بسمه تعالی

فاز اول پروژه تحقیقاتی مهندسی اینترنت

پروتکل‌های معمول اینترنت (و پروتکل‌های لایه کاربرد)

فاطمه آرزومند/ ۸۶۲۱۳۰۰۶

فهرست

HTTP -1

یک پروتکل با معماری سرویس‌دهنده- سرویس‌گیرنده است که مسئولیت ارتباط بین سرویس‌گیرندگان و سرویس‌دهندگان وب را برعهده دارد.

HTTP (Hypertext Transfer Protocol) این پروتکل که به وسیله مرورگرهای اینترنت نشان داده می شود، شبکه ای است که شما را به میزبان مرتبط می کند و با توجه به اطلاعاتی که درخواست کرده اید نتایج را نشان می دهد. با استفاده از این پروتکل می توانید فایلهای مورد نیاز خود را دریافت یا مبادله کنید. اصولاً آدرسهای اینترنتی در هر پروتکل به وسیله URL نمایش داده می شوند، آدرسهایی که درون این پروتکل قرار دارند به صورت زیر می باشدhttp://www.site.domain:که در ابتدا بعد از http دو نقطه و یک اسلش قرار می گیرد سپس نام سایت را ذکر می کنیم. اگر www را وارد کنیم صفحه اصلی سایت نشان داده می شود اما در بعضی از سایتها که به چند صفحه دیگر تقسیم می شوند بجای www می توان از کلمه دیگری که سایت به آن پیوند داده شده است استفاده کرد. لازم به ذکر است که اگر سایتی دارای چند صفحه باشد آن را به دو صورت زیر می تواند بسازد، یکی آنکه بجای www نام صفحه مورد نظر را بیاورد و دیگر آنکه بعد از نام اصلی سایت از یک اسلش استفاده کند و بعد از آن صفحه مورد نظر را بیاورد، مانند: http://mail.yahoo.com بعد از نام سایت دامین می آید، دامین ها کلمات مشخصی هستند که عبارتند از Comو Org و Net و Co و Gov همینطور هر کشور دامین مختص خود را دارد برای مثال دامین کشور ایران ir و امریکا us می باشد.

یک راه بسیار رایج برای دستیابی به اطلاعات که همگی با آن آشنا هستیم استفاده از سرویس HTTP است. همانند FTP ، این سرویس از دو بخش تشکیل شده :

الف) Client HTTP : که به Web Client، Web Browser یا به اختصار Browser هم مشهور است .

ب) HTTP Server : که به Web server نیز معروف است .

کاربران نرم افزار HTTP Client را (مانند ,Netscape Fire Fox, IE و ...) اجرا کرده و درخواست دسترسی به اطلاعات یا حتی اجرای برنامه را به سرور ارسال می کنند(Request HTTP). سرور این درخواست را بررسی کرده و پس از آماده کردن پاسخ ، آن ها را در قالب خاصی معروف به Web page به سمت Client ارسال می کند . سرویس گیرنده این صفحات را دریافت کرده و با فرمت مناسب به کاربر نشان می دهد .

تولید و توسعه این پروتکل به عهده دو موسسه کنسرسیوم وب جهانگستر می باشد. این دو موسسه با یکدیگر در نشر مستندات RFC همکاری می کنند، مانند RFC 2616 که استاندارد HTTP 1.1 نسخه جاری این پروتکل در آن آمده است.

تاریخچه

در اواسط ۱۹۹۷ میلادی تمام سرویس‌دهنده‌ها و سرویس‌گیرنده‌های وب براساس HTTP/1.0 کار می‌کردند. در اوایل ۱۹۹۷ همه سرویس-دهنده‌ها و سرویس‌گیرنده‌های وب شروع به اجرای HTTP/1.1 کردند. توجه شود که سرویس‌دهنده‌های وب HTTP/1.1 می‌توانند با مرورگرهای HTTP/1.0 اتصال برقرار کنند و مرورگرهایی که HTTP/1.1 را اجرا می‌کنند، می‌توانند با سرویس‌دهنده‌های وبی که HTTP/1.0 را اجرا می‌کنند اتصال برقرار کنند.

SSH-2

تاریخچه

در سال ۱۹۹۵ محققی به نام «تاتو یلونن» که در دانشگاه هلسینکی فنلاند تحصیل می‌کرد، اولین نسخه از پروتکل SSH را با نام SSH-1 ارائه کرد. هدف پروتکل SSH این بود که جایگزینی برای پروتکل‌های rlogin، telnet، rsh باشد زیرا این پروتکل‌ها قادر نبودند ارتباطی مطمئن و قابل اعتماد را فراهم کنند. تعداد کاربران این پروتکل در اواخر سال ۱۹۹۵ به سرعت رشد کرد. یلونن سپس در جهت بهبود و ارتقای امنیت این پروتکل گام برداشت و نسخه SSH-2 را منتشر کرد. نسخه ابتدایی پروتکل SSH به صورت آزاد ارائه شد اما انتشارهای بعدی آن جزو نرم‌افزارهای اختصاصی قرار گرفت. در سال ۱۹۹۹ برنامه‌نویسان، خواهان نسخه‌ای آزاد از این نرم‌افزار شدند و به همین دلیل به سراغ نسخه‌ای از پروتکل SSH رفتند که دارای مجوز متن‌باز بود. «جورن گرانوالز» سورس کد پروتکل SSH را توسعه داد و آن را OSSH نامید. بعد از آن برنامه‌نویسان OpenBSD رو سورس کد OSSH کار کرده و OpenSSH را ایجاد کردند. به مرور این پروتکل در سیستم‌های-عامل جایگاهی برای خود باز کرد و در سال ۲۰۰۵، OpenSSH از محبوبیت بیشتری نسبت به SSH برخوردار شد و در این میان OSSH مطرود گردید.

کاربردها

اتصال به نشست ترمینال در سیستم راه دور (جایگزین Telnet، rlogin)

اتصال به نشست گرافیکی در سیستم راه دور

اجرای دستور در سیستم راه دور (جایگزین rsh)

انتقال‌داده‌ها میان پایانه‌ها

قابلیت فشرده‌سازی اطلاعات در حین انتقال، برای بهبود ترافیک باند

احراز هویت به وسیله کلید عمومی (جایگزین سبک رمز عبور)

ایجاد پروتکل SFTP از ترکیب پروتکل‌های SSH و FTP برای انتقال مطمئن داده‌ها

ترکیب آن با پروتکل rsync برای ایجاد فایل‌های پشتیبان به صورت امن

مدیریت و خودکارسازی ثبت وقایع در سیستم راه دور

سوار کردن پوشه از سیستم راه دور

پروتکل SSH ابزاری برای مدیریت و دسترسی به شبکه از راه دور است. این پروتکل، داده‌ها را به صورت رمزشده میان دو میزبان انتقال می-دهد. پروتکل SSH ابتدا برای سیستم‌های عامل یونیکس و لینوکس ساخته شد تا جایگزینی برای Telnet و دیگر ابزارهای ناامن راه دور باشد. پروتکل‌های قدیمی از سازوکارهای امنیتی استفاده نمی‌کردند و هر شخصی به راحتی با شنودکردن، به اطلاعات بسیار ارزشمندی مانند نام کاربری و کلمه عبور راه دور دست یابد.

پروتکل SSH با رمزکردن اطلاعات در حین انتقال، مانع استراق‌سمع توسط دیگران می‌شود. درواقع این پروتکل یک تونل ارتباطی رمزشده میان دو میزبان به وجود می‌آورد تا داده‌ها تبادل شوند. بنابراین حتی در صورت به‌دست‌آوردن اطلاعات میان این دو میزبان، امکان بهره‌برداری از آن‌ها وجود ندارد. با پروتکل SSH می‌توان امنیت ارتباط را در سراسر یک شبکه ناامن (مانند اینترنت) فراهم کرد.

پروتکل SSH در دو مدل سرویس‌دهنده SSH و متقاضی SSH استفاده می‌شود. سرویس‌دهنده SSH به طور معمول به درگاه ۲۲ استاندارد TCP گوش می‌کند و در مقابل، متقاضی SSH برنامه‌ای برای اتصال یک سیستم راه دور فراهم می‌کند. این برنامه‌ها اکثراً روی همه‌ی

سیستم‌های‌عامل وجود دارد. استفاده از پروتکل SSH فقط از طریق خط فرمان امکان‌پذیر است حتی در سیستم‌های‌عامل Mac و Windows.

پروتکل SSH ابزاری مناسب برای اتصال دو میزبان در شبکه است. این پروتکل امنیت کامل را در یک ارتباط فراهم می‌کند. در حال حاضر این پروتکل در سیستم‌های‌عامل مبتنی بر یونیکس توسط OpenSSH و در سیستم‌های‌عامل ویندوزی با نرم‌افزار PuTTY پیاده‌سازی می‌شود.

SMTP -3

SMTP = Simple Mail Transfer Protocol

E-mail(Electronic mail) از این پروتکل برای فرستادن و دریافت نامه استفاده می شود .برای استفاده از این سرویس می توانید از برنامه هایی مانند outlook استفاده کنید که در این صورت به پروتکلی که این برنامه از آن استفاده می کند POP (Post Office Protocol)نام خواهد گرفت، همینطور می توانید از (Microsoft SMTP (Simple Mail Transfer Protocol استفاده کنید یا اینکه با استفاده از خدمات یک سایت نامه خود را فرستاده یا دریافت کنید.برخی از سایتهای معتبر ایمیل عبارتند از: Yahoo,Gmail,Hotmail,AOL,...ساختار آدرسهای ایمیل به صورت زیر می باشد name@site.domain :در قسمت اول نامی به دلخواه ساخته می شود و بعد از آن از علامت @ استفاده می شود، در قسمت بعد هم نام سایتی که ایمیل در آن ساخته شده همراه با دامین می آید.

پروتکل SMTP ارسال 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 TCP بین سرویس‌گیرنده و سرویس‌دهنده SMTP برقرار می‌شود. سپس، سرویس-گیرنده 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 پست الکترونیکی گیرنده تحویل داده یا در صورت لزوم آن را برای تحویل به گیرنده، به سرویس‌دهنده‌ی دیگر ارسال نماید.

