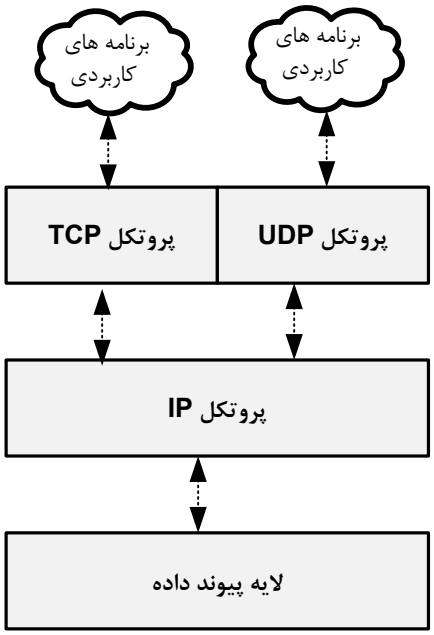
فصل نهم

پروتکل های لایه حمل دراینترنت

درمعماریTCP/IP دو پروتکل TCP و UDP درلایه حمل تعریف شده است. پروتکل TCP یک پروتکل اتصال گرا و مطئمن می باشد درحالیکه پروتکل UDP یک پروتکل بدون اتصال و بدون تضمین است. مطابق با شکل(۹-۱)،TCP و UDP بر روی پروتکلIP اجرا می شوند و سرویس های فراهم شده توسط IP را مهیا می کنند. پروتکلIP یک سرویس بدون اتصال را بین دو کامپیوتر مهیا می سازد. با استفاده ازپروتکل های TCP و UDP داده به یک فرآیند کاربردی درحال اجرا دریک کامپیوتر دور می توان تحویل داد. این فرآیند های کاربردی به وسیله شماره های درگاه شناسایی می شوند. پروتکل TCP با فراهم ساختن یک سرویس اتصال گرا می تواند از تحویل مطمئن داده به مقصد اطمینان حاصل کند، درحالیکه پروتکل UDP بدون اتصال است و نمی تواند تحویل داده ها را تضمین نماید. با این وجود UDPدر بسیاری از کاربرد ها استفاده می شود. به عنوان مثال درمواقعی که نیاز است تا داده ها به یک برنامه کاربردی خاص درحال اجرا در یک ماشین فرستاده شود و یا در وضعیتی که نیاز است داده هابه صورت همه پخشی یا چند پخشی ارسال شوند، از پروتکل UDP استفاده می گردد.



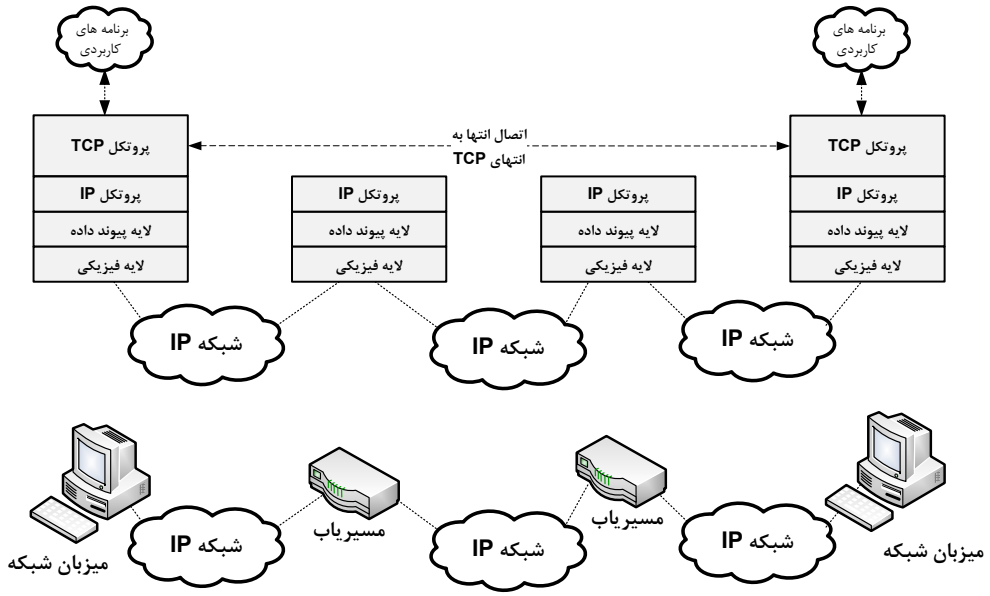
شکل(۹-۱): پروتکل های TCP و UDP

۹-۱- پروتکل کنترل حمل (TCP)

پروتکل TCP ، یک پروتکل اتصال گرا و مطمئن برای تحویل داده های برنامه های کاربردی می باشد. چون پروتکل TCP به کمال قابل توجهی رسیده است و اصلاحات زیادی برای بهبود کارآیی و اطمینان پذیری آن انجام شده است، بسیاری از برنامه های کاربردی از آن به عنوان پروتکل لایه حمل خود استفاده می کنند. همانطور که درشکل(۹-۲) نشان داده شده است، پروتکلTCP اطمینان پذیری انتها به انتها را بین دو فرآیند کاربردی اجرا شده در سیستم های کامپیوتری انتها به

انتها، مهیا می سازد. پروتکلTCP این اطمینان پذیری را با اضافه کردن سرویس های اتصال گرا در بالای پروتکلIP فراهم می سازد.

TCP فرض می کند که IP ذاتا نامطمئن است، بنابراین برای اطمینان حاصل کردن از تحویل مطمئن داده انتها بـه انتهـا، سرویس هایی را درنظر گرفته است. اتصالات انتها به انتها درTCP از نوع اتصالات مطمئن دوطرفه و به صورت مدار مجازی می باشند. امکان پیاده سازی TCP برروی پروتکل های IP نسخه ۴ و ۶ وجود دارد.



شکل(۹-۲): اتصال های انتها به انتهای TCP

برخلاف IP که برروی میزبان ها و مسیریاب های شبکه قابل پیاده سازی است، پروتکل TCP معمولا فقـط بـرروی میزبـان های انتهایی شبکه به منظور تحویل مطمئن داده ها به صورت انتها به انتها اجرا می شود. البتـه بـسیاری از مـسیریاب هـای امروزی از پروتکل های لایه حمل TCP و UDP برای انجام عملیاتی نظیر پیکره بنـدی و مـدیریت اسـتفاده مـی نماینـد. پروتکل TCP در RFC 792 و پروتکل UDP در RFC1122 توصیف شده اند.

۹-۱-۱- ویژگی های پروتکل TCP

پروتکلTCP خواص قابل ملاحظه زیر را دارد:

- حمل داده پایه ای
- اطمینان
- کنترل جریان
- تسهیم سازی
- اتصال انتها به انتها
- تقدم و امنیت

درادامه به بررسی اجمالی هریک از قابلیت های فوق می پردازیم.

۹-۱-۱-۱- حمل داده پایه ای

TCP توانـــایی حمـــل جریـــان پیوســـته ای از بایتهـــا در هـــردو جهـــت اتـــصال را دارد. بایـــت هـــا بین دوفرایند کاربردی راه دور که از پروتکل TCP درلایه حمل استفاده می کنند، ارسال می شوند. فرآیند هـای کـاربردی،

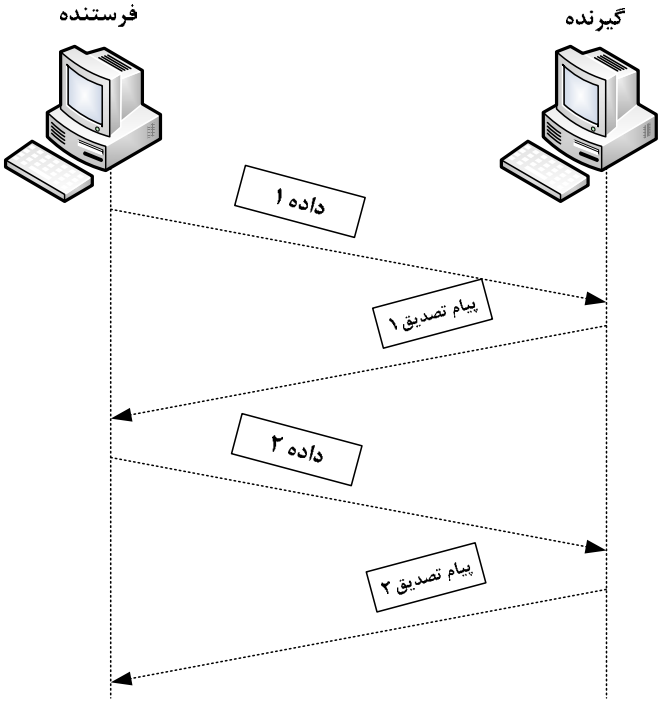
بایت های ارسالی را درقالب یک سگمنت دسته بندی می کنند. طول سگمنت های پیام اختیاری می باشد، امابه منظور بازدهی مدیریت پیام ها، معمولا اتصالات TCP دارای یک حداکثر اندازه پیام می باشند. از TCP برای فراهم ساختن چندین اتصال مدار مجازی بین دو میزبان TCP استفاده می شود. فرآیند های کاربردی که از TCP استفاده می کنند، داده ها را در هر اندازه ای که برای ارسال مناسب است می فرستند. هیچ محدودیتی برای اندازه داده های ارسالی از فرایندهای کاربردی به پروتکل TCP وجود ندارد. به عنوان مثال، یک برنامه کاربردی می تواند داده ای رابه کوچکی یک بایت ویا به بزرگی چند کیلو بایت ارسال دارد. TCP هر بایتی را که می فرستد شماره گذاری می نماید. بنابراین بایت ها به ترتیبی که ارسال شده اند به فرآیند های کاربردی گیرنده تحویل داده می شوند. این فرآیند ترتیب دهی بایتها خوانده می شود. ممکن است که فرآیند کاربردی چندین بایت داده را در یک زمان به پروتکل TCP ارسال نماید. پروتکلTCP این داده ها را بافر نموده و آنها را یا به صورت یک پیام منفرد ویا به صورت چندین پیام کوچکتر می فرستد. درهر صورت، TCP تحویل داده ها را به گیرنده به ترتیبی که ارسال شده است، تضمین می نماید. به عنوان مثال اگر یک برنامه کاربردی ۱۰۲۴ بایت داده را به پروتکل TCP ارسال دارد، پروتکل TCP می تواند همه داده ها را درقالب یک سگمنت ۱۰۲۴بایتی ارسال نموده و یا آنها را به صورت ۴ سگمنت ۲۵۶ بایتی ارسال نماید. همچنین هرترکیب دیگری که منجر به ارسال ۱۰۲۴ بایت داده فوق گردد نیز قابل قبول می باشد. چون TCP داده ها را به عنوان جریانی از بایت ها ارسال می کند، نشانگر واقعی انتهای پیام درجریان داده وجود ندارد. برای این که از ارسال همه داده های واگذار شده به ماژول TCP اطمینان حاصل شود، لازم است تا TCP یک تابع Push را پیاده سازی کند. مکانیزم Push باعث می شود تا TCP هر داده ای را که از یک برنامه کاربردی دریافت نمود، بدون معطلی ارسال نماید. مکانیزم فوق توسط بیت خاصی به نام بیت Push که دربخش های بعدی توضیح داده خواهد شد، پیاده سازی می گردد.

