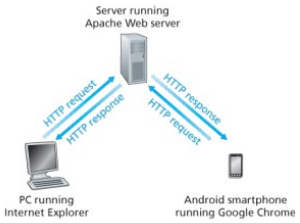
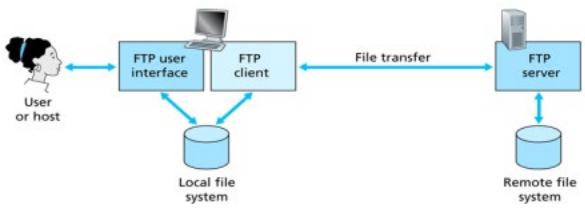
-۱

HTTP: HTTP مخفف Hypertext Transfer Protocol است. این پروتکلی است که برای ارتباط بین کلاینت (معمولا یک مرورگر وب) و سرور از طریق اینترنت استفاده می شود. هنگامی که یک آدرس وب (URL) را در مرورگر خود وارد می کنید، درخواستی را به وب سرور میزبان وب سایت ارسال می کند. این پیام درخواست حاوی نوع درخواست HTTP، URL و سایر داده ها مانند هدرها است .هنگامی که سرور درخواست را دریافت می کند، آن را پردازش می کند و پاسخی را که معمولاً حاوی صفحه وب درخواستی و سایر داده ها مانند سرصفحه ها، کدهای وضعیت و کوکی ها است، ارسال می کند.HTTP از یک مدل request-response استفاده می کند که در آن کلاینت درخواستی را ارسال می کند و سرور پاسخی را ارسال می کند. HTTP stateless است، به این معنی که هر درخواست ارسال شده توسط کلاینت به عنوان یک تراکنش جداگانه و مستقل، بدون اطلاع از درخواست های قبلی یا تعاملات بین کلاینت و سرور، تلقی می شود.HTTP همچنین مبتنی بر متن است، به این معنی که پیام های درخواست و پاسخ از متن تشکیل شده است که می تواند به راحتی توسط رایانه ها و انسان ها تفسیر شود. متن به روشی خاص با استفاده از هدرها و برچسب ها قالب بندی می شود که امکان ارتباط موثر و موثر بین کلاینت و



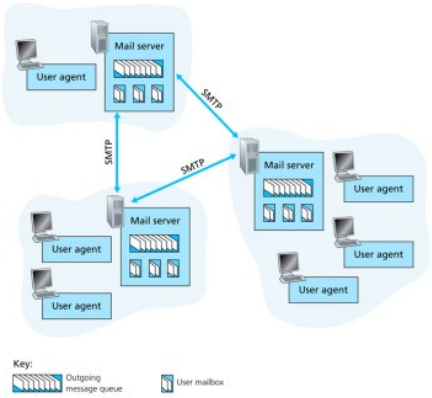
سرور را فراهم می کند. به طور کلی، HTTP پروتکل اساسی وب جهانی است که امکان انتقال اطلاعات و ارتباط بین سرورها و کلاینت ها را در سراسر جهان فراهم می کند.

