به نام خدا

پروژه تحقیقاتی

فاز ۱ : پروتکل‌های معمول اینترنت (و پروتکل‌های لایه کاربرد)

استاد : دکتر حسن حقیقی

استادیار : عباس نادری

گردآورنده: المیرا نظام فر

شماره دانشجویی: ۸۶۲۱۳۱۳۰

پست الکترونیک: e_nezamfar@yahoo.com

۱۳۸۹-۹۰

فهرست مطالب

۱ –استانداردهای انتقال روی خطوط نقطه به نقطه..... ۲

۱–۱– پروتکل SLIP **۲**

۱–۲– پروتکل PPP **۳**

۱–۳– پروتکل ICMP **۳**

۲ –لایه کاربرد..... ۵

۲–۱– پروتکل DNS **۵**

۲–۲– پروتکل SMTP**– پروتکل ساده انتقال نامه** **۵**

۲–۳– پروتکل POP3 **۸**

۲–۴– پروتکل IMAP **۹**

۲–۵– پروتکل انتقال ابرمتن HTTP **۱۰**

۲–۶– پروتکل پیکربندی پویای میزبان - DHCP **۱۱**

۲–۷– پروتکل SNMP**–پروتکل ساده مدیریت شبکه** **۱۳**

۲–۸– پروتکل TelNet **۱۴**

۲–۹– پروتکل Remote Desktop Protocol (RDP) **۱۶**

۲–۱۰– پروتکل FTP **۱۶**

۳–امنیت..... ۲۰

۳–۱– پروتکل امنیتی ipsec **۲۰**

۳–۲– پروتکل امنیتی SSL **۲۳**

۱ - استانداردهای انتقال روی خطوط نقطه به نقطه

بسیاری از کاربران اینترنت بوسیله مودم و از طریق خطوط تلفن معمولی به اینترنت متصل میشوند که کانالی نقطه به نقطه محسوب می شود . برای این که به چگونگی انتقال داده ها بین دو ماشین نقطه به نقطه پی ببریم دو پروتکل SLIP و PPP را شرح میدهم .

۱-۱- پروتکل SLIP :

این پروتکل در سال ۱۹۸۴ برای اتصال ایستگاهای Sun به وسیله یک خط سریال مثل تلفن ابداع شد . این پروتکل فوق العاده ساده و یسار سریع است. روش کار به این صورت است که به محض آنکه یک ایستگاه تمایل داشت اطلاعاتی را ارسال نماید ، علامت مشخصه یک بایتی 0xC0 را روی خط می گذارد . بنابراین قالب هر فریم در این پروتکل به صورت زیر است :

Flag	Data (Payload)	Flag
0xC0	داده ها	0xC0

با کمی دقت به قالب فریم در پروتکل SLIP ، متوجه خواهیم شد که این پروتکل معایب متعددی دارد :

- در این پروتکل هیچ گونه کد کشف خطا گنجانیده نشده است و مسئله کشف خطاهای احتمالی به لایه های بالاتر سپرده شده است .
- در درون فیلد داده از فریم پروتکل SLIP فقط بسته های IP قرار میگیرد ، در حالی که امروزه در بعضی از شبکه ه مثل Novel یل Apple Talk ، ایستگاهها قادرند از طریق خطوط سریال و پروتکلهایی به غیر از IP با ایستگاههای راه دور ارتباط برقرار کنند و SLIP در این شبکه ها قابل استفاده نیست .
- چون دو ماشین که از طریق پروتکل SLIP با هم ارتباط برقرار می کنند دو مرکز رو در رو محسوب می شوند ، این دو ایستگاه باید آدرسهای IP ثابت و شناخته شده ای داشته باشند و لیکن امروزه ارتباطی مورد نیاز است که وقتی یک ماشین میزبان به شبکه وارد شد ، قبل از هر گونه تبادل اطلاعات ابتدا هویت او تایید شده و سپس یک IP موقت به آن تخصیص داده شود. .
- پروتکل SLIP فقط برقرار کننده ارتباط را بعنوان ماشین معتبر می شناسد و هیچ راهی برای تایید و احراز هویت کاربر برقرار کننده ارتباط فراهم نکرده است و امنیت شبکه به مخاطره می افتد .
- بسیاری از سیستمهای عامل از SLIP پشتیبانی نمیکنند .

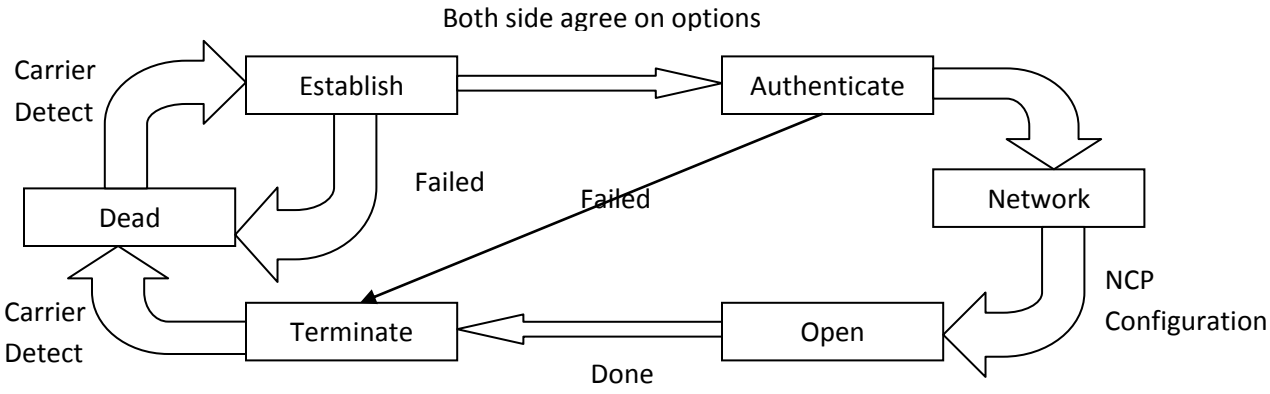
۱-۲- پروتکل PPP :

قالب فریم این پروتکل به صورت زیر است :

1 Byte	1 Byte	1 Byte	1 or 2 Byte	Variable	2 or 4 Byte	**1 Byte**
Flag 01111110	Address 11111111	Control 00000011	Protocol	Payload	Checksum	**Flag 01111110**

در این پروتکل بسیاری از معایب پروتکل SLIP رفع شده است .

مراحل برقراری و ختم یک ارتباط در پروتکل PPP با یک شکل شرح میدهیم :



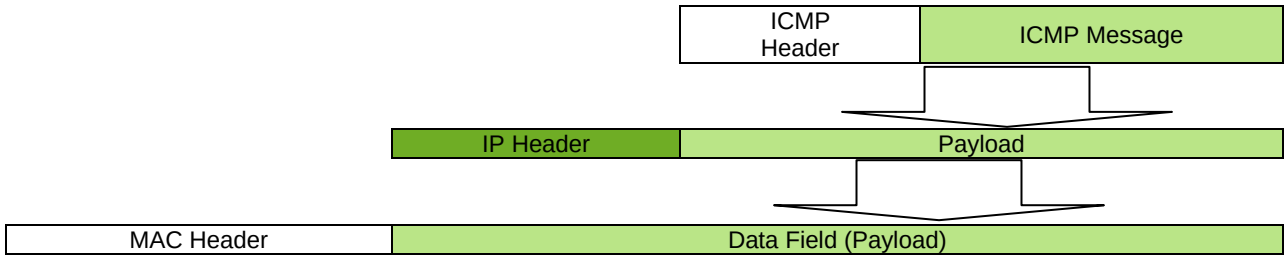
۱-۳- پروتکل ICMP :

پروتکل IP ، بدون اتصال و غیر قابل اعتماد است . بدون اتصال بدین معنا که مسیریاب هر بسته را بدون هیچگونه هماهنگی با مقصد بسته یا مسیریاب بعدی ارسال می نماید ، بدون آنکه بتواند اطلاعی از وجود یا عدم وجود مقصد داشته باشد . در ضمن هر مسیریاب پس از ارسال یک بسته آنرا فراموش می کند و منتظر پیام دریافت بسته از گیرنده آن نخواهد ماند . اگر یک بسته IP با خطا به مقصد برسد و یا اصلا به مقصد نرسد این پروتکل هیچ اطلاعی در مورد سرنوشت آن به فرستنده بسته نمی دهد .

عدم گزارش خطا به تولید کننده یک بسته منجر به تکرار خطا و حمل بیهوده و زاید بسته هایی میشود که محکوم به فنا و حذف در شبکه هستند .

