بسمه تعالی

تعریف شبکه های کامپیوتری

- تعریف **شبکه کامپیوتری**:مجموعه ای از کامپیوترهای مستقل متصل به هم که با هم تبادل داده می کنند.
- منظور از کلمه مستقل این است که یک سیستم کامپیوتری بزرگ با پایانه هایش (مثلاً یک main frame) شبکه محسوب نمیشود ، چون در واقع فقط یک کامپیوتر وجود دارد . همچنین سیستمهای master/slave را شبکه محسوب نمیکنیم ، زیرا در اینجا کامپیوترها مستقل نیستند و master کنترل slave را در دست دارد.

مزایا و کاربردهای شبکه های کامپیوتری:

- **اشتراک منابع** (سخت افزار - نرم افزار – داده ها)
- **افزایش قابلیت اعتماد** سیستم به دلیل وجود چندین نسخه از منابع
- نسبت قیمت به کارآیی کمتر در کامپیوترهای کوچک نسبت به سیستمهای بزرگ موجب شده که شبکه ای از کامپیوترهای کوچک به صرفه تر از یک کامپیوتر بزرگ باشد.
- استفاده از شبکه به عنوان بستر یک سیستم توزیع شده و امکان Load Sharing
- قابلیت ارتقاء (upgrade) شبکه بیشتر از سیستمهایی مانند Main Frame است.
- شبکه به عنوان یک رسانه ارتباطی سریع و کارا مطرح است : Email ، تجارت الکترونیکی ، آموزش از راه دور ، سرگرمیهای شبکه ای و ...

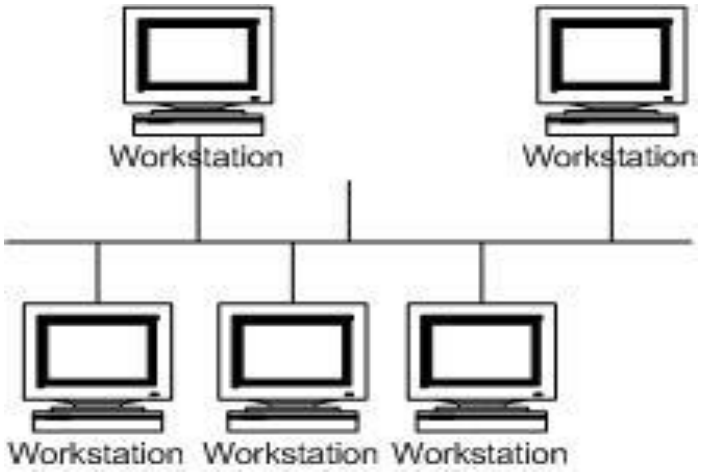
انواع شبکه از نظر کاربرد:

- **شبکه های نظیر به نظیر یا Workgroup یا peer to peer**
- در این نوع شبکه کامپیوترها همه در یک سطح هستند و هیچ کامپیوتری مدیر کل شبکه نیست .هر کامپیوتر هم نقش کلاینت و هم نقش سرور را می تواند داشته باشد.هر کاربر تصمیم می گیرد که کدام منابع خود را برای چه کسانی به اشتراک بگذارد.
- **شبکه های مبتنی بر سرور**
- در این نوع شبکه کامپیوتر سرویس دهنده مسئول مدیریت کل شبکه ، اشتراک منابع ، مدیریت کاربران، تضمین امنیت و ... است و کلاینتها که ایستگاه کاری هم خوانده می شوند استفاده کننده از سرویسها هستند.

انواع شبکه از نظر تکنولوژی انتقال داده:

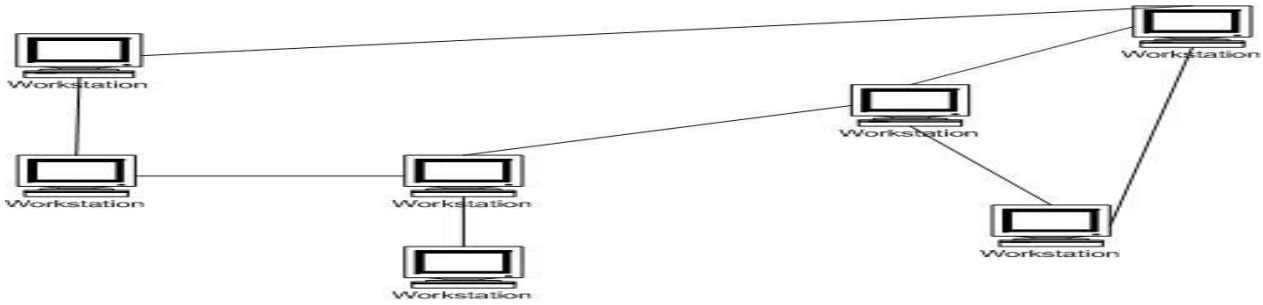
تکنولوژی پخشی

- همهٔ کامپیوترها به یک کانال ارتباطی مشترک متصلند.
-
- وقتی مبدأ بسته اطلاعاتی خود را آماده می کند در فیلد آدرس آن ، مقصد را مشخص می کند و آن را روی خط مشترک میفرستد. همه ماشینها می توانند این بسته را ببینند اما فقط مقصد آن را می گیرد.
- مسأله رقابت کامپیوترها برای ارسال روی خط مشترک وجود دارد که راه حلهای آن را بعداً خواهیم دید.



تکنولوژی نقطه به نقطه

- - بین کامپیوترها ارتباطات دوبدو وجود دارد.
-
- - برای ارسال یک بسته بین مبدأ و مقصد ماشینهای بین راه به صورت واسطه عمل می کنند . بنابراین مساله **مسیریابی** مطرح است. routing



تعریف توپولوژی و انواع آن:

- توپولوژی یا همبندی یعنی شکل فیزیکی و نحوه اتصال اجزای شبکه . سه همبندی اصلی شبکه های محلی عبارتند از خطی ، ستاره ای ، حلقوی

توپولوژی خطی :(bus)

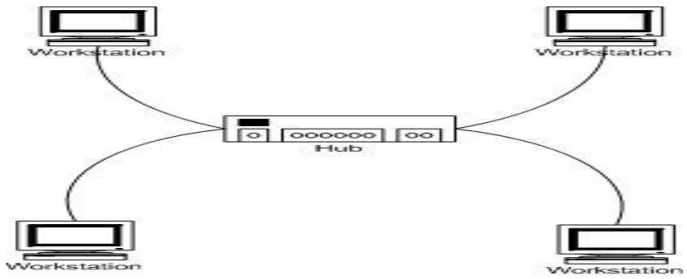
- همه کامپیوترها به یک کابل خطی وصل هستند که گاهی backbone شبکه نامیده می شود.
- از تکنولوژی پخشی استفاده می شود.
- کابل مورد استفاده معمولاً کابل هم محور است و قطعاتی مانند کانکتور BNC ، ترمیناتور نیز لازم است .
- ترمیناتور در واقع یک مقاومت الکتریکی است که در دو انتهای خط لازم است نصب شود . کار آن این است که با جذب سیگنال الکتریکی در انتهای کابل مانع از بازتابش آن می شود ، در غیر این صورت انعکاس سیگنال موجب تداخل با سیگنالهای جدید ارسالی (داده های جدید) میشود.اگر کابل شبکه در جایی قطع شود، کل شبکه مختل می شود.
- در شبکه های خطی مسأله رقابت برای ارسال از طریق کانال مشترک وجود دارد .مکانیزم اترنت برای حل این مشکل این است که اگر بسته های ارسالی کامپیوترها برخورد کرد ، هر کامپیوتر یک زمان تصادفی منتظر می ماند و دوباره تلاش می کند.