این سرویس، اتصال غیرهم‌زمان را برای افراد پدید می‌آورد. بدین معنا که افراد هر زمان مایل باشند می‌توانند اقدام به ارسال و یا مطالعه‌ی نامه‌های خود نمایند، بدون این‌که نیاز باشد این اعمال را با زمان و برنامه‌ریزی دیگران منطبق کنند. هنگامی‌که یک نامه‌ی الکترونیکی ارسال می‌شود، انتظار این است که سرویس‌دهنده‌ی پست الکترونیکی، آن نامه را به درستی به مقصد ارسال نماید. مراحل ارسال بدون توجه به سخت‌افزار و نرم‌افزار و تنها با استفاده از پروتکل‌های انتقال پست الکترونیکی انجام می‌شود.

پس از این‌که یک نامه الکترونیکی، به کمک پروتکل SMTP از سرویس‌دهنده‌ی پست الکترونیکی فرستنده به سرویس‌دهنده‌ی پست الکترونیکی گیرنده منتقل شد، به صندوق نامه‌های الکترونیکی گیرنده منتقل می‌شود. روش‌های مختلفی برای دسترسی به نامه‌های الکترونیکی وجود دارد. تا اوایل دهه‌ی ۱۹۹۰ میلادی، اتصال از طریق Telnet و سپس اجرای یک برنامه‌ی متنی پست الکترونیکی مثل Elm، روش استانداردی برای دسترسی به نامه‌های الکترونیکی محسوب می‌شد. اما امروزه کاربران، از طریق یک سرویس‌گیرنده‌ی پست الکترونیکی که بر روی رایانه‌ی شخصی، خانگی، اداری و یا قابل حمل خود نصب می‌کنند، به نامه‌های الکترونیکی دسترسی پیدا می‌کنند. کاربران با اجرای چنین نرم‌افزارهایی بر روی رایانه‌ی شخصی خود از مزایای زیادی مانند نمایش نامه‌های الکترونیکی چندرسانه‌ای به همراه پیوست‌ها برخوردار می‌شوند. از جمله‌ی این نرم‌افزارها می‌توان به Mozilla Thunderbird، Microsoft Outlook، Eudora و Netscape Messenger اشاره کرد. این نرم‌افزارها از پروتکل‌های استاندارد محیط اینترنت مثل POP و IMAP استفاده می‌کنند.

POP

یکی از پروتکل‌های استاندارد اینترنت و یک پروتکل سرویس‌گیرنده/ سرویس‌دهنده محسوب می‌شود. این پروتکل در لایه‌ی کاربردی فعالیت کرده و از درگاه شماره ۱۱۰ برای گفتگو استفاده می‌کند. سرویس‌گیرندگان پست الکترونیکی می‌توانند از این پروتکل به منظور دریافت نامه-های الکترونیکی از یک سرویس‌دهنده‌ی راه دور استفاده کنند.

POP3 از توسعه‌ی نسخه‌های قدیمی و منسوخ POP1 و POP2 (به طور غیررسمی به این اسامی معروفند) ایجاد شده است. شبیه به بسیاری از پروتکل‌های قدیمی اینترنت، POP3 نیز در ابتدا تنها از سازوکارهای ورود رمزنشده پشتیبانی می‌کرد. اگرچه در پروتکل POP3، هنوز هم به طور معمول انتقال بدون رمزنگاری کلمه‌ی عبور انجام می‌شود، اما POP3 هم‌اکنون از چندین روش احراز هویت به منظور جلوگیری از دسترسی‌های غیرمجاز به نامه‌های الکترونیکی پشتیبانی می‌کند. در یکی از این روش‌ها که APOP نام دارد، از تابع درهم‌سازی MD5 برای جلوگیری از حملات پاسخ و افشای اطلاعات پنهان به اشتراک‌گذاشته‌شده استفاده می‌شود. از جمله سرویس‌گیرندگان پست الکترونیکی که از APOP استفاده می‌کنند می‌توان به Mozilla Thunderbird، Opera، Eudora، KMail، Novell Evolution، Windows Live Mail، PowerMail و Mutt اشاره کرد. سرویس‌گیرندگان پست الکترونیکی همچنین می‌توانند به وسیله‌ی قابلیت AUTH از روش احراز هویت SASL نیز پشتیبانی کنند. همچنین سرویس‌گیرندگان پست الکترونیکی می‌توانند به کمک TLS یا SSL اقدام به رمزنگاری ارتباطات POP3 نمایند.

IMAP

این پروتکل در سال ۱۹۸۶ میلادی توسط Mark Crispin به عنوان یک پروتکل دسترسی راه دور به صندوق پست الکترونیکی طراحی گردید. این پروتکل سابق بر این به اسامی Internet Mail Access Protocol، Interactive Mail Access و Interim Mail Access Protocol مشهور بوده است. IMAP نیز یکی از پروتکل‌های استاندارد اینترنت و یک پروتکل سرویس‌گیرنده/ سرویس‌دهنده محسوب می‌شود. این پروتکل در لایه‌ی کاربردی فعالیت کرده و از درگاه شماره ۱۴۳ برای گفتگو استفاده می‌کند. از نسخه‌های قدیمی‌تر این پروتکل می‌توان به IMAP2bis، IMAP2، IMAP4 اشاره کرد. آخرین نسخه‌ی این پروتکل IMAP4rev1 (بازنگری اول) می‌باشد.

تفاوت اساسی میان POP3 و IMAP4 این است که نوع دسترسی در پروتکل POP3 دسترسی به نامه‌ی الکترونیکی رها شده می‌باشد. حتی اگر سرویس‌گیرنده‌ی پست الکترونیکی، بعضی و یا همه‌ی نامه‌های الکترونیکی را بر روی سرویس‌دهنده رها کند، صندوق نامه‌های الکترونیکی سرویس‌گیرنده، معتبر و موثق محسوب می‌شود. درمقابل، نوع دسترسی در پروتکل IMAP4 دسترسی به صندوق نامه‌های الکترونیکی می‌باشد. در این حالت سرویس‌گیرنده ممکن است از نامه‌های الکترونیکی بر روی سرویس‌دهنده نمونه‌برداری کرده و آن‌ها را در صندوق نامه‌های الکترونیکی سرویس‌گیرنده ذخیره کند، ولی این عملیات از نگاه پروتکل، یک ذخیره‌سازی موقتی محسوب می‌شود و در واقع صندوق نامه‌های الکترونیکی سرویس‌دهنده، معتبر درنظر گرفته می‌شود.

پروتکل نامه پستی امکان کنترل و دسترسی به پست الکترونیک را فراهم می آورد.

مشترکان با این پروتکل می توانند موضوعات پیغام را مرور نمایند ، فایلهای پست الکترونیکی و پیغامها را ایجاد و حذف نمایند و لازم نیستمرسوله پستی را بر روی کامپیوترشان فعال نمایند.

پرتکل معروف دیگر POP3 می باشد. با این پروتکل ، مرسوله پستی در هنگام دسترسی، بر روی کامپیوتر شخصی فعال می شود ، و از روی سرویس دهنده حذف می گردد.

هیچ یک از دو پروتکل را نباید با SMTP اشتباه گرفت ، پروتکل انتقال برای پست الکترونیکی بین دو سایت لازم است که IMAP یا POP3را برای خاندن پست الکترونیکی داشت تا بتوان در هنگام دریافت پست الکترونیکی آنرا خواند.

پروتکلی است که از طریق آن می‌توان به فایل‌ها، چاپگرها و سایر منابع پایدار شبکه که به اشتراک گذاشته‌شده‌اند، دسترسی پیدا کرد. این پروتکل که برای اولین بار در سال ۱۹۸۳ توسط شرکت Sun ارائه شد، تا به حال تغییرات زیادی پیدا کرده است و آخرین نسخه آن نسخه شماره ۴ می‌باشد. این پروتکل بیشتر در سیستم‌های‌عامل خانواده Unix کاربرد داشته و گسترش یافته‌است. در NFS عملیات دسترسی به فایل و ابزار مشترک با رد و بدل یک سری پیغام در هر دو سوی سرویس‌دهنده و سرویس‌گیرنده NFS صورت می‌گیرد.

NFS یک فایل سیستم کامپیوتری است که از به اشتراک گذاشتن فایل‌ها، چاپگرها و سایر منابع به عنوان منابع پایدار بر روی شبکه‌های کامپیوتری حمایت می‌کند. اولین سرویس‌گیرندگان فایل در دهه‌ی ۷۰ میلادی توسعه داده شدند. در سال ۱۹۸۳ شرکت Sun فایل سیستمی به نام NFS را ایجاد کرد که بعدها به پراستفاده‌ترین فایل سیستم شبکه‌ای تبدیل شد. NFS همانند سایر پروتکل‌ها براساس سیستم ONC RPC ساخته‌شده است. فایل سیستم شبکه‌ای یک استاندارد بازتعریف‌شده در RFCها می‌باشد، به طوری‌که اجازه پیاده‌سازی پروتکل را به هرکسی می‌دهد. سایر فایل سیستم‌های شبکه‌ای قابل توجه عبارتنداز AFS، NCP و SMB که به عنوان CIFS نیز شناخته می‌شود.

مزیت‌های استفاده از NFS

به علت اینکه اطلاعات مشترک می‌توانند بر روی یک ماشین ذخیره‌شده و از طریق سایر ماشین‌ها در شبکه‌ی محلی مورد دسترسی واقع شوند، بنابراین پایانه‌های کامپیوتری محلی از فضای دیسک کمتری لازم است استفاده کنند.

کاربران نیازی ندارند که دایرکتوری خانگی مجزایی بر روی هر کامپیوتر شبکه داشته‌باشند. دایرکتوری‌های خانگی می‌توانند در سرویس‌دهنده NFS برپا شوند و از طریق شبکه در دسترس باشند.

ابزارهای ذخیره‌سازی همچون دیسک‌های فلاپی، درایوهای CDROM و درایوهای ZIP توسط سایر ماشین‌ها قابل دسترس هستند. این ویژگی باعث کاهش تعداد ابزارهای جانبی ذخیره‌سازی در شبکه می‌گردد.

نسخه‌های مختلف NFS

نسخه اولیه NFS

جزییات پیاده‌سازی NFS در RFC 1094 آمده است. شرکت Sun از نسخه ۱ تنها برای اهداف آزمایشی و تحقیقاتی استفاده کرد. پس از اعمال تغییرات اساسی در نسخه ۱، تیم تحقیقاتی Sun تصمیم به انتشار نسخه جدید با عنوان نسخه ۲ کرد.

نسخه ۲ از NFS

نسخه ۲ از این پروتکل (تعریف‌شده در RFC 1094 در مارس ۱۹۸۹) در اصل به طور کامل بر روی پروتکل UDP اجرا شد. طراحان این نسخه این پروتکل را stateless نگه داشتند.