۹-۱-۱-۲- اطمینان

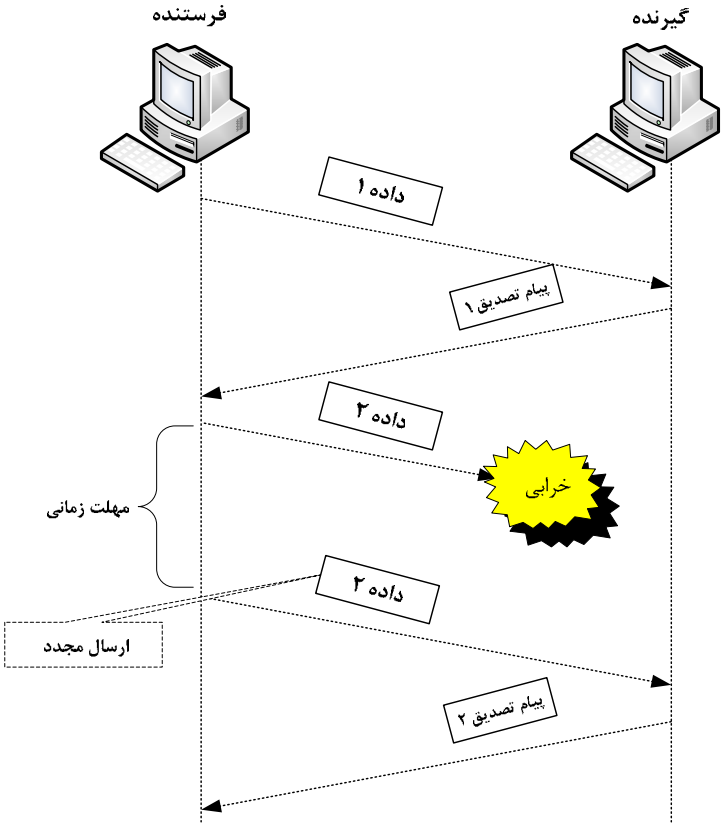
یکی از مهمترین ویژگی های TCP تحویل مطمئن داده ها به صورت انتها به انتها است . به منظور مهیا سازی اطمینان، پروتکل TCP باید داده هایی را که خراب، گم، تکرار ویا خارج از نوبت به لایه شبکه تحویل داده شده اند راجبران کند. بدین منظورTCP از مدل ارسال مجدد تصدیق مثبت (مدل PAR[1]) استفاده می نماید. درشکل (۹-۳) نحوه عملکرد مدا PAR نمایش داده شده است. همانطور که دراین شکل دیده می شود، درTCP سگمنت های جدید تنها زمانی فرستاده می شوند که سگمنت های قبلی ارسال شده تصدیق شده باشند. درشکل(۹-۴) مثالی از عملکرد TCP درقبال گم شدن یک سگمنت نشان داده شده است.

درTCP، هرسگمنت ارسالی دارای یک شماره رشته می باشد. فرستنده با ارسال هر سگمنت منتظر دریافت پیام تصدیق مثبت (ACK[2]) از طرف گیرنده می باشد. اگر ACK در یک بازه زمانی معین دریافت نشود، سگمنت قبلی دوباره ارسال می شود. در TCP ازمکانیزم شماره گزاری رشته برای مرتب کردن سگمنتهایی که خارج از نوبت دریافت شده اند و حذف سگمنت های تکراری استفاده می شود. درصورت وقوع خرابی در سگمنت ها، با استفاده از فیلدمجموع مقابله ای موجود در سرآیند بسته هایTCP، مشکل رفع می شود. درصورت هرگونه تشخیص خرابی درسگمنت های دریافتی، آن سگمنت ها از بین می روند. با کمک مکانیزم فوق، اغلب خطاهایی که ضمن انتقال سگمنت های درشبکه فیزیکی اتفاق می افتد جبران می شود. البته خطاهایی که به خاطر قطع اتصال فیزیکی و سایر مشکلات لایه فیزیکی درشبکه بوجودمی آیند، قابل رفع با کمک مکانیزم فوق نمی باشند.

[1] Positive Acknowledgement Retransmission
[2] Acknowledgment



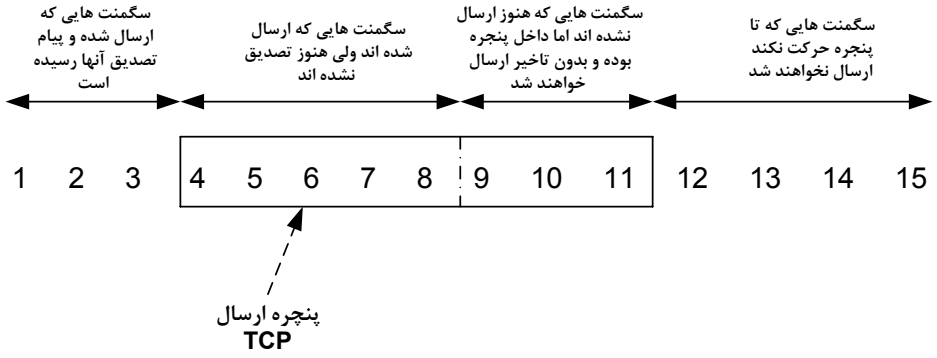
شکل(۹-۳): مدل PAR تحت عملکرد معمولی



شکل(۹-۴): نحوه برخورد با سگمنت های گم شده در مدل PAR

۹-۱-۱-۳- کنترل جریان

با توجه به تفاوت سرعت پردازنده های کامپیوتر های میزبان و همچنین تفاوت درپهنای باند شبکه، این امکان وجود دارد که یک فرستنده داده ها را با نرخ خیلی سریع تر از این که گیرنده بتواند از عهده آن برآید ارسال کند. پروتکلTCPیک مکانیزم کنترل جریان را پیاده سازی می کند که توسط آن همواره مقدار داده ارسال شده توسط فرستنده کنترل می شود. بدینمنظور پروتکل TCP از مکانیزم پنجره لغزان[1] برای پیاده سازی کنترل جریان استفاده می کند. درشکل(۹-۵) مثالی از عملیات کنترل جریان TCP به وسیله مکانیزم پنجره لغزان آورده شده است. جریان داده در TCP در سطح بایت شماره گذاری می شود. شماره ای که به هر بایت انتساب داده می شود، شماره رشته نام دارد.



شکل(۹-۵): مثالی از عملیات کنترل جریان پنجره لغزان درTCP

در شکل(۹-۵) بازه پنجره از شماره رشته ۴ تا ۱۱ است . در این مثال بایت های ۱ تا ۳ که قبلا ارسال شده اندبه طور کامل تصدیق شده واز پنجره خارج شده اند. بایت های ۴ تا ۱۱ که در بازه پنجره هستند یا ارسال شده و یا منتظر ارسال می باشند، اما هیچ کدام از آنها هنوزتصدیق نشده اند . اندازه پنجره، حداکثر تعداد بایت های تصدیق نشده ای را که TCP می تواند بفرستد، نشان میدهد. در شکل(۹-۵) بایت ۴ تا ۸ فرستاده شده انداما بایت های ۹ تا ۱۱ که درون بازه پنجره است، فرستاده نشده اند ولی بدون تاخیر فرستاده خواهند شد. بایت ۱۲ و بعد از آن چون در سمت راست بازه پنجره هستند، نمی توانند فرستاده شوند.

