پروتکل TCP/IP

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

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 IPمعادل ، 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 می گیرد .

معرفی پروتکل TCP/IP

TCP/IP، پروتکلی استاندارد برای ارتباط کامپیوترهای موجود در یک شبکه مبتنی بر ویندوز 2000 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.

لایه های پروتکل TCP/IP

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

لایه Application

لایه Application ، بالاترین لایه در پشته TCP/IP است .تمامی برنامه و ابزارهای کاربردی در این لایه ، با استفاده از لایه فوق، قادر به دستتیابی به شبکه خواهند بود .پروتکل های موجود در این لایه بمنظور فرمت دهی و مبادله اطلاعات کاربران استفاده می گردند HTTP و FTP دو نمونه از پروتکل ها ی موجود در این لایه می باشند .

پروتکل HTTP(Hypertext Transfer Protocol) . از پروتکل فوق ، بمنظور ارسال فایل های صفحات وب مربوط به وب ، استفاده می گردد .

پروتکلFTP(File Transfer Protocol) . از پروتکل فوق برای ارسال و دریافت فایل، استفاده می گردد .

لایه Transport

لایه " حمل " ، قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به لایه Application لایه بالای خود) و یا لایه اینترنت (لایه پایین خود) را بر عهده دارد. لایه فوق ، همچنین مشخصه منحصربفردی از برنامه ای که داده را عرضه نموده است ، مشخص می نماید. این لایه دارای دو پروتکل اساسی است که نحوه توزیع داده را کنترل می نمایند .

TCP. (Transmission Control Protocol) پروتکل فوق ، مسئول تضمین صحت توزیع اطلاعات است .

UDP. (User Datagram Protocol) پروتکل فوق ، امکان عرضه سریع اطلاعات بدون پذیرفتن مسئولیتی در رابطه با تضمین صحت توزیع اطلاعات را برعهده دارد.

لایه اینترنت

لایه" اینترنت"، مسئول آدرس دهی ، بسته بندی و روتینگ داده ها ، است. لایه فوق ، شامل چهار پروتکل اساسی است :

IP. (Internet Protocol) پروتکل فوق ، مسئول آدرسی داده ها بمنظور ارسال به مقصد مورد نظر است .

ARP(Address Resoulation Protocol) .پروتکل فوق ، مسئول مشخص نمودن آدرس Media Access (MAC) Controlآداپتور شبکه بر روی کامپیوتر مقصد است .

ICMP. (Internet Control Message Protocol) پروتکل فوق ، مسئول ارائه توابع عیب یابی و گزارش خطاء در صورت عدم توزیع صحیح اطلاعات است .

IGMP(Internet Group Managemant Protocol) .پروتکل فوق ، مسئول مدیریت Multicastingدر TCP/IP را برعهده دارد .

لایه Network Interface

لایه " اینترفیس شبکه " ، مسئول استقرار داده بر روی محیط انتقال شبکه و دریافت داده از محیط انتقال شبکه است . لایه فوق ، شامل دستگاه های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است . کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده) نظیر-B5-50-04-22-D4) : 66بوده که آدرس MAC ، نامیده می شود. لایه " اینترفیس شبکه " ، شامل پروتکل های مبتنی بر نرم افزار مشابه لایه های قبل ، نمی باشد .پروتکل های Ethernet و Asynchronous Transfer Mode(ATM)، نمونه هائی از پروتکل های موجود در این لایه می باشند . پروتکل های فوق ، نحوه ارسال داده در شبکه را مشخص می نمایند .

مشخص نمودن برنامه ها

در شبکه های کامپیوتری ، برنامه ها ی متعددی در یک زمان با یکدیگر مرتبط می گردند .زمانیکه چندین برنامه بر روی یک کامپیوتر فعال می گردند ، TCP/IP، می بایست از روشی بمنظور تمایز یک برنامه از برنامه دیگر، استفاده نماید. بدین منظور ، از یک سوکت (Socket) بمنظور مشخص نمودن یک برنامه خاص ، استفاده می گردد .

