گام از مسیر را نشان دهد .این ابزار به شناسایی مسیرها و مشکلات احتمالی در طول مسیر کمک می‌کند.

انواع پیام‌های ICMP:

- **Echo Request** و **Echo Reply**: برای تست قابلیت دسترسی و تأخیر ارتباط.
- **Destination Unreachable**: برای اعلام عدم دسترسی به مقصد به دلایل مختلف مانند عدم وجود مسیر، فیلتر شدن بسته توسط فایروال، و غیره.
- **Time Exceeded**: برای اعلام تمام شدن زمان زندگی (TTL)بسته در طول مسیر.
- **Redirect**: برای اعلام تغییر مسیر مناسب به فرستنده بسته.

فصل پنجم

لایه های کاربرد و انتقال

توصیف پورت‌ها و سوکت‌های TCP

پورت‌ها در لایه انتقال و کاربرد

پورت‌ها به عنوان نقاط پایانی ارتباطات در شبکه‌های کامپیوتری عمل می‌کنند .هر پورت یک عدد ۱۶بیتی ا ست که از ۰تا ۶۵۵۳۵مقدار می‌گیرد .پورت‌ها به دو دسته کلی تقسیم می‌شوند:

- **پورت‌های شناخته‌شده :(Well-Known Ports)**

این پورت‌ها در محدوده ۰تا ۱۰۲۳قرار دارند و برای پروتکل‌های شناخته‌شده مانند) HTTPپورت (۸۰، HTTPS)پورت (۴۴۳و) FTPپورت (۲۱استفاده می‌شوند .این پورت‌ها معمولاً توسط سیستم‌عامل‌ها و برنامه‌های سرویس دهنده استفاده می‌شوند.

- **پورت های پو یا :(Dynamic Ports)**این پورت‌ها در محدوده ۱۰۲۴تا ۶۵۵۳۵قرار دارند و معمولاً برای ارتباطات موقت و داینامیک مورد استفاده قرار می‌گیرند .این پورت‌ها به طور معمول توسط برنامه‌های کاربری مانند مرورگرهای وب و کلاینت‌های ایمیل استفاده می‌شوند.

سوکت‌ها در لایه انتقال و کاربرد

سوکت‌ها ترکیبی از یک آدرس IPو یک پورت هستند که به عنوان نقطه نهایی ارتباطات شبکه عمل می‌کنند .هر سوکت منح صر به فرد ا ست و ارتباطات بین د ستگاه‌ها از طریق سوکت‌ها مدیریت می شود . سوکت‌ها در لایه‌های انتقال و کاربرد مورد ا ستفاده قرار می‌گیرند .به عنوان مثال، یک برنامه کاربردی وب از یک سوکت برای برقراری ارتباط با مرورگر ا ستفاده می‌کند .این سوکت شامل آدرس IPاسرور و پورت) HTTPپورت (۸۰است.

شناسایی اجزای مختلف یک هدر TCP

هدر TCPشامل مجموعه‌ای از فیلدهاست که اطلاعات مختلفی را در مورد بسته TCPنگهداری می‌کند .اجزای مختلف هدر TCPعبارتند از:

۱. **شماره پورت مبدأ :(Source Port Number)**عدد ۱۶بیتی که نشان‌دهنده پورت مبدأ ارتباط است.

۲. **شماره پورت مق صد :(Destination Port Number)**عدد ۱۶بیتی که نشان‌دهنده پورت مقصد ارتباط است.

۳. **شماره ترتیب :(Sequence Number)**عدد ۳۲بیتی که شماره ترتیب بایت‌های داده را در یک اتصال نشان می‌دهد.

۴. **شماره تأییدیه (Acknowledgment Number)**: عدد ۳۲بیتی که تأیید دریافت بایت‌های قبلی را نشان می‌دهد.

۵. **طول هدر (Header Length)**: عدد ۴بیتی که طول هدر TCPرا مشخص می‌کند.

۶. **فیلدهای کنترلی (Control Flags)**: شامل ۹بیت است که نشان‌دهنده وضعیت مختلف اتصال مانند SYN، ACK، FIN، و غیره می‌باشد.

۷. **اندازه پنجره (Window Size)**: عدد ۱۶بیتی که نشان‌دهنده مقدار داده‌ای است که گیرنده می‌تواند دریافت کند بدون اینکه نیاز به تأییدیه باشد.

۸. **چک‌سام (Checksum)**: عدد ۱۶بیتی که برای بررسی صحت داده‌ها استفاده می‌شود.

۹. **اشاره‌گر اورژانس (Urgent Pointer)**: عدد ۱۶بیتی که به داده‌های اورژانسی اشاره می‌کند.

۱۰. **گزینه‌ها (Options)**: فیلد اختیاری که برای تنظیمات مختلف اتصال استفاده می‌شود.