نسخه ۳ از NFS

نسخه ۳ از پروتکل NFS (RFC 1813، ژوئن ۱۹۹۵) ویژگی‌های زیر را به NFS افزود:

پشتیبانی از آفست‌ها و اندازه فایل‌های ۶۴ بیتی به منظور مدیریت فایل‌های با اندازه بزرگتر از ۴ گیگابایت (GB).

پشتیبانی از نوشتن غیرهمزمان بر روی سرویس‌دهنده به منظور بهبود کارایی نوشتن.

افزایش تعداد صفات فایل‌ها در بسیاری از کپی‌ها برای جلوگیری از واکشی دوباره آن‌ها.

افزودن عملگر READDIRPLUS برای اینکه در هنگام پویش یک دایرکتوری بتوان صفات و دستگیره فایل‌ها را به همراه نام فایل‌ها به دست آورد.

به هنگام ارائه نسخه ۳، پشتیبانی از TCP به عنوان پروتکل لایه انتقال از سوی شرکت‌های مختلف در حال افزایش بود. درحالی‌که بسیاری از شرکت‌ها قبلاً قابلیت پشتیبانی از NFS نسخه ۲ را با TCP به عنوان پروتکل لایه‌ی انتقال فراهم کرده بودند، شرکت Sun در NFS نسخه ۲ همزمان با نسخه ۳ از پروتکل TCP پشتیبانی کرد. با استفاده از TCP به عنوان پروتکل لایه انتقال، پیاده‌سازی NFS بر روی WAN بسیار امکان‌پذیرتر گشت.

نسخه ۴ از NFS

نسخه ۴ (RFC 3010، دسامبر ۲۰۰۰، بازبینی شده در RFC 3530 در آپریل ۲۰۰۳) در واقع تحت تأثیر AFS و CIFS قرار گرفت. این نسخه علاوه بر این‌که باعث افزایش امنیت نیز شد، باعث بهبودهایی در کارایی نیز گشت. در این نسخه، این پروتکل به یک پروتکل Stateful تبدیل شد. نسخه ۴ اولین نسخه پس از واگذاری حق توسعه پروتکل‌های NFS از سوی Sun بود که توسط IETF توسعه یافت.

FTP -5

یکی از قدیمی ترین پروتکل های اینترنت می باشد که هنوز هم کاربرد زیادی دارد و در سال ۱۹۷۰ در اینترنت توسعه یافت. FTP مخفف **P**rotocol **T**ransfer **F**ile میباشد که یک پروتکل استاندارد در TCP/IP است. 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 سایتها 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 سایتها، 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 . به دو طریق شما می توانید از این پروتکل برای انتقال فایلها استفاده کنید، یکی از راه مرورگر وب خود و دیگری بکارگرفتن نرم افزار مخصوص FTP که به آنها FTP Client می گویند. اما برای دسترسی به محتوای دایرکتوری FTP نیاز به مشخصه کاربری یعنی UserID و کلمه رمز یعنی Password دارید که در هر دو روش باید ابتدا آنها را وارد کنید و پس از تأیید به انتقال فایل بپردازید. ورود به بعضی از دایرکتوری های FTP برای کلیه کاربرها آزاد می باشد و نیازی به وارد کردن مشخصات کاربری نیست که اصطلاحاً آنرا ورود بصورت گمنام یعنی anonymous می گویند که تنها با وارد کردن آدرس ایمیل خود می توانید به آن دایرکتوری دسترسی پیدا کنید. پس از ورود، شما می توانید برای انتقال فایلها از دستوراتی مانند copy paste استفاده کنید تا فایلی را دانلود و یا از سیستم خود به آن کامپیوتر بفرستید یعنی Upload کنید، البته این را در نظر داشته باشید که در بیشتر سایتها شما مجاز به دانلود هستید نه آپلود مگر اینکه آن دایرکتوری متعلق به خود شما باشد تا سطح دسترسی شما اجازه به آپلود فایل هم بدهد.

یکی دیگر از کاربردهای پروتکل FTP ، استفاده طراحان و مدیران وب سایتها برای انتقال محتوای سایتها می باشد که در حال حاضر این افراد بیشترین استفاده را از FTP دارند. زمانی که شما فضایی را برای میزبانی سایت خود از یک شرکت سرویس دهنده اینترنت ISP اجاره می کنید، به شما حداقل یک آدرس FTP می دهند تا عمل انتقال فایلها را از کامپیوتر خود به وب سرور و بالعکس انجام دهید که بهتر است برای امنیت و حفظ فایلها حتماً از یک نرم افزار در این زمینه استفاده کنید. به همین منظور قصد داریم، چگونگی استفاده و انتقال محتویات یک وب سایت از طریق برنامه CuteFTP را برای شما آموزش دهیم تا با بکارگیری این نرم افزار بتوانید به راحتی محتوای سایت خود را منتقل و فایلها را مدیریت کرده و با موفقیت وب سایت خود را راه اندازی کنید.

یکی از قراردادهای TCP/IP که به شما اجازه می دهد تا اطلاعات خود را از کامپیوتر به شبکه بفرستید و یا آنها را دریافت کنید یا اینکه آنها را حذف، به روز، کپی و ... کنید. این سرویس دو نوع است، یکی به صورت رایگان که همه کاربران اجازه استفاده از آن را دارند (مانند ftp://ftp.microsoft.com/) و دیگری که فقط مدیر سایت اجازه استفاده از آن را دارد. در اینترنت میلیونها فایل در FTP قرار دارند که با استفاده از سرویس Archie می توانید به جستجوی آنها بپردازید.

Telnet -6

استفاده از این پروتکل شما قادر به log in به سیستم دیگری هستید و می توانید فایلی را در کامپیوتری دیگر به اجرا برسانید. با استفاده از این سرویس شما می توانید اطلاعات مورد نظر خود را در سایتهای دولتی و ... مشاهده نمایید.

SNMP -7

پروتکل SNMP به منظور اخذ اطلاعات آماری در سیستم‌های مدیریت شبکه استفاده می‌شود.

دو یخش مهم در پروتکل SNMP عبارت‌اند از: مدیریت و Agentهای مدیریت‌شده

پیام تقاضای SNMP از دو بخش زیر تشکیل می‌شود:

سرآیند SNMP که شامل اطلاعات مربوط به ویرایش SNMP، اطلاعات مربوط به اندازه‌ی تقاضا و کلمه‌ی مخصوص

بلوکی از یک یا چند شی تقاضاشده‌ی ترکیبی در بسته‌ی پاسخ

NNTP -8

از پروتکل (Network News Transfer Protocol) NNTP برای پیام هایی که به سایتهای خبری ارسال می گردد استفاده می شود. یکی از سیستمهای رایج این گروه USENET می باشد، که با استفاده از آن آگهی هایی در برخی از سایتها یا ایمیلها یا چت رومها نشان داده می‌شود.

این گروهها که به newsgroup معروفند پیوسته در مورد تمام موضوعها کنفرانسهایی تشکیل می دهند که پیوسته در حال بحث هستند. برای این کار شما برنامه مخصوصی را دانلود می کنید و در مورد موضوع مورد نظر با دیگران صحبت می کنید. بیشتر مرورگرهای تجاری دارای این امکانات هستند.

Gopher -9

با استفاده از این پروتکل شما می توانید اطلاعات دلخواه خود را از درون لیستی پیدا کنید. اطلاعاتی که به صورت فایلها و متنها و ... هستند به فهرستهایی دسته بندی شده اند و با انتخاب آیتم مورد نظر خود به زیر مجموعه های آن دست می یابید و این کار آنقدر ادامه پیدا می کند تا به اطلاعات مورد نظر خود برسید.

JAIN -10

پروتکل JAIN مبتنی بر فناوری JAVA و به صورت یک پروتکل اختصاصی مطرح است که قابلیت تحرک‌پذیری، همگرایی و ایمنی برای دسترسی به شبکه‌های دیتا و تلفنی روی شبکه‌های یک‌پارچه‌شده را فراهم می‌کند.

پروتکل JAIN با فراهم نمودن یک سطح جدید از اینترفیس‌های جاوا برای ایجاد سرویس‌های جدید در شبکه‌ی IP، PSTN و شبکه‌های بی‌سیم، یک‌پارچه‌سازی پروتکل‌های IN و اینترنت را فراهم می‌نماید.

JAIN در سه لایه‌ی اصلی یک شبکه به شرح زیر تأثیر می‌گذارد:

لایه‌ی شبکه

در بخش PSTN: IN/AIN یا SS7 با تأکید بر INAP، ISUP و TCAP

در بخش موبایل: SS7 با MAP

در بخش اینترنت و شبکه‌ی بسته‌ای: MEGACO، MGCP، SIP و H.323

لایه‌ی سیگنالینگ

در بخش PSTN: سوییچ‌ها و یا SSPها

در بخش موبایل: MSCها

در بخش اینترنت و شبکه‌ی بسته‌ای: سافت سوییچ‌ها یا Call Agentها و Media

کنترل‌کننده‌های گیت‌وی یا GateKeeperهای H.323

لایه‌ی سرویس

در بخش PSTN: SCPها

در بخش موبایل: BSCها، HLR، VLR و MSCها

در بخش اینترنت و شبکه‌ی بسته‌ای: سرورهای کاربردها

RTP -11

پروتکل RTP یا پروتکل انتقال بلادرنگ برای حمل سرویس‌هایی که تأخیر زمانی در ارسال آن‌ها نقش حیاتی ایفاد می‌کند، به کار گرفته می‌شود.
پروتکل RTP برای پشتیبانی از حمل صوت و تصویر به صورت بلادرنگ به صورت استاندارد درآمده و در لایه‌ی انتقال نیز معمولاً از پروتکل UDP استفاده می‌کند.

RTP قابلیت رزرو آدرس‌ها را ندارد و QoS را نیز تضمین نمی‌کند.

وظایف RTP عبارت‌اند از:
جمع‌آوری اطلاعات در مورد نوع رسانه (Media)
جمع‌آوری اطلاعات در مورد تعداد مکالمات
جمع‌آوری اطلاعات در مورد شناسایی ارسال‌کننده
هم‌زمانی
آشکارسازی تلفات
تکه‌تکه کردن اطلاعات و جمع‌آوری مجدد آن‌ها
امنیت و رمزنگاری

RTCP -12

این پروتکل مکمل پروتکل RTP بوده و وظیفه‌ی تأمین سرویس‌های کنترلی را بر روی گره‌های موجود در داخل شبکه به عهده دارد.

