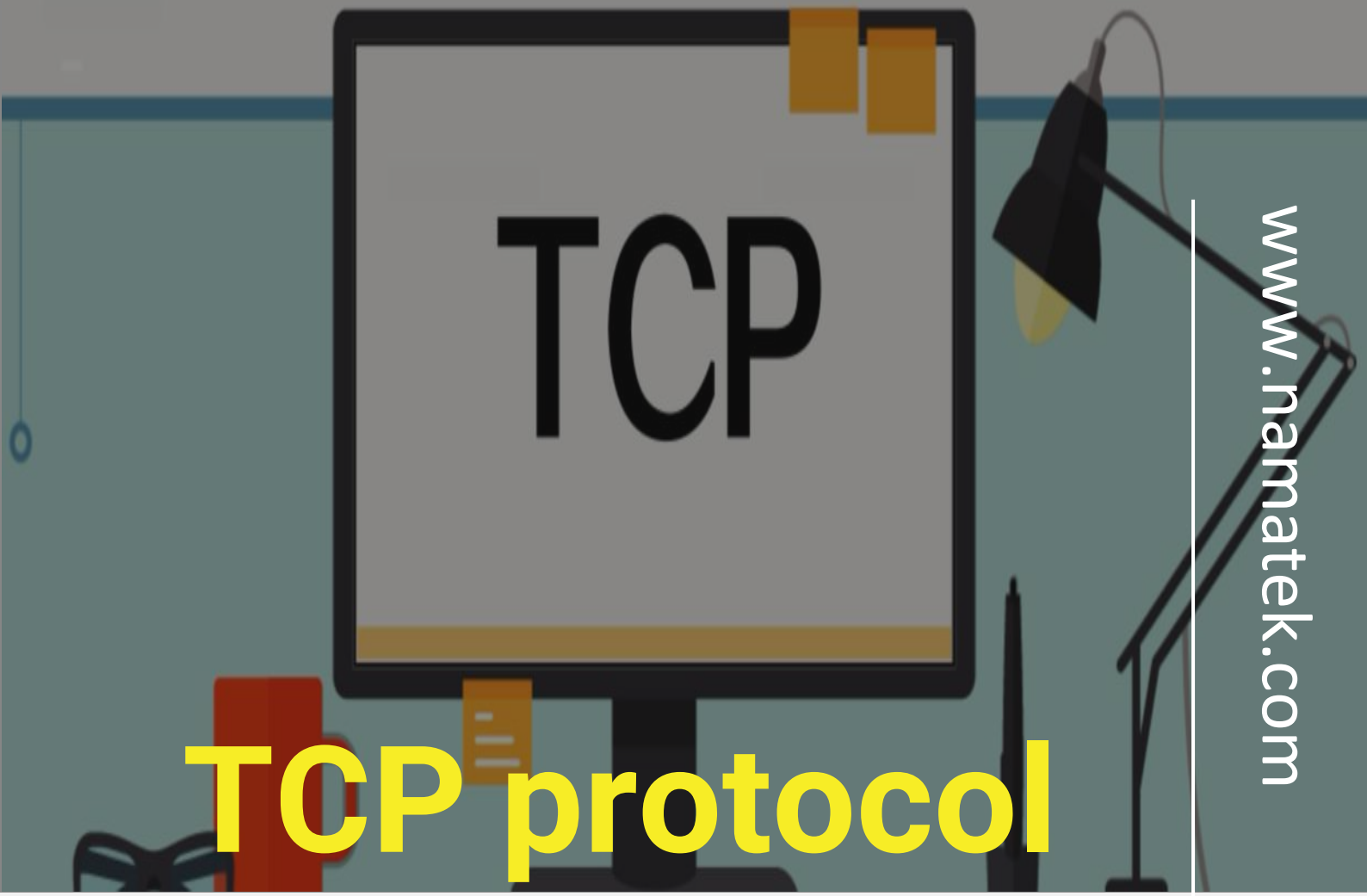
Namatek
True Education



www.namatek.com

TCP protocol

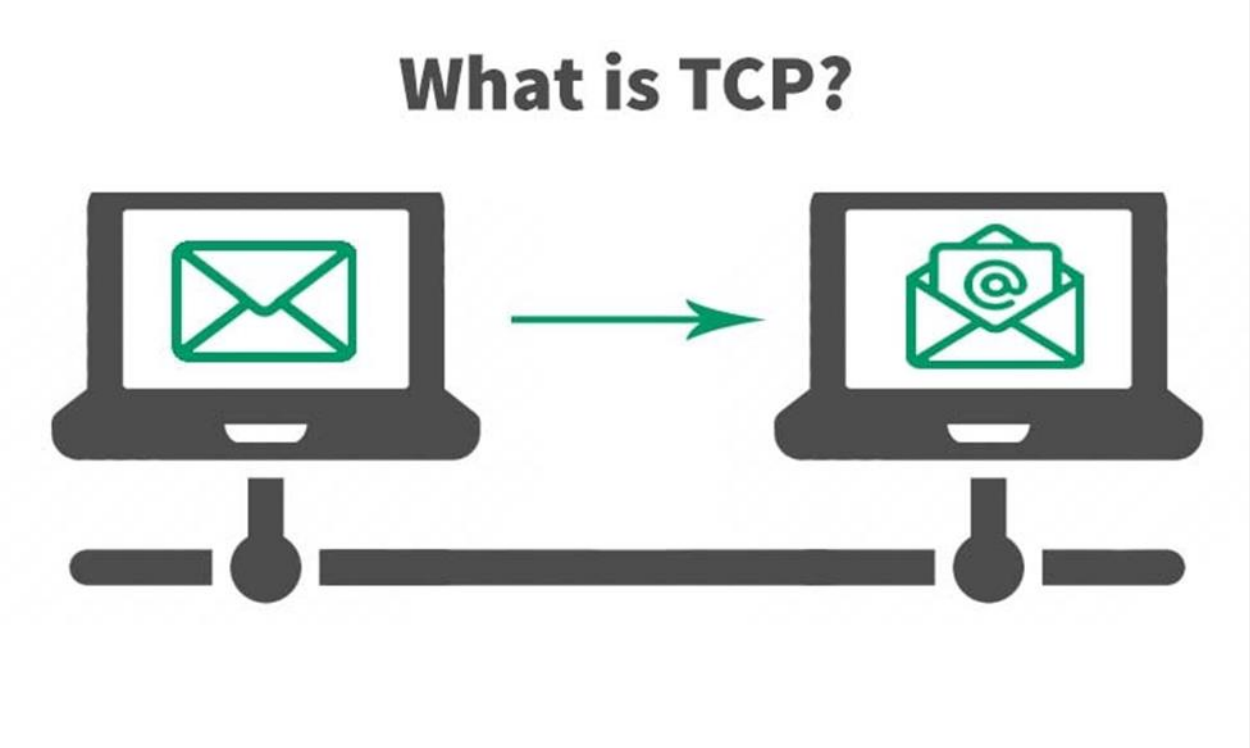
پروتکل TCP چیست؟

فهرست مطالب

حتما شما هم به عنوان یک کاربر فضای وب شنیده اید که پروتکل TCP یکی از مهم ترین پروتکل ها در اینترنت است. بدون TCP، ارسال و دریافت داده ها به صورت کامل و صحیح دچار مشکل خواهد شد. به عنوان مثال ممکن است در ارسال یک سند مهم نیمی از متن به دست گیرنده نرسد و یا دچار خطاهای متعدد باشد. بنابراین می توان گفت که بدون پروتکل TCP، محیط اینترنت برای تبادل اطلاعات ناکارآمد خواهد بود. به همین جهت در این مقاله مواردی نظیر نحوه کار، پروتکل های وابسته و جایگزین، آسیب پذیری ها و سایر ویژگی های مهم آن را مورد بررسی قرار خواهیم داد. با ما همراه باشید.

#۱ پروتکل TCP چیست؟ (TCP protocol)

پروتکل TCP یا کنترل انتقال مخفف Transmission Control Protocol یک استاندارد ارتباطی است که برنامه های کاربردی و دستگاه های محاسباتی را قادر به تبادل پیام از طریق شبکه می کند.

