بررسی برخی از پروتکل های معمول در اینترنت

استاد راهنما : دکتر حسن حقیقی

استادیار : عباس نادری

گردآورندگان:

آرمین بلقدر

مسعود فیروز آبادی

زمستان ۱۳۸۹

مقدمه

پروتکل و جایگاه آن در شبکه های کامپیوتری

کامپیوترها و سایر دستگاه های شبکه ای به منظور ارتباط با یکدیگر از پروتکل استفاده می نمایند . تاکنون پروتکل های متعددی در عرصه شبکه های کامپیوتری طراحی و پیاده سازی شده است . TCP/IP که مشتمل بر خانواده ای از پروتکل های شبکه ای است ، نمونه ای در این زمینه است که از آن در اینترنت استفاده می گردد. اینترنت متشکل از شبکه های جداگانه متعددی است که توسط روتر به یکدیگر متصل شده اند .هر پروتکل موجود در خانواده TCP/IP با یک هدف خاص طراحی و دارای وظایف از قبل تعریف شده و کاملا" مشخصی است .

معرفی پروتکل TCP/IP

TCP/IP ، یکی از مهمترین پروتکل های استفاده شده در شبکه های کامپیوتری است . اینترنت بعنوان بزرگترین شبکه موجود ، از پروتکل فوق بمنظور ارتباط دستگاه های متفاوت استفاده می نماید. پروتکل ، مجموعه قوانین لازم بمنظور قانونمند نمودن نحوه ارتباطات در شبکه های کامپیوتری است .

امروزه اکثر شبکه های کامپیوتری بزرگ و اغلب سیستم های عامل موجود از پروتکل TCP/IP ، استفاده و حمایت می نمایند. TCP/IP ، امکانات لازم بمنظور ارتباط سیستم های غیرمشابه را فراهم می آورد. از ویژگی های مهم پروتکل فوق ، می توان به مواردی همچون : قابلیت اجراء بر روی محیط های متفاوت ، ضریب اطمینان بالا ،قابلیت گسترش و توسعه آن ، اشاره کرد . از پروتکل فوق، بمنظور دستیابی به اینترنت و استفاده از سرویس های متنوع آن نظیر وب و یا پست الکترونیکی استفاده می گردد. تنوع پروتکل های موجود در پشته TCP/IP و ارتباط منطقی و سیستماتیک آنها با یکدیگر، امکان تحقق ارتباط در شبکه های کامپیوتری را با اهداف متفاوت ، فراهم می نماید. فرآیند برقراری یک ارتباط ، شامل فعالیت های متعددی نظیر : تبدیل نام کامپیوتر به آدرس IP معادل ، مشخص نمودن موقعیت کامپیوتر مقصد ، بسته بندی اطلاعات ، آدرس دهی و روتینگ داده ها بمنظور

ارسال موفقیت آمیز به مقصد مورد نظر ، بوده که توسط مجموعه پروتکل های موجود در پشته TCP/IP انجام میگیرد.

TCP/IP ، پروتکلی استاندارد برای ارتباط کامپیوترهای موجود در یک شبکه مبتنی بر ویندوز ۲۰۰۰ است. از پروتکل فوق، بمنظور ارتباط در شبکه های بزرگ استفاده می گردد. برقراری ارتباط از طریق پروتکل های متعددی که در چهار لایه مجزا سازماندهی شده اند ، میسر می گردد. هر یک از پروتکل های موجود در پشته TCP/IP ، دارای وظیفه ای خاص در این زمینه (برقراری ارتباط) می باشند . در زمان ایجاد یک ارتباط ، ممکن است در یک لحظه تعداد زیادی از برنامه ها ، با یکدیگر ارتباط برقرار نمایند. TCP/IP ، دارای قابلیت تفکیک و تمایز یک برنامه موجود بر روی یک کامپیوتر با سایر برنامه ها بوده و پس از دریافت داده ها از یک برنامه ، آنها را برای برنامه متناظر موجود بر روی کامپیوتر دیگر ارسال می نماید. نحوه ارسال داده توسط پروتکل TCP/IP از محلی به محل دیگر ، با فرآیند ارسال یک نامه از شهری به شهر، قابل مقایسه است .

برقراری ارتباط مبتنی بر TCP/IP ، با فعال شدن یک برنامه بر روی کامپیوتر مبدا آغاز می گردد . برنامه فوق ،داده های مورد نظر جهت ارسال را بگونه ای آماده و فرمت می نماید که برای کامپیوتر مقصد قابل خواندن و استفاده باشند. (مشابه نوشتن نامه با زبانی که دریافت کننده ، قادر به مطالعه آن باشد) . در ادامه آدرس کامپیوتر مقصد ، به داده های مربوطه اضافه می گردد (مشابه آدرس گیرنده که بر روی یک نامه مشخص می گردد) . پس از انجام عملیات فوق ، داده بهمراه اطلاعات اضافی (درخواستی برای تائید دریافت در مقصد) ، در طول شبکه بحرکت درآمده تا به مقصد مورد نظر برسد. عملیات فوق ، ارتباطی به محیط انتقال شبکه بمنظور انتقال اطلاعات نداشته ، و تحقق عملیات فوق با رویکردی مستقل نسبت به محیط انتقال ، انجام خواهد شد .

لایه های پروتکل TCP/IP

TCP/IP ، فرآیندهای لازم بمنظور برقراری ارتباط را سازماندهی و در این راستا از پروتکل های متعددی در پشته TCP/IP استفاده می گردد. بمنظور افزایش کارآئی در تحقق فرآیند های مورد نظر، پروتکل ها در لایه های متفاوتی، سازماندهی شده اند . اطلاعات مربوط به آدرس دهی در انتها قرار گرفته و بدین ترتیب کامپیوترهای موجود در شبکه قادر به بررسی آن با سرعت مطلوب خواهند بود. در این راستا، صرفا" کامپیوتری که بعنوان کامپیوتر مقصد معرفی شده است ، امکان باز نمودن بسته اطلاعاتی و انجام پردازش های لازم بر روی آن را دارا خواهد بود. TCP/IP ، از یک مدل ارتباطی چهار لایه بمنظور ارسال اطلاعات از محلی به محل دیگر استفاده می نماید.

Internet, Transport, Application و Network Interface ، لایه های موجود در پروتکل TCP/IP می باشند.هر یک از پروتکل های وابسته به پشته TCP/IP ، با توجه به رسالت خود ، در یکی از لایه های فوق، قرار می گیرند.