وظایف مهم این پروتکل عبارت‌اند از:

جداکردن بسته‌های متناسب با شماره‌ی درگاه

تبادل اطلاعات در مورد تلفات و تأخیرها بین دو نقطه‌ی پایانی

امکان ارسال بسته‌ها با فاصله براساس شماره سیستم پایانی و پهنای باند موجود

RSVP -13

RSVP ترافیک رشته‌های IP را اولویت‌بندی کرده و شبکه‌های IP را قادر می‌سازد، صوت را با همان کیفیت سوییچ‌های دیجیتال منتقل کنند.

پیدایش RSVP، VOIP به واقعیت پیوست.

RSVP دارای خصوصیات زیر است:

جهت آن به سمت گیرنده است.

از Unicast و Multicast پشتیبانی می‌کند.

DiffServ -14

DiffServها برخلاف IntServها ترافیک شبکه را به کلاس‌های مختلف دسته‌بندی می‌کنند و به هر کلاس (CoS) پارامترهای QoS را نسبت می‌دهند.

DiffServ از طریق یک الگوی شش بیتی که به اول بسته‌های اطلاعاتی اضافه می‌شوند، نوع سرویس را مشخص می‌کنند.

DiffServ به دو بخش علامت‌گذاری بسته و PHP تقسیم شده است.

هر DiffServ شامل نقاطی برای ورود اطلاعات و نقاطی برای خروج اطلاعات است. این نقاط بعد از دریافت بسته‌ها، DSCP بر روی آن‌ها نوشته و بعد از اعمال PHB مناسب آن‌ها را ارسال می‌کنند و در صورت Congestion آن‌ها را Drop می‌کند.

H.323-15

پروتکل H.323 یک پروتکل استاندارد ITU-T برای صوت، تصویر و تبادل اطلاعات بر روی شبکه‌های مبتنی بر IP از جمله اینترنت است.
پروتکل H.323 به سه بخش کنترلی ذیل تقسیم می‌شود:
پروتکل RAS
Media Control and Transport (H.245) Signaling
Call Control / Call Setup (H.225)

پروتکل RAS بخشی ازتوصیه‌نامه H.323 بوده و پروتکلی است که از آن بین نقاط انتهایی (پایانه‌ها و gatewayها) و Gate Keeperها استفاده می‌شود.
RAS از درگاه UDP-1719 استفاده می‌نماید.
کانال RAS قبل از هر کانال دیگری باز می‌شود و مستقل از کانال برقراری مکالمه و انتقال رسانه است.

پروتکل Q.931 یا H.225
پروتکل Q.931 که به نام H.255 نیز معروف است و برای برقراری اتصال بین نقاط انتهایی H.323 (پایانه‌ها و gatewayها) مورد استفاده قرار می‌گیرد.

پروتکل H.245
از این پروتکل جهت تبادل پیام‌های کنترلی به صورت End to End بین نقاط انتهایی درگیر در یک ارتباط استفاده می‌شود و برای تبادل اطلاعات در موارد زیر به کار می‌رود:
تبادل قابلیت‌ها
کنترل کانال‌های منطقی
پروتکل‌های مربوط به کدکننده‌های تصویری
پروتکل‌های مربوط به کدکننده‌های صوتی
از آن‌جایی که صوت در استاندارد H.323 سرویس پایه است، بنابراین کلیه‌ی پایانه‌های H.323 بایستی حداقل استاندارد G.711 (نرخ بیت 64 Kbit/s) را برای کدکننده‌های صوتی پشتیبانی نمایند.
به‌علاوه استانداردهای دیگری مثل G.722 و G724 (با نرخ بیت 8 Kbit/s) و (G.728 با نرخ بیت G.724) نیز می‌تواند مورد استفاده قرار گیرند.

MGCP-16

MGCP از ادغام پروتکل IPDC و SGCP به وجود آمد، که اهداف هر دو پروتکل را پوشش می‌دهد.

MGCP پروتکلی از نوع Master/slave است که مسؤلیت کنترل gatewayها را به عهده دارد.

MGCP یک پروتکل نسبتاً جدید Client/Server برای سیگنالینگ VOIP است.

MGCP پروتکل ارتباطی بین MGW و MGC به صورت Master/Slave است.

SigTran -17

SigTran یکی از گروه‌های کاری IETF است که در سال ۱۹۹۹ تشکیل شد.
این پروتکل در شبکه‌ی NGN از MGC و MG و SG و سرورهای کاربرد و رسانه تشکیل یافته‌است.
جهت انتقال پیام‌های سیگنالینگ شماره‌ی هفت بین SG و MGC از پروتکل فوق استفاده می‌شود.
گروه کاری SigTran، پروتکل SCTP را تعریف کرده است که کمبودهای TCP را برطرف می‌سازد.

BICC-18

از آن‌جایی که هدف از تعریف پروتکل جدید همواره پشتیبانی از سرویس‌های موجود در شبکه‌های PSTN/ ISDN است لذا سازمان ITU-T با الهام گرفتن از پروتکل ISUP و طرح یک پروتکل مشتق‌شده از آن، پروتکل BICC را تعریف و استاندارد کرده است.

پروتکل BICC هم‌چنین توانایی پشتیبانی از مکالمات PLMN را نیز دارا است.

سه فناوری خاص برای انتقال صوت در شبکه‌های دیتا مدنظر پروتکل BICC قرار گرفته‌است که عبارت‌اند از: ATMAAL2، ATM AAL1 و IP.

OSPF -19

بکارگیری پروتکل RIP در شبکه های کامپیوتری بیشتر به دلیل شرایط زمان بوده است .در دهه هفتاد و هشتاد حافظه و پردازندههای سریع ، گران قیمت بودند و پیاده سازی الگوریتمهای مسیریابی مبتنی بر روشهایی نظیر LS که هم به حافظه و هم به پردازندۀ سریع نیاز دارند ، مقرون به صرفه نبود .از طرفی شبکه ها نیز آنقدر توسعه نیافته بودند که نیاز به الگوریتم های بهینه تر احساس شود .با گسترش اینترنت و توسعۀ شبکه های خودمختار در اواخر دهۀ هشتاد ، کاستی های پروتکل RIP نمود بیشتری پیدا کرد و با سریع شدن پردازنده ها و ارزان شدن سخت افزار ، نیاز به طراحی یک پروتکل بهینه ،IETF را واداشت تا در سال1990 ،OSPF را به عنوان یک پروتکل استاندارد ارائه نماید .مسیریابهای زیادی مبتنی بر این پروتکل به بازار عرضه شده اند و احتمال می رود که در آینده تبدیل به مهمترین پروتکل مسیریابی درونی در شبکه های AS شود.

SSL -20

(SSL یا Secure Socket Layer) راه‌حلی جهت برقراری ارتباطات ایمن میان یک سرویس‌دهنده و یک سرویس‌گیرنده است که توسط شرکت Netscape ارایه شده است. در واقع SSL پروتکلی است که پایین‌تر از لایه کاربرد (لایه ۴ از مدل TCP/IP) و بالاتر از لایه انتقال (لایه سوم از مدل TCP/IP) قرار می‌گیرد.

مزیت استفاده از این پروتکل بهره‌گیری از موارد امنیتی تعبیه شده آن برای امن کردن پروتکل‌های غیرامن لایه کاربردی نظیرHTTP، IMAP،LDAP و... می‌باشد که براساس آن الگوریتم‌های رمزنگاری بر روی داده‌های خام (plain text) که قرار است از یک کانال ارتباطی غیرامن مثل اینترنت عبور کنند، اعمال می‌شود و محرمانه ماندن داده‌ها را در طول کانال انتقال تضمین می‌کند.

به بیان دیگر شرکتی که صلاحیت صدور و اعطاء گواهی‌های دیجیتال SSL را دارد برای هر کدام از دو طرفی که قرار است ارتباطات میان شبکه‌ای امن داشته باشند، گواهی‌های مخصوص سرویس‌دهنده و سرویس‌گیرنده را صادر می‌کند و با مکانیزم‌های احراز هویت خاص خود، هویت هر کدام از طرفین را برای طرف مقابل تأیید می‌کند، البته غیر از این‌کار می‌بایست تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گرفت، برای رباینده قابل درک و استفاده نباشد که این‌کار را با کمک الگوریتم‌های رمزنگاری و کلیدهای رمزنگاری نامتقارن و متقارن انجام می‌دهد.

DNS -21

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. زمانی که شما آدرس www.srco.ir را در مرورگر خود تایپ می نمائید ، نام فوق به یک آدرس IP و بر اساس یک درخواست خاص (query) که از جانب کامپیوتر شما صادر می شود ، ترجمه می گردد .

تاریخچه DNS

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 .

پروتکلDNS

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 (WINS (Windows Internet Name Service 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.srco.ir 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 سخاروش است .

DHCP -22

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.

DHCP یک 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.

MGCP-23 (RFC-2705)

این پروتکل که مخفف Media gateway control Protocol می باشد یک پروتکل کنترلی است که برای کنترل درگاههای تلفنی از طرف عناصر خارجی کنترل تماس که درگاه رسانه ای و یا عامل تماس نامیده می شوند ، استفاده می شود . درگاه تلفنی یکی از عناصر شبکه می باشد که سیگنال های سمعی تلفن را به بسته های داده ، که در شبکه اینترنت و یا سایر شبکه های packet switch جابجا می شوند . تبدیل می کند . این پروتکل توسط LETF استاندارد شده است .

MGCP این طور فرض می کند که عناصر کنترل تماس یا عامل های تماس برای فرستادن دستورات منسجم به درگاه های تحت کنترلشان با یکدیگر همزمان خواهند شد . در واقع MGCP یک پروتکل master/salve می باشد که از درگاه ها انتظار دارد که دستوراتی را که توسط عاملهای تماس فرستاده می شوند ، اجرا کنند .

SIP (RFC-2543) , (RFC-3261) -24

پروتکل SIP که مخفف Session Initiation Protocol می باشد ، یک پروتکل لایه کاربرد از نوع پروتکل های علامت دهی برای انتشار تماس های بلادرنگ در شبکه های براساس IP می باشد . این پروتکل وظیفه ایجاد ، اصلاح و خاتمه دادن به جلسات عمدتا از انواع زیر می باشند :

تلفن اینترنتی

کنفرانس های چند رسانه ای

آموزش از راه دور

این پروتکل سیگنالینگی برای کنترل و برقراری مکالمات و نشست‌های چندرسانه‌ای در شبکه‌ی IP توسط IETF تحت RFC.2543 معرفی شده‌است.

پیکره‌ی پیغام SIP توسط پروتکل شرح جلسه (SDP) که به عنوان مثال می‌تواند پیغام‌های ISUP را حمل نماید، تعریف شده‌است.

