مدل شبکه TCP/IP

امروزه در دنیا شبکه اینترنت برای تبادل اطلاعات بین کاربران مختلف استفاده می شود. دارای پروتکل های متعددی بوده که در بخش های مختلف این شبکه بکار می روند. برای طراحی پروتکل های جدید و همچنین تجزیه و تحلیل پروتکل های موجود و نحوه انتقال اطلاعات در این شبکه مدلی از آن ارائه شده که چهار لایه بصورت زیر است. با مقایسه این مدل با مدل جامع OSI میتوان گفت که در مدل TCP/IP چند لایه بصورت ادغام شده در کنار هم قرار گرفته اند.

مدل TCP/IP

لایه کاربردی (سرویس ها)	۴
لایه میزبان به میزبان	۳
لایه اینترنت	۲
لایه دسترسی به شبکه	۱

۱-لایه دسترسی به شبکه

این لایه که اولین لایه مدل TCP/IP محسوب می شود، امکان ارتباط یک کامپیوتر را به شبکه اینترنت از طریق کارت شبکه، مودم یا پورت سریال برقرار می کند. همچنین در این لایه این امکان ایجاد می شود تا بتوان از مدارات واسطه دیگری که بر روی کامپیوتر نصب شده اند با شبکه اینترنت ارتباط برقرار کرد. در صورت بکارگیری کارت شبکه و با توجه به توپولوژی شبکه محلی یکی از پروتکل های Ethernet، Token Bus و Token Ring استفاده می شود. در صورتی که از درگاه سریال یا مودم برای ارتباط با شبکه اینترنت استفاده کنیم یکی از پروتکل های SLIP و PPP بکار خواهد رفت. با مقایسه این دو پروتکل با یکدیگر می توان گفت که PPP قابلیتهای بیشتری نسبت به SLIP دارد: توانایی تصدیق یا تائید هویت (Authentication) که کاربر را وادار به وارد کردن نام کاربری و کلمه عبور جهت ورود به شبکه می نماید، همچنین قابلیت فشرده سازی داده ها و تشخیص خطای بهتر نسبت به SLIP. به همین دلیل امروزه در اکثر سیستم های عامل پروتکل PPP جهت تماس کامپیوتر با شبکه اینترنت از طریق مودم یا درگاه سریال در نظر گرفته شده است.

SLIP (Serial Line Internet Protocol)
PPP (Point to Point Protocol)

۲-لایه اینترنت

در این لایه پروتکل های متنوعی وجود دارند که برای اعمالی مانند آدرس دهی به کامپیوتر، ایجاد زیر شبکه و مسیریابی طراحی شده اند. همچنین پروتکل هایی نیز جهت تشخیص وضعیت ارتباطی شبکه در این لایه طراحی شده اند، مهمترین این پروتکل ها عبارتند از:

IP (Internet Protocol)

با استفاده از این پروتکل هر کامپیوتر در شبکه اینترنت می بایست دارای یک شماره ۴ بایتی بنام IP Address باشد. بدین ترتیب تمامی کامپیوتر ها از طریق این آدرسها که یکه می باشند از هم متمایز می شوند و طبق این پروتکل می توانیم زیر شبکه یا subnet نیز ایجاد کنیم. این کار با استفاده از شماره ۴ بایتی دیگری که به هر کامپیوتر واگذار شده و netmask نامیده می شود، انجام می گیرد، از طریق آدرسهای IP می توان اطلاعاتی را نیز از یک شبکه به شبکه دیگر منتقل نمائیم، پروتکل IP یک پروتکل با قابلیت مسیریابی است.

ARP (Address Resolution Protocol)

در شبکه محلی تبادل اطلاعات بصورت فریم به فریم بوده و با استفاده از آدرسهای MAC یا فیزیکی کامپیوترها انجام می شود. در شبکه اینترنت و شبکه هایی که از IP استفاده می کنند، تبادل اطلاعات بصورت packet به packet بوده و از طریق آدرسهای IP انجام می شود. بنابراین در صورت انتقال اطلاعات در یک شبکه محلی که از پروتکل IP نیز استفاده می کند، لازم است آدرس ۴ بایتی IP کامپیوتر مقصد به آدرس ۶ بایتی MAC متناظر با آن تبدیل شود. بر طبق پروتکل ARP ابتدا تقاضایی از سوی کامپیوتر مبدا به شبکه محلی ارسال می شود که در آن آدرس MAC یک آدرس IP سوال می شود. به این درخواست ARP Request می گویند.