لبه سمت چپ پنجره،بیانگرکوچکترین شماره بایتی است که هنوز تصدیق نشده است . هنگامی که پیام تصدیقی برای داده های ارسال شده دریافت شد لبه پنجره می تواند به سمت راست حرکت کند. اندازه پنجره، مقدار فضای در دسترس بافر برای داده جدید در گیرنده را منعکس می کند. درصورتیکه گیرنده با ازدحام مواجه باشد، بافر آن اغلب پر بوده وبنابراین مقدار اندازه پنجره کاهش می یابد. دربدترین حالت، ممکن است بافرگیرنده فقط به اندازه یک بایت فضای خالی داشته باشد و به طرف مقابل خود اندازه پنجره یک بایتی رااعلام نماید. بدین ترتیب، فرستنده فقط قادر است که یک بایت داده ارسال نماید. فرستنده نیز اقدام به ارسال سگمنت های یک بایتی به طرف مقابل می نماید. با توجه به اینکه حداقل طول سرآیند TCP و IP هرکدام ۲۰ بایت می باشد، بنابراین برای ارسال ۱ بایت داده، بیش از ۴۰ بایت سرآیند به کاررفته است که بدین ترتیب بهره وری ارسال درشبکه به شدت کم خواهد بود. این پدیده با عنوان سندروم پنجره ابله (SWS[2]) خوانده می شود. اغلب پیاده سازی های TCP، مکانیزم هایی برای اجتناب ازآن دارند. درصورتیکه درپیام ارسالی از گیرنده به فرستنده، اندازه پنجره ارسال برابر با ۰ گزارش شود، فرستنده متوجه می شود که بافرهای دریافت گیرنده پر بوده و توانایی دریافت داده های جدید را ندارد.

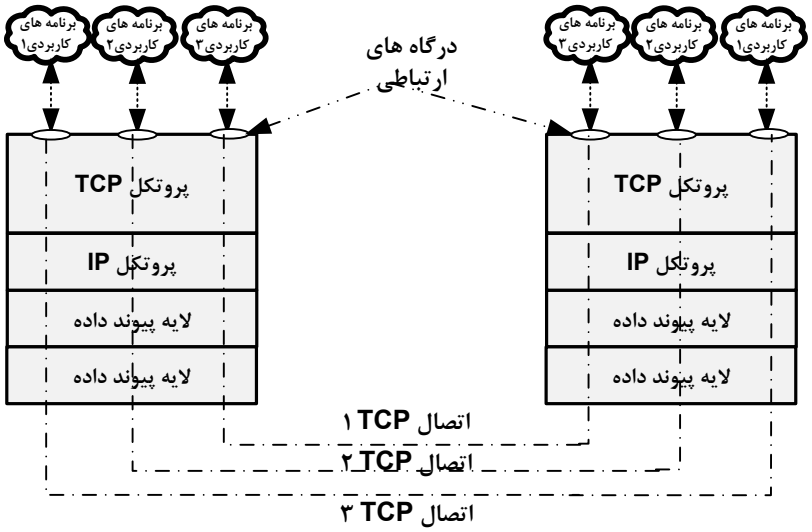
---

[1] Sliding window
[2] Silly Window Syndrome

پروتکل TCP دارای مکانیزمی است که درهنگام مواجه با ازدحام، اندازه پنجره را کاهش می دهد و هنگامی که مشکل ازدحام بر طرف می شود، اندازه پنجره را افزایش می دهد. هدف از مکانیزم پنجره لغزان، پر نگه داشتن کانال داده و کاهش تاخیر انتظارتا حد مینیمم است.

۹-۱-۱-۴- تسهیم سازی

درپروتکل TCP این امکان وجود دارد که به طور همزمان چندین سرویس ارتباطی برروی یک کامپیوتر اجرا شده و به طور همزمان داده های خود رابرای ارسال به TCP تحویل دهند. ازآنجاییکه همه فرآیند هایی که از یک واسط شبکه در یک کامپیوتر استفاده می کنند، آدرس IP مشترک دارند، برای شناسایی یک فرآیند به چیزی بیشتر از آدرسIP واسط شبکه نیاز می باشد. بدینمنظوربرای هر برنامه کاربردی، یک شماره درگاه تعریف شده است. با استفاده از شماره درگاه، امکان برقراری چندین اتصال بین فرآیندهای کاربردی راه دور فراهم می شود. استفاده مشترک چندین فرآیند لایه کاربرد از امکانات TCP/IP، تسهیم سازی نام دارد. در شکل(۹-۶) مثالی از عملیات تسهیم سازی درTCP نشان داده شده است.



شکل(۹-۶): مثالی از استفاده شماره درگاه برای انجام تسهیم سازی TCP

۹-۱-۲- اتصال های TCP

قبل ازاین که فرآیند های کاربردی قادر به ارسال داده به یکدیگر باشند، باید یک اتصال TCP بین آنها با استفاده از شماره های درگاه فرستنده وگیرنده ایجاد شود. اتصال های TCP با استفاده از زوج (شماره های درگاه، آدرسIP) مشخص می شود. آدرسIP، آدرس واسط شبکه ای است که از طریق آن، برنامه کاربردی ارتباط برقرار می کند. شماره درگاه، شماره درگاهTCPاست که برنامه کاربردی را مشخص می نماید. بنابراین نقاط پایانی درTCP هم شامل آدرس IP و هم شامل شماره درگاه TCP می باشند.

با توجه به اینکه اتصال هایTCPبین دو نقطه پایانی برقرار می شوند، بنابراین هر اتصالTCP به وسیله پارامتر های هر دو نقطه پایانی به شرح زیر مشخص می شوند:

(شماره درگاه ۲ و آدرس IP ۲، شماره درگاه ۱ و آدرس IP ۱)

این پارامتر ها، امکان اتصال چندین فرآیند کاربردی به یک نقطه پایانی دور را ممکن می سازد. یک اتصال TCP می تواند داده را در هر دو جهت حمل نموده وبه صورت دوطرفه کامل عمل نماید.

معمولا پروتکلTCP، به عنوان یک ماژول پروتکل که با سیستم عامل کامپیوتر ارتباط برقرار می کند، پیاده سازی می شود. به طور خلاصه فرآیندهای کاربردی با کمک فراخوانی های سیستمی زیربا ماژولTCP ارتباط برقرار می کنند:

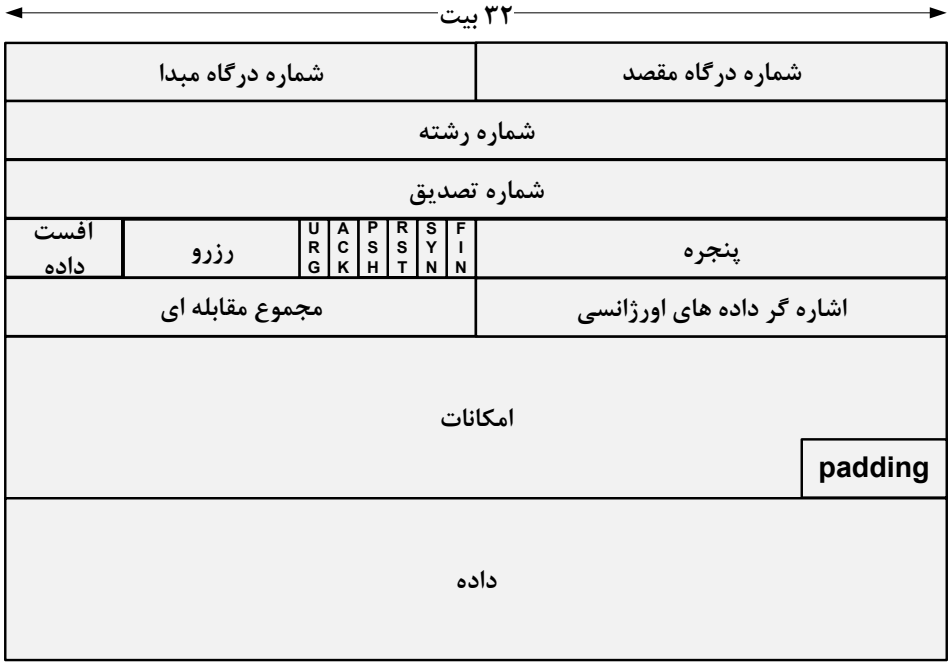
- OPEN : برای باز کردن یک اتصال
- CLOSE : برای بستن یک اتصال
- SEND: برای ارسال داده در یک اتصال باز
- RECEIVE : برای دریافت داده از یک اتصال باز
- STATUS : برای پیدا کردن اطلاعات در مورد یک اتصال

این فراخوانی های سیستم دقیقا مانند فراخوانی هایی از برنامه های کاربر بر سیستم عامل پیاده سازی می شوند. برای مثال فراخوانی های باز کردن و بستن یک اتصالTCP، شبیه فراخوانی های باز کردن و بستن یک فایل درسیستم عامل است . فراخوانی ارسال و دریافت داده، شبیه فراخوانی نوشتن یا خواندن از یک فایل است. فراخوانی های سیستمی پروتکلTCP می توانند با دیگر ماژول هایTCP در هرجایی ازاینترنت محاوره داشته باشند. پارامتر هایی نظیر آدرس های IP، نوع سرویس، تقدم، امنیت، شماره درگاه کاربرد و غیره از طریق فراخوانی های سیستمی TCP مبادله می شود.