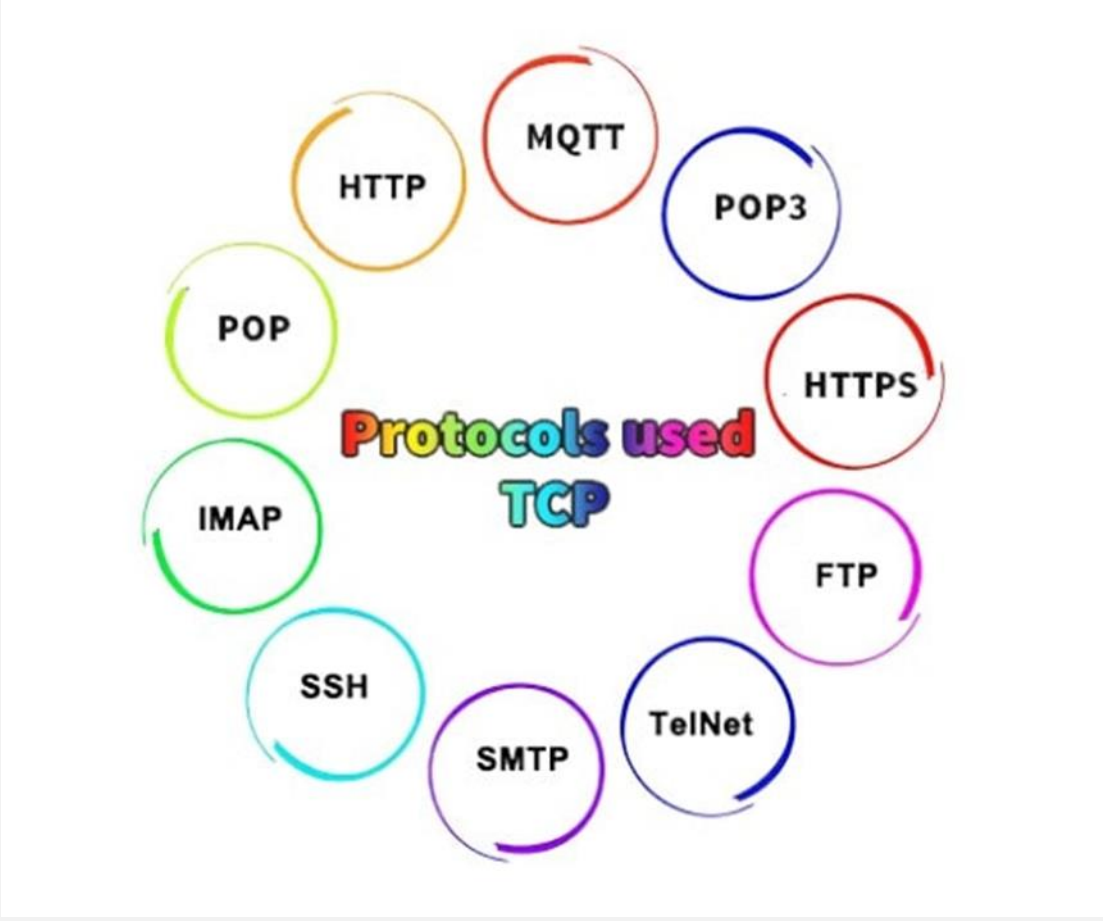


این پروتکل جهت ارسال بسته ها از طریق اینترنت و اطمینان از تحویل موفقیت آمیز آن ها از طریق شبکه طراحی شده است. TCP یکی از استانداردهای اساسی است که قوانین اینترنت را تعریف می کند و در استانداردهای تعریف شده توسط کارگروه مهندسی اینترنت یا IETF مخفف Internet Engineering Task Force گنجانده شده است.

پروتکل کنترل انتقال یا همان TCP در واقع، یکی از پروتکل های متداول در ارتباطات شبکه دیجیتال است و انتقال داده ها را به انجام می رساند. به این صورت که داده ها را سازماندهی می کند تا بتواند بین سرور و سرویس گیرنده منتقل شود. این پروتکل یکپارچگی داده های منتقل شده از طریق شبکه را تضمین می کند. TCP قبل از انتقال داده، ارتباطی بین یک منبع و مقصد برقرار کرده و از برقرار ماندن آن تا زمان ارسال داده اطمینان حاصل می کند.

#۲ پروتکل هایی که از TCP استفاده می کنند

پروتکل TCP حجم زیاد داده ها را به صورتی که ترتیب آن ها ثبت شود، به بسته های کوچکتر تقسیم می کند. به همین جهت، برای انتقال درست و بدون مشکل این بسته ها، از سایر پروتکل های سطح بالا استفاده می کند.