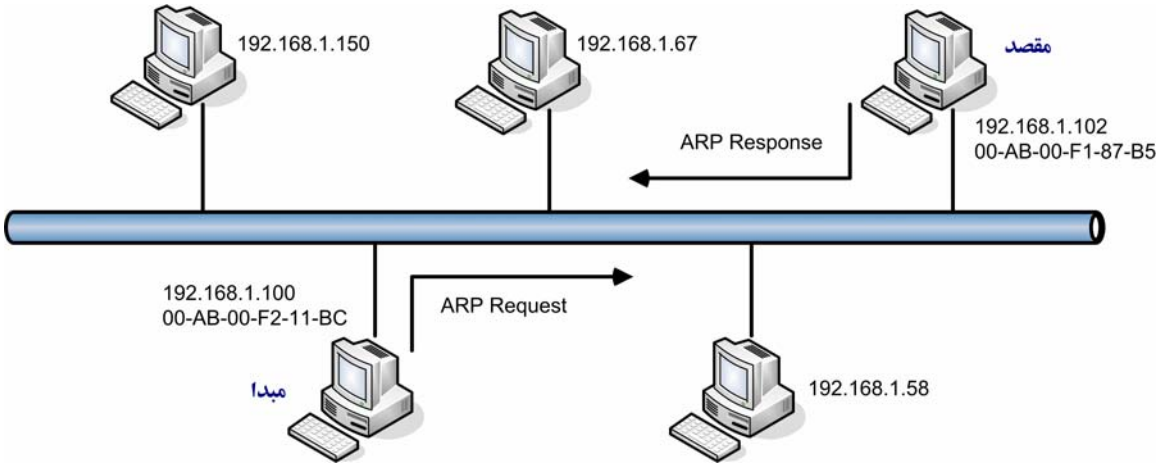
کامپیوتر مقصد پس از دریافت این درخواست آدرس MAC خود را به کامپیوتر مبدا ارسال می کند، این آدرس بطور موقت در حافظه کامپیوتر مبدا در یک جدول که به آن ARP Table می گویند، ذخیره می شود. به این پاسخ که از سوی مقصد داده می شود ARP Response می گویند.

Packet

داده	آدرس IP مقصد	آدرس IP مبدا

Frame

داده	آدرس MAC مبدا	آدرس MAC مقصد



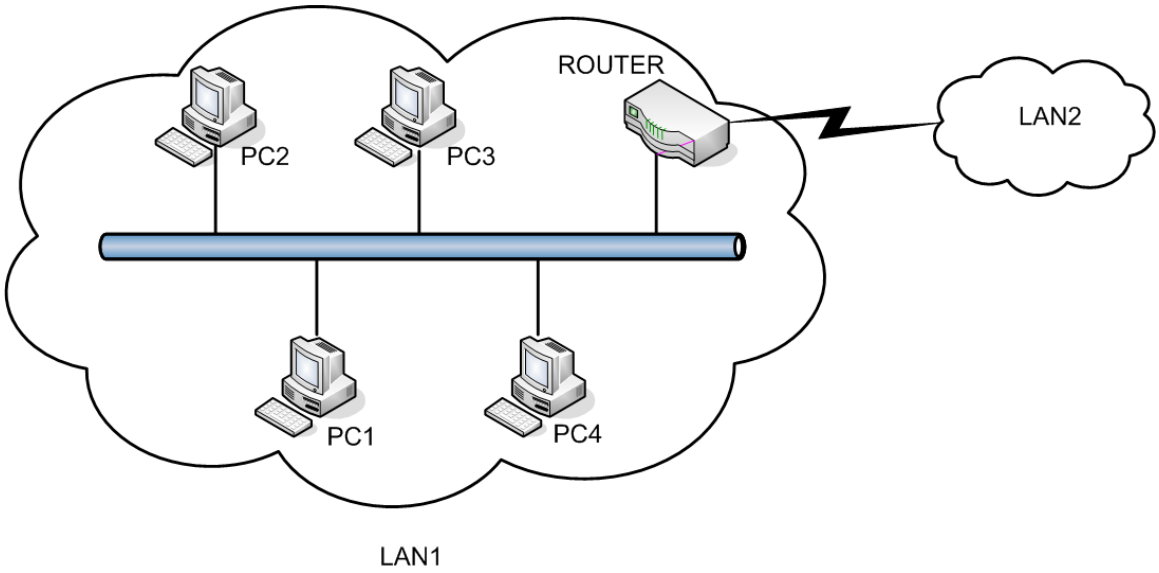
RARP (Reverse Address Resolution Protocol)