پروتکل ICMP در کنار پروتکل IP ، برای بررسی انواع خطا و ارسال پیام برای مبدا بسته در هنگام بروز اشکلات ناخواسته استفاده میشود . در حقیقت ICMP یک سیستم گزارش خطا است که بر روی پروتکل IP نصب میشود تا در صورت بروز هرگونه خطا به فرستنده بسته ، پیام مناسب را بدهد تا آن خطا تکرار نشود . در واقع ICMP وظیفه ای در قبال وقوع خطا ندارد بلکه فقط پیامی که بیانگر بروز خطا و نوع آن است

به فرستنده برمیگرداند . این پروتکل اشکالات موجود را در قالب یکسری پیام گزارش میکند که این پیام خود در یک بسته IP قرار میگیرد که از جانب یک مسیریاب یا ماشین مقصد به آدرس فرستنده بازمیگردد . در شکل زیر چگونگی قرار گرفتن یک پیام ICMP درون یک بسته IP تصویر شده است .



شکل کلی و قالب پیام ICMP در زیر مشخص شده است :

۳۱	۳۰	۲۹	۲۸	۲۷	۲۶	۲۵	۲۴	۲۳	۲۲	۲۱	۲۰	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱
Type									Code										Checksum											
Parameters																														
Data																														

- فیلد Type : در این فیلد عددی قرار می گیرد که بیانگر نوع پیام می باشد و ساختار فیلدهای Parameters و Data بسته به عددی که در این فیلد قرار می گیرد متفاوت خواهد بود .
- فیلد Code : گاهی خود نوع پیام به چند زیر نوع دیگر تقسیم می شود که کد زیر نوع در این فیلد قرار می گیرد .
- فیلد Checksum : محتوای این فیلد برای سنجش اعتبار و سلامت بسته ICMP مورد استفاده قرار میگیرد . تمامی بسته ICMP بصورت دو بایت دو بایت جمع شده و نهایتا از مکمل ۱ حاصل جمع ، عددی ۱۶ بیتی بدست می آید که درون این فیلد قرار میگیرد .

۲ -لایه کاربرد

لایه کاربرد لایه ای است که تمام کاربردهای شبکه در آن قرار درارد ، لایه های زیرین لایه کاربرد فقط برای سرویس دادن به این لایه هستند ، و هیچ کار واقعی برای کاربران انجام نمی دهند .

پروتکل های این لایه

۲-۱- پروتکل DNS :

سالها قبل در ارپانت فایلی بنام hosts.txt ، که نام کامپیوترها و آدرس IP آنها در این فایل لیست می شد. کامپیوترهای شبکه هر شب این فایل را از جایی که قرار داشت،می خواندند و خود را به روز می کردند. برای شبکه ای با دها (و صدها) کامپیوتر این روش بخوبی کار می کرد.

ولی وقتی تعداد کامپیوترهای شبکه از مرز هزاران PC و کامپیوتر بزرگ گذشت ، همه دریافتند که این روش دیگر جوابگو نیست. اولین دلیل آن بود که اندازه ی چنین فایلی بشدت بزرگ می شد ، ولی از آن مهمتر مشکل نامهای تکراری بود که ضرورت یک مدیریت مرکزی را اجتناب ناپذیر می کرد (چیزی که بزرگی و بار شبکه آنرا ناممکن می کرد) . برای غلبه بر این مشکلات بود که DNS (سیستم نام ناحیه – Domain Name System) اختراع شد .

ایده اصلی DNS یک روش نامگذاری سلسله مراتبی براساس ناحیه ها بود ، که به صورت یک پایگاه اطلاعاتی توزع یافته پیاده شازی می شد . هدف اولیه ی این سیستم تبدیل نام کامپیوترها و آدرسهای ایمیل به آدرسهای IP بود ، ولی می توانست کاربردهای دیگری هم داشته باشد .

روش کار DNS خیلی خلاصه چنین است : برای تبدیل یک نام به آدرس IP ، برنامه یک تابع کتابخانه ای به نام تبدیل کننده (resolver) را فرخوانی می کند ، و نام موردنظر را بصورت پارامتر به آن می دهد . تبدیل کننده یک بسته ی UDP به سرویس دهنده DNS محلی می فرستد ، که این DNS آدرس IP معادل نام خواسته شده را یافته و به تبدیل کننده برمی گرداند ، که آن هم به نوبه ی خود آدرس را به برنامه ی فراخوانی کننده تحویل می دهد . برنامه هم پس از بدست آوردن آدرس IP کامپیوتر مقصد ، می تواند با آن ارتباط TCP برقرار کرده یا بسته های UDP به آن بفرستد .

۲-۲- پروتکل SMTP- پروتکل ساده انتقال نامه :

مشهورترین سرویسدهنده پست الکترونیکی ، STMP نام دارد که روند عملیات آن بسیار ساده است و فرامین متنی دارد :

ماشین مبدا (یعنی ماشینی که میخواهد نامه ی نوشته و تنظیم شده ای ارسال کند) با پورت شماره ۲۵ از ماشین مقصد که سرویس دهنده ی SMTP روی آن اجرا شده یک ارتباط TCP برقرار میکند . بنابراین براحتی می تواند در ذهن خود مجسم کنید که برنامه ی سرویس دهنده یک برنامه سوکت است که به پورت ۲۵ گوش میدهد (این برنامه در محیط یونیکس به نام دایمون SMTP معروف است

. دایمونها برنامه هایی هستند که در حالت انتظار می مانند و با یک سیگنال شروع به انجام عملیات خود می نمایند) این برنامه ارتباطات TCP به پورت ۲۵ را می پذیرد.

پس از برقراری ارتباط و پذیرش آن توسط سرویس دهنده ، شروع کننده ی ارتباط (یعنی نرم افزار مشتری یا همان نامه خوان) باید آنقدر صبر کند تا سرویس دهنده ی مقصد با ارسال یک پیغام اعلام آمادگی نماید . روند اعلام آمادگی و بقیه مراحل مبادله ی نامه به صورت زیر است:

- سرویس دهنده با ارسال یک رشته متنی که معمولا بصورت زیر است به برنامه مبدا اعلام آمادگی می نماید :

SMTP service ready آدرس نام حوزه خود ۲۲۰

مثال : 220 xyz.com SMTP service ready

- پس از اعلام آمادگی (کد ۲۲۰ بمعنای اعلام آمادگی است) برنامه مبدا با ارسال یک رشته که حاوی کلمه HELO و همچنین آدرس نام حوزه خودش می باشد هویت خود را برای سرویس دهنده آشکار میکند .

مثال : HELO abc.com

- پس آنکه سرویس دهنده هویت فرستنده پیام را ارزیابی کرد در صورتی که تمایل به دریافت نامه داشته باشد با کد ۲۵۰ و رشته ای که در ادامه آن می آید اعلام آمادگی می نماید .

مثال : 250 xyz.com says hello to abc.com

- سرویس دهنده صاحب نامه را بررسی کرده و درصورتی که منعی برای دریافت نامه چنین شخصی وضع نشده باشد مجددا با کد ۲۵۰ و رشته ای که در ادامه می آید اعلام آمادگی می کند .

مثال : 250 sender ok

- برنامه مبدا گیرنده نامه را معرفی می کند .

مثال : PCPT TO:<Carolyn@xyz.com>

- بار دیگر سرویس دهنده ، گیرنده نهایی نامه را ارزیابی کرده و بررسی می ند که آیا چنین شخصی (در مثال بالا Carolyn) وجود دارد یا خیر . در صورتی که امکان دریافت نامه وجود داشته باشد برای بار سوم با کد ۲۵۰ مطابق مثال زیر اعلام آمادگی می شود :

250 recipient ok

- برنامه مبدا اعلام می کند که برای ارسال داده ها که کلا کاراکترهای اسکی با کد زیر ۱۲۸ هستند آماده است ؛ کلمه DATA بدون هیچ حرف اضافه به عنوان اعلام آمادگی برای ارسال است .

مثال : DATA

- سرویس دهنده ضمن اعلام آمادگی جهت دریافت داده ها به مبدا اعلام آمادگی می کند که پس از آخرین سطر نامه یک خط که فقط شامل تک کاراکتر "." است ارسال کند تا انتهای نامه مشخص باشد .

مثال : 354 Send mail; end with "." On a line by itself

- مبدا نامه ای را که با استاندارد RFC822 یا MIME تنظیم شده است ، ارسال می کند ؛ در انتهای نامه خطی که شامل تک حرف "." است به معنای خاتمه نامه ، ارسال می شود .
- سرویس دهنده دریافت موفقیت آمیز نامه را اعلام می کند ؛ این اعلام به صورت زیر است :

250 message accepted

- مبدا با ارسال رشته QUIT اعلام خروج می کند . (البته می تواند مجددا از مرحله دوم شروع کرده و نامه دیگری را ارسال کند.)
- فرستنده ضمن تایید خروج و معرفی مجدد خود اعلام می کند که ارتباط TCP را قطع خواهد کرد ، در این جا کار انتقال خاتمه یافته است.