این فیلدها در هر بسته TCPحضور دارند و اطلاعات لازم برای مدیریت و کنترل انتقال داده‌ها بین دستگاه‌ها را فراهم می‌کنند .در لایه کاربرد، برنامه‌ها از این اطلاعات برای برقراری و مدیریت ارتباطات شبکه‌ای خود استفاده می‌کنند.

چگونگی استفاده از TCPبرای اطمینان یکپارچگی

پروتکل TCP (Transmission Control Protocol)برای اطمینان از تحویل یکپارچه و قابل اعتماد داده‌ها طراحی شده است .تکنیک‌های مختلفی که TCPبرای اطمینان یکپارچگی استفاده می‌کند عبارتند از:

ایجاد اتصال (Connection Establishment)

TCPاز فرآیند سه‌گانه دستیابی (Three-Way Handshake)

برای ایجاد اتصال استفاده می‌کند .این فرآیند شامل مراحل زیر است:

۱. **SYN**: فرستنده یک بسته SYNبه گیرنده ارسال می‌کند.

۲. **SYN-ACK**: گیرنده بسته SYNرا دریافت کرده و یک بسته SYN-ACKبه فرستنده ارسال می‌کند.

۳. **ACK**: فرستنده بسته SYN-ACKرا دریافت کرده و یک بسته ACKبه گیرنده ارسال می‌کند.

این فرآیند تضمین می‌کند که هر دو طرف آماده برای ارتباط هستند.

کنترل جریان (Flow Control)

TCPاز مکانیزم پنجره لغزان (Sliding Window)برای کنترل جریان داده‌ها اســتفاده می‌کند .این مکانیزم به فرســتنده اجازه می‌دهد چندین بسته داده را بدون منتظر ماندن برای تأییدیه هر بسته ارسال کند .اندازه پنجره (Window Size) مشخص می‌کند که چه تعداد بایت داده می‌توانند قبل از دریافت تأییدیه ارسال شوند.

کنترل ازدحام (Congestion Control)

TCPاز تکنیک‌های مختلفی برای مدیریت ازدحام شبکه استفاده می‌کند .الگوریتم‌هایی مانند AIMD (Additive Increase Multiplicative Decrease)، TCP Tahoeو TCP Renoبرای مدیریت ســرعت ارســال داده‌ها و جلوگیری از ازدحام شبکه استفاده می‌شوند.

تأییدیه و بازپخش (Acknowledgment and Retransmission)

TCPاز شــماره‌های ترتیب (Sequence Numbers)و شــماره‌های تأییدیه (Acknowledgment Numbers)برای اطمینان از تحویل صحیح داده‌ها استفاده می‌کند .هر بسته داده‌ای که ارسال می شود دارای یک شماره ترتیب است و گیرنده باید تأییدیه دریافت آن را ارسال کند .اگر فرستنده تأییدیه‌ای دریافت نکند، بسته داده مورد نظر را مجدداً ارسال می‌کند.

بررسی صحت داده‌ها (Checksum)

TCPاز چک‌سام (Checksum)برای بررسی صحت داده‌ها استفاده می‌کند .هر بسته داده‌ای که ارسال می‌شود دارای یک چک‌سام است که با استفاده از محاسبات مختلف ایجاد می‌شود .گیرنده چک‌سام بسته دریافت شده را محاسبه می‌کند و اگر چک‌سام‌ها مطابقت نداشته باشند، بسته داده خراب در نظر گرفته شده و از بین می‌رود.

این تکنیک‌ها در لایه انتقال و لایه کاربرد استفاده می‌شوند تا اطمینان حاصل شود که داده‌ها به صورت صحیح و یکپارچه به مقصد می‌رسند.

نمونه سوالات امتحانی

شرح سوال	بارم
۱- مفهوم شبکه های کامپیوتری را شرح دهید؟	۱
۲- تقسیم بندی شبکه از لحاظ بعد جغرافیایی را نام ببرید؟	۱/۵
۳- روش های ارسال داده (Packet) در شبکه را نام برده و بطور مختصر توضیح دهید؟	۱/۵
۴- سرویس اتصال گرا در مدل مرجع OSI را شرح دهید؟	۱
۵- کدینگ یا رمزنگاری در لایه فیزیکی به چه مفهومی است؟	۱
۶- زیر لایه LLC در لایه پیوند داده ها را به اختصار شرح دهید؟	۱
۷- مسیریابی در لایه شبکه به چه مفهومی است و انواع آن را نام ببرید؟	۳
۸- کاربردهای VPN را نام ببرید؟	۲
۹- آدرس IP استاتیک را توضیح دهید؟	۱
۱۰- چهار مورد از مزایای کپسوله سازی را نام ببرید؟	۲