با استفاده از این پروتکل آدرس ۶ بایتی MAC به آدرس ۴ بایتی IP متناظر با آن تبدیل می شود. این پروتکل نسبت به ARP کاربرد کمتری داشته و بیشتر در کامپیوترهای بدون دیسک (diskless) که از طریق شبکه بوت می شوند، بکار می رود.

ARP: IP Address ---------- > MAC Address
RARP: MAC Address -------- > IP Address

RIP (Routing Information Protocol)

این پروتکل یکی از رایج ترین پروتکلها برای انجام عملیات مسیریابی در شبکه ها است. برای اتصال هر شبکه به شبکه دیگر از دستگاه های مخصوصی که به آنها مسیریاب (Router) می گویند، استفاده می شود (به این دستگاه ها دروازه یا Gateway نیز می گویند). هر مسیریاب موظف است اطلاعات مسیر مربوط به کامپیوتری را که در شبکه دیگری (مقصد) واقع شده به شبکه درخواست کننده (مبدا) تحویل دهد. برای آنکه هر یک از مسیرهای ارتباطی با شبکه های مختلف مشخص گردد، نیاز است که دستگاه مسیریاب جزئیات مسیرها را به کامپیوتر های موجود در همان شبکه ارسال کند. یکی از پروتکل ها که برای تبادل اطلاعات مسیریابی بکار می رود، RIP می باشد. در حافظه هر کامپیوتر جدول مهمی که جدول مسیریابی () نامیده می شود، ساخته شده که از طریق آن مسیرهای مختلف ارتباطی تشخیص داده می شود. اطلاعات ارسال شده از سوی مسیریاب به این جدول اضافه خواهد شد. بخش ثابت این جدول با توجه به تنظیمات پروتکل IP کامپیوتر در زمان بوت شدن آن ساخته خواهد شد.



ICMP (Internet Control Message Protocol)

از طریق این پروتکل اشکالات ارتباطی موجود در شبکه هایی که از پروتکل IP استفاده می کنند به کامپیوترهای در حال کار گزارش داده می شود. از طریق این اطلاعات کامپیوترها وضعیت ارتباطی شبکه را تشخیص داده و به کاربران بصورت پیغام های خاصی اعلام می کنند. ابزار ping که برای چک کردن ارتباط بین دو کامپیوتر بکار می رود، از این پروتکل استفاده می کند.

۳- لایه میزبان به میزبان

در این لایه پروتکل هایی جهت پیاده سازی روشهای مختلف انتقال شامل انتقال اتصال گرا و انتقال بی اتصال در نظر گرفته شده اند. پروتکل TCP (Transmission Control Protocol) و پروتکل UDP (User Datagram Protocol) در این لایه طراحی شده اند. TCP برای انتقال اتصال گرا و UDP برای انتقال بی اتصال مورد استفاده قرار می گیرند. سرویس های بکار رفته در لایه بالاتر با توجه به نوع اطلاعات و چگونگی تبادل آن یکی از این دو پروتکل را مورد استفاده قرار می دهند که بیشترین کاربرد متعلق به TCP است. ساختار پروتکل TCP نسبت به UDP پیچیده تر بوده و تشخیص خطای بهتری در آن انجام می شود. در هر packet نوع پروتکل انتقال مشخص می شود.

درگاه (port)

با نصب پروتکل اینترنت بر روی هر کامپیوتر مسیرهای مجازی مختلفی در آن تشکیل می شود که از طریق آنها می توانیم با سایر کامپیوترها در ارتباط بوده و تبادل اطلاعات نمائیم. به این مسیرهای مجازی درگاه یا port می گویند. هر درگاه با یک شماره دو بایتی از سایرین متمایز می شود. این شماره بین صفر تا ۶۵۵۳۵ می باشد. در صورت انتقال اطلاعات بین دو کامپیوتر در هر یک از آنها یک مسیر یا