یک اتصال TCP توسط فراخوانی OPEN با مشخص کردن شماره درگاه محلی مشخص می شود. خروجی فراخوانی فوق، یک مقدار صحیح بوده که درفراخوانی های بعدی اتصال به کار می رود.TCP دونوع فراخوانی OPEN را تعیین می کند که عبارتند از:OPEN فعال وOPEN غیر فعال . فراخوانی OPEN فعال درسمت شروع کننده اتصال به کار می رود درحالیکه OPEN غیرفعال درسمت گیرنده اجرا می شد. درفراخوانی OPEN فعال، فرستنده با ارسال پیام های درخواست خاص اقدام به برقراری یک اتصال TCP با طرف مقابل می نمایند. فراخوانی OPEN غیرفعال، به این مفهوم است که فرآیند می خواهد به جای این که تلاش به شروع یک اتصال کند، درخواست های اتصال ورودی را بپذیرد.

۹-۱-۳- قالب پیام TCP

شکل(۹-۷) ساختار بسته های TCP را نشان می دهد. مانند اغلب پروتکل های TCP/IP ، سرآیند TCP از قالب کلمه ۳۲ بیتی استفاده می کند. دربسته های TCP فیلدهای زیر موجود است:



شکل(۹-۷): ساختار بسته TCP

۹-۱-۳-۱- فیلد های شماره درگاه مبدا و مقصد

از فیلد های شماره درگاه مبدا و شماره درگاه مقصد برای شناسایی فرآیند های انتهایی دراتصال های مجازی TCP استفاده می شود. بعضی از شماره های درگاه، شماره درگاه های استاندارد بوده که برای برنامه های کاربردی استاندارد مثل سرویس وب، پست الکترونیکی و انقال فایل استفاده می شوند. این شماره درگاه ها بین ۰ تا ۱۰۲۳ می باشند. برخی دیگر از شماره های درگاه ها برای برنامه های کاربردی مختلف به صورت پویا تخصیص داده می شود. شماره درگاه های فوق از۱۰۲۴ به بالا می باشد.

۹-۱-۳-۲- فیلد های شماره رشته و شماره تصدیق

هرسگمنت ارسالی در TCP دارای فیلد خاصی به نام فیلد شماره رشته می باشد. شماره رشته نشان دهنده اولین بایت داده در یک سگمنت TCP ارسالی می باشد. شماره تصدیق نشان دهنده شماره بایتی است که فرستنده این پیام انتظار دریافت آن را از طرف مقابل دارد. از آنجاییکه اتصال های TCP دو طرفه می باشند، بنابراین درآن واحد هر کامپیوتر هم می تواند فرستنده باشد و هم می تواند گیرنده باشد. به عنوان مثال اگر فیلد های شماره رشته و شماره تصدیق به ترتیب برابر با ۱۰۰ و ۲۰۰ باشند، این بدان معنی است که بسته ارسالی فعلی از بایت ۱۰۰به بعد را شامل می شود.همچنین فرستنده تا بایت ۱۹۹ را از طرف مقابل دریافت کرده است و منتظر بایت ۲۰۰ به بعد از طرف گیرنده می باشد. هنگامی که فرستنده TCP اقدام به ارسال یک سگمنت TCP می نماید، یک کپی از آن را دربافر ارسال خود قرار داده و یک زمان سنج خاص را نیز فعال می نماید. درصورتیکه درفاصله فعال بودن زمان سنج، پیام تصدیق دریافت سگمنت ارسالی از طرف گیرنده دریافت شود، زمان سنج متوقف شده و سگمنت فوق نیز از بافر ارسال فرستنده حذف می شود. ولی چنانچه زمان سنج صفر شده و پیام گواهی سگمنت دریافت نشود، دراینصورت سگمنت فوق مجددا ارسال می شود.

درهنگام برقراری اتصال های TCP، پارامتری به نام شماره رشته آغازین (ISN[1]) بین دو طرف اتصال مبادله می شود.ISN نشان دهنده شماره بایت اولین سگمنت ارسالی از هر طرف می باشد. مقدار فیلد ISN درصورتی معتبر است که مقدار پرچم SYN برابر با ۱ باشد.

از فیلد شماره تصدیق برای نشان دادن شماره رشته بایت بعدی که گیرنده انتظار آن را دارد استفاده می شود. تصدیق های TCP جمعی هستند، این بدان معنی است که یک تصدیق مجرد می تواند برای تصدیق تعدادی از سگمنت های پیام قبلی TCP مورد استفاده قرار گیرد. باید توجه نمود که پیام های تصدیق TCP فقط تحویل سگمنت به پروتکل TCP مقابل را تصدیق می کند و تحویل آنها را به برنامه کاربردی لایه بالا تضمین نمی کند.

۹-۱-۳-۳- فیلد آفست داده

فیلد آفست داده، نشان دهنده تعداد کلمات ۳۲ بیتی در سرآیند TCP است. از آنجا که به خاطر وجود فیلد امکانات TCP ، طول سرآیند TCP ثابت نمی باشد، بنابراین به فیلد فوق نیاز است. درصورت عدم وجود فیلد امکانات درسرآیند TCP مقدار فیلد آفست داده برابر با ۵ (۲۰ بایت) می باشد.

۹-۱-۳-۴- فیلد پرچم ها

همانطور که درساختار سگمنت های TCP دیده می شود، درسرآیند TCP از۶ فیلد پرچم تک بیتی استفاده می شود. این پرچم ها به قرار زیر می باشند:

- **بیت ACK:** هنگامی که پرچم ACK ۱ باشد نشان می دهد که فیلد شماره تصدیق معتبر است.

[1] Initial Segment Number

- **بیت SYN:** از پرچم SYN برای نشان دادن باز شدن یک اتصال مدار مجازی استفاده می شود. درهنگام برقراری یک اتصال TCP، ازاین پرچم استفاده می شود.
- **بیت FIN:** از پرچم FIN برای قطع یک اتصال استفاده می شود. درهنگامی که نیاز به برقرارماندن یک اتصال TCP نمی باشد، مقدار پرچم فوق درپیام های ارسالی برابر با ۱ می شود.
- **بیت RST:** چنانچه دریک اتصال TCP خطای غیرقابل ترمیمی رخ دهد، از بیت RST برای درخواست ری ست اتصال فوق استفاده می شود. هنگامی که درسگمنت دریافتی، بیت RST فعال باشد، دراینصورت گیرنده باید فورا اتصال را قطع نماید. دراین صورت هردوطرف اتصال باید منابع اشغال شده را آزاد نمایند.
- **بیت PSH:** هنگامی که پرچمPSH دریک بسته TCP برابر با ۱باشد، گیرنده پیام باید فورا آن را به لایه کاربرد تحویل دهد.
- **بیت URG**: از پرچم URG برای ارسال داده های خارج از باند استفاده می شود.دراین حالت بدون این که انتظار کشیده شود تا گیرنده بایت های قبلی در جریان را پردازش کند، داده ها ارسال می گردند.

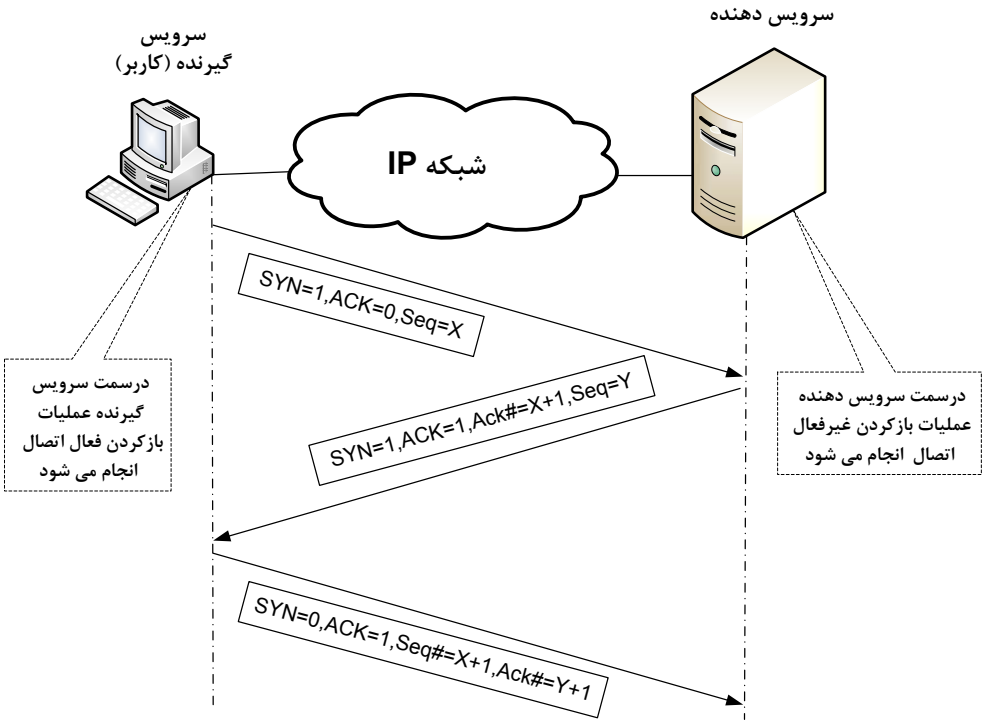
یک اتصال TCP با استفاده از روال handshake سه طرفه برقرار می شود. بدین منظور از پرچم های SYN و ACK به صورت زیر استفاده می شود:

بسته باز کردن اتصال: SYN=1 , ACK=0

بسته تصدیق باز کردن اتصال: SYN=1 , ACK=1

بسته داده یا بسته ACK : SYN=0 , ACK=1

درشکل(۹-۸)، مثالی از روال فوق نشان داده شده است.