بررسی برخی از پروتکل های معمول در اینترنت

برخی از پروتکل های معمول در لایه کاربرد[1]

- پروتکل HTTP :

در اینترنت همانند سایر شبکه های کامپیوتری از پروتکل های متعدد و با اهداف مختلف استفاده می گردد. هر پروتکل از یک ساختار خاص برای ارسال و دریافت اطلاعات (بسته های اطلاعاتی) استفاده نموده و ترافیک مختص به خود را در شبکه ایجاد می نماید .

HTTP (برگرفته از Hyper Text Transfer Protocol) ، یکی از متداولترین پروتکل های لایه application است که مسئولیت ارتباط بین سرویس گیرندگان و سرویس دهندگان وب را برعهده دارد .

دنیای شبکه های کامپیوتری دارای عمری چند ساله است و بسیاری از کاربران ، ضرورت استفاده از شبکه را همزمان با متداول شدن اینترنت در اوایل سال ۱۹۹۰ دریافتند . عمومیت اینترنت، رشد و گسترش شبکه های کامپیوتری را به دنبال داشته است . اینترنت نیز با سرعتی باورنکردنی رشد و امروزه شاهد ایجاد ده ها میلیون وب سایت در طی یک سال در این عرصه می باشیم .

تمامی وب سایت های موجود بر روی اینترنت از پروتکل HTTP استفاده می نمایند . با این که پروتکل HTTP با استفاده از پروتکل های دیگری نظیر IP و TCP ماموریت خود را انجام می دهد ، ولی این پروتکل

---

[1] Application

HTTP است که به عنوان زبان مشترک ارتباطی بین سرویس گیرنده و سرویس دهنده وب به رسمیت شناخته شده و از آن استفاده می گردد . در واقع مرورگر وب صدای خود را با استفاده از پروتکل HTTP به گوش سرویس دهنده وب رسانده و از وی درخواست یک صفحه وب را می نماید.

به منظور انجام یک تراکنش موفقیت آمیز بین سرویس گیرندگان وب (نظیر IE) و سرویس دهندگان وب (نظیر IIS) ، به اطلاعات زیادی نیاز خواهد بود . پس از handshake پروتکل TCP/IP ، مرورگر اطلاعات گسترده ای را برای سرویس دهنده وب ارسال می نماید .

سرویس گیرندگان وب به منظور استفاده از خدمات سرویس دهندگان وب از مجموعه پتانسیل های ارائه شده (دستورات) توسط پروتکل HTTP استفاده می نمایند :

- GET : سرویس گیرنده وب درخواست یک منبع موجود بر روی سرویس دهنده وب را می نماید
- POST : سرویس گیرنده وب اطلاعاتی را برای سرویس دهنده وب ارسال می نماید .
- PUT : سرویس گیرنده وب یک مستند جایگزین را برای سرویس دهنده وب ارسال می نماید .
- HEAD : سرویس گیرنده وب اطلاعات خاصی را در ارتباط با یک منبع موجود بر روی سرویس دهنده درخواست می نماید (عدم نیاز به خود منبع)
- DELETE : سرویس گیرنده وب درخواست حذف یک سند موجود بر روی سرویس دهنده را می نماید .
- TRACE : سرویس گیرندگان وب ، پراکسی مربوط به خود را تعریف می نمایند . از متد فوق اغلب در موارد اشکال زدائی استفاده می گردد .

- OPTIONS : سایر پتانسیل های موجود به منظور کار بر روی یک سند توسط یک سرویس گیرنده وب درخواست می گردد .
- CONNECT : سرویس گیرنده وب به عنوان یک پراکسی به یک سرویس دهنده HTTPS متصل می گردد .

- Https :

نسخه امن شده Http یا Secure Http است که در ان اطلاعاتی که بین سرور و رایانه شخصی مبادله می شود وبه صورت رمز در می اید تا در بین راه ربوده نشود.

- پروتکل DNS :

DNS از کلمات Domain Name System اقتباس و یک پروتکل شناخته شده در عرصه شبکه های کامپیوتری خصوصا" اینترنت است . از پروتکل فوق به منظور ترجمه اسامی کامپیوترهای میزبان و Domain به آدرس های IP استفاده می گردد.

DNS ، زمانی که اینترنت تا به این اندازه گسترش پیدا نکرده بود و صرفا" در حد و اندازه یک شبکه کوچک بود ، استفاده می گردید . در آن زمان ، اسامی کامپیوترهای میزبان به صورت دستی در فایلی با نام HOSTS درج می گردید . فایل فوق بر روی یک سرویس دهنده مرکزی قرار می گرفت . هر سایت و یا کامپیوتر که نیازمند ترجمه اسامی کامپیوترهای میزبان بود ، می بایست از فایل فوق استفاده می نمود . همزمان با گسترش اینترنت و افزایش تعداد کامپیوترهای میزبان ، حجم فایل فوق نیز افزایش و امکان استفاده از آن با مشکل مواجه گردید (افزایش ترافیک شبکه). با توجه به مسائل فوق ، در سال ۱۹۸۴ تکنولوژی DNS معرفی گردید

DNS ، یک "بانک اطلاعاتی توزیع شده " است که بر روی ماشین های متعددی مستقر می شود (مشابه ریشه های یک درخت که از ریشه اصلی انشعاب می شوند) . امروزه اکثر شرکت ها و موسسات دارای یک سرویس دهنده DNS کوچک در سازمان خود می باشند تا این اطمینان ایجاد گردد که کامپیوترها بدون بروز هیچگونه مشکلی ، یکدیگر را پیدا می نمایند . در صورتی که از ویندوز ۲۰۰۰ و اکتیو دایرکتوری استفاده می نمائید، قطعا" از DNS به منظور ترجمه اسامی کامپیوترها به آدرس های IP ، استفاده می شود . شرکت مایکروسافت در ابتدا نسخه اختصاصی سرویس دهنده DNS خود را با نام Windows Internet Name Service (WINS) طراحی و پیاده سازی نمود . سرویس دهنده فوق مبتنی بر تکنولوژی های قدیمی بود و از پروتکل هائی استفاده می گردید که هرگز دارای کارائی مشابه DNS نبودند . بنابراین طبیعی بود که شرکت مایکروسافت از WINS فاصله گرفته و به سمت DNS حرکت کند .