FTP: FTP مخفف File Transfer Protocol است. این یک پروتکل شبکه استاندارد است که برای انتقال فایل ها بین سرورها و کلاینت ها از طریق اینترنت یا سایر اتصالات شبکه استفاده می شود.FTP روشی ساده و کارآمد برای انتقال فایل‌های بزرگ، به‌روزرسانی‌های نرم‌افزار و سایر مجموعه‌های داده بین دو ماشین در مکان‌های مختلف ارائه می‌کند. اغلب توسط توسعه دهندگان وب، شرکت های نرم افزاری و سایر مشاغل برای انتقال فایل ها و مجموعه داده ها بین رایانه مشتری و سرور راه دور استفاده می شود.FTP با ایجاد یک اتصال کلاینت-سرور کار می کند، جایی که مشتری درخواست های انتقال فایل را به سرور ارسال می کند و سرور با انتقال فایل های درخواستی از طریق شبکه پاسخ می دهد. پروتکل FTP مجموعه ای از دستورات و پیام های پاسخ سرور را تعریف می کند که به مشتری و سرور اجازه می دهد با یکدیگر ارتباط برقرار کنند.FTP را می توان در دو حالت مختلف استفاده کرد: حالت فعال و حالت غیرفعال. در حالت فعال، کلاینت اتصال به سرور را شروع می کند، در حالی که در حالت غیرفعال، سرور اتصال به کلاینت را شروع می کند.FTP همچنین از مکانیسم های احراز هویت و رمزگذاری برای اطمینان از امنیت انتقال فایل پشتیبانی می کند. کاربران می توانند خود را با نام کاربری و رمز عبور احراز هویت کنند تا به منابع خاصی در سرور FTP راه دور دسترسی پیدا کنند. FTP همچنین گزینه های امن انتقال فایل مانند SFTP (پروتکل انتقال فایل امن) و FTPS (FTP از طریق SSL/TLS) را فراهم می کند. به طور کلی، FTP یک پروتکل قابل اعتماد و کارآمد برای انتقال فایل ها بین دو ماشین در مکان های مختلف است. با این حال، پروتکل های جایگزینی مانند SSH، HTTP و ذخیره سازی ابری برای به اشتراک گذاری فایل ها از طریق اینترنت وجود دارد.HTTPوFTP هر دو پروتکل انتقال فایل هستند و هر دو خیلی خصوصیات یکسانی دارند، برای مثال هر دو بر روی TCP اجرا می شوند. هر چند دو پروتکل لایه کاربرد تفاوت های مهمی با هم دارند. برجسته ترین تفاوت اینست کهFTP از دو اتصال موازیTCP برای انتقال یک فایل استفاده می کند،یک ارتباط کنترلیControl connection و یک ارتباط داده ایdata connection ارتباط کنترلی برای ارسال اطلاعات کنترلی بین دو میزبان استفاده می شود واطلاعاتی مانند کد شناسایی کاربرد ،کلمه عبوردستورات برای تغییر دیرکتوری راه دور،ودستورات برای فایل هایget" " وput"."ارتباط داده ای در واقع برای ارسال یک فایل استفاده می شود. به دلیل اینکه یک اتصال کنترلی جدا استفاده می کنند ،گفته می شود که FTPاطلاعاتی کنترلی خود را خارج از باندout-of-bandارسال می کند. هنگامی که یک کاربر یک دورهFTP با یک میزبان راه دور را شروع می کند.طرف مشتریFTP کاربر ابتدا یک ارتباطFTP کنترلی با طرف سرویس دهنده (میزبان راه



دور) در پورت شماره ۲۱سرویس دهنده بر قرار کند. طرف مشتریFTP همچنین به وسیله ارتباط کنترلی دستورات را برای تغییر دایر کتوری راه دور ارسال می کند. هنگامی که طرف سرویس دهنده بوسیله ارتباط کنترلی یک دستور برای انتقال یک فایل (از یا به میزبان راه دور) دریافت کرد.طرف سرویس دهنده یک ارتباط داده ایTCP با طرف مشتری برقرار می کند. اگر، در طول جلسه یکسان، کاربر بخواهد یک فایل دیگر را انقال دهد ، FTPارتباط داده ای دیگری را باز می کند. زیراFTP دقیقا یک فایل بوسیله ارتباط داده ای می فرستد و سپس ارتباط داده ای را می بندد. بدین ترتیب باFTP ارتباط کنترلی در کل مدت جلسه کاربر باز نگه می دارد. اما یک ارتباط داده ای جدید برا هر فایل انتقال یافته در محدوده جلسه ایجاد می کند بدین معنی که ، ارتباط داده ناپیدار است.