SIP یک پروتکل براساس تکنولوژی سرویس دهنده - سرویس گیرنده می باشد، که در آن پیام‌ها (پاسخ‌ها و درخواست‌ها) به صورت متنی است؛ هیچ وضعیتی را نگهداری نمی کند و با بکار بردن ساختار پروتکلی ساده ، سرعت عمل ، انعطاف پذیری بیشتری را فراهم می کند در عین حال SIP به هیچ پروتکلی کنترلی خاصی برای کنترل کنفرانس ها وابسته نیست ، بلکه به گونه ای طراحی شده است تا از پروتکل حمل در لایه پایین تر ، مستقل باشد SIP می تواند هم با پروتکل IP4 و هم با IP6 کار کند . SIP برای انتقال داده های بلادرنگ از (RTP RFC-1889) ، برای کنترل تحویل Streaming media از پروتکل RTSP(RFC-2326) و برای رزرو منابع شبکه از پروتکل RSVP RFC-2205)) استفاده می کند.

برای جلسات تلفن اینترنتی SIP به صورت زیر کار می کند :

وقتی یک تماس SIP ایجاد می شود . ابتدا تماس گیرنده مکان سرور مناسب را پیدا می کند و درخواست SIP خود را برای آن می فرستد .

دو طرف تماس با آدرس های SIP تعیین هویت

می شوند . رایج ترین SIP « دعوت » می باشد . پیامهای SIP توسط TCP و یا UDP فرستاده می شوند . پیامهای SIP (پیام درخواست و یا پیام پاسخ) به صورت متنی می باشند و خطوط پیام باید با CR-LF پایان یابد . ساختار نحوی بیشتر پیامها و Header ها شبیه HTTP می باشد .

مقایسه دو پروتکل SIP و H.323

در مقایسه این دو پروتکل باید گفت که به دلایل زیر SIP پروتکل ساده تری نسبت به پروتکل H.323 می باشد :

پیامهای H.323 به صورت باینری می باشد در حالی که پیامهای SIP به صورت

متن است .

SIP پروتکلی ماژولار است در حالی که H.323 خیلی ماژولار نیست .

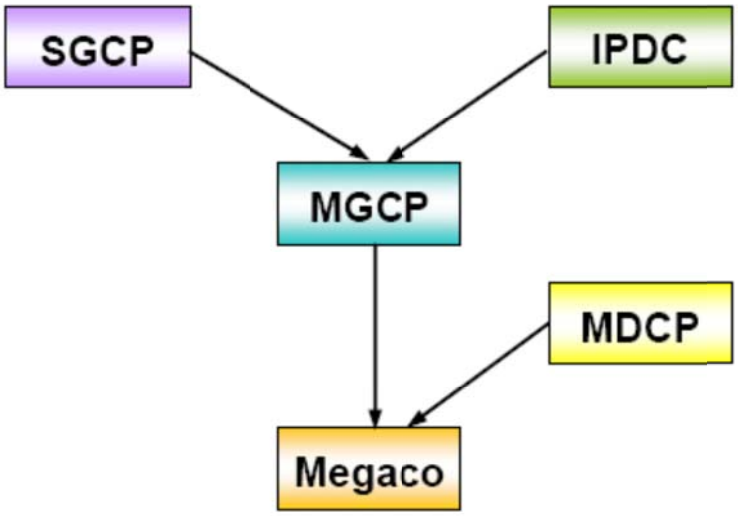
SIP علامت دهی بسیار ساده ای دارد در حالی که علامت دهی H.323 پیچیده است .

SIP فقط ۳۷ عنصر در سر صفحه دارد در حالی که H.323 صدها عنصر دارد .

Megaco/H.248 -25

پروتکل Megaco که مخفف protocol Media Gateway می باشد ، بسیار شبیه پروتکل MGCP می باشد و بین عناصر درگاه های چند رسانه ای که به صورت فیزیکی از هم جدا می باشند استفاده می شود . این پروتکل یک قالب کاری مناسب برای درگاه ها ، واحدهای کنترل چند نقطه ای و واحدهای (IVR Voice Respons Interactive) فراهم می کند . این پروتکل حاصل تلاش مشترک IETF و گروه مطالعاتی ITU-T می باشد . تعریف این پروتکل به صورت متن به همراه توصیه نامه گروه مطالعاتی ITU-T با نام H.248 می باشد.

روند تکامل پروتکل MEGACO به صورت ذیل می‌باشد:



RTP-26 (RFC - 1889)

پروتکل RTP که مخفف Real-time Transport Protocol می باشد ، سرویس هایی برای انتقال داده هایی با ویژگی های بلادرنگ مثل صوت و ویدئو ، فراهم می کند . این سرویس ها عبارتند از :

تعیین نوع payload ، شماره گذاری ترتیبی و stamping time این پروتکل معمولا" به همراه پروتکل UDP برای ارسال داده های خود استفاده می کند .

RTP به تنهایی مکانیزمی برای مانیتور کردن کیفیت سرویس (QoS) ندارد . در واقع کار مانیتور کردن را به عهده پروتکل دیگری به نام (Protocol Real-time Transport Control) نهاده و میزان تضمین کیفیت سرویس بستگی به پروتکل همکار خود در لایه حمل (مانند UDP) دارد . مهمترین ویژگی RTP که منجر به انتخاب این پروتکل توسط برنامه های کاربردی مانند کنفرانس های ویدئویی می شود ، قابلیت ارسال داده به چندین گیرنده در آن واحد می باشد و این دقیقا" همان امکانی است که برای برگزاری کنفرانس های اینترنتی دنبال می شود

RTSP (RFC-2326) **-27**

پروتکل RTSP که مخفف Real-time Streaming Protocol می باشد ، یک پروتکل لایه کاربرد می باشد و برای کنترل روی تحویل جریان داده های بلادرنگ بکار می رود . در واقع این پروتکل برای کنترل روی چندین جلسه تحویل داده طراحی شده است و از UDP و یا TCP در لایه حمل استفاده می کند . این پروتکل از لحاظ ساختار نحوی و عملکرد شبیه پروتکل HTTP 1.1 می باشد ، اما در موارد زیر با HTTP متفاوت است :

RTSP تعدادی متد جدید دارد .

سرور RTSP به صورت پیش فرض وضعیت را حفظ می کند برخلاف ماهیت عدم حفظ وضعیت که از HTTP سراغ داریم .

در RTSP ، سرویس دهنده و سرویس گیرنده هر دو می توانند درخواست بدهند .

RSVP -28 (RCF-2205)

پروتکل RSVP که مخفف Resouree Reservation Protocol می باشد توسط گیرنده برای درخواست کیفیت سرویس (QoS) خاصی از شبکه - برای جریان داده یک برنامه کاربردی - بکار می رود . همچنین این پروتکل توسط روترها برای تحویل درخواست های کیفیت سرویس به همه نودهای مسیر و حفظ این حالت در روترها بکار می رود که این خود منجر به رزرو منابع شبکه در مسیر می شود . هزینه اضافی که بخاطر رزرو منابع ایجاد می شود با افزایش تعداد گیرنده ها به صورت لگاریتمی زیاد می شود . RSVP در بالای پروتکل IP v4 و یا IP v6 کار می کند . این پروتکل بسیار شبیه پروتکل های مسیریابی می باشد ولی نباید تصور کرد که به تنهایی یک پروتکل مسیریاب می باشد ، بلکه با پروتکل های مسیریابی کار می کند.

RVP , RVPCP -29

پروتکل RVP که مخفف Remote Voice Protocol می باشد ، پروتکلی برای انتقال جلسات تلفنی دیجیتال در شبکه های مداری و یا داده ای است . این پروتکل تسهیلاتی برای ایجاد و پیکربندی تماس بین دستگاه سرویس گیرنده و دستگاه سرور و یا سوئیچ تلفن ، فراهم کرده است . RV/IP از TCP برای انتقال داده های کنترلی و از UDP برای انتقال صدا استفاده می کند .

پروتکل کنترلی RVP یا RVPCP ، برای کنترل پیامهایی که ارتباط داده ای بین سرویس گیرنده و سرویس دهنده ایجاد و حفاظت می کنند ، بکار می رود ، پروتکل کنترلی عمدتاً برای برنامه های کاربردی Point-to-point بوجود آمده است و اکثر عملکردهای آن در زمانی که از TCP/IP استفاده می شود غیر ضروری است . در عین یک جلسه RVP/IP فقط یک کلاس از پیامهای کنترلی RVP/IP ردوبدل می شود : RVPCP ADD VOICE (عملیات با کد ۱۲) . این پیام برای فرستادن پورت UDP مورد استفاده سرویس گیرنده به سرور بکار می رود . این پیام همیشه یک پارامتر از نوع RVPCP UDP PORT (نوع با کد ۹) را حمل می کند . سرور در پاسخ یک بسته که شامل پورت UDP سرور برای صوت می باشد ، ارسال می کند . این بسته شامل پیام RVPCP ADD VOICE ACK می باشد .

SDP -30 (RFC-2327)

پروتکل SDP که مخفف Session Deseription Protocol می باشد . جلسات کاری چند رسانه ای را تشریح می کند . در (Mbone (Multicast backbone اینترنت ، ابزار
directory session برای تبلیغ کنفرانس های چندرسانه ای و ابزار آنها و تبادل آدرس کنفرانسها بکار می رود .
پروتکل SDP و به همراه یک متن می باشند . این متن در واقع همان شرح جلسه کاری SDP می باشد . همچنین پیامها می توانند از طریق پست الکترونیکی و یا www ارسال شوند .
پیام متنی SDP شامل موارد زیر است :
نام و هدف جلسه کاری
زمانی که جلسه فعالی شده است
رسانه ای که جلسه در بردارد
اطلاعاتی برای دریافت رسانه (مانند آدرس و غیره)

SGCP -31

پروتکل SGCP (Simple Gateway Control Protocol) برای کنترل درگاه های تلفنی از طریق عناصر کنترل تماس بکار می رود . درگاه تلفنی یکی ازعناصر شبکه می باشد که سیگنال های صوتی را که در مدارهای تلفنی جابجا می شوند ، به بسته های داده ای در اینترنت تبدیل می کند . در واقع این پروتکل حالت ساده پروتکل MGCP می باشد . (فقط ۵ دستور
Connection Delete Connection , Create Connection , Create ،
Notification Request و Notify را با همان عملکرد دارا می باشد) .