از پروتکل DNS در مواردی که کامپیوتر شما اقدام به ارسال یک درخواست مبتنی بر DNS برای یک سرویس دهنده نام به منظور یافتن آدرس Domain می نماید ، استفاده می شود .مثلا" در صورتی که در مرورگر خود

آدرس www.yahoo.com را تایپ نمائید ، یک درخواست مبتنی بر DNS از کامپیوتر شما و به مقصد یک سرویس دهنده DNS صادر می شود . ماموریت درخواست ارسالی ، یافتن آدرس IP وب سایت یاهو است.

- پروتکل DHCP:

پروتکل پیکربندی پویای میزبان (DHCP) به شما اجازه می دهد ادرسهای IP را بصورت پویا به کامپیوترها و وسایل جانبی روی شبکه اختصاص دهید. آدرس های IP از مخزنی از آدرس های تهیه شده و به کامپیوترها اختصاص داده می شوند. اختصاص آدرس IP بصورت دائم و مو قت خواهد بود. وقتی این مسئله را در نظر بگیرید که باید به هر کامپیوتر مشتری ، آدرس IP ماسک زیر شبکه و آدرس دروازه اختصاص دهید در می یابید که احتمال خطا در اختصاص آدرس ها بسیار بالاست .

DHCPیک محیط پویا ایجاد می کند که آدرس های IP را به کامپیوترها و وسایل جانبی روی شبکه اختصاص می دهد. با این روش با دردسرهای اختصاص آدرس IP بصورت دستی روبه رو نمی شوید و اختصاص آدرس های IP به کامپیوترها با دقت بالایی انجام می گیرد .

سرور DHCP وظیفه دارد آدرس IP ، ماسک زیر شبکه، دروازه پیش ساخته، آدرس سرور DNS و آدرس سرور WINS را به مشتری DHCP ارائه دهد. مشتری DHCP هر کامپیوتر یا وسیله ای روی شبکه است که برای کسب پویای آدرس IP پیکربندی شده است. هنگامی که یک مشتری DHCP برای اولین بار راه اندازی می شود بدنبال آدرس IP می گردد. مشتری یک پیغام DHCP DISCOVER را نشان می دهند

که قرارداد IP فرستاده شده به همه سرورهای DHCP را درخواست می کند. پیام نمایش داده شده نام میزبان مشتری و آدرس سخت افزار MAC مشتری را ارائه می کند .

در مرحله بعد یک سرور DHCP که روی زیر شبکه قرار دارد توسط پیام DHCP OFFER آدرس IPپیشنهادی به همراه ماسک زیر شبکه و قرارداد IP را ارائه می کند. این پیام آدرس IP سرور DHCP را نیز شامل می شود .

هنگامی که مشتری اولین پیام DHCP OFFER را دریافت می کند یک پیام DHCP REQUESTبه همه سرورهای DHCP شبکه می فرستند و پذیرش پیشنهاد ارائه شده را اعلام می کند .این پیام آدرس IP سرور DHCP ای را در بر می گیرد که مشتری با آن موافقت نموده است .بقیه سرورهای DHCPمنتظر می مانند تا هنگامی که مشتری دیگری درخواست آدرس IP داشت به آن درخواست پاسخ دهند. درنهایت سرور DHCP که با پیشنهادش موافقت شده یک پیام تایید برای مشتری می فرستد .

- پروتکل FTP:

تصویر اولیه اینترنت در ذهن بسیاری از کاربران، استفاده از منابع اطلاعاتی و حرکت از سایتی به سایت دیگر است و شاید به همین دلیل باشد که اینترنت در طی سالیان اخیر به سرعت رشد و متداول شده است . بسیاری از کارشناسان این عرصه اعتقاد دارند که اینترنت گسترش و عمومیت خود را مدیون سرویس وب می باشد . فرض کنید که سرویس وب را از اینترنت حذف نمائیم . برای بسیاری از ما این سوال مطرح خواهد شد که چه نوع

استفاده ای را می توانیم از اینترنت داشته باشیم ؟ در صورت تحقق چنین شرایطی ، یکی از عملیاتی که کاربران قادر به انجام آن خواهند بود ، دریافت داده ، فایل های صوتی ، تصویری و سایر نمونه فایل های دیگر با استفاده از پروتکل FTP (برگرفته از File Transfer Protocol) است.

FTP ، مانند HTTP که محتوای وب را منتقل می کند یا SMTP که ایمیل ها را منتقل می کند FTP هم ساده ترین راه برای تبادل فایل از یک کامپیوتر به کامپیوتر دیگر می باشد . یکی از کاربرد های FTP ، دانلود موزیک و برنامه های کاربردی از وب سایت ها می باشد .به خاطر استفاده این پروتکل از یک پورت مجزا که پورت شماره ۲۱ است عمل دانلود بسیار سریع انجام می شود . مانند آدرسهای وب سایت ها ، FTP هم آدرس مخصوص خود را دارد چون همانند یک وب سایت ، این پروتکل بر روی هارد دیسک کامپیوتر سرور فضای مشخصی را اشغال می کند . معمولاً اگر آدرس یک وب سایت مانند آدرس زیر باشد :

http://www.domain.com

آدرس FTP آن سایت به این صورت است :

ftp://ftp.domain.com

FTP در انتقال فایل بسیار قویتر از HTTP است ولی به مراتب پیچیده تر از HTTP می باشد .جهت استفاده از پروتکل FTP شما به نرم افزارهای سرویس دهنده مانند FileZilla نیاز دارید . Cute FTP، WSFTP و FTP Voyager نیز نمونه های دیگری هستند .

ویژگیهای FTP

پروتکل FTP دارای حداکثر انعطاف لازم و در عین حال امکان پذیر به منظور استفاده در شبکه های مختلف با توجه به نوع شبکه است . این پروتکل امکان استفاده از سیستم فایل را مشابه یونیکس و یا خط دستور ویندوز در اختیار کاربران می گذارد . پروتکل FTP دارای امکانات حمایتی لازم برای ارسال داده با نوع های مختلف می باشد . پروتکل FTP منحصراً از پروتکل TCP استفاده می کند . معمولاً پروتکل های لایه Aplication از TCP استفاده می نمایند . پروتکل FTP برای انجام وظایف محوله از دو پورت استفاده می کند . از پورت شماره ۲۰ برای ارسال داده و از پورت شماره ۲۱ برای گوش دادن به فرامین استفاده می نماید .

کاربردهای FTP

یکی از کاربرد های FTP استفاده طراحان و مدیران وب سایت ها برای انتقال محتوای سایت ها می باشد که در حال حاضر این افراد بیشترین استفاده را از FTP دارند . زمانی که شما فضایی را برای سایت خود از ISP اجاره می کنید به شما حداقل یک آدرس FTP می دهند تا عمل انتقال فایل ها را از کامپیوتر خود به وب سرور و بالعکس انجام دهید .