SMTP:SMTP (پروتکل انتقال نامه ساده) پروتکلی است که برای ارسال و دریافت پیام های ایمیل از طریق اینترنت استفاده می شود. این پروتکل استاندارد برای ارسال پیام های ایمیل از یک سرور به سرور دیگر است. پروتکل SMTP با ایجاد ارتباط بین سرویس گیرنده ایمیل یا سرور و سرور ایمیلی که مسئول دریافت و ذخیره پیام است، کار می کند. هنگامی که اتصال برقرار شد، سرویس گیرنده ایمیل یا سرور، پیام ایمیل را با استفاده از SMTP به سرور ایمیل مقصد ارسال می کند.SMTP مدیر پروتکل لایه کاربر برای نامه الکترونیکی اینترنتی استSMTP .یک خدمات انتقال داده فایل احتمالTCP را برای انتقال نامه از سرویس دهنده پستی فرستنده به سرویس دهنده گیرنده استفاده می کند. بسیاری از پروتکل های لایه کاربرد،SMTP دو طرف دارد: یک طرف مشتری،که بر روی سرویس دهنده پستی فرستنده اجرا می شود و یک طرف سرویس دهنده که بر روی سرویس دهنده پستی گیرنده اجرا می شود. هر دو طرف مشتری و سرویس دهنده ، بعنوان یکSMTP مشتری عمل میکنند. هنگامی که یک سرویس دهنده پستی نامه را از دیگر سرویس دهنده های پستی دریافت کرد مانند یک سرویس دهنده SMTPعمل می کند. SMTPاز مجموعه ای از دستورات و پاسخ ها بین دو سرور ایمیل برای انتقال پیام استفاده می کند. برخی از دستورات اولیه SMTP عبارتند از:



HELO/EHLO - برای برقراری ارتباط بین دو سرور ایمیل استفاده می شود.

MAIL FROM - برای شناسایی فرستنده پیام ایمیل استفاده می شود.

RCPT TO - برای شناسایی گیرنده پیام ایمیل استفاده می شود.

DATA - برای ارسال محتوای پیام واقعی استفاده می شود.

هنگامی که پیام توسط سرور ایمیل مقصد دریافت و ذخیره شد، سرویس گیرنده یا سروری که پیام را ارسال کرده است، یک پیام تأیید از سرور دریافت می کند که پیام دریافت و تحویل داده شده است.SMTP همچنین دارای برخی از ویژگی‌های امنیتی است، مانند احراز هویت، رمزگذاری و تأیید، تا اطمینان حاصل شود که پیام به صورت ایمن تحویل داده می‌شود و از دسترسی غیرمجاز به محتوای پیام جلوگیری می‌کند.

اولا،SMTP مشتری (روی میزبان سرویس دهنده پستی فرستنده اجرا می شود) یک اتصال TCP روی پورت ۲۵ به SMTP سرویس دهنده برقرار می کند. هنگامی که این اتصال برقرار شد، سرویس دهنده و مشتری برخی توافق نمایی لایه کاربرد را انجام می دهند- مانند انسان ها که اغلب خود را قبل از انتقال اطلاعات از یکی به دیگری معرفی می کنند. سرویس دهنده و مشتری SMTP خود را قبل از انتقال اطلاعات معرفی می کنند. در طول این حوزه توافق نمایی SMTP مشتری SMTP آدرس ایمیل فرستنده (شخصی که پیام را منتشر می کند) و آدرس ایمیل گیرنده را تعیین می کند. هنگامی که SMTP مشتری و سرویس دهنده خودشان را به یکدیگر معرفی کردند مشتری پیام را ارسال می کند. SMTP می تواند به روی قابل اعتماد بودن سرویس انتقال داده TCP برای دادن پیام به سرویس دهنده بدون خطا حساب کند. مشتری پس از این پردازش را بوسیله اتصال TCP یکسان تکرار می کند اگر پیام های دیگری برای ارسال به سرویس دهنده داشته باشد و در غیر این صورت به TCP اطلاع می دهد ارتباط را ببندد.