برخی از این پروتکل ها شامل موارد ذیل هستند:

- پروتکل های اشتراک نظیر به نظیر مانند:

- File Transfer Protocol (FTP)
- Secure Shell (SSH)
- Telnet

- پروتکل های ارسال و دریافت ایمیل مانند:

- پروتکل دسترسی به پیام اینترنت (IMAP)
- پروتکل پست الکترونیکی (POP)
- پروتکل انتقال ایمیل ساده (SMTP)

- پروتکل های دسترسی وب مانند:

- انتقال متن متن (HTTP)

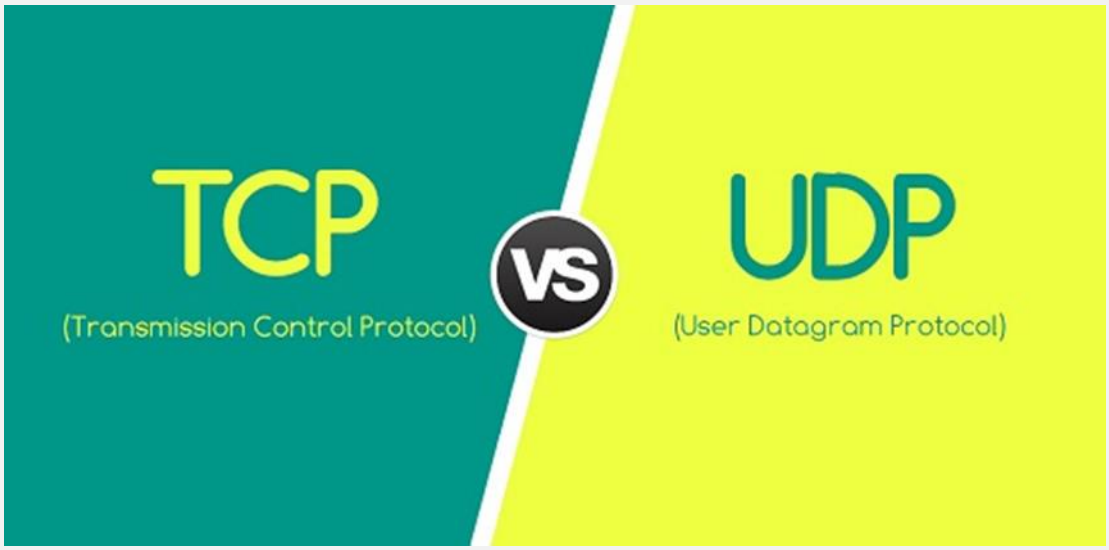
#۳ پروتکل جایگزین برای پروتکل TCP

یک گزینه جایگزین برای پروتکل TCP، پروتکل UDP یا User Datagram Protocol است که برای برقراری ارتباط با تاخیر کم بین برنامه ها و سرعت بخشیدن به انتقال داده استفاده می شود.

TCP یک ابزار گران قیمت در شبکه است؛ زیرا شامل بسته های فاقد خطا و خرابی است. چرا که با کنترل های مختلفی از انتقال داده محافظت می کند که عبارتند از:

- تاییدیه ها

- راه اندازی اتصال
- کنترل جریان



در مقابل، UDP اتصال صحیح، کنترل خطا یا رعایت توالی بسته را فراهم نمی کند؛ اما هزینه کمتری دارد. برای درک ساده تر این دو پروتکل می توان TCP را به دانلود یک فایل از طریق برنامه دانلود منیجر و UDP را به تماس تصویری تشبیه کرد. به این صورت که در دانلود فایل توسط برنامه دانلود، بسته ها با ترتیب درست و بدون خرابی دانلود شده و در کنار هم قرار می گیرند.