توپولوژی حلقه :(Ring)

- کامپیوترها به صورت یک حلقه به هم متصلند.
- سیگنال ارسالی در یک جهت حلقه حرکت می کند.از هر یک از کامپیوترها عبور می کند تا به مقصد برسد.هر کامپیوتر نقش یک تکرارگر را دارد.
- برای نوبتی کردن ارسال ، معمولا از مکانیزمی به نام نشانه استفاده می شود.token درحلقه در حال چرخش است و هر کامپیوتری که در یک لحظه آن را در اختیار دارد، حق ارسال دارد. به همین دلیل به چنین شبکه ای token ring گفته می شود.
- قطع شدن کابل یا خرابی تجهیزات کل شبکه را مختل می کند.
- مصرف کابل در این شبکه حداقل بوده لذا در پوش دادن شبکه های شهری کاربرد دارد.

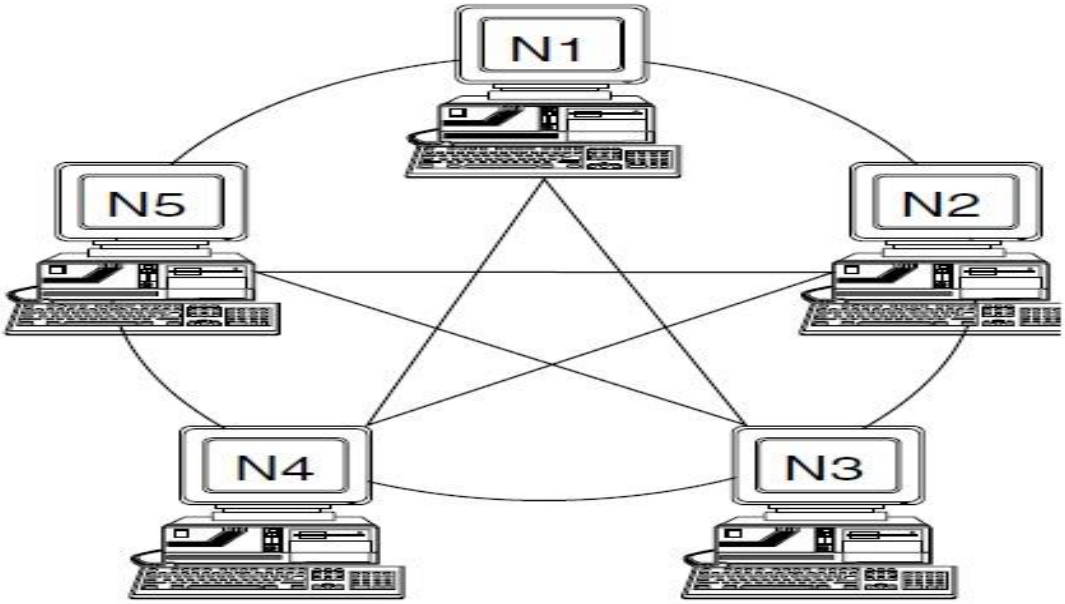
توپولوژی ستاره :(Star)

- کامپیوترها به یک واحد مرکزی به نام هاب متصل می شوند.
- کابل مورد استفاده معمولا UTP است.
- قطع شدن یکی از مسیر ها تاثیری روی کل شبکه ندارد.
- شناسایی و رفع مشکل بدلیل محدود بودن دامنه خرابی به آسانی انجام می گیرد.
- گسترش شبکه آسانتر است.
- میزان کابل مصرفی از سایر توپولوژی ها بیشتر است.



توپولوژی :(Mesh)

- این توپولوژی مختص شبکه های گسترده WAN می باشد.
- هریک از اجزای شبکه به کمک خطوط جداگانه به سایر اجزا وصل می شود.
- در صورت قطع شدن یکی از مسیر ها داده ها از مسیر دیگری منتقل می شوند.
- اجزای این شبکه به کمک مسیریاب بهم متصل می شوند.
- گسترش شبکه آسانتر است.
- امکان توزیع بار کاری بین مسیرها وجود دارد.



The number of links required to service a specified number of nodes in a mesh network is found by using the following equation:

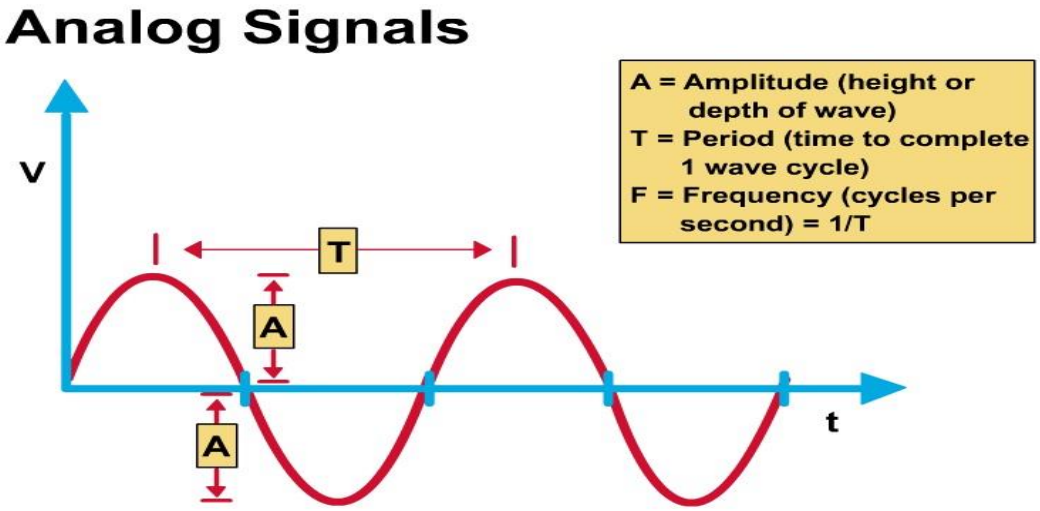
$$Ln = [Nn(Nn-1)]/2$$

where Ln = number of links required, and Nn = number of nodes in the network.