نمونه:

S : 220 hamburger. Edu
C :helo crepes.fr
S : 250 hello crepes. Fr , pleased to meet you
C : mail from <alice @ crepes.fr>
S : 250 alice @ crepes. Fr.... Sender ok
C :rcpt to : <@ hamburger. edu>
S : 250 bob @ hamburger. Edu....recipient ok
C : DATA
S : 354 enter mail , end with "0" ona line by itself
C : How about pickles?
C : 0
S : 250 message accepted for delivery

۲- لایه ترنسپورت از دو پروتکل TCP,UDP تشکیل شده است.

UDP (User Datagram Protocol) یک پروتکل بدون اتصال است که برای انتقال داده ها از طریق اینترنت یا سایر شبکه های کامپیوتری استفاده می شود. این برای استفاده در شرایطی طراحی شده است که سرعت و تأخیر کم اهمیت بیشتری نسبت به قابلیت اطمینان دارند. در اینجا برخی از ویژگی های کلیدی UDP آورده شده است:

Connectionless برخلاف TCP، UDP بدون اتصال است. این بدان معنی است که قبل از انتقال داده، اتصال برقرار نمی کند. در عوض، بسته های UDP را می توان بلافاصله بدون انتظار برای پاسخ از دستگاه گیرنده منتقل کرد.

Unreliable: این پروتکل غیرقابل اعتماد است زیرا تضمین نمی کند که بسته ها به مقصد مورد نظر خود برسند، یا اگر رسیدند، به ترتیبی که ارسال شده اند. بسته‌ها ممکن است گم شوند، تکرار شوند یا بدون سفارش تحویل داده شوند.

No Error Correction: هیچ تصحیح خطا در UDP وجود ندارد، به این معنی که بسته های خراب دوباره ارسال نمی شوند و هیچ تضمینی وجود ندارد که داده های ارسال شده دقیق باشند.

سریع: به دلیل سادگی و عدم بررسی خطا، UDP بسیار سریعتر از TCP است. معمولاً در موقعیت‌هایی که سرعت مهم‌تر از قابلیت اطمینان است، مانند بازی‌های آنلاین استفاده می‌شود.

Datagram-oriented: یک پروتکل دیتاگرام گرا است. هر بسته UDP (داده گرام) مستقل است و می تواند به طور جداگانه از سایر بسته ها منتقل و مسیریابی شود.

سربار کم: این پروتکل سربار کمی دارد، به این معنی که از منابع شبکه کمتری نسبت به TCP استفاده می کند. اغلب در برنامه های کاربردی با پهنای باند کم که منابع شبکه محدود هستند استفاده می شود.

برای پخش استفاده می شود: UDP معمولاً برای پخش پیام به چندین دستگاه یا مشتری استفاده می شود. این بسته ها را به تمام دستگاه های موجود در یک آدرس پخش شبکه می فرستد که امکان اشتراک گذاری کارآمد داده ها را فراهم می کند.

به طور خلاصه، UDP یک پروتکل سریع، سبک و قابل اعتماد است که برای انتقال داده هایی که نیازی به قابلیت اطمینان یا سربار TCP ندارد، مناسب است. معمولاً در برنامه‌هایی مانند بازی‌های آنلاین، پخش ویدیو و VoIP استفاده می‌شود، جایی که سرعت و تأخیر کم مهم‌تر از قابلیت اطمینان هستند.

TCP (Transmission Control Protocol) یک پروتکل اتصال گرا است که برای انتقال داده ها از طریق اینترنت یا سایر شبکه های کامپیوتری استفاده می شود. برای اطمینان از انتقال مطمئن داده ها بین دستگاه ها طراحی شده است و معمولاً برای برنامه هایی استفاده می شود که دقت و کامل بودن داده ها بسیار مهم است. در اینجا برخی از ویژگی های کلیدی TCP آورده شده است:

Connection-oriented: TCP قبل از انتقال داده ها، یک ارتباط بین دو دستگاه برقرار می کند. اتصال در طول فرآیند انتقال داده تا زمانی که انتقال کامل شود حفظ می شود. این تضمین می کند که داده ها به طور دقیق بین دستگاه ها ارسال و دریافت می شوند.