Skinny -32 (Cisco protocol)

این پروتکل توسط شرکت Cisco برای کنترل Cisco 7960 و ترمینال VoIP (تلفن) تعریف شده است . پیام های این پروتکل توسط پروتکل TCP و با شماره پورت ۲۰۰۰ حمل می شوند . سایر شرکتها مانند Symbol Tecnologies و SocketIP این پروتکل را در ترمینالها و کنترل کننده های درگاه های خود (Media Gateway) پیاده سازی کرده اند .

IPsec -33

IPSec یا همان Internet Protocol Security عبارت است از مجموعه‌ای از چندین پروتکل که برای ایمن سازی پروتکل اینترنت در ارتباطات بوسیله احراز هویت و رمز گذاری در هر بسته (packet) در یک سیر داده به کار می‌رود. این پروتکل محصول مشترک مایکروسافت و سیسکو سیستمز می‌باشد که در نوع خود جالب توجه است .

مزایا

IPsec بر خلاف دیگر پروتکلهای امنیتی نظیر SSL, TSL, SSH که در لایه انتقال (لایه ۴) به بالا قرار دارند در لایه شبکه یا همان لایه ۳ مدل مرجع OSI کار می‌کند یعنی لایه ای که IP در آن قرار دارد. که باعث انعطاف بیشتر این پروتکل می‌شود به طوری که می‌تواند از پروتکل های لایه ۴ نظیر TCP و UDP محافظت کند. مزیت بعدی IPsec به نسبت بقیه پروتکلهای امنیتی نظیر SSL این است که نیازی نیست که برنامه بر طبق این پروتکل طراحی شود.

کاربرد:

Ipsec معمولا" برای ایجاد و راه اندازی شبکه خصوصی مجازی (VPNs) مورد استفاده قرار می گیرد.

ساختار

خانواده پروتکل IPSec شامل دو پروتکل است: **H**eader **A**uthentication (AH) و **ESP** که هر دوی این پروتکل ها از IPSec مستقل می باشد.

پروتکل AH

بطور خلاصه پروتکل AH در واقع تأمین کننده سرویسهای امنیتی زیر خواهد بود:

- تمامیت داده ارسالی
- احراز هویت مبدا داده ارسالی
- رد بسته‌های دوباره ارسال شده

این پروتکل برای تمامیت داده ارسالی از **HMAC** استفاده می‌کند و برای انجام این کار مبنای کارش را مبتنی بر کلید سری قرار می‌دهد که payload پکت و بخشهایی تغییر ناپذیر سرآیند IP شبیه IP آدرس خواهد بود. بعد از اینکار این پروتکل سرآیند خودش را به آن اضافه می‌کند.

پروتکل AH، 24 بایت طول دارد.

فیلدهای پروتکل AH:

۱. اولین فیلد همان Next Header می‌باشد. این فیلد پروتکلهای بعدی را تعیین می‌کند. در حالت Tunnel یک دیتاگرام کامل IP کپسوله می‌شود بنابراین مقدار این فیلد برابر ۴ است. وقتی که کپسوله کردن یک دیتا گرام TCP در حالت انتقال (Transport Mode) باشد، مقدار این فیلد برابر ۶ خواهد شد

۲. فیلد Payload Length همانطوریکه از نامش پیداست طول Payload را تعیین می‌کند.

۳. فیلد Reserved از دو بایت تشکیل شده است.برای آینده در نظر گرفته شده است.

۴. فیلد security parameter Index یا SPI از ۳۲ بیت تشکیل شده است. این فیلد از SA تشکیل شده که جهت باز کردن پکت های کپسوله شده بکار می‌رود. نهایتاً ۹۶ بیت نیز جهت نگهداری احراز هویت پیام Hash یا (HMAC) بکار می‌رود.

۵. HMAC حفاظت تمامیت دادهء ارسالی را برعهده دارد. زیرا فقط نقاط نظیر به نظیر از کلید سری اطلاع دارند که توسط HMAC بوجود آمده و توسط همان چک می‌شود. چون پروتکل HA حفاظت دیتاگرام IP شامل بخشهای تغییر ناپذیری مثل IP آدرسها نیز هست، پروتکل AH اجازه ترجمه آدرس شبکه را نمی‌دهد. NAT یا ترجمه آدرس شبکه در فیلد IP آدرس دیگری (که معمولاً IP آدرس بعدا می‌باشد) قرار می‌گیرد. وبه این جهت تغییر بعدی HMAC معتبر نخواهد بود. در شکل زیر حالتهای انتقال و تونل در پروتکل AH به نمایش در آمده است.همان طور که می بینید این پروتکل در این دو حالت ارتباط امن بین دو نقطه انتهائی که در دو شبکه مجزا قرار دارند را فراهم می‌آورد ،همچنین ارتباط امن بین دو نقطه در یک شبکه داخلی و یک نقطه انتهائی و یک مسیر یاب یا حفاظ دیواره آتش (Firewall) را ممکن می سازد.

پروتکل Encapsulation Security Payload (ESP)

پروتکل ESP سرویسهای امنیتی زیر را ارائه می‌کند:

- محرمانه بودن
- احراز هویت مبدا داده ارسالی
- رد بسته‌های دوباره ارسال شده

در واقع پروتکل ESP هم امنیت تمامیت داده (سلامت داده‌های ارسالی) پکت هایی که از HMAC استفاده می‌کنند را تامین کنید و هم محرمانگی از طریق اصول رمزنگاری (Encryption principle) بکار گرفته شده .بعد از رمزنگاری پکت و محاسبات مربوط به HMAC ، سرآیند ESP محاسبه و به پکت اضافه می‌شود.

فیلدهای پروتکل ESP:

۱. اولین ۳۲ بیت سرآیند ESP همان SPI است که درSA بکار گرفته شده و جهت بازگشایی پکت کپسوله شده ESP بکار می‌رود.

۲. دومین فیلد همان شماره توالی یا Sequence Number می‌باشد که به جهت حفاظت از تهاجمات داده‌های بازگشتی استفاده می‌شود.

۳. سومین فیلد همان بردار مقدار اولیه یا IV یا همان initial vector می‌باشد. این فیلد نیز برای پردازش رمزنگاری بکار می‌رود. الگوریتمهای رمزنگاری متقارن اگر از IV استفاده نکنند، مورد تهاجم متوالی روی پکت قرار می‌گیرد. IV این اطمینان را می‌دهد تا دو مشخصه Payload روی دو Payload رمز شده مختلف قرار گیرد.
پردازش رمزنگاری در IPSec در دو بلوک رمز (Cipher) بکار می‌رود. بنابراین اگر طول Payload ها تک تک باشند. Payload IPSec , ها را به شکل لایه لایه قرار می‌دهد. و از اینرو طول این لایه‌ها همواره در حال اضافه شدن است. طول لایه (Pad length) 2 بایت است.

۴. فیلد بعدی که همان Next header می‌باشد، سرآیند بعدی را مشخص می‌کند.

۵. این پروتکل HMAC است که مانند پروتکل HA از تمامیت و سلامت داده‌های ارسالی حفاظت می‌کند. فقط این سرآیند است که می‌تواند به Payload اعتبار دهد. سرآیند IP شامل پروسه محاسبه نمی‌باشد.

NAT هیچ دخلی به کار ESP ندارد و این بخش هنوز هم ممکن است بخشی از IPSec باشد و با آن ترکیب گردد. NAT پیمایشی (NAT-Traversal) راه حلی است در کپسوله کردن پکت‌های ESP به همراه پکت های UDP. در شکل زیر حالتهای انتقال و تونل در پروتکلESP به نمایش در آمده است.

همان طور که می بینید این پروتکل در این دو حالت ارتباط امن بین دو نقطه انتهائی که در دو شبکه مجزا قرار دارند را فراهم می‌آورد، همچنین ارتباط امن بین دو نقطه در یک شبکه داخلی و یک نقطه انتهائی و یک مسیر یاب یا حفاظ دیواره آتش (Firewall) را ممکن می سازد.

RDP-34

Remote Desktop Protocol

همانند Telnet است با این تفاوت که گرافیکی است . در مایکروسافت ، برنامه ی Remote Desktop از سرویس RDP استفاده کرده و کامپیوتر شخصی را تبدیل به یک ترمینال گرافیکی می کند .

همچون دیگر سرویس های TCP/IP، RDP نیز از دو بخش تشکیل شده .

الف) RDP Client : که به Terminal Client نیز معروف بوده و در مایکروسافت ، همان برنامه ی Remote Desktop است.(mstsc.exe)

ب) RDP Server : که به Server Terminal نیز مشهور بوده و در مایکروسافت ، همان سرویس Remote_Desktop است که از طریق System Properties فعال می شود . البته در ویندوز های ۲۰۰۰ و ۲۰۰۳ Server یک نسخه کامل تر از این سرویس به نام ترمینال سرویس از طریق زیر نصب و فعال می شود :

Terminal Service <- Windows Components <- Add/Remove Programs

TCP/IP -35

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 .در مجموعه مقالاتی که ارائه خواهد شد به بررسی این پروتکل خواهیم پرداخت . در این بخش مواردی همچون : فرآیند انتقال اطلاعات ، معرفی و تشریح لایه های پروتکل TCP/IP و نحوه استفاده از سوکت برای ایجاد تمایز در ارتباطات ، تشریح می گردد.

مقدمه

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.

معرفی پروتکل TCP/IP

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 چهارلایه 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 .

سرویس هایTCP/ IP

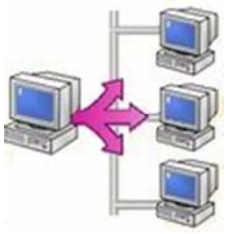
TCP/IP از سرویس های متنوعی تشکیل شده که اغلب نیازهای کاربران در شبکه را مستقیماً و بدون نیاز به برنامه نویسی اضافه پاسخ می دهد . اغلب این سرویس ها برای کاربران آشنا بوده و در کاربردهای روزمره ی خود در اینترنت از آن استفاده می کنند .
پروتکل TCP/IP در ابتدا توسط وزارت دفاع آمریکا و در سیستم عامل UNIX ایجاد شد .

امروزه این پروتکل تقریباً کلیه رقبا را کنار زده و در اکثر شبکه ها اعم از کوچک و بزرگ و توسط کلیه ی سیستم عامل ها پشتیبانی می شود .
در اهمیت TCP/IP توجه به این نکته کافی است که ارتباط در ایترنت بدون TCP/IP تقریباً غیرممکن است و اکثر سرویس های اینترنت تحت قوانین TCP/IP عرضه می شوند.