آدرس IP

برقراری ارتباط در یک شبکه ، مستلزم مشخص شدن آدرس کامپیوترهای مبداء و مقصد است شرط اولیه بمنظور برقراری ارتباط بین دو نقطه ، مشخص بودن آدرس نقاط درگیر در ارتباط است. آدرس هر یک از دستگاه های درگیر در فرآیند ارتباط ، توسط یک عدد منحصربفرد که IPنامیده می شود ، مشخص می گردند. آدرس فوق به هریک از کامپیوترهای موجود در شبکه نسبت داده می شود : IP . 10. 10.1.1 ، نمونه ای در این زمینه است .

پورت TCP/UDP

پورت مشخصه ای برای یک برنامه و در یک کامپیوتر خاص است .پورت با یکی از پروتکل های لایه "حمل "TCP(و یا) UDPمرتبط و پورت TCP و یا پورت UDP ، نامیده می شود. پورت می تواند عددی بین صفر تا ۶۵۵۳۵ را شامل شود. پورت ها برای برنامه های TCP/IP سمت سرویس دهنده ، بعنوان پورت های "شناخته شده " نامیده شده و به اعداد کمتر از ۱۰۲۴ ختم و رزو می شوند تا هیچگونه تعارض و برخوردی با سایر برنامه ها بوجود نیاید. مثلا" برنامه سرویس دهنده FTP از پورت TCPبیست و یا بیست ویک استفاده می نماید .

سوکت (Socket)

سوکت ، ترکیبی از یک آدرس IP و پورت TCP ویا پورت UDP است . یک برنامه ، سوکتی را با مشخص نمودن آدرس IP مربوط به کامپیوتر و نوع سرویس (TCP برای تضمین توزیع اطلاعات و یا UDP)و پورتی که نشاندهنده برنامه است، مشخص می نماید. آدرس IP موجود در سوکت ، امکان آدرس دهی کامپیوتر مقصد را فراهم و پورت مربوطه ، برنامه ای را که داده ها برای آن ارسال می گردد را مشخص می نماید.

TCP/IPچیست ؟

اینترنت بر اساس مجموعه ای از شبکه ها بنا میشود این شبکه ها شامل انواع بسیار زیادی از کامپیوتر ها می باشد ، بنابراین زبان مشترکی بین همه کامپیوتر ها وجود دارد که آن را TCP/IP مینامند.

اینترنت بر اساس مجموعه ای از شبکه ها بنا میشود این شبکه ها شامل انواع بسیار زیادی از کامپیوتر ها می باشد ، بنابراین زبان مشترکی بین همه کامپیوتر ها وجود دارد که آن را TCP/IP مینامند .
TCP/IPبصورت پنج حرف جداگانه TCP/IP تلفظ میشود.

TCP/IP نام متداولی برای مجموعه ای از قراردادها میباشد کـه بـرای متـصل سـاختن کامپیوترهـا و شـــبکه هـــا اســـتفاده میـــشود نـــام واقعـــی TCP/IP از دو قـــرارداد مهـــم مـــی آیـــد .

- TCP -Transmission Control Protocol IP- Internet Protocol

در شبکه اینترنت اطلاعات (داده ها) به بسته های کوچکی بـه نـام Packet تقـسیم بنـدی میـشوند . سپس Packet ها از طریق شبکه منتقل میشوند در اینجا کار IP آن است که آنها را به میزبان راه دور منتقل کند TCP .در انتهای دیگر بسته ها را دریافت و وجود خطاها را بررسی میکند اگـر خطـایی رخ داده باشد TCP میتواند ارسال مجدد بسته بخصوص را درخواست نماید . بعد از اینکه تمام بسته ها بـه درستی دریافت شـدند ، TCPاز شـماره تـوالی بـرای سـاختن مجـدد پیـام اصـلی اسـتفاده میکنـد . به عبارت دیگر کار IP انتقال داده های خام Packet ها از یک مکان به مکان دیگر اسـت. کـار TCP کنترل امور و تضمین صحت داده ها می باشد .