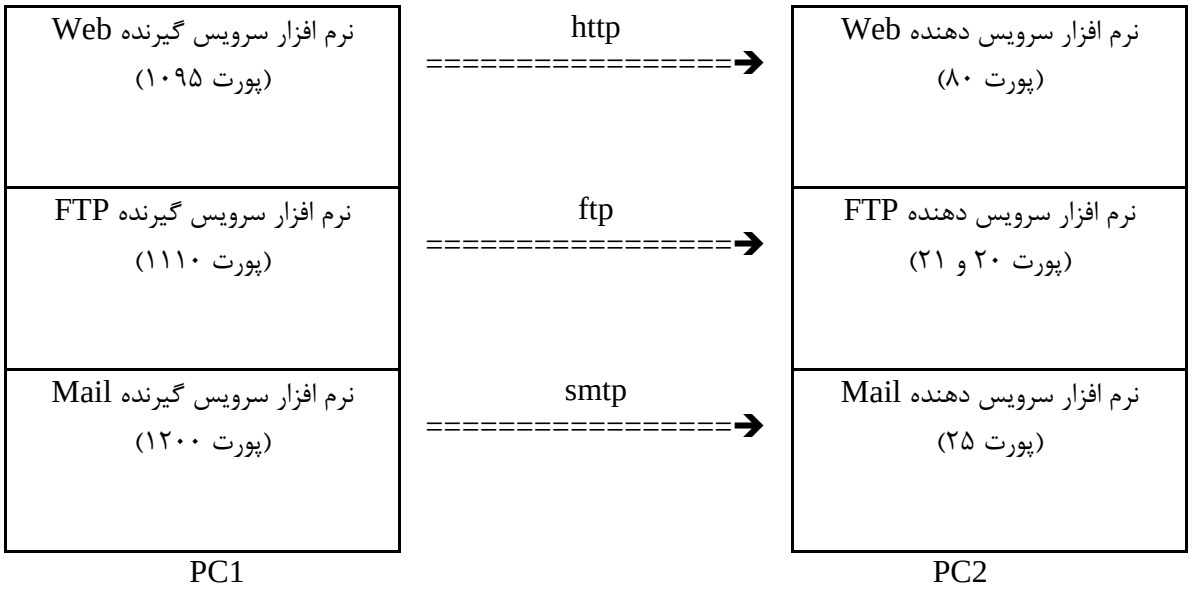
پورت اشغال شده که با توجه به نوع اطلاعات و نحوه تبادل آن شماره پورت های اشغال شده متفاوت خواهد بود. هر یک از سرویس های ارائه شده در لایه آخر مدل TCP/IP از پورت مخصوصی که برای آن در نظر گرفته شده، استفاده می کند. در قرارداد اینترنت سرویس های مختلفی استفاده می شوند که معمولا بطور پیش فرض پورت های ۰ تا ۱۰۲۳ را بکار می برند.
برای مثال:

سرویس وب : پورت مورد استفاده ۸۰
سرویس انتقال فایل: پورتهای مورد استفاده ۲۰ و ۲۱
سرویس پست الکترونیک: پورت ۲۵

در هر packet دو بایت برای شماره پورت مبدا و دو بایت برای شماره پورت مقصد در نظر گرفته شده است. بدین ترتیب از طریق یک packet می توان تشخیص داد که هر کامپیوتر به کدام دستگاه متصل شده و از چه مسیر مجازی و پورتی برای تبادل اطلاعات استفاده می کند.

داده	شماره پورت مقصد	شماره پورت مبدا	آدرس IP مقصد	آدرس IP مبدا

Packet قرارداد اینترنت



نحوه اتصال دو کامپیوتر به یکدیگر بصورت خادم/مخدوم

سوکت (socket)

به زوج آدرس IP و شماره پورت، سوکت گفته می شود.

شماره پورت: آدرس IP

مثال: 192.168.10.5:80

۴- لایه کاربردی (سرویس ها)

در این لایه پروتکل های مختلف طراحی شده اند تا بتوان از طریق آنها سرویسهای خاص را در شبکه اینترنت یا شبکه هایی که از قرارداد IP استفاده می کنند، اجرا نمود. با استفاده از این پروتکل ها نرم افزارهایی طراحی شده و در شبکه بکار گرفته می شوند.