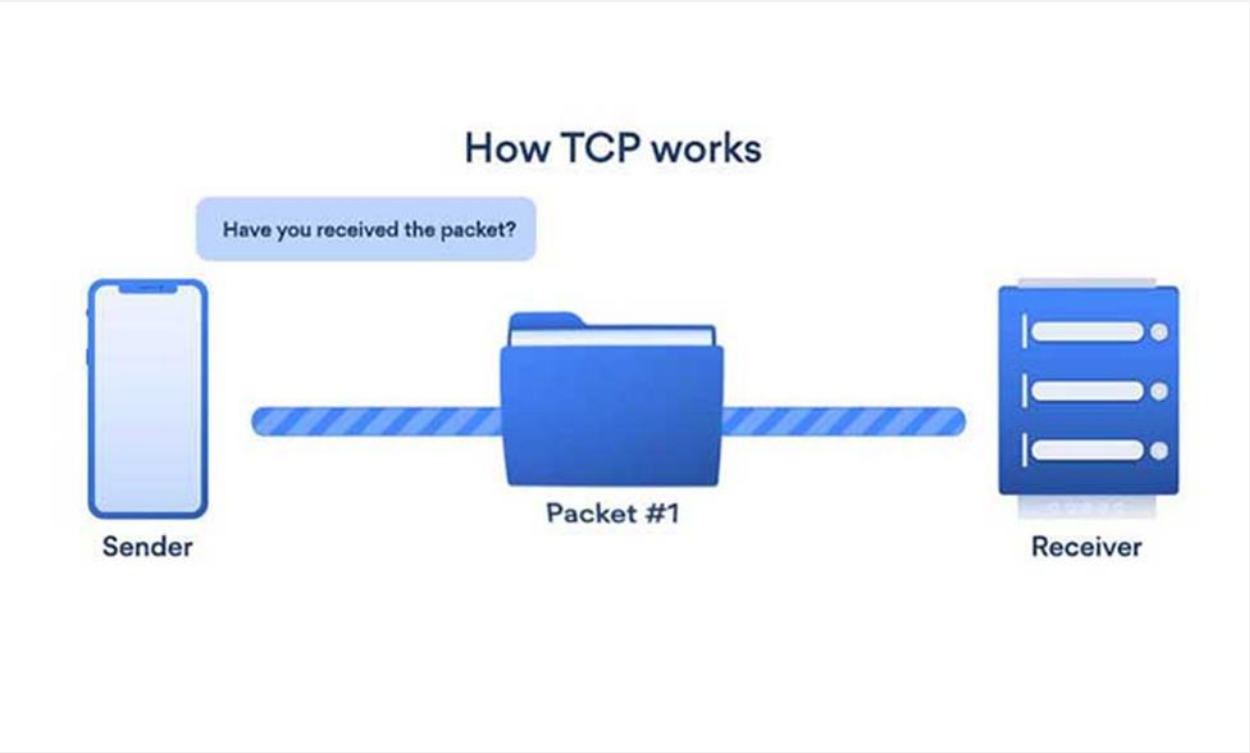
هر بسته خراب یا دارای خطا می بایست حذف شده و مجددا ارسال شود. در غیر این صورت فایل کلی غیر قابل استفاده خواهد بود. در این حالت پروتکل TCP تضمین می کند که همه داده ها به طور صحیح و بدون مشکل دانلود و در اختیار کاربر قرار بگیرد؛ اما در پروتکل جایگزین آن، یعنی UDP این اتفاق نمی افتد. همان طور که اگر در تماس تصویری برای چند ثانیه اینترنت قطع یا کند شود و بسته ها به مقصد نرسند، امکان

ارسال دوباره وجود ندارد و ادامه بسته ها پس از رفع مشکل دریافت می شوند. یا ممکن است بسته های خراب به مقصد برسند که قابل فهم نیستند. بنابراین پروتکل UDP برای موقعیت های حساس به زمان، مانند جستجوی سیستم نام دامنه (DNS)، پروتکل انتقال صدا از طریق اینترنت (VoIP) و رسانه هایی نظیر تلویزیون و ماهواره، گزینه خوبی است.

#۴ TCP چگونه کار می کند؟

TCP به عنوان واسطه بین دو برنامه ای که نیاز به تبادل داده دارند، عمل می کند. هنگامی که یک برنامه می خواهد داده را انتقال دهد، TCP اطمینان می دهد که:

- داده ها به ترتیب می رسند.
- داده ها حداقل خطا را دارند.
- داده های تکراری حذف می شوند.
- بسته های گمشده یا حذف شده دوباره ارسال می شوند.