خدمات ارائه شده توسط FTP

۱. تهیه لیستی از فایل های موجود از سیستم فایل کامپیوتر از راه دور .
۲. حذف ، تغییر نام و جابجا کردن فایل های کامپیوتری از راه دور .
۳. جستجو در شاخه های (دایرکتوری) کامپیوتر از راه دور .
۴. ایجاد یا حذف شاخه روی کامپیوتر از راه دور .
۵. انتقال فایل از کامپیوتر راه دور به کامپیوتر میزبان .

۶. انتقال فایل و ذخیره آن از کامپیوتر میزبان به کامپیوتر راه دور .

۷. ارتباط بین سرویس گیرنده و سرویس دهنده

برای شروع یک " نشست " بین برنامه سرویس دهنده و سرویس گیرنده باید دو ارتباط همزمان از نوع TCP برقرار شود . به هریک از این ارتباطات در ادبیات پروتکل TCP، یک "کانال" گفته می شود .

این دو کانال عبارتند از :

کانال داده : یک ارتباط TCP با پورت شماره ۲۰ از سرویس دهنده که روی آن داده ها مبادله می شوند .

کانال فرمان : یک ارتباط TCP با پورت شماره ۲۱ که روی آن فرامین لازم برای مدیریت فایل ها رد و بدل می شوند .

دلیل لزوم برقراری دو کانال مجزا بین سرویس دهنده و سرویس گیرنده آن است که بتوان بدون قطع جریان داده ها فرامین را به طور همزمان مبادله کرد . بعنوان مثال در حین انتقال یک فایل می توان روی کانال فرمان دستور لغو انتقال یا تغییر مورد انتقال را صادر کرد .

ذکر این نکته ضروریست که در پروتکل FTP همه عملیات انتقال فایل در "پیش زمینه" انجام می شود . بدین معنی که پروتکل FTP مانند سیستمهایی مثل مدیریت چاپ که درخواست های چاپ پرونده را به صف کرده و یک به یک آنها را رسیدگی می کند ، نیست و عملیات انتقال فایل را به صورت بلادرنگ انجام می دهد . پروتکل FTP ، دو پروسه همزمان ایجاد می کند که یکی وظیفه مدیریت ارتباط روی کانال فرمان را به عهده داشته و اصطلاحاً "مفسر پروتکل" یا پروسه PI نامیده می شود . وظیفه پروسه دیگر مدیریت انتقال داده هاست و به DTP یا "پروسه انتقال داده" معروف است . پروسه PI همیشه به پورت شماره ۲۱ و پروسه DTP به پورت شماره ۲۰ مقید شده اند .

مقایسه FTP با HTTP

پروتکل FTP از مدل سرویس گیرنده – سرویس دهنده استفاده می نماید بر خلاف HTTP که یک حاکم مطلق در عرصه مرورگرهای وب و سرویس دهندگان وب است ، نمی توان ادعای مشابهی را در رابطه با این پروتکل را در FTP داشت و هم اینک مجموعه ای گسترده از سرویس گیرندگان و سرویس دهندگان FTP وجود دارد .

معایب و نواقص FTP

FTP این قابلیت را ندارد که بتوان همانند پروتکل Telnet برنامه ای را بر روی ماشین از راه دور اجرا کرد ، بلکه فقط روشی سریع ، ساده و مطمئن برای خدمات کاربران راه دور محسوب می شود .

FTP هیچ گونه رمزنگاری را پشتیبانی نمی کند . FTP حتی کلمات عبور را نیز بصورت رمز نشده انتقال می دهد و بدین ترتیب اجازه سو استفاده آسان از سیستم را می دهد .

FTP به عنوان یک روش امن مورد توجه نیست مگر اینکه درون یک کانال امن مانند SSL یا IPsec قرار گیرد .

- پروتکل SMTP:

مخفف عبارت Simple Mail Transfer Protocol است. از این پروتکل برای ارسال پیام‌های الکترونیکی (E-mail)استفاده می‌شود. این پروتکل امروزه دیگر برای خواندن پیام‌های الکترونیکی استفاده نمی‌شود.

پروتکل SMTPارسال و مسیریابی نامه‌های الکترونیکی را از فرستنده به گیرنده با استفاده از آدرس‌های پست الکترونیکی امکان‌پذیر می‌سازد. عملکرد این پروتکل، بدین صورت است که یک اتصال TCPبین سرویس‌گیرنده و سرویس‌دهنده SMTPبرقرار می‌شود. سپس، سرویس‌گیرنده آدرس پست الکترونیکی فرستنده (ها) و گیرنده (ها) را به اطلاع سرویس‌دهنده می‌رساند. در صورتی که مراحل فوق به درستی پیش روند، سرویس‌گیرنده نامه‌ی الکترونیکی را به سرویس‌دهنده منتقل می‌کند. پس از آن سرویس‌دهنده تلاش می‌کند تا نامه‌ی الکترونیکی را به صندوق پست‌الکترونیکی تحویل داده یا در صورت لزوم آن را برای تحویل به گیرنده، به سرویس‌دهنده‌ی دیگر ارسال نماید.

SMTP قرارداد ساده انتقال نامه است. این پروتکل انتقال صحیح پست الکترونیکی را بر عهده دارد و برای انجام این کار از دنباله‌ای از دستورات ساده اسکی (رشته‌ای) استفاده می‌کند. انتقال پست الکترونیکی با برقراری یک اتصال TCP از ماشین مبدأ به پورت ۲۵ ماشین مقصد صورت می‌گیرد. ماشین مقصد می‌تواند گیرنده نهایی یا یک واسط باشد. دستورات SMTP توسط فرستنده ایجاد و به گیرنده فرستاده می‌شوند و پاسخ این دستورات از گیرنده به فرستنده ارسال می‌شود و این کار تا زمانی که ارتباط قطع نشود(نامه‌ای جهت ارسال وجود داشته باشد)، ادامه دارد.

- پروتکل POP3 :

مخفف عبارت Post Office Protocol 3 است و یک پروتکل (قانون) استاندارد برای دریافت ایمیل از سرور است. به طور خلاصه کارش این است که نامه‌های شما را بدون مراجعه مستقیم به صندوق پستی با استفاده از نرم افزارهای ویژه مثل Outlook بر روی هارد ذخیره می‌کند. در حالت پیش‌فرض تمام نامه‌های موجود در پوشه Inbox از روی سرور به پوشه Inbox محلی منتقل شده و از روی سرور حذف می‌گردند حتی اگر ویروسی باشند بنابراین از باز کردن و خواندن نامه‌هایی که گیرنده‌ی نامه را نمی‌شناسید خودداری کنید. از مزایای pop3این است که به صورت) OffLine عدم اتصال به سرور پست الکترونیک) نیز می‌توانید نامه‌های الکترونیکی خود را که قبلاً دانلود کرده‌اید ببینید.