مثال : 221 xyz.com closing connection

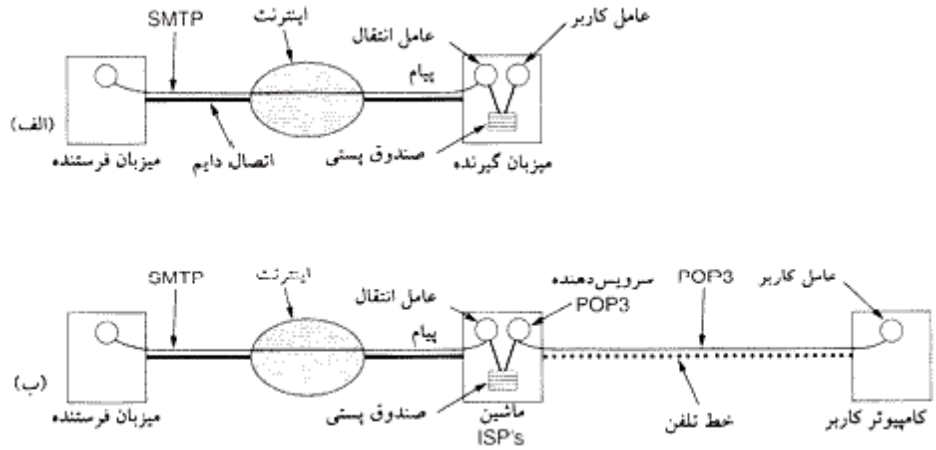
تحویل نهایی نامه :

در اینجا با یک سوال روبرو هستیم و آن اینکه کاربری که بطور نامنظم و پراکنده به شبکه اینترنت متصل می شود جگونه می تواند روی سیستمش SMTP را نصب و شبانه روز سیستم خود را برای دریافت نامه های خود روشن و فعال نگه دارد ؟

جواب این سوال ساده است کاربر باید وظیفه دریافت نامه هایش را به یک کارگزار مطمئن که به صورت دائم فعال است و سیستم SMTP را فراهم کرده بسپارد. هر موقع کهنامه ای برای او ارسال می شود کارگزارش آنرا دریافت و ذخیره می نماید. هنگامی که کاربر تمایل داشت سری به نامه های رسیده اس بزند و نامه ای را دریافت نماید بایستی با این کارگزار ارتباط برقرار نماید.

۲-۳- پروتکل POP3 :

POP3 پروتکل ساده برای دریافت نامه های الکترونیکی از سرویس دهنده ی کارگزار شما است. این پروتکل مجموعه ای از فرامین برای برقراری اتصال ، قطع اتصال ، دریافت پیام ها و حذف آن ها می باشد. این پروتکل نیز همانند SMTP فرامین متنی دارد .



(الف) وضعیتی که فرستنده و گیرنده دسترسی دائم به اینترنت دارند، و عامل کاربر و عامل انتقال پیام هر دو روی یک ماشین اجرا می‌شوند.

(ب) خواندن ایمیل در حالتی که گیرنده از طریق تلفن و با واسطهٔ یک ISP به اینترنت وصل می‌شود.

بدون آنکه بخواهیم وارد نکات ریز این پروتکل بشویم امکانات کلی آنرا معرفی می کنیم :

- ✓ **نصب فیلتر** : شما از سیستم پست الکترونیکی می خواهید که نامه های دزیافتی از یک آدرس خاص را اصلا تحویل نگیرد یا نامه هایی که قسمت موضوع آن شامل کلمات کلیدی خاص می شود را حذف کند یا مثلا نامه هایی را که کلمه ای خاص در آدرس فرستنده اش یافت میشود حذف نماید .
- ✓ **ارسال نامه های رسیده به آدرسی دیگر**
- ✓ **Vacation Daemon** : میتوانید سیستم پستی را وادار کنید که ضمن دریافت نامه ها یک پیغام برای ارسال کنندگان نامه بفرستد .

۲-۴- پروتکل IMAP :

برای کاربری که فقط با یک ISP کار می کند و همیشه هم از یک PC به آن وصل می شود ، POP3 بهترین گزینه است (بخصوص که ساده و کارآمد هم هست) . ولی در دنیای کامپیوتر اصلی بدیهیست که می گوید ،«وقتی چیزی دارد خوب کار میکند ، بلافاصله یکی پیدا می شود که بیشتر می خواهد.» برای ایمیل هم همین اتفاق افتاد. برای مثال خیلی از مردم هستند که فقط یک آدرس ایمیل دارند و میخواهند هر کجا که هستند با همان آدرس کار کنند. با اینکه POP3 میتواند از عهده ی این کار برآید ، اما کاربر بزودی متوجه می شود که ایمیل هایش روی چندین کامپیوتر پراکنده شده است (کامپیوترهایی که شاید بعضی از آن ها حتی متعلق به وی نباشند) .

این مشکل POP3 منجر به ارایه راه حلی بنام IMAP (پروتکل دسترسی پیام اینترنتی –Access Protocol Internet Message) شد . برخلاف POP3 که اساسا فرض می کند کاربر تمام پیامهایش را به کامپیوتر خود منتقل کرده و سپس ارتباط اینترنت را قطع می کند ، IMAP پیامها را برای همیشه روی کامپیوتر سرویس دهنده نگه داشته و آنها را در چندین صندوق پستی حفظ می کند. IMAP دارای مکانیزمهای پیشرفته ای برای خواندن پیامهاست ، که حتی اجازه می دهند کاربر فقط بخشهایی از یک پیام بخواند ؛ از آنجاییکه در IMAP فرض بر آن است که پیامها به کامپیوتر کاربر منتقل نمی شود ، مکانیزم هایی برای نوشتن ایمیل ، از بین بردن آنها ، یا مدیریت پیامهای رسیده (مانند دسته بندی آنها برحسب فرستنده) روی سرویس دهنده ایمیل درنظر گرفته شده است .

یکی از قابلیت های جالب IMAP دسته بندی و نمایش پیامهای رسیده بر حسب فرستنده ایمیل – یا ویژگی های دیگر – است . IMAP (بر خلاف POP3) فقط پروتکلی برای دریافت ایمیل نیست ، بلکه می تواند ارسال نامه ها را هم انجام دهد . روش کار IMAP بسیار شبیه POP3 است ، با این تفاوت که دستورات بسیار متنوعتری دارد . سویس دهنده IMAP به پورت ۱۴۳ گوش میکند . در جدول زیر مقایسه ای بین POP3 و IMAP آورده شده است . اما همین جا باید تذکر داد که تمام ISP ها (و همچنین برنامه های ایمیل) از هر دو پروتکل پشتیبانی نمی کنند.

ویژگی	POP3	IMAP
سطح تعریف پروتکل	RFC 1939	RFC 2060
پورت	110	143
سرویس دهنده	کاربرPC	سرویس دهنده
محل ذخیره شدن ایمیل	خارج خط	روی خط
محل خوانده شدن ایمیل	کم	زیاد
زمان اتصال	حداقل	گسترده
استفاده از منابع سرویس دهنده	خیر	بلی
صندوق پستی های متعدد	کاربر	ISP
مسئول گرفتن پشتیبان	خیر	بلی
مناسب برای کاربران سیار	کم	زیاد
کنترل بار کردن محتویات	خیر	بلی
بار کردن قسمتی از پیامها	خیر	گاهی
مشکل محدودیت دیسک	خیر	خیر
پیاده سازی ساده است	بلی	در حال و شد
پشتیبانی گسترده	بلی	

۲-۵- پروتکل انتقال ابرمتن HTTP :

پروتکل انتقال ابرمتن مجموعه ای از فرامین استانداردی است که از سمت مشتری به سمت سرویس دهنده ارسال می شود . در حقیقت این پروتکل طریقه صحبت کردن سرویس دهنده و مشتری را تبیین کرده است . درخواست ها از نوع متنی (ASCII) هستند ، و پاسخ سرویس دهنده یکی از انواع RFC822 MIME . تمام مشتری ها و سرویس دهنده ها باید از این پروتکل پیرو کنند .

اتصال

مرورگرها معمولا از طریق اتصال TCP به پورت ۸۰ سرویس دهنده با آن ارتباط برقرار می کند ، اگرچه الزامی رسمی نیست . خوبی اتصال TCP ان است که مرورگر یا سرویس دهنده هیچکدام لازم نیست نگران گم شدن پیام ها ، پیام های تکراری یا خیلی بلند و یا برگرداندن تصدق دریافت باشند ، چون تمام این کارها را TCP انجام می دهد.

در HTTP 1.0 ، بعد از برقراری اتصال یک درخواست فرستاده شده و یک پاسخ دریافت میشود و پس از آن اتصال قطع خواهد شد. در آن زمانی که صفحات HTML فقط متن بودند ، این روش کاملا کفایت میکرد اما خیلی زود صفحات وب پر شد از تصویر ، آیکون و چیزهایی مانند آن ، که برقراری یک اتصال TCP برای انتقال هر کدام از آن ها اصلا مقرون بصرفه نبود .