Reliable: TCP تضمین می کند که داده ها به طور دقیق و به ترتیب ارسال و دریافت می شوند. این شامل مکانیسم‌های تشخیص خطا، بازیابی خطا و کنترل جریان است که تضمین می‌کند داده‌ها در حین انتقال از بین نمی‌روند یا خراب نمی‌شوند.

Acknowledgments: TCP به دستگاه دریافت کننده نیاز دارد تا دریافت داده ها را تأیید کند. این تضمین می کند که فرستنده می داند که آیا داده ها با موفقیت منتقل شده اند یا خیر.

Congestion control: TCP از مکانیسم کنترل تراکم استفاده می کند تا اطمینان حاصل کند که داده ها با سرعتی که شبکه را تحت الشعاع قرار نمی دهد منتقل می شود. این پروتکل بر سرعت انتقال نظارت می کند و در صورت نیاز آن را برای جلوگیری از ازدحام شبکه تنظیم می کند. درواقع سرعت را طوری تنظیم میکند که بافر روتر پر نشود.

Flow control: سرعت ارسال ر طوری تنظیم میکند که بافر گیرنده پر نشود و دیتا دراپ نشود.

کندتر: به دلیل سربار مربوط به قابلیت اطمینان و بررسی خطا، TCP کندتر از UDP است. با این حال، قابل اعتمادتر و دقیق تر است.

Stream-oriented: TCP جریان گرا است، به این معنی که با بخش هایی از داده ها به عنوان یک جریان پیوسته و نه به عنوان بسته های مستقل سروکار دارد.

برای مرور وب، ایمیل، انتقال فایل استفاده می شود: TCP معمولاً در برنامه هایی مانند مرور وب، ایمیل و انتقال فایل استفاده می شود که دقت و کامل بودن داده ها بسیار مهم است. به طور خلاصه، TCP برای اطمینان از انتقال مطمئن و دقیق داده ها بین دستگاه ها طراحی شده است. این شامل ویژگی هایی مانند انتقال اتصال گرا، تشخیص خطا، بازیابی خطا و مکانیسم های کنترل جریان است. TCP در حالی که کندتر از UDP است، قابل اعتمادتر و دقیق تر است و برای برنامه هایی مانند مرور وب، ایمیل و انتقال فایل مناسب است.

مقایسه:

TCP service:

- *reliable transport* between sending and receiving process
- *flow control:* sender won't overwhelm receiver
- *congestion control:* throttle sender when network overloaded
- *connection-oriented:* setup required between client and server processes
- *does not provide:* timing, minimum throughput guarantee, security

UDP service:

- *unreliable data transfer* between sending and receiving process
- *does not provide:* reliability, flow control, congestion control, timing, throughput guarantee, security, or connection setup.

application	application layer protocol	transport protocol
file transfer/download	FTP [RFC 959]	TCP
e-mail	SMTP [RFC 5321]	TCP
Web documents	HTTP [RFC 7230, 9110]	TCP
Internet telephony	SIP [RFC 3261], RTP [RFC 3550], or proprietary	TCP or UDP
streaming audio/video	HTTP [RFC 7230], DASH	TCP
interactive games	WOW, FPS (proprietary)	UDP or TCP