توجه: در استفاده از این پروتکل برای افزایش سرعت دستیابی به پیام‌ها سعی کنید حجم و تعداد نامه‌ها در پوشه‌ی Inboxبر روی سرویس‌دهنده کم باشد.

- پروتکل IMAP :

مخفف عبارت Internet Message Access Protocol است و همانند POP3 یک پروتکل استاندارد برای دریافت ایمیل از سرور است اما دارای مزایایی نسبت به پرتکل POP3می‌باشد. در POP3 پس از دریافت ایمیل‌ها، ایمیل‌ها از روی سرور پاک می‌شود. شما از طریق IMAP این امکان را خواهید داشت که بدون دانلود کردن ایمیل‌های خود از روی سرور ، درون ایمیلهای خود جستجو کنید ، پوشه بسازید ، نامه‌های الکترونیکی را پاک کنید و mailbox خود را برای نامه‌های الکترونیکی جدید چک کنید . این امکانات بتدریج باعث جایگزینی IMAPبه جای POP3 می شود. یکی از پر استفاده‌ترین موارد استفاده ازIMAP حالت اشتراکی است مثلا در شرکتی که باید چند نفر اجازه دسترسی به پست الکترونیک شرکت را داشته باشند IMAPراه حل مناسبی است.

مقایسه‌ی دو پروتکل IMAP و POP3

۱. پروتکل pop3 نامه‌های الکترونیکی موجود در پوشه‌ی Inbox روی سرویس‌دهنده را مرور کرده و تمام پیام‌های جدید را یک مرتبه و خیل سریع بر روی کامپیوتر شما دانلود می‌کند. پروتکل IMAP سربرگ (Headers) تمام پیام‌های جدید را دانلود کرده و زمانی که شما قصد خواندن آن پیام را دارید و بر روی آن کلیک می‌کنید آنگاه پیام را بر روی سیستم شما دانلود می‌کند. به همین دلیل سرعت بازیابی پیام‌ها در IMAP کم‌تر می‌باشد.

۲. پروتکل) pop3 زمانی که با سرویس دهنده‌ی پست الکترونیکی ارتباط ندارید نیز قابل دسترس خواهد بود ولی در پروتکل IMAP حتماً باید با سرویس دهنده‌ی پست الکترونیکی در ارتباط باشید.

۳. پروتکل pop3 در مواردی مفید است که شما نامه‌های پستی خود را تنها از روی یک کامپیوتر بررسی می‌کنید ولی مواقعی که می‌خواهید از روی چند کامپیوتر (منزل، اداره و ...) نامه‌های پستی خود را بررسی کنید استفاده از پروتکل imap مفیدتر خواهد بود.

۴. در پروتکل IMAP پیام‌های شما از جمله پیام‌هایی که در پوشه‌ی Sent-mail ذخیره شده است از روی کامپیوتر دیگر قابل مشاهده نیست.

۵. در پروتکل pop3 پیام‌های پوشه‌ی Inbox از روی سرویس دهنده پاک می‌شود و شما تنها به همان پیام‌ها دسترسی دارید ولی در پروتکل IMAP تمام پوشه‌های ایجاد شده بر روی سرویس دهنده قابل مشاهده و قابل پیمایش خواهد بود و تغییرات انجام شده بر روی سرویس دهنده نیز اعمال می‌گردد.

۶. در پروتکل pop3 برای دستیابی به آخرین بروزرسانی باید بر روی دکمه‌ی Send/Receive کلیک کنید ولی در در پروتکل IMAP همواره با رسیدن پیام جدید خود به صورت خودکار بروزرسانی می‌گردد.

۷. در پروتکل pop3 به دلیل اینکه پیام‌ها بر روی فضای هارد دیسک ذخیره می‌شوند مشکل محدودیت فضای جعبه پستی را نخواهید داشت، اما در پروتکل IMAP به دلیل اینکه پیام‌ها فضای MailBox را اشغال می‌کند ممکن با مشکل محدودیت فضا روبرو می‌شوید.

۸. تمام ISP ها و برنامه‌های پست الکترونیکی پروتکل POP3 را پشتیبانی می‌کنند ولی به دلیل پیچیدگی پروتکل IMAP تعداد کمی از ISP ها و برنامه‌های پست الکترونیکی پروتکل IMAP را پشتیبانی می‌کنند.

۹. در پروتکل IMAP انتقال حساب کاربری میل از یک سیستم به سیستم دیگر آسان است، ولی در پروتکل POP3 به دلیل اینکه میل‌ها به صورت فایل بر روی سیستم ذخیره می‌شود مشکل است و ممکن است انتقال میل‌ها از یک برنامه به برنامه‌ی دیگر به دلیل پشتیبانی نکردن از آن نوع سیستم فایل امکان‌پذیر نباشد.

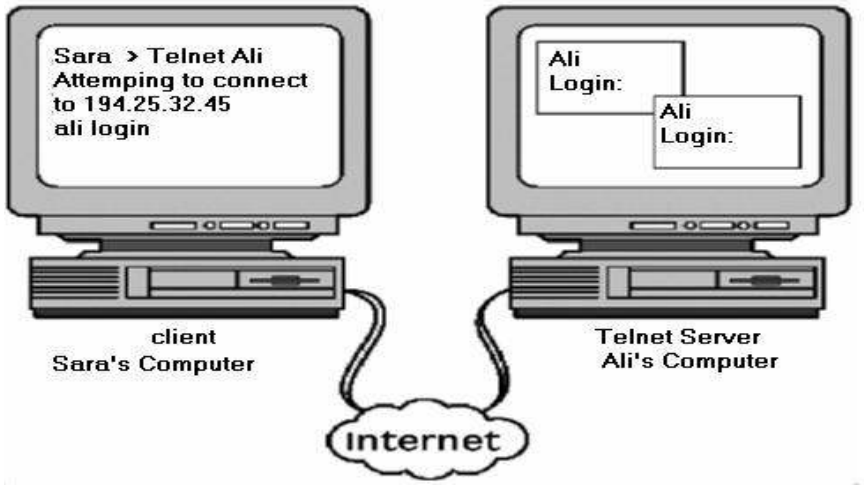
- پروتکل TELNET :

یک پروتکل در شبکه است که در انواع شبکه ها از جمله شبکه های محلی و اینترنت کاربرد های فراوان دارد و برای برقراری ارتباطات دو طرفه بین دستگاه ها استفاده می شود.