برای حل این کشکل HTTP 1.1 عرضه شد ، که از اتصال پایدار پشتیبانی می کرد . اتصال پایدار ، اتصالیست که می توان روی چندین بار درخواست و پاسخ ردوبدل کرد . بدین ترتیب سرباره ی TCP برای هر صفحه وب بسیار کمتر خواهد شد . در این روش امکان استفاده از تکنیک خط لوله هم وجود دارد ، که سرعت بارکردن صفحات را بسیار بهتر میکند .

متد

با اینکه HTTP برای استفاده در وب طراحی شد اما طراحان آن نگاهی به آینده ی برنامه شی گرا نیز داشتند . بهمین دلیل در HTTP عملیاتی غیر از درخواست صفحات وب نیز پیش بینی شده است ، که به آنها متد میگویند . هر درخواست HTTP یک خط متن ASCII است که با نام متد شروع میشود . در جدول زیر متدهایی که HTTP پشتیبانی میکند را میبینید . اضافه کردن متدهای جدید به HTTP نیز امکان پذیر است . نام متدها در HTTP به نوع حروف حساس است بنابراین متد GET را نمیتوان به صورت get نوشت .

نام فرمان	توضیح
GET	تقاضا برای دریافت یک صفحه وب از سرویس دهنده
HEAD	تقاضا برای دریافت سرآیند یک صفحه وب
PUT	تقاضا برای ذخیره کردن یک صفحه وب روی یک سرویس دهنده

POST	تقاضا برای ضمیمه کردن اطلاعاتی به یک منبع (مثل فایل یا صفحه وب)
DELETE	تقاضا برای حذف یک صفحه وب
LINK	تقاضا برای برقراری پیوند بین دو منبع موجود
UNLINK	تقاضای خاتمه پیوند دو منبع موجود

نمونه ای از کاربرد HTTP

از آنجاییکه HTTP یک پروتکل متنی است هیچ نیازی نیست مرورگر باشید تا بتوانید با یک سرویس دهنده ی وب تماس بگیرید ، فقط کافیست یک اتصال TCP به پورت ۸۰ سرویس دهنده داشته باشید . برای شروع فرمان زیر را باید وارد کرد :

Telne www.ietf.org 80 >log

Get /rfc.html HTTP/1.1

Host: www.ietf.org

Close

این فرمان یک اتصال TCP به ژورت ۸۰ سرویس دهنده ی وب IETF (www.ietf.org) برقرار میکند . نتیجه ی کار به فایل log هدایت می شود ، تا بعدا بتوان آنرا بهتر بررسی کرد . پس از آن فرمان GET (به همراه نام فایل و پروتکل) می آید ، و خط بعدی سرآیند اجباری Host است . خط خالی بعدی نیز اجباری است (این خط خالی به سرویس دهنده می گوید که ارسال سرآیندها از طرف ما تمام شده است . با فرمان Close هم به برنامه ی telnet گفته میشود که ارتباط قطع شود .

۲-۶- پروتکل پیکربندی پویای میزبان - DHCP

پروتکلی می باشد که توسط دستگاه های شبکه ای بکار می رود تا پارامترهای مختلف را که برای عملکرد برنامه های منابع گیر در پروتکل اینترنت ضروری می با شند را بدست آورد . با بکار گیری این پروتکل ، حجم کار مدیریت سیستم به شدت کاهش می یابد و دستگاه ها می توانندباحداقل تنظیمات و یا بدون تنظیمات دستی به شبکه اضافه شوند .

عملی بودن

پروتکل DHCP (پروتکل پیکر بندی پویای کامپیوتر میزبان) روشی برای اداره کردن جایگزینی پارامتر شبکه در یک سرور DHCP مستقل و یا گروهی از چنین سرور هایی است که به شیوه ای مقاوم در برابر اشکال چیده می شوند و با DHCP تکمیل شده اند . حتی در شبکه ای که چند ماشین سیستم DHCP مفید می باشد زیرا یک ماشین توسط شبکه ای محلی و با کمی تلاش قابل افزودن می باشد .

این برای تخصیص مستقیم نشانی ها در سرور ها و سیستم های رومیزی مفید می باشد و نیز بواسطه یک پروتکل نقطه به نقطه برای شماره

گیری و میزبان های پهن باند در صورت درخواست و نیز برای خروجی ها (برگردان آدرس شبکه) و مسیر یا ب ها مورد کاربرد دارد DHCP . معمولاً برای زیر ساخت (خدمات بنیادین) مانند مسیریاب های غیر حاشیه ای و سرور های DNS مناسب نمی باشند .

عملیات پروتکل

پروتکل پیکر بندی میزبان پویا(DHCP) تخصیص نشانه های آی پی ، پوشش های زیر شبکه ، دروازه پیش فرض (ورود گاه قراردادی)و دیگر پارامتر های آی پی را به صورت خودکار در می آورد. وقتی یک برنامه منابع گر با ترکیب DHCP به یک شبکه متصل شود ، (خواه یک کامپیوتر باشد یا هر وسیله مرتبط با شبکه)،برنامه منابع گیر DHCP آن یک سئوال سرتاسری ارسال می کندو از سرور DHCP اطلاعات ضروری را در خواست می کند. سرور DHCP مجموعه ای از اطلاعات و آدرس های آی پی را در مورد پارامتر های پیکر بندی منابع گیر مانند دروازه پیش فرض ،نام قلمرو، سرورهای DNS و سرورهای دیگر همچون سرورهای زمانی و غیره را مدیریت می کند .

بر اساس دریافت یک درخواست معتبر این سرور به کامپیوتر یک نشانی آی پی و یک مدت اجاره(طول زمانیکه تخصیص در آن اعتبار دارد)و دیگر پارامتر های پیکر بندی TCP/IP مانند پوشش زیر شبکه و ورود گاه قراردادی اختصاص خواهد داد. این پرس و جو نوعاً سریعاً پس از راه اندازی آغاز می شود و باید پیش از آنکه برنامه منابع گیر بتواند ارتباط مبتنی بر آی پی را با دیگر میزبان ها شروع کند تکمیل شود . DHCP سه حالت برای تخصیص نشانی های آی پی فراهم می کند .

حالت شناخته شده ،پویا (دینامیک) می باشد که در آن برای برنامه خدمات دیگر یک اجاره نامه روی نشانی IPبرای یک دوره زمانی فراهم می آید. منوط به ثبات شبکه این اجاره نامه می تواند از چند ساعت (شبکه بی سیم در یک فرودگاه) تا چند ماه (برای رومیزی ها در یک آزمایشگاه سیم بندی شده)وجود داشته باشد. به هر حال پیش از اینکه اجاره نامه منتفی شود ، DHCPمی تواند در خواست تمدید اجاره نامه را روی نشانی آی پی موجود بدهد .

یک برنامه منابع گیر با کار کرد مناسب ساز و کار تمدید را برای حفظ همان نشانی IP در سر تا سر اتصا لش به یک شبکه مستقل بکار می برد، در غیر اینصورت ممکن است خطر از دست دادن اجاره نامه اش (مدت اجاره)را در حین اتصال موجب شود، بنا بر این در حالیکه مجدداً برای نشانی IP اصلی یا جدیدش با سرور مذاکره می کند اتصال به شبکه دچار اختلال و اشکال شود .

دو حالت دیگر برای تخصیص نشانی های IP خودکار (اتوماتیک) و دستی می باشند ، که در حالت خودکار نشانی به طور دائم جایگزین منابع گیر می شود و در حالت دستی نشانی توسط منابع گیر انتخاب می شود و پیام های پروتکل DHCP برای مطلع کردن سرور نسبت به جایگزینی نشانی ، مورد استفاده قرار می گیرند.

روشهای دستی و خودکار به طور کلی زمانیکه کنترل دقیق تری روی نشانی IP مورد نیاز باشد بکار می روند (عموماً از نوع نصب دیواره آتش محکم با استقامت) ، اگرچه عموماً یک دیواره آتش امکان دسترسی به گستره ای از نشانی های IP را می دهد که می تواند به صورت پویایی توسط سرور DHCP جایگزین شوند .

۲-۷- پروتکل SNMP-پروتکل ساده مدیریت شبکه

نظارت بر وضعیت شبکه و اجزای آن و همچنین توانایی اعمال مدیریت بر روی ماشینهای میزبان و اجزای یک زیرشبکه (شامل مسیریابها ، پلها و ...)از ملزومات شبکه ی اینترنت محسوب می شود . در این راستا پروتکلهای مدیریت شبکه بوجود آمده اند . بدلیل ناهمگونی سخت افزار ارتباطی شبکه ها لاجرم نرم افزارهای مدیریت شبکه باید در لایه کاربرد پیاده سازی شوند .پیاده سازی نرم افزار مدیریت در لایه کاربرد باعث می شود پروتکل های مدیریت ، مستقل از سخت افزار شبکه طراحی گردند که در اینصورت مدیر شبکه می تواند با انواع مسیریابها و ماشینهای میزبان به یک روش مشابه ارتباط برقرار نماید و پروتکل مدیریت شبکه برای تمام اجزای آن یکسان و واحد باشد . از معایب پیاده سازی نرم افزار مدیریت در لایه کاربرد آن است که قابلیت اطمینان آن پایین می آید چراکه به هنگام بروز هر گونه مشکل پشته TCP/IP در یکی از عناصر شبکه قبل ار آنکه بتوان راهی را برای کشف و رفع عیب آن ارائه کرد ، نرم افزار مدیریت را از کار خواهد انداخت .