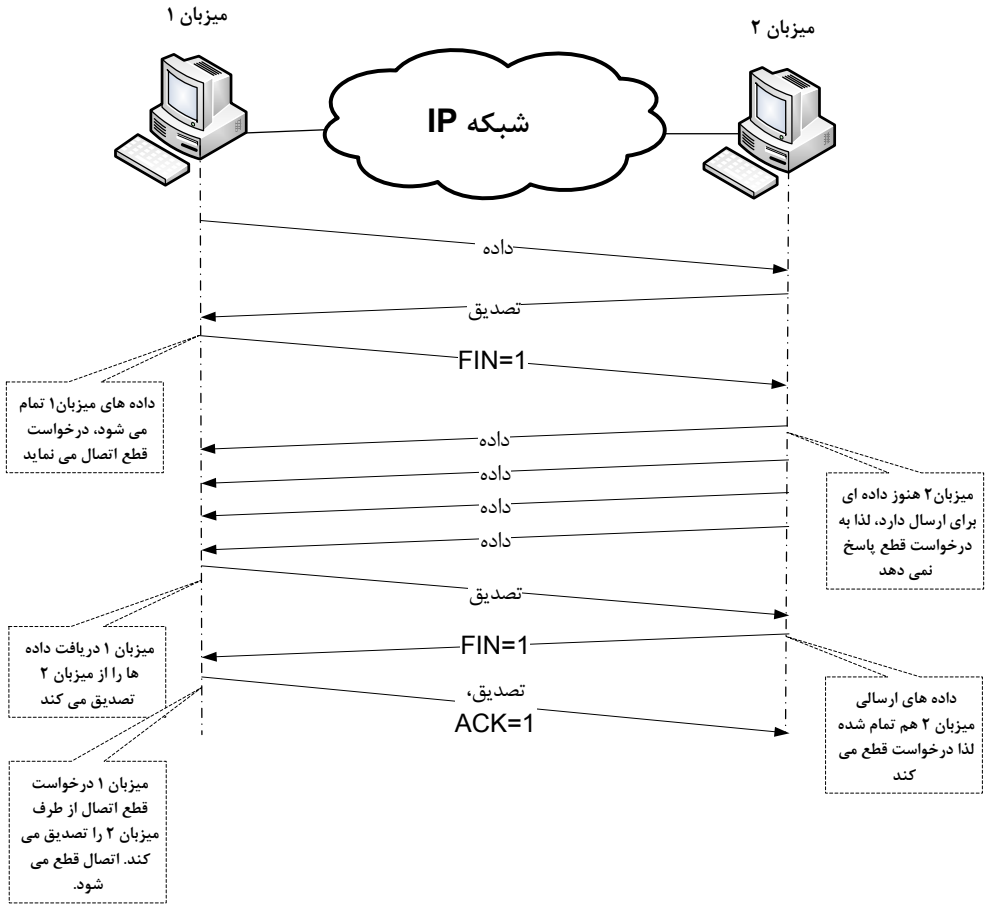
شکل(۹-۸): نحوه استفاده از پرچم SYN برای برقراری یک اتصال TCP

مراحل روال hand shake سه طرفه به طور خلاصه به صورت زیر می باشد:

- مرحله ۱ : مبدا شماره رشته آغازین(ISN) ارسال خود را می فرستد.

- مرحله ۲ : گیرنده دریافت پیام فوق را با ارسال یک شماره تصدیق که ۱ واحد بزرگتر از شماره رشته آغازین مبدا و یا مقدار داده ارسالی مبدا است، تصدیق می کند. دراتصال های دوطرفه،گیرنده نیز شماره رشته آغازین خود را به طرف مقابل می فرستد.
- مرحله ۳ : مبدا یک شماره تصدیق را برای تصدیق دریافت ISN گیرنده می فرستد.

پس از برقراری یک اتصالTCP، پرچم ACK همیشه ۱ است تا نشان دهد که فیلد شماره تصدیق معتبراست. بعداز آن ارسال داده های دوطرف ادامه پیدا کرده تا هنگامی که یک طرف اتصال مایل به قطع اتصال باشد. دراین حالت ازپرچم کنترلی FIN استفاده می شود. در TCP هنگامی که یکی از دوطرف اتصال TCP یک پرچمFIN را ارسال می دارد، اتصال به طور خود کار بسته نمی شود بلکه هر دو طرف اتصال باید یک پرچم FIN را فرستاده و برای بستن اتصال توافق کنند. این نوع بستن یک اتصال TCP، که درآن اطمینان حاصل می شود که اتصال ناگهانی بسته نمی شود بسته شدن مطلوب[1] خوانده می شود.درشکل(۹-۹) مثالی از این نوع بستن یک اتصال TCP نشان داده شده است.



شکل(۹-۹): استفاده از پرچم FIN TCP برای عملیات بسته شدن مطلوب

یکی دیگر از پرچم های مهم در TCP، بیت PSH می باشد. هنگامی که یک برنامه کاربردی از طریق فراخوانی SEND یکسری داده را برای ارسال به پروتکل TCP تحویل می دهد، TCP می تواند که داده ها را دربافر خود نگهداری نماید تا اینکه به اندازه طول یک سگمنت شده و بعد آنها را ارسال دارد. به طور مشابه هنگامی که یک سری سگمنت با بیت PSH غیرفعالدریافت شوند، پروتکلTCP می تواند بدون این که داده ها را به برنامه کاربردی گیرنده پاس دهد، آنها را به طور داخلی دریک بافرقرار دهد. باید توجه نمود که بیت PSH یک نشانگرکورد نبوده و از مرزهای سگمنت مستقل است.

[1] graceful close

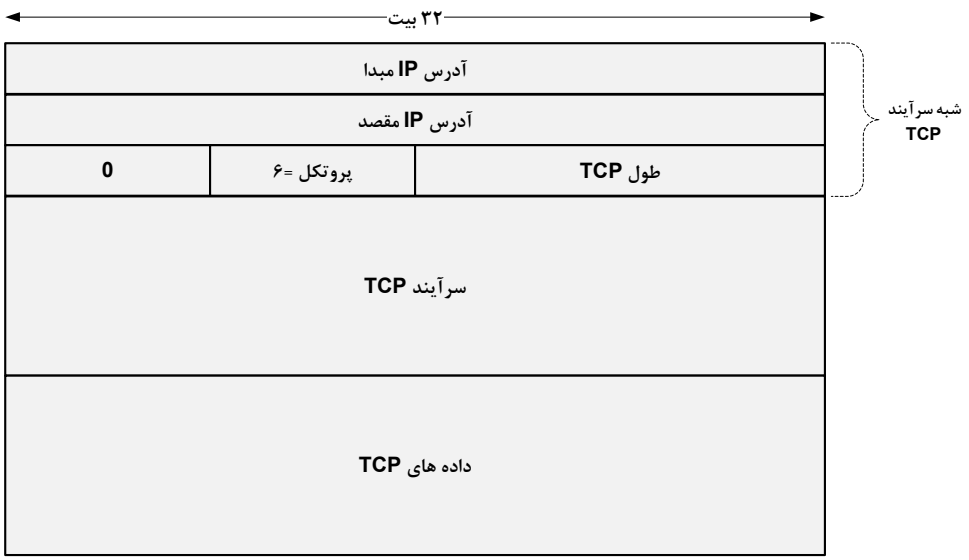
بنابراین بیت فوق هم درطرف فرستنده و هم درطرف گیرنده کاربرد دارد. درسمت فرستنده، نشان دهنده این است که TCP باید کلیه داده های موجود دربافر خود را به هرمیزان که باشند، سریعا درقالب یک سگمنت ارسال دارد. درسمت گیرنده نیز به آن معنی است که گیرنده TCP باید کلیه بافر خود را تخلیه نموده و آنها را به برنامه کاربردی ارسال دارد.
TCP دارای مکانیزمی است که با استفاده از پرچم URG می تواند داده هارا خارج از باند ارسال کند. این ویژگی، فرستنده را قادر می سازد تا سیگنال های وقفه را بدون قرار گرفتن درانتهای صف داده، به گیرنده ارسال نماید. این داده ها ، داده های اورژانسی نامیده می شوند. محل داده های اورژانسی درسگمنت ارسالی، توسط اشاره گرداده های اورژانسی که درسرآیند بسته های TCP قرار دارد، شناسایی می گردد. داده های اورژانسی بدون اینکه منتظر بمانند، سریعا ارسال و دریافت می شوند.

۹-۱-۳-۵- فیلد پنجره

گیرنده از فیلد پنجره برای پیاده سازی کنترل جریان استفاده می کند. مقدار فیلد پنجره نشان دهنده حداکثر تعداد بایت هایی است که گیرنده قادر به دریافت آنها می باشد.