در واقع بوسیله تلنت شما می توانید به خط فرمان یک سیستم به صورت ریموت دسترسی یابید. این ارتباط به وسیله ی یک ترمینال مجازی ۸ بیتی انتقال دیتا در TCP برقرار می شود. اطلاعات کاربری که ارتباط برقرار کرده به صورت درونی با اطلاعات ارتباط آمیخته خواهد شد. تلنت در سال ۱۹۶۹ ایجاد شد و به زودی توسط IETF استاندارد STD8 – یکی از اولین استاندارد ها در اینترنت- را کسب کرد.

در واقع از تلنت بیشتر در ارتباطات کاربری/سروری – Client /Server استفاده میشود. به صورت پیش فرض این ارتباط از طریق پورت ۲۳ در پروتکل TCP/IP ، پورتی که برنامه تلنت سرور در آن به گوش ایستاده است، برقرار می شود. برای مثال شما قصد برقراری ارتباط از نوع تلنت با سروری را دارید ، برای این کار با برقرار کردن این ارتباط از طریق پورت ۲۳ – که پورتی پیش فرض است- به ورودی تلنت سرور مورد نظر متصل می شوید. برنامه تلنت در سرور که با پروتکل های رسمیت یافته در IETF برنامه ریزی شده است، اجازه های دسترسی شما را بررسی کرده و در صورت لزوم از شما پسورد و نام کاربری را دریافت کرده و سپس خط فرمان یا Shell سرور را در اختیار شما قرار میدهد.

امروزه استفاده از تلنت برای ورود های از را دور با Remote login ، برقراری ارتباط با خدمتی خاص در سرور و کار اشکال یابی مورد استفاده قرار میگیرد. برای مثال در کار اشکال یابی و نگهداری در سرور ها ، شما می توانید با تلنت به سروری خاص مثل یکSMTP سرور متصل شده و با اجرای دستورات و مشاهده پاسخ های سرور به اشکال یابی آن بپردازید. مثلا در همین نوع از سرور ها رله های باز و بسته را مشاهده و به مدیریت آنها بپردازید.



در همین زمینه نرم افزار هایی هم ایجاد شده اند که با برقراری ارتباط های تبادل داده از طریق تلنت امکانات خارق العاده ای را برای ما فراهم می کنند. برای مثال نرم افزار netcat در ویندوز و یونیکس و socat در یونیکس – که نسخه ویندوز آن PuTTY نام دارد- را می توان نام برد.

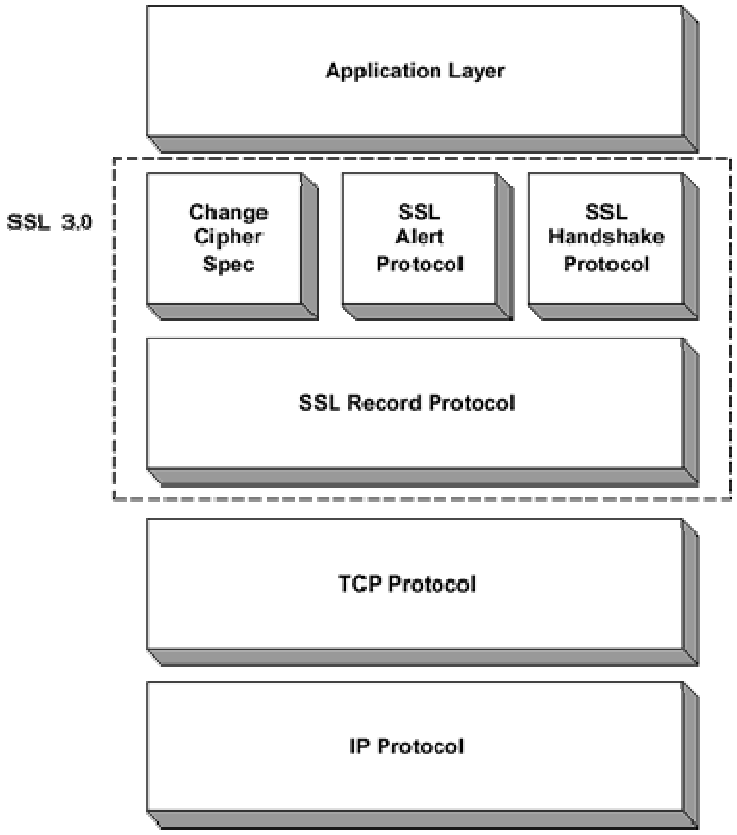
البته استفاده از تلنت فقط به shell گرفتن از سرور محدود نمی شود . شما می توانید با تلنت به هر پورتی از پورت های باز سرور متصل شده و از خدمات آن استفاده کنید. مثلا می توانید به پورت ۳۳۴۶ در سرور شطرنج جهانی متصل شده و به بازی شطرنج بپردازید! حتی همین لحظه در دانشگاه آکسفورد دانشجویان و اساتید از همین روش برای متصل شدن به سرور کتابخانه دانشگاه استفاده می کنند! البته در آن دانشگاه سیستم های نوین تر برای دسترسی به کتاب ها نیز وجود دارد اما اکثر افراد هنوز تلنت را به سیستم های مدرن امروزی تر جیح می دهند.

تا کنون بیش از ۲۰ RFC درباره این پروتکل تدوین شده است.

- پروتکل TLS/SSL :

پروتکل امنیتی لایهٔ انتقال (Transport Layer Security)، بر پایه لایهٔ سوکت‌های امن (Secure Sockets Layer) که یکی از پروتکل‌های رمزنگاری است بنا شده‌است. این پروتکل امنیت انتقال داده‌ها را در اینترنت برای مقاصدی چون کار کردن با پایگاه‌های وب، پست الکترونیکی، نمابرهای اینترنتی و پیام‌های فوری اینترنتی به کار می‌رود. اگرچه TLS و SSL با هم تفاوت‌های اندکی دارند ولی قسمت عمده‌ای از این پروتکل کم و بیش یکسان مانده است.