محاسن : Packet

تقسیم بندی داده ها به Packet ها فواید بسیاری دارد . اول اینکه امکان ارائه خـدمات بیـشتر بـه کاربران بیشتر را فراهم میکند. در مسیر اینترنتی بسته ها (Packet) علی رغم داشتن مقـصدهای متفاوت با یکدیگر در حرکت میباشند. نظیر بزرگراهـی کـه در آن اتوموبیلهـای متفـاوت بـا وجـود داشتن مقصدهای متفاوت همگی راه مشترکی دارند .

بسته ها همواره در سفر هستند تا زمانی که به مقصد نهایی خود برسند. اگر اتصال بخصوصی خراب شود کامپیوترهایی که جریان داده ها را کنترل میکنند میتوانند مسیر جایگزینی پیـدا کننـد. ایـن امکان وجود دارد که داده های بسته های مختلف در مسیرهای مختلف به سمت یک مقصد جریـان پیدا کنند .

همچنین شبکه میتواند از بهترین مسیری که در آن شرایط قابل دسترسی است استفاده کند مثلا : وقتی که بار بخش بخصوصی از شبکه بیش از حد متعارف میشود بسته ها از طریق خطوطی که بار کمتری دارند منتقل میشوند .

مزیت دیگر استفاده از این بسته ها آن است که در هنگام بوجود آمدن هر گونه خطـایی در انتقـال، به جای انتقال کل پیام فقط نیاز به ارسال مجدد بسته ای منفرد خواهد بود. این ویژگی سرعت کلی اترنت را افزایش میدهد .

در هر صورت TCP/IP انتقال صحیح و موفقیت آمیز داده ها را تضمین میکند. در حقیقت حتی با وجود این که ممکن است میزبان ها هزاران مایل از یکدیگر دور باشند و بسته ها مجبور به عبـور از چندین کامپیوتر اصلی باشند، اینترنت آنقدر خوب عمل میکند که ارسال پرونده ای از یک میزبـان به میزبان دیگر فقط چند ثانیه طول میکشد .

بطور خلاصه TCP/IP : خانواده ای بزرگ از قراردادهایی است که برای سازمان دهی کامپیوتر هـا و ابزارهای ارتباطی در شبکه استفاده میشود .

پروتکل وب و دیگر پروتکلها

Web

وب بر اساس مدل سرویسگر/(server)سرویسگیر (client)عمل میکند .مدل سرویسگر و سرویس گیر در سیستم شبکه های کامپیوتری شامل ۳ جزء است . سرویس گر ، سرویس گیر و شبکه . سرویـسگیر یک نرم افزار است که بر روی کامپیوتر کاربر اجرا میشود و سرویـسگر نـرم افـزاری اسـت کـه بـر روی کامپیوتری که عمل تغذیه اطلاعاتی را به عهده دارد انجام میشود. کاربر از طریق این نرم افـزار میتوانـد درخواستهایی را برای دریافت اطلاعات و انجام امور ارسـال دارد . ایـن درخواسـت از طریـق شـبکه بـه کامپیوتر سرویس گر میرسدو سرویس گر اعمال لازم را انجام می دهد. تمام اطلاعاتی که بر اساس مدل سرویسگر و سرویسگیر عمل میکنند از یکسری ضوابط یا پروتکل هـایی پیـروی میکننـد کـه بـرای آن سیستم تعریف شده اند. این شکل فعالیت عرضه و تقاضا که از طریق مدل سرویسگر و سرویسگیر اجـرا

میشود توانائیهای زیادی دارد رابطه سرویسگیر و سرویسگر بر اساس یک پروتکل از پیش تعیین شده برقرار میشود .

نرم افزار سرویسگر میتواند برای هر نوع سخت افزار خاصی طراحی شود در واقع Server دیگر نگران اینکه کاربر از چه نوع کامپیوتری استفاده میکند نخواهد بود زیرا میداند که زبان مشترکی با Client دارد که صرفنظر از سیستم سخت افزاری کاربر هر دوی آنها به این زبان با همدیگر ارتباط برقرار میکنند در واقع این طراحی در سطح نرم افزار Client صورت گرفته و همین امر است که وب را به صورت یک پدیده مستقل از سیستم (Platform Independent) در آورده است .