۹-۱-۳-۶- فیلد مجموع مقابله ای

فیلد مجموع مقابله ای برای بررسی خطاهای احتمالی دربسته های TCP به کار می رود. این فیلد به صورت مکمل ۱مجموع مکمل ۱ های همه کلمات ۱۶ بیتی موجود در بسته TCP محاسبه می شود. علاوه برسرآیند TCP از یک شبه سرآیند ۹۶ بیتی که به سرآیند TCP الحاق می شود، نیز برای محاسبه فیلد فوق استفاده می شود. ساختار این شبه سرآیند درشکل (۹-۱۰) نشان داده شده است. از شبه سرآیند برای مشخص کردن رسیدن بسته به مقصد درست استفاده می شود. شبه سرآیند،پروتکل TCP را در برابر سگمنت هایی که به اشتباه مسیریابی شده اند، محافظت می کند. شبه سرآیند شامل فیلدهای شناسه پروتکل (۶ برای TCP) وآدرسIP مبدا و مقصد است.



شکل(۹-۱۰): ساختار شبه سرآیند مورد استفاده در محاسبه مجموع مقابله ایTCP

۹-۱-۳-۷- فیلد امکانات

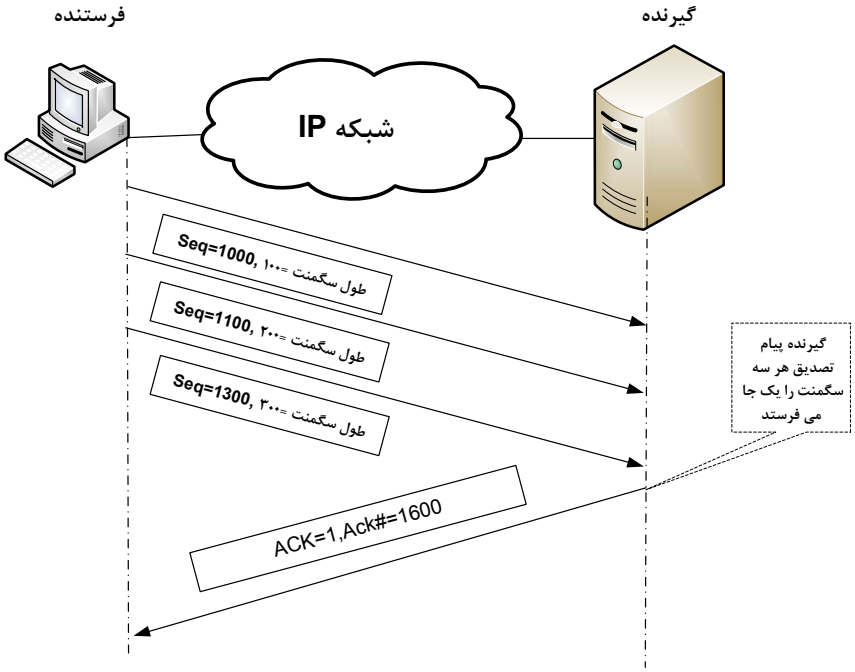
پروتکل TCP، مشابه با پروتکل IP دارای یکسری امکانات اختیاری می باشد. ازاین امکانات TCP برای افزودن قابلیت های اضافی به پروتکل TCP استفاده می شود. طول فیلد امکانات TCP همواره مضربی از بایت می باشد. یکی از مهمترین امکانات TCP، امکان مذاکره حداکثر اندازه سگمنت (MSS[1]) می باشد. از این قابلیت برای مذاکره درمورد طول سگمنت های ارسالی استفاده می شود.

کاربردفیلد padding دربسته های TCP مشابه بسته های IP می باشد.

۹-۱-۴- ACK های جمعی در TCP

دراغلب پروتکل های لایه حمل، شماره رشته به شماره بسته ارسالی اشاره می کند اما درپروتکل TCP این گونه نیست. درپروتکل TCP شماره رشته به شماره بایت ها اشاره می کند. هر بایت درTCP شماره گذاری می شود. TCP بایت ها را در سگمنت هایی با طول های متغیر می فرستد. هنگامی که پیام تصدیقی از طرف مقابل دریافت نشود، سگمنت ها مجددا ارسال می شوند. تضمینی نیست که سگمنت های دوباره ارسال شده دقیقا همان سگمنت ارسالی اصلی باشد. ازآنجاییکه ممکن است برنامه کاربردی فرستنده پس از ارسال سگمنت اصلی، داده های دیگری تولید کرده باشد، بنابراین ممکن است سگمنت ارسال شده، دارای داده های اضافی باشد. با توجه به این مطلب، شماره تصدیق نمی تواند به سگمنت ارسال شده اشاره کند.

درپروتکل TCP، شماره تصدیق، مکانی ازجریان داده ها را که داده به وسیله ماژول TCP گیرنده دریافت وتصدیق شده است را نشان می دهد. به طور دقیق تر، مقدار شماره تصدیق به شماره بایت بعدی که لازم است ارسال شود اشاره می کند. شماره تصدیق به لبه چپ پنجره TCPتعلق دارد. شماره های تصدیق TCP جمعی هستند از این جهت که شماره تصدیق نشان می دهد چه مقدار از جریان داده تا اینجا جمع شده است. البته می توان با استفاده از یک شماره تصدیق منفرد، بایت های دریافت شده در چند سگمنت داده را تصدیق نمود. به عنوان مثال، شکل (۹-۱۱) نشان می دهد که ۳ سگمنت ارسالی توسط فرستنده به وسیله یک شماره تصدیق منفرد تصدیق شده اند.



شکل(۹-۱۱): تصدیق مجرد برای چند سگمنت داده

[1] Maximum Segment Size

تصدیق های جمعی این مزیت را دارند که مجبور نیستیم تصدیق های گمشده را دوباره ارسال کنیم. بنابراین حتی اگر یک پیام تصدیق درهنگام ارسال گم شود، پیام های تصدیق بعدی همه داده ای را که تا کنون دریافت شده است، تصدیق می کنند. با این وجود هنگامی که بستهTCP درضمن ارسال گم می شود، تصدیق های جمعی کارآیی خودرا ازدست می دهند. به عنوان مثال فرض کنید که دریک اتصال TCP سه سگمنت از مبدا به مقصد ارسال می شوند. فرض کنید سگمنت های ۲و۳ به طور موفقیت آمیز دریافت شده اند اما سگمنت ۱ درهنگام ارسال گم شود. با وجود این که سگمنت های۲ و۳ به طور موفق دریافت شده اند ولی فقدان سگمنت۱، یک فاصله را در جریان داده در گیرنده نمایان می کند. ازآنجاییکه فرستنده، پیام تصدیقی درباره سگمنت ۱ دریافت نکرده است بنابراین نمی تواند پنجره خود را جلو ببرد. همچنین مکانیزمی وجود ندارد تا گیرنده به فرستنده بگوید که سگمنت های ۲و۳را به طور موفقیت آمیز دریافت کرده است. دراین حالت دو وضعیت زیر می تواند روی دهد :

۱. مهلت زمانی فرستنده تمام می شود و سگمنت های ۱،۲ و۳ مجددا ارسال می شوند. در این حالت سگمنت های ۲و۳ غیرضروری فرستاده می شوند، چون قبلا به طور سالم به گیرنده رسیده اند. بنابراین ارسال مجدد سگمنت های۲و۳ ضرورتی نداشته و به ترافیک شبکه اضافه می شود.
۲. مهلت زمانی فرستنده تمام می شود و فرستنده فقط سگمنت ۱رامجددا می فرستد. قبل از تصمیم گیری در مورد ارسال سگمنت های دیگر، منتظر برگشت پیام تصدیق می باشد. هنگامی که گیرنده ۱ را دریافت نمود، یک پیام تصدیق جمعی ارسال نموده و طی آن دریافت صحیح سگمنت ۱ و سگمنت های فرستاده شده قبلی یعنی سگمنت ۲ و۳ را به فرستنده اعلام می کند. اگر چه ممکن است این حالت کارآمدتراز حالت قبل به نظر برسد اما باید در نظر داشت که فرستنده قبل از ارسال سگمنت ۲و۳ باید برای تصدیق سگمنت ۱منتظر بماند. این انتظار به این مفهوم است که فرستنده از مزیت اندازه پنجره بزرگ خود استفاده نمی کند و در هر زمان فقط یک سگمنت را می فرستد.

۹-۱-۵- مهلت های زمانی وفقی در TCP

پروتکل TCP درابتدا برای شبکه های گسترده WAN طراحی شده بود ولی بعدها برای شبکه های محلی نیز مورد استفاده قرار گرفت. سگمنت های TCP دردل بسته های IP قرار گرفته و ارسال می شوند. نکته قابل توجه درشبکه هایIP این است که حتی اگر لایه IP یک پیام را ازیک مسیر یکسان در دو زمان مختلف بفرستد، تاخیر زمانی رسیدن به مقصد بنابر عواملی نظیر ترافیک متغیر شبکه و تاخیر صف بندی، متغیر می باشد. از آنجاییکه سگمنت های TCP از طریق پروتکل IP ارسال می شوند، این احتمال وجود دارد که بسته های TCP متوالی در یک اتصال از یک مسیر یکسان فرستاده نشوند و تاخیر های متفاوتی را درشبکه تجربه کنند. هنگامی که TCPپیامی را می فرستد قبل از این که بتواند پنجره خود را جلو ببرد، باید برای پیام تصدیق آن منتظر بماند. سوالی که مطرح است این است که میزان زمان انتظار فوق که که توسط زمان سنج TCP مشخص می شود، چه مقدار بوده وبه چه صورت محاسبه می شود؟ به دلیل مغایرت های زیاد در تاخیر زمانی بین ارسال های متوالی درTCP، TCP از یک تایمر زمانی وفقی استفاده می کند.