پروتکل TCP در واقع یک نوع پیک برای اینترنت است. به عبارت ساده TCP پس از برقراری ارتباط و تعریف تعامل، داده ها را بسته بندی کرده، آن ها را روی کامیون های جداگانه بارگیری کرده و از طریق بزرگراه IP به مقصد می فرستد. در جاده، ترافیک (ازدحام شبکه)، مسیرهای انحرافی (توازن بار ترافیک) و تصادفات رانندگی (خطاهای شبکه) می تواند باعث شود که داده ها از رده خارج شوند یا از رسیدن به موقع آن ها جلوگیری شود.

در مرحله بعد با ورود بسته های داده، گیرنده تاییدیه آن ها را امضا می کند. به عنوان مثال من بسته ٤ را دریافت کردم. اگر فرستنده این تایید را در مدت زمان مشخصی دریافت نکند، داده را مجددا ارسال می کند تا تمام داده ها ارسال و تاییدیه رسیدن آن ها به مقصد دریافت شود. پس

از رسیدن همه داده ها، TCP اتصال را قطع می کند. کل این روند در سه مرحله مشخص اتفاق می افتد.

- ایجاد اتصال
- انتقال داده
- قطع اتصال

نام این مراحل به خودی خود اتفاقات درون خود را توضیح می دهند؛ اما در هر مرحله از روند اتفاقات خیلی بیشتری می افتد. به عنوان مثال در مرحله انتقال داده، TCP داده های منتقل شده را می پذیرد، آن ها را به بسته های مرتب تقسیم می کند. همچنین یک هدر (header) (توضیحات و کدهای مورد نیاز) اضافه می کند و با استفاده از پروتکل اینترنت به گیرنده ارسال می کند.

#۵ دلیل استفاده از پروتکل TCP

پروتکل کنترل انتقال یا TCP یکی از مولفه های اساسی استفاده روزمره از اینترنت است. هنگام مرور وب و بازدید از یک صفحه وب، وب سرور با استفاده از پروتکل HTTP اطلاعات وب سایت را به دستگاه شما ارسال می کند.

HTTP برای اتصال سرور به رایانه شما و اطمینان از این که فایل به درستی به سیستم شما منتقل می شود به پروتکل TCP متکی است. به این معنا که پروتکل های سطح بالای دیگر به TCP وابسته هستند.

به عنوان مثال:

- پروتکل SMTP که جهت ارسال و دریافت ایمیل استفاده می شود.
- پروتکل FTP که برای به اشتراک گذاری فایل ها استفاده می شود.
- MQTT که جز اصلی مولفه های اینترنت اشیا است.

هر زمان دقت از سرعت انتقال مهم تر باشد، شبکه ها احتمالا برای حفظ اتصالات و انتقال قابل اعتماد داده ها به TCP نیاز خواهند داشت.

#۶ آسیب پذیری های TCP

پروتکل کنترل انتقال از آدرس های پروتکل اینترنت برای ایجاد ارتباط بین کلاینت ها و سرورها استفاده می کند.

در نتیجه، این آسیب پذیری ذاتی را دارد که چالش های امنیت سایبری را ایجاد کند که دو مورد از مهم ترین آن ها عبارتند از:

۱. حمله DoS یا Denial of Service

پروتکل TCP منابع شبکه را برای حفظ ارتباطات مصرف می کند. نرم افزارهای مخرب می توانند با استفاده از جعل IP و درخواست های نامعتبر برای هرزنامه استفاده کنند که TCP سعی در پیگیری آن ها دارد. با افزایش حجم درخواست ها، TCP می تواند بیش از حد منابع سرور را مصرف کرده و باعث خرابی آن شود. به این حمله Denial of Serviceیا محروم سازی از سرویس گفته می شود.

۲. حمله Connection hijacking

اگر ارتباط بین برنامه ها ایمن نباشد، یک هکر می تواند انتقال داده را شنود کند. از آن جا که هدرهای TCP (header)، اندازه هر بسته داده و بخش TCP را مشخص می کنند، یک هکر می تواند قسمت ها و بسته های جعلی با همان اندازه ایجاد کند و گیرنده را فریب دهد تا آن ها را بپذیرد. علاوه بر این هکر ها می توانند اتصال بین گیرنده و فرستنده را در اختیار بگیرند که بسیار خطرناک است؛ زیرا از این طریق هکر ها می توانند تمام داده های مخرب خود را به مقصد ارسال و یا داده ها را جهت شنود یا دستکاری دریافت کنند. به این حمله Connection hijacking یا سرقت اتصال گفته می شود.