برای درک بهتر موضوع ارتباط Client/ Server سیستم پخش تلویزیونی را در نظر بگیرید که در آن برنامه های تلویزیون از طریق هر دستگاه تلویزیون دریافت میشود. اطلاعات از یک سیستم پخش امواج بر اساس ساختار استاندارد انتشار می یابند و از دستگاه تلویزیون قابل دریافت میباشد .

مرورگر های Web میتوانند به اطلاعات چند پروتکلی دسترسی داشته باشند مرورگرهای وب چند پروتکلی هستند. این بدان معناست که مرورگر ها میتوانند به انواع مختلفی از سرویسگرها که بر اساس پروتکل های مختلفی ارتباط برقرار میکنند دسترسی داشته باشند مهمترین پروتکل هایی که مرورگرها میتوانند با استفاده از آنها به سرویسگرها متصل شوند عبارتند از

۱ : HTTP -Hyper Text Transmission Protocol (این پروتکل مخصوص وب است و برای انتقال ابر متن ها از طریق شبکه طراحی شده

۲ :FTP -File Transmission Protocol (این پروتکل به منظور استفاده و برداشت سریع و آسان فایلها توسط کاربران طراحی شده است .

۳ : Telnet

برای ورود به سیستم یک کامپیوتر میزبان (معمولا از راه دور) مثلاً هنگامی که به Gopher-server متصل است بعنوان یک سرویسگر گوفر و وقتی که به یک اخبار یوزنت متصل است مانند یک سرویسگر اخبار عمل میکند.

TCP/IPپروتکل استاندارد در اکثر شبکه های بزرگ است . با اینکه پروتکل فوق کند و مستلزم استفاده از منابع زیادی است ، ولی بدلیل مزایای بالای آن نظیر : قابلیت روتینگ ، حمایت در اغلب پلات فورم ها و سیستم های عامل همچنان در زمینه استفاده از پروتکل ها حرف اول را می زند. با استفاده از پروتکل فوق کاربران با در اختیار داشتن ویندوز و پس از اتصال به شبکه اینترنت، براحتی قادر به ارتباط با کاربران دیگر خواهند بود که از مکینتاش استفاده می کند.

امروزه کمتر محیطی را می توان یافت که نیازبه دانش کافی در رابطه با TCP/IP نباشد. حتی سیستم عامل شبکه ای ناول که سالیان متمادی از پروتکل IPX/SPX برای ارتباطات استفاده می کرد، در نسخه شماره پنج خود به ضرورت استفاده از پروتکل فوق واقف و نسخه اختصاصی خود را در این زمینه ارائه نمود.

پروتکل TCP/IP در ابتدا برای استفاده در شبکه) ARPAnet نسخه قبلی اینترنت) طراحی گردید. وزارت دفاع امریکا با همکاری برخی از دانشگاهها اقدام به طراحی یک سیستم جهانی نمود که دارای قابلیت ها و ظرفیت های متعدد حتی در صورت بروز جنگ هسته ای باشد. پروتکل ارتباطی برای شبکه فوق ، TCP/IPدر نظر گرفته شد.

اجزای پروتکلTCP/IP

پروتکل TCP/IP از مجموعه پروتکل های دیگر تشکیل شده که هر یک در لایه مربوطه، وظایف خود را انجام می دهند .پروتکل های موجود در لایه های Transport و Network دارای اهمیت بسزائی بوده و در ادامه به بررسی آنها خواهیم پرداخت.

پروتکل های موجود در لایه Network پروتکلTCP/IP

پروتکل (Transmission Control Protocol(TCP ، مهمترین وظیفه پروتکل فوق اطمینان از صحت ارسال اطلاعات است . پروتکل فوق اصطلاحا Connection-oriented "نامیده می شود. علت این امر ایجاد یک ارتباط مجازی بین کامپیوترهای فرستنده و گیرنده بعد از ارسال اطلاعات است .

پروتکل هائی از این نوع ، امکانات بیشتری را بمنظور کنترل خطاهای احتمالی در ارسال اطلاعات فراهم نموده ولی بدلیل افزایش بار عملیاتی سیستم کارائی آنان کاهش خواهد یافت . از پروتکل TCP بعنوان یک پروتکل قابل اطمینان نیز یاد می شود. علت این امر ارسال اطلاعات و کسب آگاهی لازم از گیرنده اطلاعات بمنظور اطمینان از صحت ارسال توسط فرستنده است . در صورتیکه بسته های اطلاعاتی بدرستی دراختیار فرستنده قرار نگیرند، فرستنده مجددا "اقدام به ارسال اطلاعات می نماید.