مهمترین خصوصیات این پروتکل :

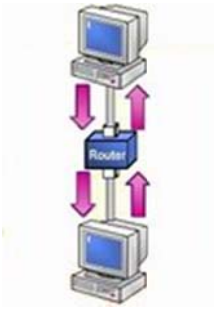
۱. پشتیبانی انواع شبکه
۲. پشتیبانی انواع سیستم عامل
۳. مورد استفاده به عنوان پروتکل اصلی
۴. مسیریابی
۵. حق انتخاب در انتقال اطلاعات به صورت عادی و سفارشی
۶. ارسال گروهی
۷. پیکربندی پیچیده

UDP -36 : لایه Transport



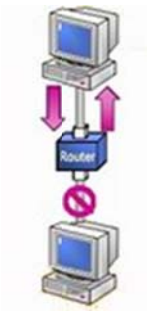
User Datagram Protocol (UDP)، پروتکلی در سطح لایه "حمل" بوده که برنامه مقصد در شبکه را مشخص نموده و از نوع بدون اتصال است . پروتکل فوق، امکان توزیع اطلاعات با سرعت مناسب را ارائه ولی در رابطه با تضمین صحت ارسال اطلاعات ، سطح مطلوبی از اطمینان را بوجود نمی آورد . UDP در رابطه با داده های دریافتی توسط مقصد ، به Acknowledgment نیازی نداشته و در صورت بروز اشکال و یا خرابی در داده های ارسال شده ، تلاش مضاعفی بمنظور ارسال مجدد داده ها ، انجام نخواهد شد . این بدان معنی است که داده هائی کمتر ارسال می گردد ولی هیچیک از داده های دریافتی و صحت تسلسل بسته های اطلاعاتی ، تضمین نمی گردد .از پروتکل فوق ، بمنظور انتقال اطلاعات به چندین کامپیوتر با استفاده از Broadcast و یا Multicast ، استفاده بعمل می آید . پروتکل UDP ، در مواردیکه حجم اندکی از اطلاعات ارسال و یا اطلاعات دارای اهمیت بالائی نمی بانشد ، نیز استفاده می گردد. استفاده از پروتکل UDP در مواردی همچون Multicasting Streaming media ، (نظیر یک ویدئو کنفرانس زنده) و یا انتشار لیستی از اسامی کامپیوترها که بمنظور ارتباطات محلی استفاده می گردند ، متداول است . بمنظور استفاده از UDP ، برنامه مبداء می بایست پورت UDP خود را مشخص نماید دقیقا" مشابه عملیاتی که می بایست کامپیوتر مقصد انجام دهد . لازم به یادآوری است که پورت های UDP از پورت های TCP مجزا و متمایز می باشند (حتی اگر دارای شماره پورت یکسان باشند).

IP -37 : لایه Internet



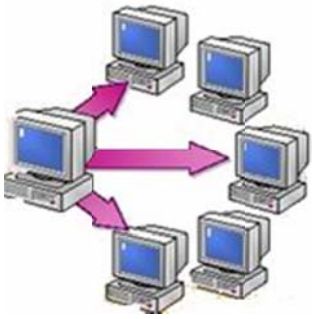
Internet Protocol (IP) ، امکان مشخص نمودن محل کامپیوتر مقصد در یک شبکه ارتباطی را فراهم می نماید. IP ، یک پروتکل بدون اتصال و غیرمطمئن بوده که اولین مسئولیت آن آدرس دهی بسته های اطلاعاتی و روتینگ بین کامپیوترهای موجود در شبکه است . با اینکه IP همواره سعی در توزیع یک بسته اطلاعاتی می نماید ، ممکن است یک بسته اطلاعاتی در زمان ارسال گرفتار مسائل متعددی نظیر : گم شدن ، خرابی ، عدم توزیع با اولویت مناسب ، تکرار در ارسال و یا تاخیر، گردند.در چنین مواردی ، پروتکل IP تلاشی بمنظور حل مشکلات فوق را انجام نخواهد داد (ارسال مجدد اطلاعات درخواستی) .آگاهی از وصول بسته اطلاعاتی در مقصد و بازیافت بسته های اطلاعاتی گم شده ، مسئولیتی است که بر عهده یک لایه بالاتر نظیر TCP و یا برنامه ارسال کننده اطلاعات ، واگذار می گردد . IP پروتکلی است که آدرس سایت را به صورت عددی ۱۲ رقمی نشان می دهد.

ICMP -38 : لایه Internet



ICMP (Control Message Protocol Internet) ، 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 ، ICMP یک 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 ICMP به 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 .

IGMP -39: لایه Internet

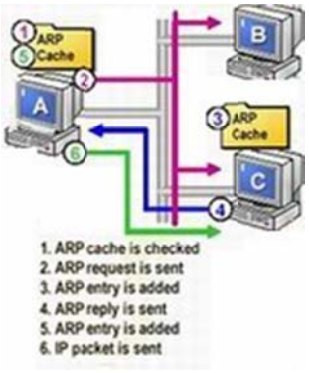


IGMP (Group Managment Protocol Internet)، پروتکلی است که مدیریت لیست اعضاء برای IP Multicasting ، در یک شبکه TCP/IP را بر عهده دارد . IP Multicasting، فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرندگان که گروه multicat نامیده می شوند ؛ ارسال می گردد . IGMP لیست اعضاء را نگهداری می نماید .

مدیریت Multicasting IP

تمامی اعضاء یک گروه multicast ، به ترافیک IP هدایت شده به یک آدرس Multicast IP ، گوش داده و بسته های اطلاعاتی ارسال شده به آن آدرس را دریافت می نمایند. زمانیکه چندین کامپیوتر نیازمند دستیابی به اطلاعاتی نظیر Streaming media باشند، یک آدرس IP رزوشده برای multicasting استفاده می گردد. روترها که بمنظور پردازش multicast پیکربندی می گردند، اطلاعات را انتخاب و آنها را برای تمامی مشترکین گروه multicast ارسال (Forward) می نمایند . بمنظور رسیدن اطلاعات Multicast به گیرندگان مربوطه ، هر یک از روترهای موجود در مسیر ارتباطی می بایست ، قادر به حمایت از Multicasting باشند . کامپیوترهای مبتنی بر سیستم عامل وینوز ۲۰۰۰ ، قادر به ارسال و دریافت IP Multicast ، می باشند .

ARP -40: لایه Internet



Address Resolution Protocol (ARP) ، پروتکلی است که مسئولیت مسئله " نام به آدرس" را در رابطه با بسته های اطلاعاتی خروجی (Outgoing) ، برعهده دارد . ماحصل فرآیند فوق، Mapping آدرس IP به آدرسMAC (Control Media Access) ، مربوطه است . کارت شبکه از آدرس MAC ، بمنظور تشخیص تعلق یک بسته اطلاعاتی به کامپیوتر مربوطه ، استفاده می نمایند . بدون آدرس های MAC ، کارت های شبکه ، دانش لازم در خصوص ارسال بسته های اطلاعاتی به لایه بالاتر بمنظور پردازش های مربوطه را دارا نخواهند بود . همزمان با رسیدن بسته های اطلاعاتی به لایه IP بمنظور ارسال در شبکه، آدرس های MAC مبداء و مقصد به آن اضافه می گردد. ARP ، از جدولی خاص بمنظور ذخیره سازی آدرس های IP و MAC مربوطه ، استفاده می نماید. محلی از حافظه که جدول فوق در آنجا ذخیره می گردد ، Cache ARP نامیده می شود. ARP Cache هر کامپیوتر شامل mapping لازم برای کامپیوترها و روترهائی است که صرفا" بر روی یک سگمنت مشابه قرار دارند.

BGP -41

Border Gateway Protocol – RFC ۱۷۷۱

BGP پروتکلی است که در هسته Routing اینترنت از آن استفاده می شود. BGP پروتکل مسیریابی در شبکه یا گروهی از شبکه‌ها که دارای خط مشی یکسان هستند، است. وظیفه‌ی BGP تبادل اطلاعات مسیریابی در اینترنت است.

پایگاه داده‌های مسیریابی BGP در حال حاضر دارای بیش از ۹۰۰۰۰ مسیر است.

اگر از این پروتکل برای ارتباط بین دو شبکه استفاده شود به آن EBGP و اگر در داخل یک شبکه استفاده شود به آن IBGP می‌گویند.

وظیفه این پروتکل اتصال و Routing بین Autonomous System ها و شبکه های بزرگ IP است. بطور مثال ارتش برای اتصال شبکه های نیروهای زمینی،هوائی و دریایی خود – که هر کدام شبکه ای بزرگ IP دارند – از BGP بعنوان Exterior Routing Protocol استفاده میکند.

در واقع BGP حامل اطلاعات Autonomous هاست تا از این طریق شبکه های IP (در درون Autonomous) را پیدا کند. از مشخصات کلی این پروتکل میتوان به موارد زیر اشاره کرد:

یک پروتکل Path Vector است تا Vector Distance.

VLSM و CIDR را پشتیبانی میکند.

ارتباط با همسایگان را روی پورت TCP 179 برقرار میکند و با Keep-alive آن را نگه میدارد.

Routing Table مستقل خود را دارد.

Metric در این پروتکل، Attribute نامیده می شود.

نسبت به پروتکل های Interior کاملا متفاوت بوده و برای ارتباط بین AS هاست. بعبارتی Inter-autonomous Systems Routing Protocol است.

انعطاف پذیر (Flexibility) بوده و با Policy-based Routing حرفه ای همراه است. به هرحال Routing در اینترنت بصورت Hop-by-hop است و سیاست های شما در طول مسیر بوسیله روترهای میان راه – که کنترلی رویشان ندارید – ممکن است بکار گرفته نشود.

مثل RFC 1918 جهت اختصاص IP برای استفاده Private، AS Number نیز طبق RFC 1930 از ۶۴۵۱۲ به انتها (یعنی تا ۶۵۵۳۵) برای مصارف Private در نظر گرفته شده است.

EIGRP -42

Enhanced Interior Gateway Routing Protocol یا EIGRP در اوایل دهه ۹۰ توسط سیسکو ارائه شد. با اینکه EIGRP نسخه بهبود یافته IGRP است اما از نظر کارائی و عملکرد تفاوت هایی زیر بنائی با کلیه Distance Vector دارد و از این لحاظ بیشتر دارای شباهت و خصوصیاتی Link State گونه است بطوریکه به آن Hybrid Routing Protocol گفته میشود و سیسکو آنرا Advance Protocol Distance Vector می نامد.