هر دو پروتکل‌های لایه انتقال هستند که ارتباط از طریق اینترنت را تسهیل می‌کنند. با این حال، آنها از چند جهت متفاوت هستند: اتصال گرا در مقابل بدون اتصال: TCP اتصال گرا است، به این معنی که قبل از انتقال داده، یک ارتباط بین دو میزبان برقرار می کند. از سوی دیگر، UDP بدون اتصال است و انتقال داده بدون ایجاد اتصال قبلی انجام می شود. قابلیت اطمینان: TCP انتقال داده قابل اعتماد را تضمین می کند، به این معنی که تضمین می کند که تمام داده ها به ترتیب صحیح و بدون از دست دادن، تکرار یا خطا به میزبان مقصد تحویل داده می شود. از سوی دیگر، UDP تضمینی برای قابلیت اطمینان ارائه نمی دهد زیرا مقرراتی برای بررسی خطا، بازیابی یا ارسال مجدد ندارد. سرعت: UDP سریع‌تر از TCP است، زیرا سربار برقراری اتصال یا بررسی خطا را ندارد. اندازه بسته: پروتکل‌های TCP می‌توانند تنها اندازه بسته‌های محدود ۶۵۵۳۵ بایت را مدیریت کنند، در حالی که پروتکل‌های UDP می‌توانند تا ۶۴ کیلوبایت انتقال دهند که امکان انتقال سریع‌تر داده را فراهم می‌کند. برنامه ها: TCP برای برنامه هایی استفاده می شود که به انتقال داده های قابل اعتماد نیاز دارند، مانند مرور وب یا انتقال فایل. UDP برای برنامه‌های بلادرنگ مانند پخش ویدیو یا پخش صدا استفاده می‌شود، جایی که تأخیر کوچک یا از دست دادن بسته قابل قبول است، اما انتقال سریع بسیار مهم است. به طور خلاصه، TCP برای برنامه هایی که نیاز به قابلیت اطمینان دارند مناسب است، در حالی که UDP برای برنامه هایی که نیاز به انتقال سریع و کارآمد دارند ایده آل است. هر دو نمیتوانند پهنای باند و تاخیر و jitter را گارانتی کند.

۳-

دانلودهای موازی به ۱۰ اتصال اجازه می دهد تا پهنای باند ۱۵۰ بیت در ثانیه را به اشتراک بگذارند و به هر کدام فقط ۱۵ بیت در ثانیه می دهد. بنابراین، کل زمان مورد نیاز برای دریافت همه اشیا به صورت زیر داده می شود:

(200/150+Tp + 200/150 +Tp + 200/150+Tp + 100,000/150+ Tp) + (200/(150/10)+Tp + 200/ (150/10) +Tp + 200/(150/10)+Tp + 100,000/ (150/10)+ Tp) = 7377 + 8Tp (seconds)

یک اتصال HTTP دائمی و پایا:

(200/150+Tp + 200/150 +Tp + 200/150+Tp + 100,000/150+ Tp)+ 10*(200/150+Tp + 100,000/150+ Tp) =7351 + 24Tp (seconds)

سرعت نور $3*10^8$ متر بر ثانیه در نتیجه $Tp=10/(3*10^8)=0.03$ میکروثانیه. بنابراین Tp در مقایسه با تاخیر انتقال ناچیز است.

بنابراین، می بینیم که HTTP پایا به طور قابل توجهی سریعتر (کمتر از ۱ درصد) از حالت غیر پایا با دانلود موازی نیست.

۴- زمان مورد نیاز برای ارسال درخواست، دریافت و نمایش محتوا به عوامل مختلفی مانند سرعت اتصال به اینترنت، زمان پاسخگویی سرور و پیچیدگی فایل HTML مورد نیاز برای تولید محتوا بستگی دارد.

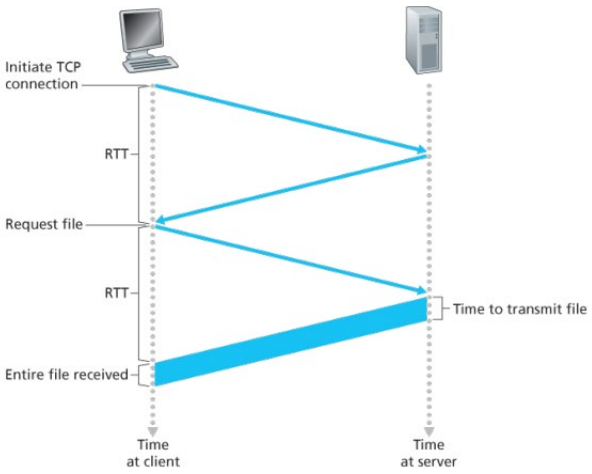
برقراری ارتباط با سرور - این مرحله شامل ارسال درخواستی به سرور برای برقراری ارتباط است. زمان مورد نیاز برای این مرحله بسته به فاصله بین سرور و کلاینت و سرعت اتصال به اینترنت تقریباً بین ۲۰ تا ۱۰۰ میلی ثانیه تخمین زده می شود.