پروتکل . (UDP)User Datagram Protocol پروتکل فوق نظیر پروتکل TCP در لایه " حمل " فعالیت می نماید UDP .بر خلاف پروتکل TCP بصورت " بدون اتصال " است . بدیهی است که سرعت پروتکل فوق نسبت به TCP سریعتر بوده ولی از بعد کنترل خطاء تظمینات لازم را ارائه نخواهد داد. بهترین جایگاه استفاده از پروتکل فوق در مواردی است که برای ارسال و دریافت اطلاعات به یک سطح بالا از اطمینان ، نیاز نداشته باشیم.

پروتکل . (IP)Internet Protocol پروتکل فوق در لایه شبکه ایفای وظیفه کرده و مهمترین مسئولیت آن دریافت و ارسال بسته های اطلاعاتی به مقاصد درست است . پروتکل فوق با استفاده از آدرس های نسبت داده شده منطقی، عملیات روتینگ را انجام خواهد داد.

پروتکل های موجود در لایه Application پروتکلTCP/IP

پروتکل TCP/IP صرفا" به سه پروتکل TCP ، UDPو IP محدود نشده و در سطح لایه Applicationدارای مجموعه گسترده ای از سایر پروتکل ها است . پروتکل های فوق بعنوان مجموعه ابزارهائی برای مشاهده ، اشکال زدائی و اخذ اطلاعات و سایر عملیات مورد استفاده قرار می گیرند.در این بخش به معرفی برخی از این پروتکل ها خواهیم پرداخت.

پروتکل . (FTP)File Transfer Protocol از پروتکل فوق برای تکثیر فایل های موجود بر روی یک کامپیوتر و کامپیوتر دیگر استفاده می گردد. ویندوز دارای یک برنامه خط دستوری بوده که بعنوان

سرویس گیرنده ایفای وظیفه کرده و امکان ارسال و یا دریافت فایل ها را از یک سرویس دهنده FTP فراهم می کند.

پروتکل . (SNMP(Simple Network Management Protocol از پروتکل فوق بمنظور اخذ اطلاعات آماری استفاده می گردد. یک سیستم مدیریتی، درخواست خود را از یک آژانس SNMP مطرح و ماحصل عملیات کار در یک (MIB(Management Information Base ذخیره می گردد MIB .یک بانک اطلاعاتی بوده که اطلاعات مربوط به کامپیوترهای موجود در شبکه را در خود نگهداری می نماید .(مثلا" چه میزان فضا ی هارد دیسک وجود دارد)

پروتکل . TelNet با استفاده از پروتکل فوق کاربران قادر به log on ، اجرای برنامه ها و مشاهده فایل های موجود بر روی یک کامپیوتر از راه دور می باشند. ویندوز دارای برنامه های سرویس دهنده و گیرنده جهت فعال نمودن و استفاده از پتانسیل فوق است.

پروتکل . (SMTP(simple Mail Transfer Protocol از پروتکل فوق برای ارسال پیام الکترونیکی استفاده می گردد.

پروتکل . (HTTP(HyperText Transfer Protocol پروتکل فوق مشهورترین پروتکل در این گروه بوده و از آن برای رایج ترین سرویس اینترنت یعنی وب استفاده می گردد. با استفاده از پروتکل فوق کامپیوترها قادر به مبادله فایل ها با فرمت های متفاوت (متن، تصاویر ،گرافیکی ، صدا، ویدئو و ...)خواهند بود. برای مبادله اطلاعات با استناد به پروتکل فوق می بایست ، سرویس فوق از طریق نصب سرویس دهنده وب فعال و در ادامه کاربران و استفاده کنندگان با استفاده از یک مرورگر وب قادر به استفاده از سرویس فوق خواهند بود.