EIGRP برای حل مشکلات رشد شبکه های IGRP و کلا ضعف های Distance Vector ها بوجود آمد و نهایتا منجر به کاهش زمان Convergence در شبکه شد. (زمانی که شبکه صرف میکند تا به حالت نرمال برگردد)

ین پروتکل بر اساس DUAL یا Algorithm Diffusing Update کار میکند و برای ارتباط با همسایگان خود از Multicast (برخلاف RIP نسخه یک که Broadcasr است) استفاده میکند. (آدرس ۲۲۴.۰.۰.۱۰)

روتر Neighbor یا همسایه به محض دریافت این Packet به فرستنده Unicast، ACK (رسید) ارسال میکند.

برای جلوگیری از Loop در مسیر، روتر مسیر Backup (نام دیگر آن Feasible Successor) را نیز ذخیره میکند. تا در موقع مورد نیاز از آن استفاده کند. همچنین EIGRP برای Summarization برخلاف پروتکلی نظیر OSPF نیازی به تعریف Area ندارد و هرجائی از شبکه این امکان وجود دارد.

EIGRP بعنوان یک Routing Protocol قابلیت Route پروتکلهای IPX،IP و AppleTalk را داراست و برای هریک، Routing Table مجزا میسازد. (همچنین IPv6)

از آنجا که قابلیت Route کردن پروتکل های مختلف را داراست، به ازای هر پروتکل سه جدول وضع میکند:

Neighbor Table, Topology Table و Table Routing.

IGRP -43

IGRP (برگرفته شده از Routing Protocol Interior Gateway) یکی از پروتکل روتینگ distance-vector طراحی شده توسط شرکت سیسکو است . این بدان معنی است در صورت استفاده از پروتکل فوق در یک شبکه ، می بایست تمامی روترها از نوع سیسکو باشند . شرکت سیسکو هدف از ایجاد پروتکل IGRP را غلبه بر برخی محدودیت های پروتکل RIP عنوان کرده است .

IGRP می تواند حداکثر دارای ۲۵۵ ، hop باشد که مقدار پیش فرض آن ۱۰۰ در نظر گرفته می شود . این وضعیت در شبکه های بزرگ بسیار مفید است و مشکل داشتن حداکثر ۱۵ hop در یک شبکه مبتنی بر پروتکل RIP را برطرف نماید .

IGRP از یک روش متفاوت نسبت به RIP جهت محاسبه متریک استفاده می کند . در این پروتکل ، بطور پیش فرض از پهنای باند و تاخیر خط به عنوان شاخص هائی جهت تعیین بهترین مسیر استفاده می گردد . به فرآیند فوق متریک ترکیبی(composite metric) گفته می شود . همچنین برای محاسبه متریک از شاخص هائی دیگر نظیر قابلیت اعتماد ، میزان load و MTU (برگرفته شده از maximum transmission unit) استفاده می گردد (از شاخص های اشاره شده بطور پیش فرض در محاسبه متریک استفاده نمی گردد) .

پروتکل IGRP با RIP دارای تفاوت های عمده ای است که به برخی از آنها اشاره می گردد :

- امکان استفاده از IGRP در شبکه های بزرگ
- IGRP برای فعال شدن از یک number AS (برگرفته شده از autonomous system) استفاده می نماید .
- IGRP در هر ۹۰ ثانیه یک مرتبه بهنگام سازی جدول روتینگ را بطور کامل انجام می دهد .
- IGRP از پهنای باند و تاخیر خط به عنوان یک متریک استفاده می نماید .

برای کنترل کارآئی ، پروتکل IGRP از تایمرهای مختلف زیر با مقادیر پیش فرض استفاده می نماید :

- Update timers ، فرکانس ارسال پیام های بهنگام روتینگ را مشخص می نماید . مقدار پیش فرض ۹۰ ثانیه در نظر گرفته شده است .
- Invalid timers ، مدت زمانی را که یک روتر می بایست منتظر بماند قبل از این که یک مسیر نادرست را به دیگران اعلام نماید (در صورتی که در بازه زمانی مورد نظر یک بهنگام جدید دریافت نگردد) ، مشخص می نماید . مقدار پیش فرض سه برابر زمان Update timer است .
- Holddown timers ، مدت زمان holddown را مشخص می نماید . مقدار پیش فرض سه برابر زمان Update timer به اضافه ۱۰ ثانیه در نظر گرفته شده است .
- Flush timers، مشخص می نماید که چه مدت زمانی می بایست سپری شود قبل از این که بتوان یک مسیر را از جدول روتینگ حذف کرد . مقدار پیش فرض هفت برابر زمان Update timer در نظر گرفته می شود . در صورتی که مقدار Update timer برابر با ۹۰ ثانیه در نظر گرفته شود ، ۳۶۰ ثانیه طول خواهد کشید تا بتوان یک مسیر را از جدول روتینگ حذف کرد .

OSPF -44

پروتکل OSPF (Open Shortest Path First) بر اساس حالتی است که شبکه دارای مسیریاب‌های متعددی است و این مسیریاب‌ها به صورت مسیریابی سلسله مراتبی به یکدیگر پیوند داده شده‌اند.

ریشه یا رأس هرم سلله مراتب یک مسیریاب مستقل دیگری متصل می‌شود. مرحله بعدی در بالاترین منطقه OSPF مسیریاب های ستون مهره‌ای هستند. مسیریاب های مرزی به مناطق متعددی متصل شده‌اند و می‌توانند کپی های متعددی از الگوریتم مسیریابی را اجرا کنند. در انتها مسیریاب‌های داخلی هستند که بک پایگاه اطلاعاتی برای یک منطقه را اجرا می کنند.

با تقسیم شبکه به یک سلسله مراتب مسیریابی، مشکلات گذشته حل خواهد گردید. هر سطح برای خود یک جدول مسیر انتقال کوچک دارد و زمان طولانی و ترافیک برای بهنگام‌سازی این جدول را نخواهیم دشت.

این پروتکل برای پیدا کردن Neighbor (همسایه) – یا در واقع روترهای متصل به خود – از Hello Message استفاده میکند. پیام Hello به آدرس Multicast 224.0.0.5 ((AllSPFRouters ارسال میگردد اگر در رسانه ای خاص Multicast قابل استفاده نباشد، از Unicast استفاده میکند (در این حالت آدرس همسایه باید از قبل تنظیم شده باشد).

پس از ارتباط همسایگی، اگر در مدت زمان مشخصی پیام سلام از همسایه دریافت نشود، به قطع شدن پی میبریم. همسایه ها اطلاعات دسترسی خود به شبکه ها (لینک ها) را در اختیار هم قرار داده و Routing Database را بر اساس الگوریتم SPF یا Shortest Path First که بر اساس الگوریتم Dijkstra است ایجاد میکنند. هر روتر نسخه ای از آن Database را درون خود داشته و بر اساس آن Routing Table خود را میسازد.

مبنای الگوریتم SPF بر پایه الگوریتم ریاضی است که توسط Edsger – Wybe – Dijkstra ارائه شده که با ایجاد Topology Table به ازای یک Area کار خود را انجام می دهد. هر روتر دارای زاویه دید و Perspective خود از شبکه بوده و شبکه را بصورت درختی میبینند که خود در راس آن قرار دارد و مسیرها را بصورت گراف پردازش میکند.

به ازای هر تغییر در شبکه، LSA ارسال شده و در Area به همه ارسال می‌شود (Flood،LSA میشود) و نهایتا پس از هر تغییر Table Topology دوباره از سر ساخته میشود.

RIP -45

(برگرفته شده از Routing Information Protocol) به معنی واقعی یک پروتکل distance-vector است . پروتکل فوق در هر ۳۰ ثانیه تمام اطلاعات موجود در جدول روتینگ را برای تمامی اینترفیس های فعال ارسال می نماید . RIP صرفا" از تعداد hop برای تعیین بهترین مسیر به شبکه راه دور استفاده می نماید .حداکثر تعداد hop می تواند عدد ۱۵ را داشته باشد و نسبت دهی عددی بالاتر از ۱۵ به منزله غیرقابل دسترس بودن شبکه است.

RIP در شبکه های کوچک به خوبی کار می کند ولی برای شبکه های بزرگ که دارای لینک های ارتباطی WAN (برگرفته شده از wide area network) کند و تعداد بسیار زیادی روتر هستند مناسب نمی باشد .

در نسخه شماره یک RIP صرفا" از روتینگ classful استفاده می گردد . این بدان معنی است که تمامی دستگاه های موجود در شبکه می بایست از subnet mask مشابهی استفاده نمایند . محدودیت فوق به دلیل ماهیت ارسال اطلاعات بهنگام می باشد. در نسخه شماره یک RIP ، اطلاعات بهنگام ارسال شامل اطلاعات mask subnet نمی باشند .

در RIP نسخه دو ، ویژگی جدیدی به نام روتینگ Prefix ارائه شده است که به کمک آن امکان ارسال اطلاعات subnet mask به همراه مسیرهای بهنگام شده فراهم می گردد . به این نوع روتینگ ، اصطلاحا" روتینگ classless گفته می شود .

RIP از سه نوع تایمر مختلف برای تنظیم کارآئی خود استفاده می نماید .

Route update timer ، فاصله زمانی ارسال یک نسخه کامل از اطلاعات بهنگام روتینگ را مشخص می نماید . در بازه زمانی فوق ، روتر یک نسخه کامل از اطلاعات موجود در جدول روتینگ خود را برای تمامی همسایگان ارسال می نماید . این زمان معمولا" ۳۰ ثانیه در نظر گرفته می شود .

Route invalid timer، مدت زمانی را مشخص می نماید که پس از سپری شدن آن ، روتر به این نتیجه خواهید رسید که یک مسیر غیرمعتبر است . این زمان معمولا" ۱۸۰ ثانیه در نظر گرفته می شود و اگر یک روتر در بازه زمانی فوق هیچگونه اطلاعات جدیدی را در خصوص یک مسیر خاص دریافت ننماید ، آن مسیر را غیرمعتبر می نماید . در صورت تحقق چنین شرایطی ، روتر اقدام به ارسال اطلاعات بهنگام برای تمامی همسایگان خود می نماید تا به آنها بگوید که مسیر غیرمعتبر است .

Route flush timer، مدت زمان بین غیرمعتبر اعلام شدن یک مسیر و حذف آن از جدول روتینگ را مشخص می نماید . این زمان معمولا" ۲۴۰ ثانیه در نظر گرفته می شود . قبل از این که یک مسیر از جدول روتینگ حذف گردد ، روتر این موضوع را به اطلاع همسایگان خود می رساند . مقدار Route invalid timer می بایست کمتر از route flush timer باشد تا روتر زمان کافی جهت اطلاع به همسایگان خود را قبل از بهنگام سازی جدول در اختیار داشته باشد .