با توجه به اینکه تبادل اطلاعات بصورت client/server یا خادم/مخدوم انجام می شود. بر طبق پروتکل طراحی شده برای یک سرویس معین نرم افزارهای سرویس دهنده و سرویس گیرنده طراحی و تولید می شوند. ارتباط کاربران با نرم افزارهای سرویس دهنده جهت دریافت اطلاعات از طریق نرم افزار client یا سرویس گیرنده برقرار می شود. پروتکل های رایج در قرارداد اینترنت عبارتند از:

HTTP (Hyper Text Transfer Protocol)

از طریق این پروتکل تبادل اطلاعات از نوع ابرمتن امکان پذیر خواهد بود. این نوع اطلاعات که شامل متن، تصویر، صدا و ... می باشد، به صفحات web معروف بوده و از طریق این پروتکل قابل انتقال هستند. با استفاده از این پروتکل که از نوع TCP است نرم افزارهای سرویس دهنده وب (web server) و سرویس گیرنده وب (web client) طراحی می شود. به سرویس گیرنده وب اصطلاحاً مرورگر (browser) می گویند. بطور پیش فرض این پروتکل از پورت شماره 80 استفاده می کند.

FTP (File Transfer Protocol)

از این پروتکل برای انتقال فایل در شبکه اینترنت استفاده می نمایند. این پروتکل از نوع TCP بوده و از پورتهای 20 و 21 استفاده می کند. هر کاربر از طریق نرم افزار FTP Client به سرویس دهنده FTP متصل شده و پس از وارد کردن نام کاربری و کلمه عبور وارد سیستم سرویس دهنده شده و قادر به تبادل فایل می باشد. در شبکه اینترنت تعداد زیادی سرویس دهنده FTP مشغول بکار بوده که به کاربران اینترنت نرم افزارهای مختلفی را ارائه می کنند. هر کاربر برای ورود به این سرویس دهنده ها از نام کاربری anonymous (بینام) استفاده می کنند. به همین دلیل به این نوع سرویس دهنده ها اصطلاحاً Anonymous FTP Server می گویند.

SMTP (Simple Mail Transport Protocol)

از این پروتکل برای تبادل پیام الکترونیک یا e-Mail استفاده می شود. این پروتکل از نوع TCP بوده و از پورت شماره 25 استفاده می کند. هر کاربر از طریق نرم افزار مخصوص e-Mail (مانند نرم افزار Outlook Express) و پس از وارد کردن آدرس پست الکترونیک گیرنده پیام خود را به سرویس دهنده e-Mail تحویل می دهد.این سرویس دهنده پس از مدتی پیام را تحویل سرویس دهنده مقصد داده و سپس پیام مورد نظر در صندوق پستی گیرنده که Inbox نامیده می شود، قرار می گیرد. هر کاربر برای دریافت پیامهای خود از روی سرویس دهنده نیاز به بکارگیری پروتکل های دیگری دارد. آدرس پست الکترونیک یا e-Mail بصورت زیر تعریف می شود:

نام ناحیه یا نام میزبان@نام کاربر

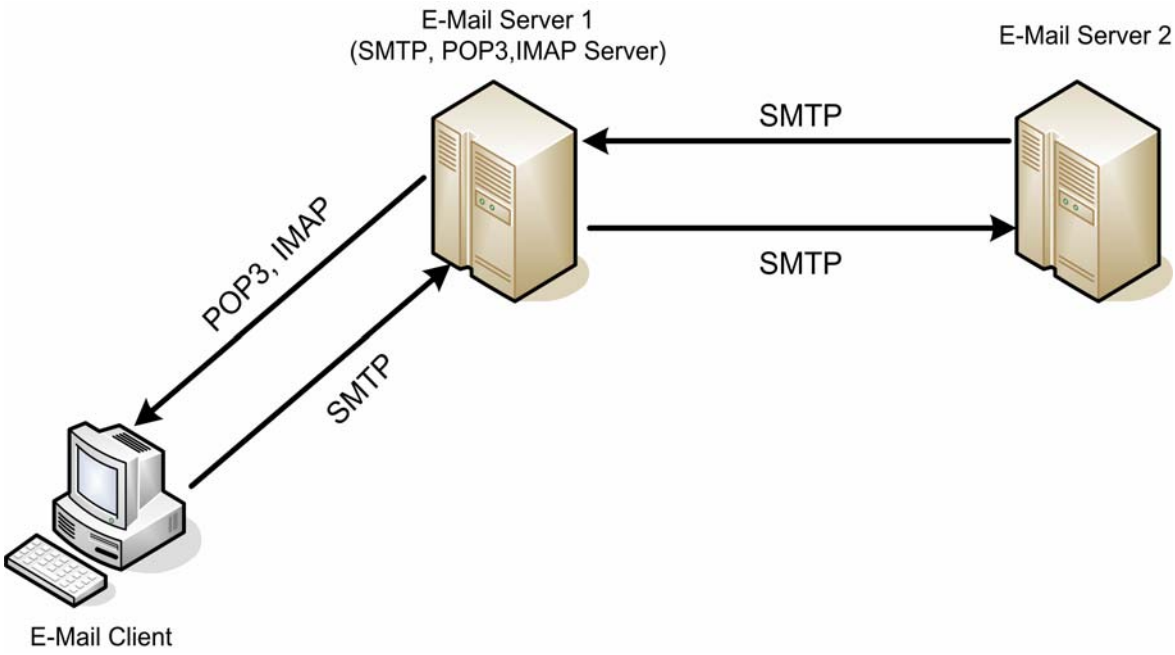
مانند: ali@yahoo.com

POP (Post Office Protocol)

یکی از پروتکل های رایج برای دریافت پیام از روی سرویس دهنده های e-Mail پروتکل POP می باشد. در هر سرویس دهنده پوشه مخصوصی برای نگهداری پیام ها در نظر گرفته شده که از طریق این پروتکل می توان به آن دسترسی پیدا کرد. بعد از اتصال به سرویس دهنده از طریق این پروتکل (نرم افزار POP Client) نیاز به وارد کردن نام کاربری و کلمه عبور می باشد. این پروتکل از نوع TCP بوده و رایج ترین نسخه آن POP3 است که از پورت شماره 110 استفاده می کند.

IMAP (Interactive Mail Access Protocol)

این پروتکل نیز از نوع TCP بوده و از پورت شماره 143 استفاده می کند. این پروتکل نسبت به POP قابلیت بیشتری برای دسترسی به سرویس دهنده e-Mail دارد. از جمله امکان ایجاد یا حذف پوشه بر روی سرویس دهنده و امکان نسخه برداری یا انتقال پیام ها از یک پوشه به پوشه دیگر. در صورت بکارگیری این پروتکل نیاز به وارد کردن نام کاربری و کلمه عبور جهت دریافت پیام از سرویس دهنده می باشد.



DNS (Domain Name System)

در شبکه اینترنت اتصال کامپیوترها به یکدیگر از طریق آدرسهای IP انجام می شود. بکارگیری آدرسهای IP و بخاطر سپردن آنها از سوی کاربران مشکلاتی را برایشان ایجاد می کند. برای مثال تغییر مکان هر سرویس دهنده باعث تغییر آدرس IP آن شده که برای دسترسی کاربران به آن باید آدرس IP جدید به اطلاع آنان رسانده شود. همچنین بخاطر سپاری آدرسهای IP سرویس دهنده ها برای کاربران بسیار دشوار است. برای رفع این مشکلات پروتکلی جهت واگذاری نام به کامپیوترها طراحی شده که به آن DNS می گویند. بر طبق این پروتکل به هر آدرس IP می توان نامی را واگذار کرد که به آن نام میزبان (Hostname) می گویند. این اسامی به همراه آدرسهای IP متناظر با آنها بر روی سرویس دهنده های DNS که در شبکه اینترنت موجود می باشند، قرار می گیرند. در هر کامپیوتر آدرس IP یک سرویس دهنده DNS در تنظیمات قرارداد IP آن وارد می شود تا بتوان از طریق آن نام میزبانی که از سوی کاربر وارد می شود را به آدرس IP متناظر با آن تبدیل کرد. در غیر اینصورت امکان اتصال به کامپیوتر مورد نظر از طریق نام میزبان وجود ندارد. این پروتکل از نوع UDP بوده و از پورت شماره 53 استفاده می کند. نام میزبان بصورت زیر تعریف می شود. بخش نام ناحیه باید در شبکه اینترنت ثبت (register) شود.

نام میزبان= نام ناحیه.نام سیستم

مانند: caspian.guilan.ac.ir

DHCP (Dynamic Host Configuration Protocol)

از طریق این پروتکل می توان در یک شبکه محلی تنظیمات قرارداد اینترنت کامپیوترهای موجود را بطور خودکار و از راه دور انجام داد. از طریق این پروتکل می توان آدرس IP، شماره netmask، آدرس دروازه، آدرس سرویس دهنده DNS، نام میزبان و غیره را در زمان بوت شدن کامپیوترهای شبکه بصورت از راه دور به آنها واگذار نمائیم. این پروتکل از نوع UDP بوده و از پورت 68 استفاده میکند.