لایهٔ سوکت‌های امن (Secure Sockets Layer) یا اس‌اس‌ال (SSL) پروتکلی است که توسط شرکت Netscape برای ردّ و بدل کردن سندهای خصوصی از طریق اینترنت توسعه یافته است. SSL از یک کلید خصوصی برای به رمز درآوردن اطلاعاتی که بر روی یک ارتباط SSL منتقل می‌شوند استفاده می نماید. هر دو مرورگر Netscape Navigator و Internet Explorer (و امروزه تمام مرورگرهای مدرن) از این پروتکل پشتیبانی می‌نمایند. هم‌چنین بسیاری از وب‌سایت‌ها برای فراهم کردن بستری مناسب جهت حفظ کردن اطلاعات محرمانهٔ کاربران (مانند شمارهٔ کارت اعتباری) از این پروتکل استفاده می‌نمایند.



طبق آن‌چه در استاندارد آمده است. URLهایی که نیاز به یک ارتباط از نوع SSL دارند با :https به جای :http شروع می‌شوند. SSL یک پروتکل مستقل از لایه برنامه است (Application Independent).بنابراین، پروتکل‌هایی مانند FTP، HTTP و Telnet قابلیت استفاده از آن را دارند. با این وجود SSL برای پروتکل‌های FTP، HTTP و IPSec بهینه شده‌است.

پروتکل TLS به برنامه‌های Client/Server اجازه می‌دهد که در شبکه از طریقی که از Eavesdropping (شنود)، Message Forgery(جعل پیام) جلوگیری می‌کند با یکدیگر ارتباط برقرار

کنند. Authentication TLS (احراز هویت) و Communications Confidentiality (ارتباط مطمئن) در اینترنت را از طریق استفاده از cryptography (رمز نگاری) فراهم می‌کند. برای بهره‌مندی از این پروتکل، سرویس‌دهنده و سرویس‌گیرنده با یک‌دیگر یک قرارداد تبادلی اطلاعات را مذاکره می‌کنند. در خلال این مذاکرات، سرویس‌دهنده و سرویس‌گیرنده بر سر پارامترهای مختلفی که برای برقراری امنیت مورد نیاز است، به توافق می‌رسند

در پیاده‌سازی های نخستین لایه سوکت‌های امن، به علّت محدودیت‌های اعمال شده بر روی صادرات تکنولوژی رمزنگاری از طرف دولت ایالات متحده، از کلیدهای متقارن با طول ۴۰ استفاده می‌شد.

برخی از پروتکل های معمول در لایه انتقال[۲]

- TCP :

TCP از حروف اول کلمات Transmission Control Protocol گرفته شده و یکی از پروتکلهای اصلی در شبکه های مبتنی بر TCP/IP است.

TCP برقرارای ارتباط بین دو هاست و انتقال داده بین اون ها رو برقرار و صحت انجام این کار رو ضمانت می کنه .

TCP در RFC 793 به طور کامل تشریح شده. و سه ویژگی رو برای اون ذکر کرده :

۱. Connection Oriented
۲. Reliable
۳. Stream Oriented

یک پروتکل اتصال گرا (Connection Oriented) یعنی قبل از اتقال واقعی داده بین دو هاست باید ارتباط بین آن ها برقرار یا اصطلاحا باز شود. ارتباط به صورت full duplex است یعنی ارسال و دریافت داده ها بر روی یک خط ارتباطی میسر است. همچنین پس از انتقال داده باید این اتصال رو بست تا منابع سیستم آزاد بشه. هر دو هاستی که در دو سمت این اتصال قرار دارند از باز بودن و شروع اتصال و همچنین از پایان آن اطلاع دارند. و انتقال داده ها بدون توافق طرفین اتصال بر برقراری اتصال امکان پذیر نیست.

---

[۲] Transport

Reliable یعنی قابل اعتماد. به این مفهوم که صحت ارسال و دیافت داده ها رو تضمین می کنه.

Stream Orientedیعنی داده ها به صورت رشته ای از بایت ها انتقال می یابند و هیچ چیز قابل مشهود برای مشخص کردن حدود داده وجود ندارد. گیرنده هیچ اطلاعی از چگونگی داده های اولیه که ارسال شده ندارد .ممکن است فرستنده داده را در قالب چندین قطعه کوچک بفرستد و گیرنده تنها یک رشته بزرگ از داده ها را دریافت کند و یا برعکس. فرستنده یک رشته طولانی از داده ها را ارسال کند ولی در آن سمت گیرنده چند قطعه کوچک از داده ها را دریافت کند.تنها چیزی که در این میان اهمیت داره و گارانتی میشه ارسال و دریافت داده ها بدون هیچ خطائی است .که اگر هم خطائی رخ دهد با تقاضای ارسال مجدد داده ها در واقع خطا برطرف می شود.

ایزوله کردن این سرویس ها در سطح یک لایه، به برنامه های کاربردی ما این امکان رو میده که بدون نیاز به کنترل خطا ها و در نظر گرفتن اونها طراحی و پیاده سازی بشه.

- UDP

UDP از حروف اول کلمات User Datagram Protocol گرفته شده و یک پروتکل غیر اتصال گرا (Connectionless) است که مثل TCP در بالاترین لایه اجرا می شود. برخلاف TCP در پروتکل UDP امکان بروز خطا وجود دارد.

تشریح کامل آن در RFC 768 آمده. یک ارتباط غیراتصال گرا بین دو هاست برقرار می کنه و هر بسته از داده کاربر و کمترین میزان سرایند تشکیل شده که به آن UDP دیتاگرام گفته می شود.

UDP غیراتصال گرا است .یعنی یک دیتاگرام در هر لحظه ای میتونه ارسال بشه ، بدون نیاز به هر گونه اعلام قبلی، مذاکره و یا هیچ آماده سازی از قبل.فقط داده رو ارسال می کنه و امیدواره که گیرنده داده ها رو دریافت کنه.

یک ارتباط غیرقابل اعتماد ایجاد می کنه . یعنی هیچ تضمینی برای اطمینان از تحویل داده ها در مقصد وجود ندارد. نه تنها هیچ اطمینانی از رسیدن داده ها به مقصد وجود نداره بلکه حتی به صحت و درستی داده هائی که به مقصد رسیده هم نمیشه اطمینان داشت. ممکنه بسته ای رو دو بار دریافت کنیم!! برنامه ما که بر اساس این پروتکل کار میکنه باید آمادگی مواجه شدن با تمام این موقعیت ها رو داشته باشه: از دست دادن دیتاگرام ، دیتاگرام تکراری و یا دریافت دیتاگرام با ترتیب غلط.