ارسال درخواست برای فایل HTML - پس از برقراری ارتباط اولیه، مشتری درخواست فایل HTML را به سرور ارسال می کند. این مرحله ممکن است حدود ۱۰ تا ۲۰۰ میلی ثانیه طول بکشد، بسته به زمان پاسخگویی سرور، اندازه فایل HTML و میزان اشغال سرور.

بازیابی فایل HTML - هنگامی که سرور درخواست را دریافت کرد، پردازش فایل HTML را که حاوی محتوا است آغاز می کند. زمان صرف شده برای بازیابی و تولید این فایل HTML و ارسال آن به مشتری بسته به اندازه و پیچیدگی فایل HTML، عملکرد شبکه و سرور و دسترسی به پایگاه داده می تواند بسیار متفاوت باشد. این مرحله می تواند از چند صد میلی ثانیه تا چند ثانیه طول بکشد.

نمایش فایل HTML دریافتی - هنگامی که مشتری فایل HTML را دریافت کرد، مرورگر وب شروع به پردازش آن برای نمایش محتوا می کند. زمان لازم برای تکمیل رندر کردن فایل به پیچیدگی آن و اینکه آیا شامل اسکریپت ها، تصاویر یا سایر فایل های چندرسانه ای است که باید بارگذاری شوند، بستگی دارد و همچنین به سرعت رایانه ای که مرورگر روی آن اجرا می شود بستگی دارد.

به طور کلی، زمان صرف شده برای ارسال درخواست، دریافت فایل HTML و نمایش محتوا بسته به این عوامل می تواند به طور قابل توجهی متفاوت باشد، اما به طور کلی، ممکن است از چند صد میلی ثانیه تا چند ثانیه طول بکشد تا کل فرآیند تکمیل شود.



۵-

هر دو پروتکل های بازیابی ایمیل هستند، اما از چند جهت با هم تفاوت دارند:

روش بازیابی: POP3 تمام پیام‌های ایمیل را از سرور به دستگاه مشتری دانلود می‌کند، در حالی که IMAP به کاربر اجازه می‌دهد پیام‌ها را مستقیماً از سرور بخواند.

همگام‌سازی: IMAP همه پیام‌ها را روی سرور ذخیره می‌کند و تغییرات (مانند وضعیت خواندن یا ایمیل‌های حذف شده) را بین دستگاه مشتری و سرور همگام‌سازی می‌کند، در حالی که POP3 پیام‌ها را در دستگاه مشتری دانلود می‌کند و هیچ تغییری در سرور ایجاد نمی‌کند.

مدیریت ایمیل ها در سرور: IMAP به کاربران اجازه می دهد ایمیل ها را در پوشه ها و زیرپوشه ها سازماندهی کنند، در حالی که POP3 این کار را نمی کند.

حالت آفلاین: POP3 را می توان در حالت آفلاین استفاده کرد، به این معنی که کاربر می تواند ایمیل ها را حتی بدون اتصال به اینترنت بخواند. IMAP را می توان به صورت آفلاین استفاده کرد، اما فقط برای ایمیل هایی که قبلا دانلود شده اند.

امنیت پروتکل: POP3 یک پروتکل نسبتا ناامن است که روی پیام‌های متنی ساده کار می‌کند، در حالی که IMAP از پروتکل‌های جدیدتر مانند SSL/TLS پشتیبانی می‌کند تا اتصال امن‌تری را ارائه دهد.