در مدل SNMP کلیه عناصر یک شبکه خودمختار (AS) به چهار رده ی زیر تقسیم بندی می شوند :

- نودهای تحت مدیریت : شامل ماشینهای میزبان ، مسیریابه ، پلها ، چاپگرها و هر ماشین دیگری که بتواند اطلاعاتی از وضیعیت خود به ایستگاههای مدیر ارسال نماید و از فرامین آنها تبعیت کند . یک نود تحت مدیریت باید قادر به اجرای پروسه ی کاربردی SNMP باشد . در این حالت به آن ایستگاه نمایندگی SNMP گفته میشود. هر نود تحت مدیریت ممکن است در کنترل چند ایستگاه مدیریت باشد که هر یک از این ایستگاههای مدیر ، سطوح دسترسی متفاوتی به آن ایستگاه دارند .
- ایستگاههای مدیریت : این ایستگاهها مراکز مدیریت شبکه می باشند و معمولا کامپیوترهای همه منظوره ای هستند که نرم افزار لازم برای مدیریت بر روی آنها نصب شده است . این ایستگاها با نمایندگیهها ارتباط برقرار کرده ، دستوراتی را صادر و پاسخهایی را دریافت می کنند . ممکن است نرم افزار مدیریت ، دارای رابط گرافیکی باشد که مسئول شبکه به سادگی وضعیت شبکه را نظارت کند .
- اطلاعات مدیریت : هر ایستگاه یک یا چند " متغیر وضعیت " را در حافظه سازماندهی و نگهداری می کند که این متغیرها وضعیت فعلی آنرا توصیف می کنند . در ادبیات پروتکل SNMP این متغیرها اشیا نامیده شده اند.
- قرداد مدیریت : روشی است استاندارد و مستقل که بر اساس آن ، ایستگاه مدیر با نمایندگیها ارتباط برقرار می کند و قادر است حالت اشیا (متغیرهای وضیعت) آنها را تقاضا کرده و در صورت لزوم آنها را تغییر دهد .

هسته ی اصلی پروتکل SNMP مجموعه ای از اشیا (متغیرهای وضعیت) است که می تواند توسط ایستگاههای مدیریت خوانده یا نوشته شوند . برای آنکه تمام ایستگاههای شبکه با هرگونه اختلاف بنیادی از لحاظ سخت افزار و نرم افزار قادر به ارتباط با مدیریت شبکه باشند باید ساختار اشیا دقیقا استاندارد باشد . زبان توصیفی ASN.1 استانداردی است که با آن اشیا و متغیرهای حالت تعریف میشوند.

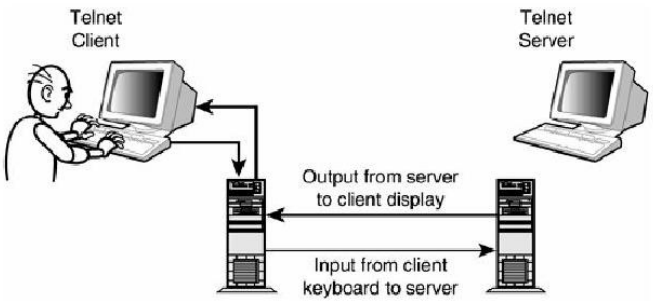
مدیریت شبکه درخواستی را به نمایندگی می فرستد و اطلاعاتی را از وی خواسته و یا در صدد تغیر حالت برمی آید . در SNMP حدود ۱۷۵ متغیر حالت و وضیعیت تعریف شده که هر یک به نحوی برای نظارت و مدیریت شبکه بکار می آید . در SNMP از یک روش واکشی جالب استفاده می شود به این ترتیب که تمامی عملیات و فرمانها در قالب روش واکشی و ذخیره ی متغیرهای حالت انجام می شود . پروتکل SNMP مجموعا دارای هفت فرمان است که شش فرمان از هفت فرمان آن در جدول زیر آورده شده است :

Message	توضیح
Get-request	**درخواست مقدار یک یا چند متغیر حالت**
Get-next-request	**درخواست متغیر بعدی**
Get-bulk-request	**واکشی جداول بزرگتر**
Set-request	**بهنگام سازی متغیرهای حالت**
Inform-request	**یک مدیر به مدیر دیگر متغیری را که در حال مدیریت آن است اعلام میکند**
SnmpV2-trap	**جهت گزارش یک رخداد از طرف یکی از ایستگاهها به مدیر**

پروتکل SNMP برخلاف اسم آن چندان هم ساده نیست و مستندات آن ۶۰۰ صفحه را در برمیگیرد .

۲-۸- پروتکل TelNet

TelNet یکی از پروتکلهای شبکه است که در اتصالات اینترنت و شبک ههای محلی مورد استفاده قرار میگیرد. در واقع از TelNet برای مکالمه دو سیستم با هم استفاده می شود . TelNet یکی از قدیم یترین استانداردهای شبکه است و پیدایش آن به سال 1969 میلادی باز میگردد . کاربرد اصلی TelNet ایجاد دسترسی به رابط خط فرمان یک ماشین واقع در راه دور است .برای رسیدن به چنین هدفی متخصصانی که این پروتکل را تعریف و طراحی کردند همانند سایر پروتکلها یک معماری متقاضی / سرویس دهنده / (Client/Server) را در نظر گرفتند . در این صورت برای یک ارتباط Telnet باید سیستمی به عنوان متقاضی، درخواستی داشته باشد و در صورت سیستم سرویس دهنده ارتباط برقرار میشود.



ارتباط متقاضی با سرویس دهنده با استفاده از TelNet

TelNet نیاز به سخت افزار خاصی ندارد .همچنین اصول فرمانی آن به یک نرم افزار یا سیستم عامل خاص محدود نمیشود.

در واقع طیف وسیعی از سخت افزارهای شبکه و سیستم های عامل مختلف از جمله یونیکس 4 و سولاریس 5 نیز این پروتکل را به راحتی پشتیبانی میکنند .پس همان طور که ذکر شد این مهم نیست که کدام برنامه بر روی کدام سیستم عامل یا سخت افزار در حال استفاده از TelNet است .تنها لازم است یک ارتباط گیرنده /فرستنده وجود داشته باشد که از TCP/IP استفاده کند.

TelNet در واقع یکی از پر استفادهترین ابزارها برای شبکههای داخلی یونیکس است که طیف وسیعی از عملیات را پشتیبانی می کند. برای مثال یک مدیر سیستمی می تواند از راه دور با استفاده از TelNet عملیات مورد نظرش را بر روی میزبان هدف انجام دهد .از جمله این عملیات می توان به حذف و اضافه کردن فایلها با ایجاد دایرکتوری ها و غیره اشاره کرد .لازم است بدانید که این پروتکل به صورت پیش فرض از درگاه ۲۳ استفاده میکند، اما این بدان معنا نیست که نمیتوان از این سرویس در سایر درگاهها استفاده کرد .فقط در صورت استفاده از درگاه دیگری به غیر از درگاه پیش فرض، تواناییهای ارتباط با سرویس دهنده TelNet از بین می رود یعنی برنامه TelNet میزبان قادر به گرفتن دستورات متناظر با TelNet مقابل نخواهد بود .

از آنجا که پیدایش پروتکل به سالهای 1969 میلادی برمیگردد و در این سا لها کلیه کاربرانی که به شبکه های مورد استفاده درمؤسسات دسترسی داشتند از کارمندان آنها بودند، بنابراین امنیت جایگاه زیادی نداشت و موارد امنیتی در این پروتکل به صورت کامل لحاظ نشده بود. علی رغم کاربرد فراوان پروتکل Telnet و موارد استفاده بسیار آن در مؤسسات، رفته رفته استفاده از ان منسوخ شده است و نسل جدیدی از آن با نام SSH که قابلیت رمزنگاری اطلاعات ارسالی را داراست عرضه شده است .از این جهت در صورتی که موارد امنیتی در شبکه شما از اهمیت برخوردار است استفاده از پروتکل TelNet پیشنهاد نمیشود.

۲-۹- پروتکلRemote Desktop Protocol (RDP)

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 ، RDPنیز 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 Terminal Server نیز مشهور بوده و در مایکروسافت ، همان سرویس Remote_Desktop است که از طریق System Propertiesفعال 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 .