پروتکل . (NNTP(Network News Transfer Protocol از پروتکل فوق برای مدیریت پیام های ارسالی برای گروه های خبری خصوصی و عمومی استفاده می گردد. برای عملیاتی نمودن سرویس فوق می بایست سرویس دهنده NNTP بمنظور مدیریت محل ذخیره سازی پیام های ارسالی نصب و

در ادامه کاربران و سرویس گیرندگان با استفاده از برنامه ای موسوم به NewsReader از اطلاعات ذخیره شده استفاده خواهند کرد

مدل آدرس دهی IP

علاوه بر جایگاه پروتکل ها، یکی دیگر از عناصر مهم در زیرساخت شبکه های مبتنی بر TCP/IP مدل آدرس دهی IP است . مدل انتخابی می بایست این اطمینان را بوجود آورد که اطلاعات ارسالی بدرستی به مقصد خواهند رسید. نسخه شماره چهار) IP نسخه فعلی) از ۳۲ بیت برای آدرس دهی استفاده کرده که بمنظور تسهیل در امر نمایش بصورت چهار عدد صحیح (مبنای ده (که بین آنها نقطه استفاده شده است نمایش داده می شوند.

نحوه اختصاص IP

نحوه اختصاص IP به عناصر مورد نیاز در شبکه های مبتنی بر TCP/IP یکی از موارد بسیار مهم است . اختصاص IP ممکن است بصورت دستی و توسط مدیریت شبکه انجام شده و یا انجام رسالت فوق بر عهده عناصر سرویس دهنده نرم افزاری نظیر DHCP و یا NAT گذاشته گردد

Subletting

یکی از مهمترین عملیات در رابطه با اختصاص IP مسئله Subletting است . مسئله فوق بعنوان هنر و علمی است که ماحصل آن تقسیم یک شبکه به مجموعه ای از شبکه های کوچکتر (Subnet) از طریق بخدمت گرفتن ?? بیت با نام Subnet mask بوده که بنوعی مشخصه (ID) شبکه را مشخص خواهد کرد.

کالبد شکافی آدرس های IP

هر دستگاه در شبکه های مبتنی بر TCP/IP دارای یک آدرس منحصر بفرد است . آدرس فوق IP نامیده می شود. یک آدرس IP مطابق زیر است:

216.27.61.137

بمنظور بخاطر سپردن آسان آدرس های IP ، نحوه نما یش آنها بصورت دسیمال (مبنای دهدهی) بوده که توسط چهار عدد که توسط نقطه از یکدیگر جدا می گردند ، است . هر یک از اعداد فوق را octetمی گویند. کامپیوترها برای ارتباط با یکدیگر از مبنای دو (باینری) استفاده می نمایند. فرمت باینری آدرس IP اشاره شده بصورت زیر است:

11011000.00011011.00111101.10001001

همانگونه که مشاهده می گردد ، هر IP از ۳۲ بیت تشکیل می گردد. بدین ترتیب می توان حداکثر ۴,۲۹۴,۹۶۷,۲۹۶ آدرس منحصر بفرد را استفاده کرد(۲۳۲) . مثلا" آدرس ۲۵۵,۲۵۵,۲۵۵,۲۵۵ برای Broadcast (انتشار عام) استفاده می گردد . نمایش یک IP بصورت چهار عدد (Octet) صرفا" برای راحتی کار نبوده و از آنان برای ایجاد " کلاس های " IP نیز استفاده می گردد. هر Octet به دو بخش مجزا تقسیم می گردد: شبکه (Net) و میزبان . (Host) اولین octet نشاندهنده شبکه بوده و از آن برای مشخص نمودن شبکه ای که کامپیوتر به آن تعلق دارد ، استفاده می گردد. سه بخش دیگر octet ، نشاندهنده آدرس کامپیوتر موجود در شبکه است

پنج کلاس متفاوت IP بهمراه برخی آدرس های خاص ، تعریف شده است:

. Default Network -آدرسIP 0.0.0.0 ، برای شبکه پیش فرض در نظر گرفته شده است .آدرس فوق برای مواردیکه کامپیوتر میزبان از آدرس خود آگاهی ندارد استفاده شده تا به پروتکل هائی نظیر DHCP اعلام نماید برای وی آدرسی را تخصیص دهد.