مدیریت پیوست ایمیل: IMAP به کاربران امکان می دهد پیوست های ایمیل را روی سرور مدیریت کنند، از جمله حذف یا ذخیره آنها، در حالی که POP3 پیوست های ایمیل را در دستگاه مشتری دانلود می کند و کاربر آنها را از آنجا مدیریت می کند.

به طور خلاصه، POP3 برای کاربرانی ایده آل است که فقط در یک دستگاه به ایمیل خود دسترسی دارند و دسترسی آفلاین به پیام های خود را در اولویت قرار می دهند. IMAP همه کاره تر است و برای کاربرانی مناسب است که نیاز به دسترسی به ایمیل خود از چندین دستگاه دارند و ترجیح می دهند پیام های ایمیل را در سرور ذخیره و مدیریت کنند.

۶-

۱. کاربر «sbu.ac.ir» را در یک مرورگر وب تایپ می کند و درخواست به اینترنت ورد میشود و توسط یک DNS recursive resolver (محلی) دریافت می شود. پیام درخواست شامل نام میزبانی است که باید ترجمه شود.

۲. سپس DNS محلی به یک سرور DNS root nameserver کوئری میزند. یعنی سرور DNS محلی پیام کوئری را به سرور DNS ریشه ارسال می کند.

۳. سپس سرور روت با آدرس سرور DNS دامنه سطح بالا (TLD) (مانند .com یا .net که در اینجا ir. مقال زدیم)، که اطلاعات را برای دامنه های خود ذخیره می کند، به DNS محلی پاسخ می دهد و لیستی از آدرس های IP سرورهای TLD مسئول ir را به سرور DNS محلی برمی گرداند. یعنی هنگام جستجو برای sbu.ac.ir ، درخواست ما به سمت TLD .ir است.

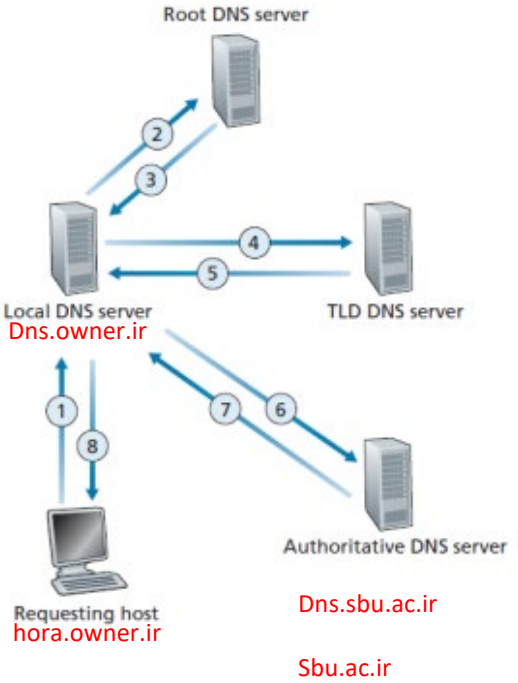
۴. سپس سرور DNS محلی پیام کوئری را به یکی از این سرورهای TLD ارسال می کند.

۵. سرور TLD پسوند ac.ir را یادداشت می کند و با آدرس IP سرور DNS معتبر برای دانشگاه ، مثلا dns.sbu.ac.ir پاسخ می دهد.

۶. در نهایت، سرور DNS محلی پیام کوئری را مستقیماً به dns.sbu.ac.ir ارسال می کند که

۷. با آدرس sbu.ac.ir IP پاسخ می دهد. یعنی آدرس IP برای sbu.ac.ir از nameserver به DNS محلی بازگردانده می شود.

۸. سپس حل‌کننده DNS با آدرس IP دامنه درخواستی ابتدا به مرورگر وب پاسخ می‌دهد.



فرض کنید میزبان hora.owner.ir آدرسIP sbu.ac.ir را می خواهد.
همچنین فرض کنید که سرور DNS محلی ما dns.owner.ir است. و
dns.sbu.ir یک سرور DNS معتبر برای sbu.ac.ir نامیده می‌شود.