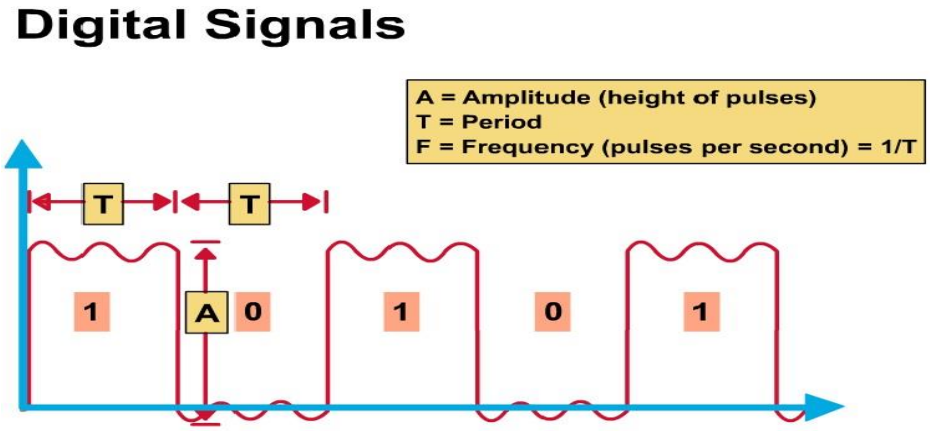
مفاهیم انتقال داده

انواع سیگنال ها

- سیگنال آنالوگ : در سیگنال آنالوگ سیگنال در حوزهٔ زمان به طـور پیوسـته وجـود دارد . اطلاعـات موجـود در سیگنال آنالوگ ممکن است هنگام برخورد با نویز ادغام شوند و در این صـورت نـویز وارد سیسـتم گیرنـده مـی شود و سیگنال اصلی (پیام) دچار آسیب می شوند.



- سیگنال دیجیتال : این نوع سیگنال شامل دو حالت پایه ای از سیگنال آنالوگ هستند کـه فقـط در دو وضـعیت وجود دارد . اطلاعات در این نوع سیگنال به صورت تکه تکه هستند . تجهیزاتی که با این نوع سیگنال کـار مـی کنند، حفاظت بیشتری نسبت به نویز دارند و قدرت تشخیص نویز و تداخل را دارا می باشند.



امواج و فرکانس:

تعریف فرکانس: اندازه گیری تعداد تکرار اتفاق در واحد زمان است. برای محاسبه فرکانس بر روی یک بازه زمانی ثابت، تعداد دفعات وقوع یک حادثه را در آن بازه می شماریم و سپس این تعداد را بر طول بازه زمانی تقسیم می کنیم. پس از فیزیک دان آلمانی هاینریش رودولف هرتز، در سیستم واحدهای SIفرکانس با هرتز (Hz) اندازه گیری می شود. یک هرتز به این معنی است که یک واقعه یک بار بر ثانیه رخ می دهد.

ادامه تعریف فرکانس: در اندازه گیری فرکانس صدا، امواج الکترومغناطیسی (مانند امواج رادیویی یا نور)، سیگنال های الکتریکی یا دیگر امواج، فرکانس بر حسب هرتز، تعداد سیکل های شکل موج تکراری است. اگر موج یک صدا باشد، فرکانس آن چیزی است که زیر و بمی این موج را مشخص می کند.

- فرکانس رابطه معکوسی با مفهوم طول موج دارد. فرکانس fبرابر است با سرعت vیک موج تقسیم بر طول موج &lambdaاست

طول موج : طول موج فاصله بین دو نقطه نظیر هم روی یک موج است. بطور معمول طول موج را از یک قله موج تا قله‌ی دیگر آن اندازه می‌گیرند.

مزیتهای انتقال دیجیتال در مقایسه با روش آنالوگ:

- چون فقط دو سطح سیگنال ممکن وجود دارد ، تقویت سیگنال در مسافتهای طولانی به راحتی امکان پذیر است.
- کمیتهای مختلف از قبیل داده ها ، صوت ، تصویر و ... همه می توانند به صورت بیت بیان شوند و سپس به شکل یکنواختی از طریق تجهیزات انتقال دیجیتال منتقل شوند.
- امکان ردیابی و کنترل خطا در روش دیجیتال بیشتر است.

تعریف پهنای باند

- تعریف پهنای باند در سیستم های آنالوگ: به حد فاصل بین پایین ترین و بالاترین فرکانسی که یک رسانه از خود عبور می دهد. واحد آن هرتز می باشد. به عنوان مثال پهنای باند خطوط انتقال تلفن شهری در حدود ۳ تا ۳,۴ KHZاست که در مقایسه با پهنای باند صدای انسان به وضوح کمتر است .
- تعریف پهنای باند در سیستم های دیجیتال: به ظرفیت انتقال اطلاعات گفته می شود. واحد آن بیت در ثانیه است. bps به عنوان مثال پهنای باند ارسال داده های دیجیتال روی خطوط انتقال تلفن شهری ۵۶ کیلو بیت در ثانیه می باشد.
- مثال : با یک مودم با پهنای باند 56 kbps در یک دقیقه حداکثر چه مقدار داده می توان انتقال داد ؟
- 60 * 56 Kb
- که جواب ۴۲۰KB می شود.

روش های انتقال داده ها با استفاده از پهنای باند

- **باند پایه BaseBand**

در این روش از تمام پهنای باند برای ارسال یا دریافت اطلاعات استفاده می شود. یعنی در هر لحظه فقط یک سیگنال از باند عبور می کند. و اطلاعات پشت سر هم مبادله می شوند. در شبکه های محلی از این روش استفاده می شود.

- **باند پهن BroadBand**

در این روش باند یا رسانه ارتباطی در آن واحد یک یا چند سیگنال را از خود عبور می دهد. از این روش در سیستم های انتقال آنالوگ استفاده می شود.

نکته:

- پهنای باند ظرفیت انتقال یک رسانه است. در صورتی که سرعت انتقال اطلاعات، سرعت ارسال اطلاعات در واحد زمان است.

نویز، تضعیف، اعوجاج، تاخیر :

- **تعریف نویز:** سیگنالی ناخواسته است که شکل سیگنال‌ها را تغییر می‌دهد و باعث بروز اختلال می‌شود.

در شبکه‌های رایانه‌ای حرارت، القا و همشنوایی سبب ایجاد نویز می‌شوند.

حرارت باعث می‌شود الکترون‌ها در جهات نامشخص آغاز به حرکت کنند، این حرکت گاهی با سیگنال‌ها هم‌جهت شده و اندازه و شکل آن‌ها را که همان الگوهای سیگنال‌هاست، تغییر می‌دهد و نویز پدید می‌آید.

موتورهای مکانیکی مانند موتور خودرو یا موتورهای الکتریکی وسایل خانگی نویز القایی ایجاد می‌کنند. این وسایل مانند یک آنتن فرستنده کار می‌کنند و می‌توانند نویز را ارسال کنند و کابل شبکه، مانند یک آنتن گیرنده نویزهای ارسال‌شده را دریافت می‌کند. کابل‌های برق فشار قوی یا رعد و برق نیز نویز القایی ایجاد می‌کنند.

هم‌شنوایی اثر میدان‌های مغناطیسی یک کابل کنار خود است.