۹-۱-۶- کمینه کردن اثر ازدحام در TCP

هنگامی که یک شبکه دچار ازدحام می شود، پیام های تصدیق در بازه زمانی مناسب دریافت نشده و فرستندهTCP با تنظیم مهلت زمانی و ارسال مجدد بسته های گم شده عکس العمل نشان می دهد. با این وجود، ارسال مجدد با افزایش مقدار داده ای که شبکه باید پردازش کند می تواند بر مشکلات ازدحام فعلی اضافه کند. هنگامی که درشبکه ازدحام رخ می دهد، نیاز به روشی می باشد که ارسال داده به شبکه را کم نماید. مسیریابی که ازدحام را تشخیص می دهد، با کمک پیام

های ICMP فرو نشاندن مبدا از فرستنده درخواست می کند که نرخ ارسال خود را کاهش دهد. فرستنده نیز با کاهش پنجره ارسال خود، به پیام دریافتی عکس العمل نشان داده و نرخ ارسال خود را کاهش می دهد. درشبکه های TCP، دو نوع اندازه پنجره تعریف می شوند که عبارتند از پنجره TCP و پنجره ازدحام. پنجره TCP نشان دهنده میزان ظرفیت بافر دریافت درسمت گیرنده می باشد. پنجره ازدحام، وضعیت ازدحام درشبکه را مشخص کرده و نشان دهنده میزان بایتی است که شبکه قادر به دریافت آن می باشد. هنگامی که درشبکه ازدحام رخ دهد، پنجره ازدحام کاهش می یابد. اندازه فعلی پنجره مورد استفاده، همواره مینیمم اندازه پنجره ازدحام و اندازه پنجره گیرنده TCP است.

هنگامی که درشبکه ازدحامی وجود ندارد، میزان فعلی پنجره برابر با اندازه پنجره TCP است، ولی درهنگام وجود ازدحام درشبکه، اندازه فعلی پنجره توسط اندازه پنجره ازدحام تعیین می شود. درحالت ازدحام درشبکه، اگراندازه پنجره ازدحام قبل ازاین که شبکه بتواند به طور کامل از ازدحام خارج شود، خیلی سریع افزایش یابد، این امر می تواند به ترافیک شبکه اضافه کند. اگر ازدحام دوباره مشاهده شود، اندازه پنجره ازدحام سریعا کاهش می یابد. این افزایش و کاهش اندازه پنجره ازدحام سبب می شود که اندازه پنجره ازدحام سریعا نوسان کند. الگوریتم Jacobson با استفاده از تکنیک اجتناب از ازدحام، از افزایش خیلی سریع اندازه پنجره ازدحام جلوگیری می کند. در این تکنیک هنگامی که اندازه پنجره ازدحام کمتر از یک حد آستانه خاص باشد (که معمولا برابر با نصف اندازه پنجره اصلیTCP است)، پنجره ازدحام به صورت نمایی افزایش می یابد. بدین معنی که با ارسال هر سگمنت TCP درصورتی که پیام تصدیق آن درزمان معین دریافت شد، تعداد بسته های ارسالی و درنتیجه پنجره ازدحام دو برابر می شود. هنگامی که پنجره ازدحام به مقدار حد آستانه رسید، از آن به بعد مقدار پنجره ازدحام به صورت خطی افزایش می یابد.

۹-۱-۷- رسیدگی به اتصالات TCP از کار افتاده

هنگامی که کامپیوتر میزبان گیرنده از کار بیافتد و یا اتصال فیزیکی کامپیوتر میزبان به شبکه قطع گردد، کلیه اتصال های TCP عبوری از آن کامپیوتراز کار می افتند. شبکه باید به مکانیزمی برای تشخیص اتصال های قطع شده TCP باشد، تا قادر به رهاسازی منابع خود باشد. یکی از روش های قطع اتصال های TCP، استفاده از پیام های ICMP است. هنگامی که یک پیام TCP مبنی بر دردسترس نبودن مقصد به فرستنده برسد، فرستنده اقدام به قطع اتصال TCP نموده و منابع خود را آزاد می نماید. درصورتیکه بسته های ICMP فوق، درشبکه گم شوند، نمی توان اتصال های TCP را به کمک آنها قطع نمود. هنگامی که هیچ یک از نقاط پایانی برای مدت زمانی طولانی داده ای نفرستند، اتصال درحالت بیکار نگهداری می شود. در وضعیت بیکار، اتصال همچنان منابع را مصرف می کند حتی اگر شبکه یا یکی از نقاط پایانی دیگر از کار افتاده باشند. برای رفع مشکل فوق، بعضی از پیاده سازی های TCP یک پیام Keep Alive را می فرستند که به طور متناوب زنده بودن اتصال را بررسی می کند. هنگامی که پیام فوق فرستاده می شود، فرستنده انتظار دریافت پیام تصدیق از گیرنده را دارد. پیش فرض پیشنهادی برای زمان سنج زنده نگهداری فوق۲ ساعت است. البته در بعضی از پیاده سازی های TCP پیش فرض خیلی کوچکتر است (برای مثال ۱۵-۱۰ دقیقه). زمان سنج زنده نگهداری باید طوری تعیین شود که برای اکثریت کاربردهای در حال اجرای در میزبان TCP با معنی باشد. درصورت صفر شدن زمان سنج فوق، اتصال TCP قطع شده و منابع آن آزاد می شود.

۹-۲- پروتکل بسته کاربر (UDP)

برخی از برنامه های کاربردی اینترنت نیاز به همه توانایی های TCP نداشته و فقط به یک پروتکل حمل ساده که بتواند برنامه های کاربردی را در کامپیوتر ها شناسایی کند و یک بررسی خطای ساده مهیا سازد، نیاز دارند. پروتکل UDP این قابلیت ها را فراهم می سازد. بر خلاف TCP که اتصال گراست، پروتکلUDP بدون اتصال می باشد و تلاشی برای ایجاد یک اتصال نمی کند. داده با بسته بندی در سرآیند UDP و پاس دادن آن به لایه IP ارسال می شوند. لایه IP، بسته

UDP را در یک بسته IP قرار داده و ارسال می کند. پروتکلUDP تلاشی برای فراهم کردن ترتیب دهی داده ها نمی کند. بنابراین ممکن است داده با ترتیبی متفاوت از آنچه ارسال شده است، به مقصد برسد. برنامه های کاربردی که نیاز به سرویس های ترتیب دهی دارند، یا باید مکانیزم ترتیب دهی خودشان را به عنوان قسمتی از برنامه کاربردی پیاده سازی کنند و یا باید از TCP به جای UDP استفاده کنند. پروتکل UDP در کاربردهایی که دستور/ پاسخ گرا هستند و دستورها و پاسخ ها می توانند در یک بسته مجرد ارسال شوند مفید است. سرباری در باز کردن وبستن یک اتصال وجود ندارد، فقط مقدار کمی داده فرستاده می شود. مزیت دیگر UDP برای کاربرد هایی است که نیاز به همه پخشی/ چند پخشی دارند. به عنوان مثال در TCP اگر یک بسته همه پخشی باید به ۱۰۰۰ ایستگاه فرستاده شود، فرستنده TCP باید ۱۰۰۰ اتصال را باز کرده وداده را به هر اتصال بفرستد و سپس ۱۰۰۰ اتصال را ببندد. سربار باز کردن این اتصالات، نگهداری آنها (بهره گیری از منابع) و سپس بسته آنها بسیار بالاست. اما چنانچه ازپروتکل UDP استفاده شود، فرستنده می تواند داده را به ماژول IP با درخواست توزیع همه پخشی / چند پخشی بفرستد. پروتکلUDP یک شکل ساده اختیاری کنترل خطا را برای تمام داده ها فراهم نموده است. اگر شبکه زیرین مطمئن باشد، عملاً نیازی به مکانیزم بررسی خطای UDP نبوده و مکانیزم فوق غیر فعال می شود. بدین ترتیب سرعت پردازش UDP بالا خواهد رفت.

ویژگی های UDP به شرح زیر خلاصه شده است :

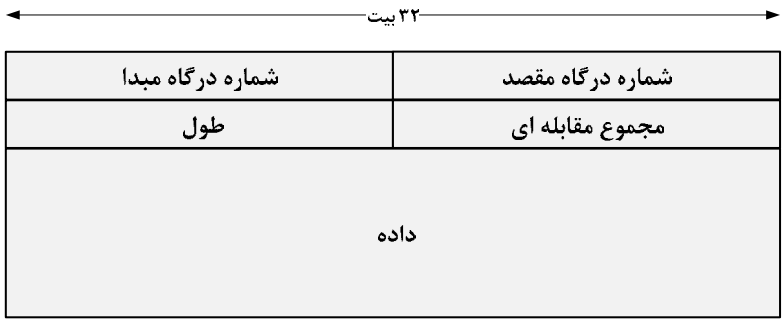
- UDP فرآیند های کاربردی را با استفاده از شماره های درگاه UDP شناسایی می نماید.
- UDP بسته گراست و برخلاف TCP، سرباری برای باز کردن، نگهداری و بستن یک اتصال ندارد.
- UDP برای کاربردهای همه پخشی/ چند پخشی کارآمد است.
- درUDP ترتیب دهی داده وجود ندارد و نمی تواند تحویل داده را به درستی ضمانت کرد.
- UDP از بررسی خطای اختیاری تنها برای داده استفاده می کند.
- UDP از TCP سریع تر، ساده تر و کارامدتر است، هر چندکه قدرت آن از TCP کم تر است .