مهمترین محاسن UDP اینه که محدوده داده ها در ان مشخص شده ، در ارسال های broadcast میشه از این پروتکل استفاده کرد و همچنین سریعه.

و مهمترین معایب غیرقابل اعتماد بودن آن و در نتیجه پیچیده بودن برنامه نویسی در سطح لایه application است.

مقایسه‌ی دو پروتکل TCP و UDP

آدرس دهی

TCP و UDP از یک مدل آدرس دهی استفاده می کنند : یک آدرس IP و شماره پورت مورد نظر

آدرس IP برای هدایت بسته به هاست منظور در شبکه ی مشخص شده و شماره پورت برای هدایت به پروسه منتظر. معمولا یک پورت برای یک برنامه اختصاص داره.

محاسن TCP

سیستم عامل همه کار رو برای شماانجام میده. دیگه باگهای ابتدائی که هر کس در اولین کارش با اون ها روبرو میشه رو مرتکب نمیشید. برای اینکه تمام این ها برای ما توسط سیستم عامل انجام و رفع شده.

کارهائی که سیستم عامل برای دریافت و ارسال بسته های TCP انجام میده نیازی به سوئیچ کردن مود کرنل به مود کاربر نداره. چون اغلب کارها مثل اسمبل کردن مجدد بسته های رسیده، پاسخ مبنی بر دریافت بسته ها (ACK) ، گزارش خطاها،و... توسط کرنل انجام می شود.

TCP سه چیز رو برای شما گارانتی میکنه : داده های ما به مقصدبرسه ، داده ها با ترتیب صحیحی برسه ، داده ها بدون تکرار در مقصد دریافت شود.

مسیریاب ها در مواجهه با بسته های TCP رفتارهای خاص متناسب رو انجام میدن . مثلا در صورت لزوم می تونند تقاضای ارسال مجدد بسته کنند.

محاسن UDP

محدود و ملزم به رعایت از مدل ارتباطی connection oriented نیستیم.

کنترل خطاها، پاسخ به فرستنده (ACK) و... به برنامه بستگی داره و ما به عنوان برنامه نویس ویژگیهائی را که نیاز داریم پیاده سازی و استفاده می کنیم.

انتقال های broadcast و multicast در UDP امکان پذیره.

معایبTCP

TCP ویژگیهای فوق العاده ای رو برای شما فراهم می کنه که شاید خیلی از اونها رو نیاز نداشته باشید. در نتیجه برای کار شما، پهنای باند و یا زمان رو هدر میده و بیخود صرف می کنه.

در TCP داده ها هیچ محدوده ای مشخص نشده و ما باید خودمان محدوده داده را مشخص کنیم.

TCP برای انتقال های broadcast و یا multicast نمیتونه مورد استفاده قرار بگیره.

معایب UDP

با وجود UDP هیچ گارانتی وجود نداره. ممکنه بسته ای تحویل مقصد داده شه ، یا دو بار داده بشه و یا اینکه به ترتیب تحویل داده نشه. و با بروز هریک از این خطاها ما متوجه نمیشویم، مگر اینکه برنامه ای که به داده ها گوش می دهد، در صورت بروز هر یک از خطا ها بخواهد کاری انجام دهد. UDP برای خطاهای احتمالی هیچ گونه مکانیزمی ندارد و پیاده سازی کشف و رفع خطاها به عهده برنامه نویس است.

برخی از پروتکل های معمول در لایه شبکه[۳]

- پروتکل IP :

یک پروتکل بدون اتصال است و تمام کارها در مدل TCP/IP مبتنی بر این پروتکل IP میباشد این پروتکل آدرس وسیله میزبان و وسائل شبکه را برای بر قراری ارتباط فراهم میکند .

پروتکل IP (برگرفته از Internet Protocol) یکی از اعضاء خانواده پروتکل TCP/IP است که در لایه شبکه فعالیت می نماید . از پروتکل فوق به منظور انتقال دیتاگرام (datagram) بین کامپیوترها استفاده می گردد . دیتاگرام از یک هدر و فیلد داده تشکیل می گردد . هر هدر دیتاگرام شامل آدرس مقصد است (اطلاعات مورد نیاز برای توزیع دیتاگرام به مقصد مورد نظر) . بدین ترتیب ، امکان ارسال هر دیتاگرام به صورت جداگانه وجود خواهد داشت . دیتاگرام هائی که دارای یک session می باشند می توانند از مسیرهای مختلفی ارسال گردند . بدیهی است در چنین مواردی همواره این احتمال وجود خواهد داشت که دیتاگرام ها با همان اولویتی که ارسال شده اند به مقصد مورد نظر نرسند و با توجه به شرایط موجود ، اولویت دریافت آنها در مقصد متفاوت از اولویت ارسال در مبداء باشد .

هر اینترفیس شبکه در شبکه های داخلی بزرگ دارای یک و یا چندین آدرس IP منحصربفرد است . یک اینترفیس شبکه می تواند دارای یک و یا چندین آدرس IP باشد ولی یک آدرس IP نمی تواند به چندین اینترفیس شبکه نسبت داده شود .

---

[۳] Network

- پروتکل ICMP:

(ICMP) Internet Control Message Protocol، امکانات لازم در خصوص اشکال زدائی و گزارش خطاء در رابطه با بسته های اطلاعاتی غیرقابل توزیع را فراهم می نماید. با استفاده از ICMP ، کامپیوترها و روترها که از IP بمنظور ارتباطات استفاده می نمایند ، قادر به گزارش خطاء و مبادله اطلاعاتی محدود در رابطه وضعیت بوجود آمده می باشند. مثلا" در صورتیکه IP ، قادر به توزیع یک بسته اطلاعاتی به مقصد مورد نظر نباشد ، ICMPیک پیام مبتنی بر غیرقابل دسترس بودن را برای کامپیوتر مبداء ارسال می دارد. با اینکه پروتکل IP بمنظور انتقال داده بین روترهای متعدد استفاده می گردد ، ولی ICMPبه نمایندگی از TCP/IP، مسئول ارائه گزارش خطاء و یا پیام های کنترلی است . تلاش ICMP ، در این جهت نیست که پروتکل IP را بعنوان یک پروتکل مطمئن مطرح نماید ، چون پیام های ICMP دارای هیچگونه محتویاتی مبنی بر اعلام وصول پیام (Acknowledgment) بسته اطلاعاتی نمی باشند ICMP . ، صرفا" سعی در گزارش خطاء و ارائه فیدبک های لازم در رابطه با تحقق یک وضعیت خاص را می نماید.