نویز، تضعیف، اعوجاج، تاخیر

- **تعریف تضعیف Attenuation :** سیگنالهای الکتریکی در هنگام عبور از یک لینک مقداری انرژی از دست می‌دهند.

تضعیف مقدار انرژی را که یک سیگنال از زمان شروع تا رسیدن به مقصد از دست می‌دهد را می گویند. تضعیف با طول رسانه رابطه مستقیم دارد.

تعریف اعوجاج Distortion : هر گونه تغییر نامطلوب در شکل موج یک سیگنال الکتریکی که از درون یک مدار که شامل یک دستگاه انتقال می‌باشد ، عبور می‌کند.

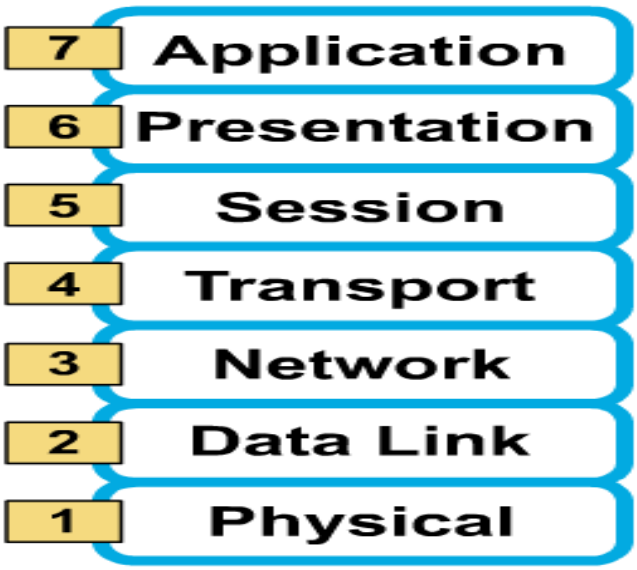
تعریف تاخیر Latency : تاخیر که نشاندهنده میزان تاخیر در پردازش داده در شبکه است، یکی دیگر از عناصر مهم در ارزیابی کارآیی و سرعت یک شبکه است که دارای ارتباطی نزدیک با پهنای باند می‌باشد. از لحاظ تئوری سقف پهنای باند ثابت است. پهنای باند واقعی متغیر بوده و می‌تواند عامل بروز تاخیر در یک شبکه گردد. وجود تاخیر زیاد در پردازش داده در شبکه و در یک محدوده زمانی کوتاه می‌تواند باعث بروز یک بحران در شبکه شده و پیامد آن پیشگیری از حرکت داده بر روی محیط انتقال و کاهش استفاده موثر از پهنای باند باشد.

معماری شبکه های کامپیوتری- مدلهاي مرجع:

- منظور از مدل مرجع ، مدلهای استانداردی هستند کـه معمـاری شـبکه (یعنـی تعـداد و وظـایف هـر بخـش) را پیشنهاد می کنند و میتوان شبکه را بر اساس آن طراحی کرد .
- دو مدل مرجع مهم عبارتند از مدل OSI و مدل TCP/IP

مدل مرجع OSI -Open Systems Interconnection:

- بخش شبکه و ارتباطات سازمان استاندارد بین المللی (ISO) ، بخش ارتباط سیستمهای باز یا OSI نامیـده مـی شود. OSI یک مدل هفت لایه ای برای شبکه های کامپیوتری پیشنهاد کرده است که لایه های آن از پـایین بـه بالا عبارتند از :



مسایل قابل توجه در طراحي لايه اي شبكه:

- برای تصمیم گیری درباره تعداد لایه ها و تقسیم وظایف بین آنها ابتدا باید مهمترین مسایل مطـرح در شـبکه را در نظر بگیریم
- آدرس دهی کامپیوترها در شبکه (آدرس فیزیکی کارت شبکه-شماره تلفن خط ارتباطی –آدرس IP-آدرسـهای از نوع دامنه)
- نحوه ارتباط دو کامپیوتر:

– روش **یکطرفه** یا simplex : یک کامپیوتر برای دیگر کامپیوترها اطلاعات می فرستد و بقیه فقط گیرنده هستند.

– روش **نیمه دو طرفه** یا half duplex : در یک لحظه یک طرف فرستنده و طرف دیگر گیرنده است و در یک زمـان دیگـر کار بر عکس می شود.

– روش **کاملاً دو طرفه** یا full duplex : دو کامپیوتر در یک زمان می توانند برای یکدیگر داده ارسال کنند.

مدل مرجع OSI

سرویسهاي مبتني بر اتصال و بدون اتصال

خدماتی که هر لایه ارائه می کند می تواند یکی از دو نوع باشد :

خدمات مبتني بر اتصال

ابتدا یک طرف از طرف مقابل در خواست برقراری اتصال می کند . بعد در صورت موافقت طرف مقابل ، اتصال برقـرار مـی شود . سپس ارسال و دریافت متقابل داده ها انجام می شود و در نهایت از طرف یکی از کامپیوترها اتصال قطع می شـود . چنین سرویسی را می توان به تماس تلفنی تشبیه کرد .

خدمات بدون اتصال

در این روش بدون هماهنگی قبلی و ایجاد اتصال ، اطلاعات از یک کامپیوتر به دیگری فرستاده می شود.

این سرویس شبیه ارسال نامه با پست عادی است .

در مواردی که قابلیت اعتماد و دقت انتقال داده ها مهم باشد ، سرویس مبتنی بر اتصال مناسب تر است.

در این نوع سرویس به دلیل هماهنگی دو طرف درست رسیدن و به ترتیب رسیدن اطلاعات تا حد زیادی تضمین میشود . اما این هماهنگیها ارتباط را کند میکند . بنابراین اگر سرعت انتقال اولویت داشته باشد ، سرویس بدون اتصال مناسب تر است .

پروتکل تحلیل آدرس ARP

پروتکل تحلیل آدرس(ARP: Aerodrome Reference Point)

پروتکل تحلیل آدرس ، دومین پروتکل کلیدی TCP/IP موجود در لایه اینترنت می باشد هدف ARP تحلیل و بدست آوردن آدرس فیزیکی از یک آدرس IP می باشد ARP . آدرس فیزیکی ماشینهای موجود در شبکه محلی را پرس وجو و همچنین زوج آدرس های فیزیکی IP را در حافظه نگهداری می کند.

هر وقت که IP نیاز به ارتباط با کامپیوتر دیگری داشته باشد ، حافظه سریع ARP بررسی می شود تا مشخص گردد آدرس IP مورد نظر مربوط به کامپیوتری محلی و یا مربوط به مسیریاب موجود درحافظه می باشد . اگر آدرس IP در حافظه سریع ARP موجود باشد ، از آدرس فیزیکی متناظر با آن

برای ارسال مستقیم داده گرام برای ارسال به آداپتور شبکه فیزیکی استفاده می شود . اگر آدرس IP درحافظه سریع ARP نباشد ، ARP پیغامی را در LAN منتشر می کند . درخواست ARP شامل آدرسIPکامپیوتر و یا مسیریاب محلی مورد نظر است . ماشینهای موجود در LAN آدرس IP موجود در

درخواست ARP را بررسی می کنند در صورت تطابق آدرس IP با آدرس یکی از کامپیوترها آن کامپیوتر پاسخ ARPکه شامل آدرس فیزیکی متناظر است را ارسال می دارد . سپس ARP ترکیب آدرس فیزیکی و IP را به حافظه سریع خود اضافه می کند و IP می تواند به کار خود ادامه داده و داده

گرامش را به صورت مستقیم به آداپتور شبکه مورد نظر ارسال نماید.