TELNET

از این پروتکل برای اجرای از راه دور نرم افزارهای متنی که بر روی سرویس دهنده ها قرار گرفته اند، استفاده می شود. هر کاربر از راه دور به سرویس دهنده متصل شده و با وارد کردن نام کاربری و کلمه عبور وارد آن می شود. با اجرای هر برنامه نتایج آن بر روی صفحه نمایش کامپیوتر خود (سرویس گیرنده) خواهد دید. بعبارتی دیگر از طریق این پروتکل می توان بصورت ترمینالی و از راه دور به کامپیوتر سرویس دهنده متصل شد. امروزه از این پروتکل برای تنظیم از راه دور بعضی از دستگاه های مسیر یاب و مودم های بی سیم استفاده می شود. این پروتکل از نوع TCP بوده و از پورت شماره 23 استفاده می کند.

SSH (Secure Shell)

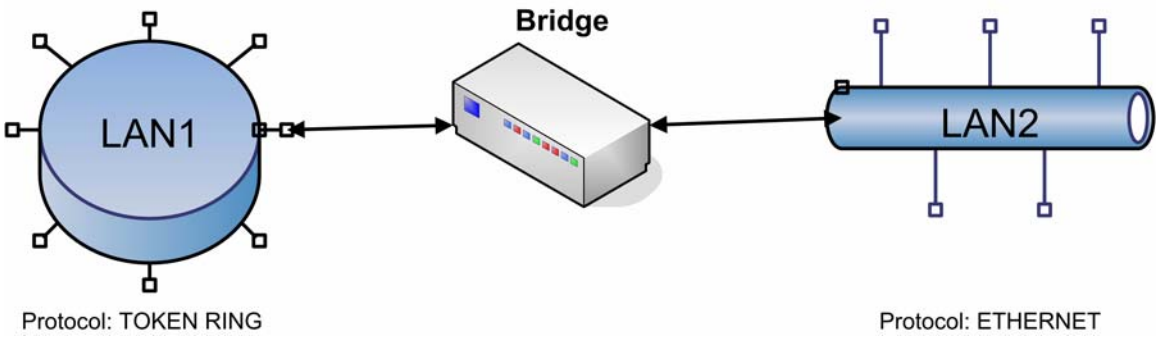
این پروتکل شبیه به TELNET بوده و برای اجرای از راه دور برنامه های متنی استفاده می شود. این پروتکل از امنیت بالاتری نسبت به TELNET برخوردار است، به این صورت که تبادل اطلاعات بین سرویس دهنده و سرویس گیرنده بصورت رمز شده انجام می شود. این پروتکل از نوع TCP بوده و پورت شماره 22 استفاده می کند.

IRC (Internet Relay Chat)

برای انجام گفتگوی نوشتاری بین کاربران اینترنت از این پروتکل استفاده می شود. در شبکه اینترنت تعداد زیادی سرویس دهنده IRC وجود داشته که اجازه ورود به کاربران را جهت انجام گفتگو در زمینه های مختلف می دهد. هر کاربر پس از اتصال به سرویس دهنده با نام مستعار یا nickname وارد آن شده و برای گفتگو در زمینه خاصی وارد کانال یا channel مربوط به آن شده و به کاربران حاضر در کانال ملحق می شود. این پروتکل دارای قابلیت انتقال فایل بین کاربران نیز می باشد. این پروتکل از نوع TCP بوده و معمولاً از پورت های 6666 الی 6669 استفاده می کند.

Bridge و Router

از دستگاه پُل (Bridge) برای اتصال دو شبکه محلی یا LAN که در هر یک از آنها از پروتکل ارتباطی خاصی استفاده می شود. در این اتصال دو شبکه محلی به یک شبکه محلی مجازی تبدیل می شوند. عملکرد این دستگاه در لایه دوم مدل OSI می باشد.



برای اتصال دو شبکه محلی که مستقل از هم بوده و بطور جداگانه فعالیت می کنند، می توان از دستگاه مسیریاب (Router) استفاده کرد. بدین ترتیب یک شبکه گسترده ایجاد خواهد شد. عملکرد دستگاه مسیریاب در لایه سوم مدل OSI است.