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

۲-۱۰- پروتکل FTP

امروزه از پروتکل های متعددی در شبکه های کامپیوتری استفاده می گردد که صرفا" تعداد اندکی از آنان به منظور انتقال داده طراحی و پیاده سازی شده اند . اینترنت نیز به عنوان یک شبکه گسترده از این قاعده مستثنی نبوده و در این رابطه از پروتکل های متعددی استفاده می شود.

برای بسیاری از کاربران اینترنت همه چیز محدود به وب و پروتکل مرتبط با آن یعنی HTTP است ، در صورتی که در این عرصه از پروتکل های متعدد دیگری نیز استفاده می گردد. FTP نمونه ای در این زمینه است .

یکی از عملیاتی که کاربران اینترنت قادر به انجام آن هستند ، دریافت داده ، فایل های صوتی ، تصویری و سایر نمونه فایل های دیگر با استفاده از پروتکلFTP برگرفته از (File Transfer Protocol) است .

ویژگی های پروتکل FTP

- پروتکل FTP ، اولین تلاش انجام شده برای ایجاد یک استاندارد به منظور مبادله فایل بر روی شبکه های مبتنی بر پروتکل TCP/IP است که از اوایل سال ۱۹۷۰ مطرح و مشخصات استاندارد آن طی RFC 959 در اکتبر سال ۱۹۸۵ ارائه گردید .
- پروتکل FTP دارای حداکثر انعطاف لازم و در عین حال امکان پذیر به منظور استفاده در شبکه های مختلف با توجه به نوع پروتکل شبکه است .
- پروتکل FTP از مدل سرویس گیرنده - سرویس دهنده تبعیت می نماید . برخلاف HTTP که یک حاکم مطلق در عرصه مرورگرهای وب و سرویس دهندگان وب است ، نمی توان ادعای مشابهی را در رابطه با پروتکل FTP داشت و هم اینک مجموعه ای گسترده از سرویس گیرندگان و سرویس دهندگان FTP وجود دارد .
- برای ارسال فایل با استفاده از پروتکل FTP به یک سرویس گیرنده FTP نیاز می باشد . ویندوز دارای یک برنامه سرویس گیرنده FTP از قبل تعبیه شده می باشد ولی دارای محدودیت های مختص به خود می باشد . در این رابطه نرم افزارهای متعددی تاکنون طراحی و پیاده سازی شده است:

ulletProof FTP ، WS FTP Professional، FTP Explorer و Smart FTP نمونه هائی در این زمینه می باشند .

- پروتکل FTP را می توان به عنوان یک سیستم پرس وجو نیز تلقی نمود چراکه سرویس گیرندگان و سرویس دهندگان گفتگوی لازم به منظور تائید یکدیگر و ارسال فایل را انجام می دهند. علاوه بر این، پروتکل فوق مشخص می نماید که سرویس گیرنده و سرویس دهنده، داده را بر روی کانال گفتگو ارسال نمی نمایند . در مقابل ، سرویس گیرنده و سرویس دهنده در خصوص نحوه ارسال فایل ها بر روی اتصالات مجزا و جداگانه (یک اتصال برای هر ارسال داده) با یکدیگر گفتگو خواهند کرد (نمایش لیست فایل های موجود در یک دایرکتوری نیز به عنوان یک ارسال فایل تلقی می گردد) .
- پروتکل FTP امکان استفاده از سیستم فایل را مشابه پوسته یونیکس و یا خط دستور ویندوز در اختیار کاربران قرار می دهد .
- سرویس گیرنده در ابتدا یک پیام را برای سرویس دهنده ارسال و سرویس دهنده نیز به آن پاسخ خواهد داد و در ادامه ارتباط غیرفعال می گردد . وضعیت فوق با سایر پروتکل هائی که به صورت تراکنشی کار می کنند ، متفاوت می باشد (نظیر پروتکل HTTP) . برنامه های سرویس گیرنده زمانی قادر به شبیه سازی یک محیط تراکنشی می باشند که از مسائلی که قرار است در آینده محقق شوند ، آگاهی داشته باشند . در واقع ، پروتکل FTP یک دنباله stateful از یک و یا چندین تراکنش است.

- سرویس گیرندگان ، مسئولیت ایجاد و مقداردهی اولیه درخواست ها را برعهده دارند که با استفاده از دستورات اولیه FTP انجام می گردد. دستورات فوق ، عموما" سه و یا چهار حرفی می باشند (مثلا " برای تغییر دایرکتوری از دستور CWD استفاده می شود). سرویس دهنده نیز بر اساس یک فرمت استاندارد به سرویس گیرندگان پاسخ خواهد داد (سه رقم که به دنبال آن از space استفاده شده است به همراه یک متن تشریحی) . سرویس گیرندگان می بایست صرفا " به کد عددی نتیجه استناد نمایند چراکه متن تشریحی تغییر پذیر بوده و در عمل برای اشکال زدائی مفید است (برای کاربران حرفه ای) .
- پروتکل FTP دارای امکانات حمایتی لازم برای ارسال داده با نوع های مختلف می باشد . دو فرمت متداول، اسکی برای متن (سرویس گیرنده با ارسال دستور TYPE A ،موضوع را به اطلاع سرویس دهنده می رساند) و image برای داده های باینری است (توسط TYPE I مشخص می گردد) . ارسال داده با فرمت اسکی در مواردی که ماشین سرویس دهنده و ماشین سرویس گیرنده از استانداردهای متفاوتی برای متن استفاده می نمایند ، مفید بوده و یک سرویس گیرنده می تواند پس از دریافت داده آن را به فرمت مورد نظر خود ترجمه و استفاده نماید . مثلا " در نسخه های ویندوز از یک دنباله carriage return و linefeed برای نشان دادن انتهای خط استفاده می گردد در صورتی که در سیستم های مبتنی بر یونیکس صرفا " از یک linefeed استفاده می شود . برای ارسال هرنوع داده که به ترجمه نیاز نداشته باشد،می توان از ارسال باینری استفاده نمود.
- اتخاذ تصمیم در رابطه با نوع ارسال فایل ها در اختیار سرویس گیرنده است (برخلاف HTTP که می تواند به سرویس گیرنده نوع داده ارسالی را اطلاع دهد) . معمولا " سرویس گیرندگان ارسال باینری را انتخاب می نمایند و پس از دریافت فایل ، ترجمه لازم را انجام خواهند داد . ارسال باینری ذاتا " دارای کارآئی بیشتری است چراکه سرویس دهنده و سرویس گیرنده نیازی به انجام تراکنش های on the fly نخواهند داشت . ارسال اسکی گزینه پیش فرض انتخابی توسط پروتکل FTP است و در صورت نیاز به ارسال باینری ، سرویس گیرنده می بایست این موضوع را از سرویس دهنده درخواست نماید .
- پروتکل FTP منحصرا" از پروتکل TCP استفاده می نماید(هرگز از پروتکل UDP استفاده نمی شود) . معمولا " پروتکل های لایه Application (با توجه به مدل مرجع OSI) از یکی از پروتکل های TCP و یا UDP استفاده می نمایند (به جزء پروتکل DNS) . پروتکل FTP نیز از برخی جهات شرایط خاص خود را دارد و برای انجام وظایف محوله از دو پورت استفاده می نماید . این پروتکل معمولا" از پورت شماره ۲۰ برای ارسال داده و از پورت ۲۱ برای گوش دادن به فرامین استفاده می نماید . توجه داشته باشید که برای ارسال داده همواره از پورت ۲۰ استفاده نمی گردد و ممکن است در برخی موارد از پورت های دیگر استفاده شود .
- اکثر سرویس دهندگان FTP از روش خاصی برای رمزنگاری اطلاعات استفاده نمی نمایند و در زمان login سرویس گیرنده به سرویس دهنده ، اطلاعات مربوط به نام و رمز عبور کاربر به صورت متن معمولی در شبکه ارسال می گردد . افرادی که دارای یک Packet sniffer بین سرویس گیرنده و سرویس دهنده می باشند ، می توانند به سادگی اقدام به سرقت نام و رمز عبور نمایند

. علاوه بر سرقت رمزهای عبور ، مهاجمان می توانند تمامی مکالمات بر روی اتصالات FTP را شنود و محتویات داده های ارسالی را مشاهده نمایند . پیشنهادات متعددی به منظور ایمن سازی سرویس دهنده FTP مطرح می گردد ولی تا زمانی که رمزنگاری و امکانات حفاظتی در سطح لایه پروتکل IP اعمال نگردد (مثلا" رمزنگاری توسط IPsecs) ، نمی بایست از FTP استفاده گردد خصوصا" اگر بر روی شبکه اطلاعات مهم و حیاتی ارسال و یا دریافت می گردد .