به منظور افزایش کارائی ، هر کامپیوتری که درخواست ARP را دریافت می کند ، زوج آدرس IP ،آدرس فیزیکی را به حافظه سریع ARP خود می افزاید . بدین ترتیب در صورت نیاز به اتصال به کامپیوتر ذکر شده درخواست ARP ، آدرس فیزیکی از قبل در حافظه سریع ARP جای گرفته است.

Connection-oriented ---Transmission Control Protocol

مهم ترین وظیفه پروتکل فوق اطمینان از صحت ارسال اطلاعات است . پروتکل فوق را اصطلاحاً(بالا) نامیده می شود.علت این امر ایجاد یک ارتباط مجازی بین کامپیوترهای فرستنده و گیرنده بعد از ارسال اطلاعات است . پروتکل هائی از این نوع ، امکانات بیشتری را بمنظور کنترل خطاهای احتمالی در ارسال اطلاعات فراهم نموده بعنوان یک پروتکل TCPولی بدلیل افزایش بار عملیاتی سیستم کارائی آنان کاهش خواهد یافت . از پروتکل قابل اطمینان نیز یاد می شود. علت این امر ارسال اطلاعات و کسب آگاهی لازم از گیرنده اطلاعات بمنظور اطمینان از صحت ارسال توسط فرستنده است . در صورتیکه بسته های اطلاعاتی بدرستی دراختیار فرستنده قرار نگیرند، فرستنده مجددا" اقدام به ارسال اطلاعات می نماید.

آشنایی باTCP/IP مخفف transmission Control Protocol/Internet Protocol

پروتکل استاندارد در اکثر شبکه های بزرگ است . با اینکه پروتکل فوق کند و مستلزم استفاده از TCP/IP منابع زیادی است ، ولی بدلیل مزایای بالای آن نظیر : قابلیت روتینگ ، حمایت در اغلب پلات فورم ها و سیستم های عامل همچنان در زمینه استفاده از پروتکل ها حرف اول را می زند. با استفاده از پروتکل فوق کاربران با در اختیار داشتن ویندوز و پس از اتصال به شبکه اینترنت، براحتی قادر به ارتباط با کاربران دیگر خواهند بود که از TCP/IPمکینتاش استفاده می کند امروزه کمتر محیطی را می توان یافت که نیازبه دانش کافی در رابطه با برای ارتباطات استفاده می IPX/SPXنباشد. حتی سیستم عامل شبکه ای ناول که سالیان متمادی از پروتکل کرد، در نسخه شماره پنج خود به ضرورت استفاده از پروتکل فوق واقف و نسخه اختصاصی خود را در این زمینه (نسخه قبلی اینترنت) طراحی ARPAnet در ابتدا برای استفاده در شبکه TCP/IPارائه نمود. پروتکل گردید. وزارت دفاع امریکا با همکاری برخی از دانشگاهها اقدام به طراحی یک سیستم جهانی نمود که دارای قابلیت ها و ظرفیت های متعدد حتی در صورت بروز جنگ هسته ای باشد. پروتکل ارتباطی برای شبکه فوق ، در نظر گرفته شد. TCP/IP

پروتکل تحلیل آدرس(ARP:): Protocol Reverse Address Resolution
پروتکلی که آدرس اینترنتی را به آدرس IP تبدیل کند.

RARPمختصر ARP برعکس ، می باشد . عکس عمل ARP را انجام می دهد . هنگامی که آدرسIP در دست است و آدرس فیزیکی ناشناخته ، به کار می رود RARP . هنگامی به کار می آید که آدرس فیزیکی شناخته شده است ، اما آدرس IP در دسترس نیست RARP . همچنین در رابطه با پروتکل BOOTPو راه اندازی ایستگاههای کاری بدون دیسک به کار می رود.
طراحان سیستم ارتباط بین شبکه ای یک راه حل جالب برای تفکیک آدرس در شبکه هایی مانند کی سی و یا اترنت که قابلیت پخش گسترده دارند ؛ ارائه داده اند . این راه حل اجازه می دهد که ماشین های جدید بدون ترجمه مجدد و یا نگهداشت بانک اطلاعات مرکزی به سیستم اضافه شوند . برای اجتناب از نگهداشت جدول نگاشت ها ؛ از یک پروتکل سطح پایین برای ذخیره سازی پویای آدرس استفاده می شود که پروتکل تفکیک آدرس)) ARP نامیده می شود . این پروتکل مکانیزمی کارا دارد و نگهداشت آن نیز ساده است.
ایده تفکیک پویای آدرس با ARP ساده است . وقتی میزبان A تصمیم به تفکیک آدرس ارتباط بین شبکه ای IB می گیرد ، بسته های ویژه ای را به صورت گسترده پخش می کند که از میزبان با آدرس ارتباط بین شبکه ای IBمی خواهد با آدرس فیزیکیخودPB: PluggedBack جواب دهد . تمام میزبان ها از جمله Bاین پیغام را دریافت می‌کنند . از میان میزبان ها فقط B آدرس ارتباط بین شبکه ای خود را تشخیص می

دهد و با آدرس فیزیکی خود جواب می دهد . وقتی A جـواب را دریافـت کـرد ، از آدرس فیزیکـی B بـرای ارسال بسته های ارتباط بین شبکه ای به B استفاده می کند.
به طور خلاصه می توان گفت : پروتکل تفکیکی آدرس ARP ، به یک میزبـان اجـازه مـی دهـد کـه آدرس میزبان دیگری را روی همان شبکه فیزیکی ، فقط با استفاده از آدرس IP آن به دست آورد.

قالب پروتکلARP

برخلاف اکثر پروتکل ها ، بسته های ARP دارای سرآیند با قالب ثابتی نیستند . درعـوض پیـام طـوری طـرح شده که برای فن آوری های مختلف شبکه سودمند باشد . باتوجه به این موضوع در فیلدهای ابتدایی سرآیند ، شماره هایی قرار دارند که طول‌فیلدهای بعدی را معین می کنند . در حقیقت ARP می تواند بـا آدرس هـای فیزیکی اختیاری و آدرس های پروتکلی اختیاری به کار گرفته شود . مثال شکل زیر قالب پیام 28 بایتی را به هنگام تفکیک آدرس های پروتکل (IP که چهار بایتی هستند) نشان می دهد که در یک سخت افزار اترنت (که در آن آدرس فیزیکی 48 بیت و یا 6بایت است) به کار رفته است.
شکل زیر یک پیغام ARP را به شکل چهار بایت در هر خط نشان می دهد.
متأسفانه برخلاف بیشتر پروتکل ها ، بخش های با طول متفاوت در بسته هایARP کاملا ا در شـروع کلمـات 32بیتی قرار نمی گیرند . در نتیجه خواندن شکل را مشـکل مـی کننـد . بـرای مثـال آدرس سـخت افـزار فرستنده ، با نام SENDER HA ، شش بایت متوالی را در بر می گیرد که در نتیجه در دو خط متـوالی شـکل آمده است.