UDP سرویس های تحویل نامطمئن و بدون اتصال را در بالای IP مهیا می سازد. UDP به عنوان پروتکل لایه حمل در نظر گرفته می شود. البته با توجه به بدون اتصال و بدون گارانتی بودن UDP نمی توان به عنوان یک پروتکل لایه حمل به آن اطمینان کرد. ازآنجاییکه وظیفه اصلی یک پروتکل لایه حمل، تهیه بی عیب داده انتها به انتها است، نمی توان از UDP به طور مطمئن برای این کار استفاده نمود. ولی علیرغم این مشکل بزرگUDP، تنها به خاطر سادگی و بالاسری کم آن، تعداد زیادی از برنامه های کاربردی شبکه برمبنای UDP طراحی شده اند. برخی از این کاربرد ها عبارتند از: TFTP[1] ,DNS[2],NFS[3], SNMP[4] و RIP[5] . همچنین خیلی از سرویس های همه پخشی از پروتکل UDP استفاده می نمایند.

۹-۲-۱- قالب سرآیند UDP

سرآیند UDP یک طول ثابت ۸ بایتی دارد. در شکل (۹-۱۲) قالب بسته های UDP نشان داده شده است .

[1] Trivial File Transfer Protocol
[2] Domain Name System
[3] Network File System
[4] Simple Network Management Protocol
[5] Routing Information Protocol



شکل(۹-۱۲): قالب بسته های UDP

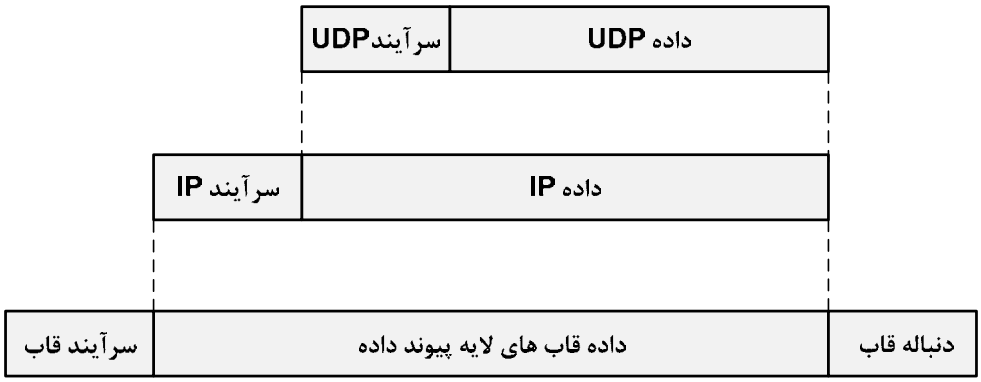
درگاه مبدا فیلدی ۱۶ بیتی است. این فیلد اختیاری است ونشان دهنده شماره درگاه فرآیند کاربردی مبدا می باشد. چنانچه از این فیلد استفاده نشود، دراین صورت مقدار آن همواره صفر می باشد. فیلد درگاه مقصد، فرآیندکاربردی مقصد را مشخص می کند. این فرآیند باید داده UDP ارسالی را دریافت نماید. همانند TCP، پروتکل UDP نیز عملیات غیرتسهیم سازی داده به فرآیند مقصد را با استفاده از مقادیر شماره درگاه انجام می دهد. اگر UDP بسته ای را با شماره درگاهی نامعتبر دریافت کند (برنامه کاربردی UDP همراه با شماره درگاه وجود ندارد)، یک پیام خطای ICMP ازنوع دردسترس نبودن درگاه مقصدتولید می کند و بسته را نمی پذیرد. فیلد طول، طول این بسته UDP برحسب بایت است. این طول شامل سرآیند UDP و داده آن می باشد. کمترین مقدار این فیلد ۸ است. دراین صورت داده ای دربسته وجود نداشته و فیلد داده با اندازه صفر را نشان می دهد.

فیلد مجموع مقابله ای، مکمل۱، مجموع مکمل۱ های فیلدهای ۱۶ بیتی موجود درشبه سرآیند و خود سرآیند UDP است. روال بررسی خطا درUDP همانند روال استفاده شده درTCP است. شبه سرآیندی که به طور مفهومی به سرآیند UDP اضافه شده است، شامل آدرس مبدا، آدرس مقصد، پروتکل (شماره پروتکل ۱۷ است) و طول UDP است . ساختار شبه سرآیند درشکل(۹-۱۳) نشان داده شده است.

شکل(۹-۱۳): شبه سرآیند UDP استفاده شده در محاسبه فیلد مجموع مقابله ای

پروتکل UDP بالای IP اجرا می شود. بررسی خطایIP فقط برروی سرآیند آن انجام می شود در صورتی که بررسی خطای UDP علاوه برسرآیند، برروی داده نیز انجام می گردد. بررسی خطای UDP برای ضمانت صحت فیلد داده لازم است.

برنامه های کاربردی که بالایUDP اجرا می شوند، دارای یک شماره درگاه UDP هستند. شماره درگاه UDP در یک فضای آدرس متفاوت با فضای آدرس شماره درگاه TCP است. بنابراین امکان داشتن شماره درگاه TCP ۱۰۱۷و شماره درگاه UDP ۱۰۱۷ برای اشاره به فرآیند های کاربردی جداگانه وجود دارد. درشکل (۹-۱۴) فرآیند بسته سازی UDP نشان داده شده است.



شکل(۹-۱۴): بسته بندی UDP

پرسش های فصل

۱. نحوه مشخص کردن برنامه های کاربردی لایه بالا درمعماری TCP/IP به چه صورت می باشد؟
۲. نحوه تخصیص شماره درگاه را درپروتکل TCP و UDP را نوشته و با یکدیگر مقایسه نمایید.
۳. ویژگی های اصلی TCP را نوشته و به اختصار توضیح دهید.
۴. نحوه تامین اطمینان درارسال سگمنتهای TCP را با رسم شکل مناسب توضیح دهید.
۵. دلیل استفاده از روال های کنترل جریان را درپروتکل های لایه حمل توضیح داده و سپس عملیات کنترل تراکم درTCP را تشریح نمایید.
۶. دلیل نامگذاری روش پنجره لغزان TCP را توضیح دهید.
۷. ساختار سگمنت های TCP را رسم نمایید.
۸. کاربرد فیلدهای شماره رشته ارسال و شماره تصدیق را با ذکر یک مثال توضیح دهید.
۹. حداقل و حداکثر طول سگمنت های TCP به چه صورت تعیین می شود؟
۱۰. مفهوم تسهیم سازی و غیرتسهیم سازی را درTCP توضیح داده و نحوه اجرای آن را بنویسید.
۱۱. کاربرد هریک از پرچم های TCP را با ذکر یک مثال توضیح دهید.
۱۲. فرض کنید که دریک اتصال TCP، فرستنده از طرف گیرنده پیامی با مقدار بیت ACK برابر با یک و شماره تصدیق ۲۰۰ دریافت می نماید. اندازه پنجره ارسال فرستنده ۳۰۰۰ بایت است. با رسم شکل، اندازه پنجره جدید و لبه بالا و پایین آن را بدست آورید.
۱۳. با ذکر یک مثال ، مفهوم نقاط پایانی را دراتصال های TCP توضیح دهید.
۱۴. مفهوم OPEN فعال و غیرفعال را توضیح دهید.
۱۵. مفهوم داده های اورژانسی درTCP را نوشته و نحوه سرویس دهی به آنها را توضیح دهید.
۱۶. بارسم شکل مناسب عملیات hand shake سه طرفه را توضیح دهید.
۱۷. نحوه تعیین شماره رشته آغازین دریک اتصال TCP به چه صورت می باشد؟
۱۸. مهوم بستن مطلوب یک اتصال TCP را با رسم شکل مناسب توضیح دهید.
۱۹. دلیل استفاده از تصدیق های جمعی درTCP را با ذکر مثال توضیح دهید. مشکلات تصدیق جمعی را نیز بنویسید.
۲۰. نحوه تعیین مهلت های زمانی وفقی دریک اتصال TCP به چه صورت می باشد؟
۲۱. مفهوم ازدحام درشبکه را توضیح داده و عملکرد TCP را درقبال مواجه با آن بنویسید.
۲۲. پدیده سندروم پنجره ابله (SWS) را با ذکر یک مثال توضیح دهید. به نظر شما به چه صورت می توان از این پدیده اجتناب کرد؟

۲۳. چنانچه یک اتصال TCP برای مدت زیادی برقرار بوده و ازآن استفاده نشود، منابع شبکه به صورت مطلوب استفاده نمی شوند. چگونه می توان مشکل فوق را حل نمود؟

۲۴. دلیل استفاده از UDP را نوشته و با TCP مقایسه نمایید.

۲۵. ساختار بسته های UDP را با رسم شکل توضیح دهید.

۲۶. برنامه های کاربردی که ازUDP استفاده می کنند را نام ببرید.

۲۷. به نظر شما درچه مواقعی بهتر است که از UDP استفاده کرد و درچه مواقعی از TCP؟