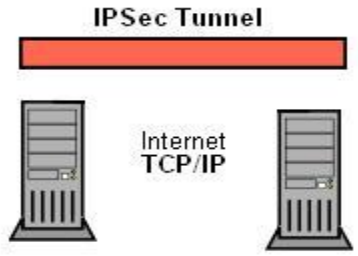
FTP، یک پروتکل ارسال فایل است که با استفاده از آن سرویس گیرندگان می توانند به سرویس دهندگان متصل و صرفنظر از نوع سرویس دهنده اقدام به دریافت و یا ارسال فایل نمایند .

و اما یک نکته دیگر در رابطه با پروتکل FTP

در صورتی که در زمان دریافت یک فایل با استفاده از پروتکل FTP مشکلات خاصی ایجاد که منجر به قطع ارتباط با سرویس دهنده FTP گردد ، سرویس گیرنده می تواند با مشخص کردن یک offset از فایل دریافتی به سرویس دهنده اعلام نماید که عملیات ارسال را از جایی که ارتباط قطع شده است ، ادامه دهد (سرویس گیرنده از محلی شروع به دریافت فایل می نماید که ارتباط غیرفعال شده بود) . استفاده از ویژگی فوق به امکانات سرویس دهنده FTP بستگی دارد .

۳-امنیت

۳-۱- پروتکل امنیتی ipsec



IPSec بسته های TCP/IP را در طول مسیر رمز میکند

این پروتکل برای این منظور طراحی شده که بتواند بسته (Packet) های اطلاعاتی TCP/IP را توسط کلید عمومی رمز کند تا در طول مسیر، امکان استفاده غیر مجاز از آنها وجود نداشته باشد.

به بیان دیگر کامپیوتر مبدا" بسته اطلاعاتی TCP/IP عادی را بصورت یک بسته اطلاعاتی IPSec بسته بندی (Encapsulate) می کند و برای کامپیوتر مقصد ارسال میکند. این بسته تا زمانی که به مقصد برسد رمز شده است و طبیعتا " کسی نمی تواند از محتوای آنها اطلاع بدست آورد .

بدیهی ترین نکته آن است که استفاده از این پروتکل زمان نقل و انتقال اطلاعات را بیشتر می کند چرا که هم حجم اطلاعات بیشتر می شود و هم زمانی برای رمز کردن و رمزگشایی .

IPSec Policy

شما می توانید با دادن یک سری دستورالعمل ها به Windows ، او را تعلیم دهید که تحت چه شرایطی از IPSec استفاده کند. تحت این شرایط شما در واقع مشخص می کنید که ترافیک کدام گروه از IP ها باید توسط IPSec انجام شود و کدامیک نشود برای این منظور معمولا " از روش فیلتر کردن IP استفاده می شود. فهرست خاصی از IP های فیلتر شده که شما تهیه می کنید می تواند مرجعی برای استفاده از پروتکل IPSec برای ویندوز باشد .

IP Security یا IPSec رشته ای از پروتکلهاست که برای ایجاد VPN مورد استفاده قرار می گیرند. مطابق با تعریف IETF پروتکل IPSec به این شکل تعریف می شود:

یک پروتکل امنیتی در لایه شبکه تولید خواهد شد تا خدمات امنیتی رمزنگاری را تامین کند. خدماتی که به صورت منعطفی به پشتیبانی ترکیبی از تایید هویت ، جامعیت ، کنترل دسترسی و محرمانگی بپردازد.

در اکثر سناریوها مورد استفاده ، IPSec به شما امکان می دهد تا یک تونل رمزشده را بین دو شبکه خصوصی ایجاد کنی د . همچنین امکان تایید هویت دو سر تونل را نیز برای شما فراهم می کند.اما IPSec تنها به ترافیک مبتنی بر IP اجازه بسته بندی و رمزنگاری می دهد و درصورتی که ترافیک غیر IP نیز در شبکه وجود داشته باشد ، باید از پروتکل دیگری مانند GRE در کنار IPSec استفاده کرد .

IPSec به استاندارد de facto در صنعت برای ساخت VPN تبدیل شده است .

انواعIPSec VPN

شیوه های مختلفی برای دسته بندی IPSec VPN وجود دارد اما از نظر طراحی ، IPSec برای حل دو مسئله مورد استفاده قرار می گیرد :

۱- اتصال یکپارچه دو شبکه خصوصی و ایجاد یک شبکه مجازی خصوصی

۲- توسعه یک شبکه خصوصی برای دسترسی کاربران از راه دور به آن شبکه به عنوان بخشی از شبکه امن

بر همین اساس ، IPSec VPNها را نیز می توان به دو دسته اصلی تقسیم کرد:

۱ - پیاده سازی LAN-to-LAN IPSec

این عبارت معمولا برای توصیف یک تونل IPSec بین دو شبکه محلی به کار می رود. در این حالت دو شبکه محلی با کمک تونل IPSec و از طریق یک شبکه عمومی با هم ارتباط برقرار می کنند به گونه ای که کاربران هر شبکه محلی به منابع شبکه محلی دیگر، به عنوان عضوی از آن شبکه، دسترسی دارند IPSec . به شما امکان می دهد که تعریف کنید چه داده ای و چگونه باید رمزنگاری شود .

۲- پیاده سازی Remote-Access Client IPSec

این نوع از VPN ها زمانی ایجاد می شوند که یک کاربر از راه دور و با استفاده از IPSec client نصب شده بر روی رایانه اش، به یک روتر IPSec یا Access server متصل می شود . معمولا این رایانه های دسترسی از راه دور به یک شبکه عمومی یا اینترنت و با کمک روش dialup یا روشهای مشابه متصل می شوند . زمانی که این رایانه به اینترنت یا شبکه عمومی متصل می شود ، IPSec client موجود بر روی آن می تواند یک تونل رمز شده را بر روی شبکه عمومی ایجاد کند که مقصد آن یک دستگاه پایانی IPSec ، مانند یک روتر ، که بر لبه شبکه خصوصی مورد نظر که کاربر قصد ورود به آن را دارد ، باشد.

در روش اول تعداد پایانه های IPSec محدود است اما با کمک روش دوم می توان تعداد پایانه ها را به ده ها هزار رساند که برای پیاده سازی های بزرگ مناسب است.

ساختارIPSec

IPSec برای ایجاد یک بستر امن یکپارچه ، سه پروتکل را با هم ترکیب می کند :

۱ - پروتکل مبادله کلید اینترنتی (Internet Key Exchange) یا IKE

این پروتکل مسئول طی کردن مشخصه های تونل IPSec بین دو طرف است. وظایف این پروتکل عبارتند از:

- طی کردن پارامترهای پروتکل
- مبادله کلیدهای عمومی
- تایید هویت هر دو طرف
- مدیریت کلیدها پس از مبادله

IKE مشکل پیاده سازی های دستی و غیر قابل تغییر IPSec را با خودکار کردن کل پردازه مبادله کلید حل می کند. این امر یکی از نیازهای حیاتیIPSec است IKE .خود از سه پروتکل تشکیل می شود:

- SKEME : مکانیزمی را برای استفاده از رمزنگاری کلید عمومی در جهت تایید هویت تامین می کند.
- Oakley : مکانیزم مبتنی بر حالتی را برای رسیدن به یک کلید رمزنگاری، بین دو پایانه IPSec تامین می کند.
- ISAKMP : معماری تبادل پیغام را شامل قالب بسته ها و حالت گذار تعریف می کند.

با وجودی که IKE کارایی و عملکرد خوبی را برای IPSec تامین می کند، اما بعضی کمبودها در ساختار آن باعث شده است تا پیاده سازی آن مشکل باشد ، لذا سعی شده است تا تغییراتی در آن اعمال شود و استاندارد جدیدی ارائه شود که IKE v2 نام خواهد داشت.

۲ - پروتکل (Encapsulating Security Payload) یاESP

این پروتکل امکان رمزنگاری ، تایید هویت و تامین امنیت داده را فراهم می کند.

۳- پروتکل سرآیند تایید هویت (Authentication Header) یا AH

این پروتکل برای تایید هویت و تامین امنیت داده به کار می رود .

۳-۲- پروتکل امنیتی SSL

SSL یا Secure Socket Layer راه حلی جهت برقراری ارتباطات ایمن میان یک سرویس دهنده و یک سرویس گیرنده است که توسط شرکت Netscape ارایه شده است. در واقع SSL پروتکلی است که پایین تر از لایه کاربرد لایه ۴ از مدل (TCP/IP) و بالاتر از لایه انتقال لایه سوم از مدل (TCP/IP) قرار می گیرد. مزیت استفاده از این پروتکل، بهره گیری از موارد امنیتی تعبیه شده آن برای امن کردن پروتکل های غیرامن لایه کاربردی نظیر HTTP ، LDAP، IMAPو... می باشد که براساس آن الگوریتم های رمزنگاری بر روی داده های خام (plain text) که قرار است از یک کانال ارتباطی غیرامن مثل اینترنت عبور کنند، اعمال می شود و محرمانه ماندن داده ها را در طول کانال انتقال تضمین می کند .