قالب پروتکلARP

فیلد HARDWARE TYPE ، نوع واسط سخت افزاری را ، که فرستنده آن را به عنـوان جـواب جسـتجو مـی کند ، معین می کند . این مقدار در اترنت برابر 1 است . به طور مشـابه ، فیلـد PROTOCOL TYPE ، نـوع آدرس های پروتکل رده بالا را در فرستنده معین می کند . مقدار آن برای آدرس های » IP برابـر 080016 است فیلد OPERATION « نوع عملکرد را نشان می دهد :برای درخواست) 1) ARP ، برای جـواب ARP 2)،(برای درخواست) 3) RARP و برای جواب) 4) RARP فیلدهای HLEN و PLEN به ARP اجـازه می دهند که با هر شبکه ای تماس برقرار کند ؛ زیرا آن ها طول آدرس سخت افزار و آدرس پروتکل سطح بالا را معین می کنند . فرستنده آدرس سخت افـزار و آدرس IP خـود را در صـورت معـین بـودن در فیلـد هـای SENDER HAو SENDER IP قرار می دهد.

قالب پروتکلARP

در هنگام وجود یک درخواست ، فرستنده آدرس IP مقصد(ARP (یا آدرس سخت افزاری مقصد) RARP (را از فیلدهای TARGET IP و TARGET HA درخوست می کند . قبل از این که ماشین مقصد جواب دهد ، آدرس مفقود را تأمین می کند ، زوج آدرس فرستنده و مقصد را با هم عوض می کند و نوع عمل خود را به پاسخ تغییر می دهد.

در نتیجه ، یک پاسخ ، آدرس های IP و سخت افزاری مبدأ درخواست کننده و آدرس های IP و سخت افزاری

ماشینی را که ذخیره سازی آدرس برای آن در نظر گرفته شده است ، با خود حمل می کند ▪

پروتکل تفکیک معکوس آدرس RARP

طراحان پروتکل TCP/IP دریافته اند که یک مشخصه یکتای دیگر نیز علاوه بر مشخصات سخت افزاری وجود دارد که به آسانی قابل دسترسی است که آن ، آدرس فیزیکی ماشین در شبکه است . استفاده از آدرس فیزیکی به عنوان معرف یک شناسه یکتا ، دو مزیت دارد.

-اول اینکه میزبان آدرس های فیزیکی خودش را از سخت افزار واسط شبکه به دست می آورد و ایـن آدرس ها همیشه در دسترس هستند و لزومی ندارد که توسط سیستم عامل مشخص شوند.

-دوم ، به دلیل اینکه اطلاعات شناسایی به شبکه بستگی دارد و از مدل و فروشنده پردازنده مسـتقل اسـت ، در نتیجه مسأله به عکس تفکیک آدرس تبدیل میشود :با در دست داشتن یک آدرس فیزیکی ، طرحی عرضـه می شود که به یک کارگزار امکان نگاشت آن را به آدرس ارتباط بین شبکه ای می دهد

پروتکل تفکیک معکوس آدرس(RARP)

یک ماشین بدون دیسک از یک پروتکل TCP / IP به نام پروتکل تفکیک معکـوس آدرس RARP بـرای بـه دست آوردن آدرس IPخود از کارگزار ، استفاده می کنند . این پروتکل از پروتکل ARP که در بخش پیشـین گفته شد ، به دست آمده است و از همان قالب های پیام ، که در شکل زیر نشان داده شده اند ، استفاده مـی کند . در عمل پیام های RARP برای به دست آوردن آدرس ارتباط بین شبکه ای ارسال می شوند ، کمی عام تر از چیزی است که در بالا بدان اشاره شد . این پروتکل اجازه می دهد که در شبکه های فیزیکـی

مختلف استخراج آدرس معکوس امکان پذیر باشد ▪

پروتکل تفکیک معکوس آدرس(RARP

مشابه یک پیام ARP ، پیام های RARP از یک ماشین به ماشین دیگر ، در قسمت داده یک چارچوب اترنت محصور می شوند . یک چارچوب اترنت که حاوی درخواست RARP است ، حاوی سرآیند معمول با آدرس های مبدأ و مقصد در اترنت و نوع بسته در ابتدای هر بسته است . نوع چارچوب حاوی عدد 803516 » برای مشخص کردن بسته به عنوان یک پیام RARP « است.

بخش داده چارچوب شامل 28 بایت است که پیام RARP را در خود جای می دهد. یک میزبان چگونه ARP را به کار می گیرد . فرستنده یک درخواست RARPرا که در آن ، خودش هم به عنوان ماشین مبدأ و هم به عنوان ماشین مقصد مشخص شده و آدرس شبکه فیزیکی خود را در فیلد آدرس سخت افزاری مقصد قرار داده است ، در شبکه پخش گسترده می کند . تمام ماشین های روی شبکه ، این درخواست را دریافت می کنند ،

اما فقط آنهایی که مجاز به ارائه سرویس RARP هستند ، درخواست را پردازش و جواب زا ارسال می کنند.

پروتکل تفکیک معکوس آدرس(RARP)

این ماشین ها به عنوان کارگزارهای RARP شناخته شده اند . برای این که یک درخواست RARPاجرا شود ، شبکه باید حداقل دارای یک کارگزار RARP باشد.

کارگزارها با پر کردن فیلد آدرس پروتکلی مقصد و تغییر نوع پیام از درخواست به پاسخ، به درخواست ها جواب می دهند . ماشین درخواست کننده این پاسخ را از تمام کارگزارهای RARPبه رغم کافی بودن یکی از آنها دریافت می دارد.

به خاطر داشته باشید که در تمام ارتباطات بین ماشینی که آدرس IP خود را جستجو می کند و کارگزار ، باید با استفاده از آدرس فیزیکی انجام شود . به علاوه این پروتکل اجازه می دهد که یک میزبان درباره هر مقصد دلخواه اطلاعاتی را از کارگزار دریافت کند . در نتیجه ، فرستنده آدرس سخت افزاری خود را جدا از آدرس سخت افزار مقصد ارائه می دهد و کارگزار باید مراقب ارسال جواب به آدرس سخت افزار ی فرستنده باشد . در روی اترنت که یک فیلد برای آدرس سخت افزاری فرستنده دارد ، این عمل ممکن است غیر ضروری به نظر برسد ، زیرا این اطلاعات در سرآیند چارچوب اترنت وجود دارد . هر چند تمام سخت افزار

های اترنت به سیستم عامل اجازه دست یابی به سر آیند چارچوب را نمی دهند.

پروتکل پیغام کنترلی اینترنت(ICMP)

این پروتکل سومین پروتکل کلیدی است که در لایه اینترنت جای گرفته است . اهم کـاربرد ایـن پروتکـل در مسیریاب ها می باشند . داده ارسالی به کامپیوتر از راه دور از میان یک یا بیشتر مسیریاب عبور می کند ؛ این مسیر یاب ها ممکن است در ارسال پیغام به مقصدشان با مشکلاتی مواجه شوند و به همین خاطر از پیغامهای ICMPبرای آگاه کردن IP منبع از وقوع این مشکلات استفاده می گردد.
پر کاربردترین پیغامهای ICMP در اینجا آورده شده اند . برخی شرایط دیگر هم باعث تولید پیغامهای ICMP می شوند اما تواتر وقوع آنان بسیار پایین است.
انعکاس درخواست و انعکاس پاسخ ICMP - اغلب هنگام ارزیابی به کار می رود. وقتی یک تکنیسین از دستور pingبرای چک کردن ارتباط با میزبانی دیگر استفاده می کند ، در واقع ICMP را به کار مـی بنـدد ping . دیتاگرامی را به یک آدرس IP می فرستد و از کامپیوتر مقصد می خواهد که داده ارسالی را طی یک دیتـاگرام پاسخ بازگرداند . دستوراتی که در عمل مورد استفاده قرار می گیرند ، انعکاس درخواست و پاسخ می باشند.

پروتکل پیغام کنترلی اینترنت(ICMP)

توقف منبع - اگر کامپیوتر سریعی مقادیر زیادی داده را به کامپیوتر راه دوری ارسال کند، مسـیریاب ممکـن است در حجم بالای اطلاعات غوطه ور شود . در این حالت این احتمال وجود دارد که مسیر یاب با استفاده از ICMPیک پیغام توقف منبع به IP منبع ارسال کند و از آن بخواهـد نـرخ ارسـال داده را کـاهش دهـد . در صورت لزوم ممکن است پیغامهای توقف منبع بیشتری به IP منبع ارسال شوند.

مقصد غیر قابل دسترس - اگر مسیریاب دیتاگرامی را دریافت کند که امکان تحویل آن وجود نداشته باشـد ، ICMP یک پیغام مقصد غیر قابل دسترس به IP منبع می فرستد . یک دلیل آنکه مسیریاب نمی تواند پیغام را تحویل دهد ، پایین بودن (غیر فعال) شبکه بنابر خرابی تجهیزات یا انجام عملیات نگهداری است.

فرا رفتن زمان - در صورتی که داده گرامی به خاطر صفر شدن TTL از بین برود ، ICMPیک پیغام فرا رفتن زمان به IP منبع می فرستد این نشانگر این مسئله است که مقدار TTLکنونی برای رسیدن به مقصد با توجـه به جهش های مسیریابی موجود کافی نیست و یا اینکه جدول مسیریابی اشکالهایی دارد که باعـث مـی شـود دیتاگرام مرتبا بین چند مسیر یاب به گردش در آید.

در سیستم های نامتصل که تا به حال بحث کردیم ، هر دروازه به طور خود مختار ، مسیریابی و تحویل دیتاگرام های وارد شده را بدون هماهنگی با فرستنده اصلی انجام می دهد.

این سیستم در صورت درست کار کردن تمام ماشین ها و توافق بر نحوه تعیین مسیر ، می تواند به طور مناسبی کار کند ، اما هیچ سیستمی نمی تواند برای همیشه درست کار کند.
علاوه بر خطاهای خطوط ارتباطی و پردازنده ها ، IP در صورت قطع موقت و یا دایم ارتباط ماشین مقصد از شبکه ، از تحویل داده گرام خودداری میکند ، همچنین اگر زمان پایندگی دیتاگرام تمام شود و یا دروازه های بین راه تراکم به وجود آید به طوری که نتواند ترافیک ورودی را پردازش کند ، نیز دیتاگرام تحویل داده نمی شود . تفاوت عمده بین یک شبکه سخت افزاری حقیقی با سیستم ارتباط بین شبکه ای مبتنی بر نرم افزار این است که در مورد اول ، طراح به سخت افزار شبکه برای مطلع کردن ماشین ها در هنگام بروز مشکلات تکیه می کند . در یک سیستم ارتباط بین شبکه ای ، که چنین سخت افزاری را ندارد ، فرستنده نمی تواند بگوید که عدم تحویل از عملکرد بد محلی و یا از یک محل دور است و بنابراین اشکال زدایی بسیار مشکل می شود . پروتکل IP در خود چیزی ندارد که به فرستنده کمک کند تا آزمون ارتباط را انجام دهد و یا چنین خطاهایی را بیازماید.

برای این که به دروازه ها در یک سیستم ارتباط بین شبکه ای اجازه داده شود که خطاها را گزارش کنند یا اطلاعاتی درباره پیشامدهای غیر قابل پیش بینی فراهم سازند ، طراحان ، یک مکانیزم ویژه پیام به پروتکل TCP/IPاضافه کرده اند.
مکانیزم ، که پروتکل پیام کنترل ارتباط بین شبکه ای) ICMP (نامیده می شود ، به عنوان جزء لازمی در IPاست و باید در هر پیاده سازی IP گنجانده شود.
مشابه سایر ترافیک ها ، پیام های ICMP در قسمت دیتاگرام IP در سیستم ارتباط بین شبکه ای گذر می کنند . مقصد نهایی پیام ICMP یک برنامه کاربردی و یا یک کاربر روی ماشین مقصد نیست و به نرم افزار پروتکل ارتباط بین شبکه ای روی آن ماشین تحویل داده می شود . یعنی وقتی که یک پیام خطای ICMP وارد شود ، ماجول نرم افزار ICMP آن را تحویل می گیرد و بررسی و پردازش می کند.
البته اگر ICMP تشخیص دهد که یک پروتکل سطح بالاتر و یا برنامه کاربردی باعث به وجود آمدن مسأله شده است ، ماجول مرتبط با آن را باخبر می کند.

می توانیم به طور خلاصه بیان کنیم که:

پروتکل پیام کنترل بین شبکه ای ، به دروازه ها اجازه می دهد که پیام های خطا و یا کنترل را به دروازه های دیگر و یا میزبان ها ارسال کنند ، ICMP ارتباط بین نرم افزار پروتکل ارتباط بین شبکه ای روی یک ماشین را با نرم افزار پروتکل ارتباط بین شبکه ای روی ماشین دیگر ، فراهم میسازد.

ICMPدر ابتدا برای این که دروازه ها بتوانند پیام خطاهای تحویل را به میزبان ها گزارش کنند ، به وجود آمد ، اما استفاده از آن فقط به دروازه ها محدود نشده است . اگر چه رهنمودها ، استفاده از بعضی پیام های ICMPرا محدود می کند ، یک ماشین می تواند یک پیام ICMP برای ارتباط با یک دروازه و یا میزبان دیگری استفاده کند . حسن عمده استفاده از ICMP به وسیله میزبان ها ، این است که یک مکانیزم منفرد برای تمامی پیام های کنترل و خطا به کار برده می شود.