SSL Handshake Protocol	**SSL Change Cipher Spec Protocol**	**SSL Alert Protocol**	**HTTP**
SSL Record Protocol			
TCP			
IP			

به بیان دیگر شرکتی که صلاحیت صدور و اعطای گواهی های دیجیتال SSL را دارد برای هر کدام از دو طرفی که قرار است ارتباطات میان شبکه ای امن داشته باشند، گواهی های مخصوص سرویس دهنده و سرویس گیرنده را صادر می کند و با مکانیزم های احراز هویت خاص خود هویت هر کدام از طرفین را برای طرف مقابل تایید می کند، البته غیر از این کار می بایست تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گرفت، برای رباینده قابل درک و استفاده نباشد که این کار را با کمک الگوریتم های رمزنگاری و کلیدهای رمزنگاری نامتقارن و متقارن انجام می دهد .

- ملزومات یک ارتباط مبتنی بر پروتکل امنیتیSSL

برای داشتن ارتباطات امن مبتنی بر SSL عموما به دو نوع گواهی دیجیتال SSL یکی برای سرویس دهنده و دیگری برای سرویس گیرنده و یک مرکز صدور و اعطای گواهینامه دیجیتال یا CA نیاز می باشد. وظیفه CA این است که هویت طرفین ارتباط، نشانی ها، حساب های بانکی و تاریخ انقضای گواهینامه را بداند و براساس آن ها هویت ها را تعیین نماید .

- مکانیزم های تشکیل دهندهSSL

۱ -تایید هویت سرویس دهنده

با استفاده از این ویژگی در SSL ، یک کاربر از صحت هویت یک سرویس دهنده مطمئن می شود. نرم افزارهای مبتنی بر SSLسمت سرویس گیرنده، مثلا یک مرورگر وبنظیر Internet Explorer از تکنیک های استاندارد رمزنگاری مبتنی بر کلید عمومی و مقایسه با کلیدهای عمومی یک سرویس دهنده، (مثلا یک برنامه سرویس دهنده وب نظیر IIS می تواند از هویت او مطلع شود و پس از اطمینان کامل، کاربر می تواند نسبت به وارد نمودن اطلاعات خود مانند شماره کارت های اعتباری و یا گذرواژه ها اقدام نماید .

۲ -تایید هویت سرویس گیرنده

برعکس حالت قبلی در اینجا سرویس دهنده است که می بایست از صحت هویت سرویس گیرنده اطمینان یابد. طی این مکانیزم، نرم افزار مبتنی بر SSL سمت سرویس دهنده پس از مقایسه نام سرویس گیرنده با نام های مجاز موجود در لیست سرویس گیرنده های مجاز که در داخل سرویس دهنده تعریف می شود و در صورت وجود، اجازه استفاده از سرویس های مجاز را به او می دهد .

۳ -ارتباطات رمز شده

کلیه اطلاعات مبادله شده میان سرویس دهنده و گیرنده می بایست توسط نرم افزارهای موجود در سمت سرویس دهنده و سرویس گیرنده رمزنگاری (Encrypt) شده و در طرف مقابل رمزگشایی (Decrypt) شوند تا حداکثر محرمانگی (Confidentiality) در این گونه سیستم ها لحاظ شود .

- نحوه عملکرد داخلی پروتکلSSL

همان طور که می دانید SSL می تواند از ترکیب رمزنگاری متقارن و نامتقارن استفاده کند. رمزنگاری کلید متقارن سریع تر از رمزنگاری کلید عمومی است و از طرف دیگر رمزنگاری کلید عمومی تکنیک های احراز هویت قوی تری را ارایه می کند. یک جلسه (SSL Session) SSL با یک تبادل پیغام ساده تحت عنوان SSL Handshake شروع می شود. این پیغام اولیه به سرویس دهنده این امکان را می دهد تا خودش را به سرویس دهنده دارای کلید عمومی معرفی نماید و سپس به سرویس گیرنده و سرویس دهنده این اجازه را می دهد که یک کلید متقارن را ایجاد نمایند که برای رمزنگاری ها و رمزگشایی سریع تر در جریان ادامه مبادلات مورد استفاده قرار می گیرد. گام هایی که قبل از برگزاری این جلسه انجام می شوند براساس الگوریتم RSA Key Exchange عبارتند از :

۱ -سرویس گیرنده، نسخه SSL مورد استفاده خود، تنظیمات اولیه درباره نحوه رمزگذاری و یک داده تصادفی را برای شروع درخواست یک ارتباط امن مبتنی بر SSL به سمت سرویس دهنده ارسال می کند .

۲ -سرویس دهنده نیز در پاسخ نسخه SSL مورد استفاده خود، تنظیمات رمزگذاری و داده تصادفی تولید شده توسط خود را به سرویس گیرنده می فرستد و همچنین سرویس دهنده گواهینامه خود را نیز برای سرویس گیرنده ارسال می کند و اگر سرویس گیرنده از سرویس دهنده، درخواستی داشت که نیازمند احراز هویت سرویس گیرنده بود، آن را نیز از سرویس گیرنده درخواست می کند .

۳ -سپس سرویس گیرنده با استفاده از اطلاعاتی که از سرویس دهنده مجاز در خود دارد، داده ها را بررسی می کند و اگر سرویس دهنده مذکور تایید هویت شد، وارد مرحله بعدی می شود و در غیر این صورت با پیغام هشداری به کاربر، ادامه عملیات قطع می گردد .

۴ -سرویس گیرنده یک مقدار به نام Secret Premaster را برای شروع جلسه ایجاد می کند و آن را با استفاده از کلید عمومی (که اطلاعات آن معمولا در سرویس دهنده موجود است) رمزنگاری می کند و این مقدار رمز شده را به سرویس دهنده ارسال می کند .

۵ -اگر سرویس دهنده به گواهینامه سرویس گیرنده نیاز داشت می بایست در این گام برای سرویس دهنده ارسال شود و اگر سرویس گیرنده نتواند هویت خود را به سرویس دهنده اثبات کند، ارتباط در همین جا قطع می شود .

۶ -به محض این که هویت سرویس گیرنده برای سرویس دهنده احراز شد، سرویس دهنده با استفاده از کلید اختصاصی خودش مقدار Premaster Secretرا رمزگشایی می کند و سپس اقدام به تهیه مقداری به نام Master Secret می نماید .

۷ -هم سرویس دهنده و هم سرویس گیرنده با استفاده از مقدار Master Secret کلید جلسه (Session Key) را تولید می کنند که در واقع کلید متقارن مورد استفاده در عمل رمزنگاری و رمزگشایی داده ها حین انتقال اطلاعات است و در این مرحله به نوعی جامعیت داده ها بررسی می شود .

۸ -سرویس گیرنده پیغامی را به سرویس دهنده می فرستد تا به او اطلاع دهد، داده بعدی که توسط سرویس گیرنده ارسال می شود به وسیله کلید جلسه رمزنگاری خواهد شد و در ادامه، پیغام رمز شده نیز ارسال می شود تا سرویس دهنده از پایان یافتن Handshake سمت سرویس گیرنده مطلع شود .

۹ -سرویس دهنده پیغامی را به سرویس گیرنده ارسال می کند تا او را از پایان Handshake سمت سرویس دهنده آگاه نماید و همچنین این که داده بعدی که ارسال خواهد شد توسط کلید جلسه رمز می شود .

۱۰ -در این مرحله SSL Handshake تمام می شود و از این به بعد جلسه SSL شروع می شود و هر دو عضو سرویس دهنده و گیرنده شروع به رمزنگاری و رمزگشایی و ارسال داده ها می کنند .

نمایش قفل امنیتSSL

پیچیده گیهای یک پروتکل SSL برای کاربران شما پوشیده است لیکن مرورگر اینترنت آنها در صورت برقراری ارتباط امن , وجود این ارتباط را توسط نمایش یک قفل کوچک در پایین صفحه متذکر میشود .

کلیک برروی قفل کوچک باعث نمایش گواهینامه شما به همراه سایر جزئیات میشود .

گواهینامه های SSL تنها برای شرکتها و اشخاص حقیقی معتبر صادر میشوند. به طور مثال یک گواهینامه SSL شامل اطلاعاتی در مورد دامین , شرکت , آدرس , شهر , استان , کشور و تاریخ ابطال گواهینامه و همینطور اطلاعاتی در مورد مرکز صدور گواهینامه که مسؤول صدور گواهینامه میباشد .

زمانیکه یک مرورگر اینترنت به یک سایت از طریق ارتباط امن متصل میشود , علاوه بر دریافت گواهینامه) SSL کلید عمومی) , پارامترهایی را نظیر تاریخ ابطال گواهینامه , معتبر بودن صادرکننده گواهینامه و مجاز بودن سایت به استفاده از این گواهینامه نیز بررسی میکند و هرکدام از موارد که مورد تایید نباشد به صورت یک پیغام اخطار به کاربر اعلام میدارد .