تحویل پیام:ICMP

پیام های ICMP به دو مرحله محصور سازی مطابق شکل احتیاج دارند.
هر پیام ICMP از میان سیستم ارتباط بین شبکه ای ، در قسمت داده مربوط به دیتاگرام IP عبور می کند ، که آن هم در هر شبکه فیزیکی در قسمت داده ای یک چار چوب قرار می گیرد.
دیتاگرام هایی که پیام های ICMP را حمل می کنند ، مشابه دیتاگرام هایی هستند که برای کاربرها ارسال می شوند و هیچ اطمینان و یا تقدم اضافی در ارسال آنها در نظر گرفته نمی شود . در نتیجه ، پیام های خطا ممکن است گم شوند و یا دور انداخته شوند . علاوه بر این، در شبکه ای که قبلا ا تراکم زیادی داشته باشد ، پیام های خط ممکن است تراکم را بیشتر کنند . در صورتی که پیام ICMP خود ایجاد خطا کند ، یک استثنا از برنامه بررسی خطا به وجود می آید . این استثنا برای جلوگیری از ایجاد پیام های خطا درباره پیام های خطا است و مشخص می کند پیام های ICMP برای خطاهایی که از دیتاگرام های حاوی ICMP به وجود آمده اند ، ایجاد شده است .

باید در نظر داشت که هرچند پیام های ICMP با استفاده از IP محصور سازی و ارسال می شوند ، ICMP به عنوان یک پروتکل سطح بالا تلقی نمی شود . این قسمت به عنوان بخش لازمی از IP محسوب می شود .
دلیل اینکه از IP برای تحویل پیام های ICMP استفاده می شود ، این است که پیام ها در طول مسیر ممکن است از چند شبکه فیزیکی عبور کنند تا به مقصد نهایی برسند . در نتیجه پیام ها را نمی توان از طریق

ارسال فیزیکی تحویل داد ▪

شکل :

دو مرحله محصور سازی ICMP ، پیام ICMP در یک دیتاگرام IP محصور میشود که آن هم در یک چارچوب برای ارسال محصور شده است . برای مشخص کردن ICMP ، فیلد پروتکل دیتاگرام مقدار 1 را دارد.

داده ICMP	سرآیندICMP
ناحیه داده ای دیتاگرام	سرآیند دیتاگرام
ناحیه داده ای فریم	سرآیند فریم

قالب پیامICMP مخفف Internet Control Message Protocol

در تعریف پروتکلی برای کنترل فرستادن پیام می باشد

اگرچه هر پیام ICMP قالب خودش را دارد ، همه پیام ها با سه فیلد مشابه شروع می شوند : یک عدد صحیح 8 بیتی برای فیلد TYPE که نوع پیام را مشخص می کند ، یک هشت بیتی فیلد CODE که اطلاعات بیشتری در مورد نوع پیام عرضه می کند و یک فیلد 16) CHECKSUM بیتی ICMP)از همان الگوریتم مجموع مقابله ای IP استفاده می کند ، اما مجموع مقابله ای ICMP فقط پیام ICMP را در برمی گیرد .علاوه بر این ، پیام های ICMP که خطاها را گزارش می کنند همیشه سرآیند و 64 بیت اول دیتاگرامی را که باعث

مسأله شده است ، در بردارند ▪

دلیل اینکه چیزی بیش از سرآیند دیتاگرام برگردانیده می شود این است که به گیرنده امکان تشخیص پروتکل ها و برنامه کاربردی مسؤل دیتا گرام را با دقت بیشتری بدهد . همان طور که بعدا خواهیم دید ، پروتکل های سطوح بالاتر TCP/IP بگونه ای طرح شده اند که اطلاعات ضروری در 64 بیت اول قرار گیرد. فیلد TYPE معنی پیام را به همراه قالب آن تعیین می کند.

پروتکل دیتا گرام کاربر(UDP):

در مجموعه پروتکل TCP/IP ، پروتکل دیتاگرام کاربر(UDP) یک مکانیزم اولیه را فراهم می کند که برنامه های کاربردی از آن برای ارسال دیتاگرام ها به برنامه کاربردی دیگری استفاده می‌کنند.

UDPاز درگاه های پروتکل برای تشخیص چندین برنامه که روی یک ماشین اجرا می شـوند ، اسـتفاده مـی کند . یعنی علاوه بر داده ای که فرستاده می شود ، هر پیام UDP حاوی شماره درگاه مقصد و شـماره درگـاه مبدأ است و بدین وسیله این امکان به وجود می آید که نرم افزار UDP در مقصد پیـام را بـه دریافـت کننـده صحیح بدهد و جواب آن را نیز به فرستنده حقیقی بدهد ▪

انواع مختلف به قرار زیر هستند:

نوع فیلد	نوع پیامICM
0	پاسخ انعکاس
3	مقصد غیر قابل دسترس
4	ترمز مبدا(منسوخ شده)
5	تغییر مسیر
8	درخواست انعکاس
11	زمان بیش از حدبرای یک دیتاگرام
12	مشکل پارامتر در یک دیتاگرام
13	درخواست برچسب زمانی
14	پاسخ برچسب زمان
15	درخواست اطلاعات (منسوخ شده)
16	برگشت اطلاعات(منسوخ شده)
17	درخواست ماسک آدرس
18	پاسخ یا جواب ماسک آدرس

پروتکل دیتا گرام کاربر(UDP) مخفف User Datagram Protocol

هدف اولیه پروتکل UDP ، ارائه دیتاگرام ها به لایه کاربرد است . بدین ترتیب ، پروتکل UDP خود به تنهایی کار کمی را انجام می دهد و بنابراین ساختار سرآیند ساده ای دارد. RFC ای که این پروتکل را شرح می دهد، RFC75 می باشد که تنها از سه صفحه تشکیل یافته است UDP . دیتاگرام های خراب یا از دست رفته را دوباره ارسال نمی کند و اتصالها را ایجاد یا پایان نمی بخشد UDP . در اصل مکانیزمی است برای ارسال یا دریافت دیتاگرام ها بدون سربار یک اتصال TCP سرآیند UDP از چهار فیلد 16 بیتی تشکیل شده است

پروتکل فوق نظیر پروتکل TCP در لایه " حمل " فعالیت می نماید. UDP بر خلاف پروتکل TCP بصورت " بدون اتصال " است . بدیهی است که سرعت پروتکل فوق نسبت به TCP سریعتر بوده ولی از بعد کنترل خطاء تظمینات لازم را ارائه نخواهد داد. بهترین جایگاه استفاده از پروتکل فوق در مواردی است که برای ارسال و دریافت اطلاعات به یک سطح بالا از اطمینان ، نیاز نداشته باشیم .