-کلاس . A کلاس فوق برای شبکه های بسیار بزرگ نظیر یک شرکت بین المللی در نظر گرفته می شود. آدرس هائی که اولین octet آنها ۱ تا ۱۲۶ باشد ، کلاس A می باشند. از سه octet دیگر بمنظور مشخص نمودن هر یک از کامپیوترهای میزبان استفاده می گردد. بدین ترتیب مجموع شبکه های کلاس A ، معادل ۱۲۶ و هر یک از شبکه های فوق می توانند 16.777.214 کامپیوتر میزبان داشته باشند. (عدد فوق از طریق حاصل ۲ - ۲۲۴ بدست آمده است) .بنابراین تعداد تمام

کامپیوترهای میزبان در شبکه های کلاس A معادل (231) 2.147.483.648 است . در شبکه های کلاس A ، بیت با ارزش بالا در اولین octet همواره مقدار صفر را دارد.

. LoopBack -آدرس IP 127.0.0.1 برای LoopBack در نظر گرفته شده است . کامپیوتر میزبان از آدرس فوق برای ارسال یک پیام برای خود استفاده می کند.(فرستنده و گیرنده پیام یک کامپیوتر می باشد) آدرس فوق اغلب برای تست و اشکال زدائی استفاده می گردد.

-کلاس . B کلاس فوق برای شبکه های متوسط در نظر گرفته می شود.(مثلا "یک دانشگاه بزرگ) آدرس هائی که اولین octet آنها ۱۲۸ تا ۱۹۱ باشد ، کلاس B می باشند. در کلاس فوق از دومین octetهم برای مشخص کردن شبکه استفاده می گردد. از دو octet دیگر برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد بدین ترتیب ۱۶,۳۸۴ (۲۱۴) شبکه از نوع کلاس B وجود دارد. تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل ۶۵,۵۳۴ (۲ - ۲ ۱۶) است . بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس B معادل ۱,۰۷۳,۷۴۱,۸۲۴ (۲۳۰) است در شبکه های کلاس B ، اولین و دومین بیت در اولین octet به ترتیب مقدار یک و صفر را دارا می باشند.

-کلاس . C کلاس فوق برای شبکه های کوچک تا متوسط در نظر گرفته می شود.آدرس هائی که اولین octet آنها ۱۹۲ تا ۲۲۳ باشد ، کلاس C می باشند. در کلاس فوق از دومین و سومین octet هم برای مشخص کردن شبکه استفاده می گردد. از آخرین octet برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد . بدین ترتیب (2 21) 2.097.152 شبکه کلاس Cوجود دارد.تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل ۲۵۴ (۲ - ۸ ۲) است . بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس C معادل ۵۳۶,۸۷۰,۹۱۲ (۲۲۹) است

. در شبکه های کلاس C ، اولین ، دومین و سومین بیت در اولین octet به ترتیب مقدار یک ، یک و صفر را دارا می باشند.

کلاس . D از کلاس فوق برای multicasts استفاده می شود. در چنین حالتی یک گره (میزبان) بسته اطلاعاتی خود را برای یک گروه خاص ارسال می دارد. تمام دستگاه های موجود در گروه ، بسته اطلاعاتی ارسال شده را دریافت خواهند کرد. (مثلا "یک روتر سیسکو آخرین وضعیت بهنگام شده خود را برای سایر روترهای سیسکو ارسال می دارد) کلاس فوق نسبت به سه کلاس قبلی دارای ساختاری کاملا" متفاوت است. اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و صفر می باشند.۲۸ بیت باقیمانده بمنظور مشخص نمودن گروههائی از کامپیوتر بوده که پیام Multicastبرای آنان در نظر گرفته می شود. کلاس فوق قادر به آدرسی دهی ۲۶۸,۴۳۵,۴۵۶ (۲۲۶) کامپیوتر است

-کلاس . E از کلاس فوق برای موارد تجربی استفاده می شود. کلاس فوق نسبت به سه کلاس اولیه دارای ساختاری متفاوت است . اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و یک می باشند.۲۸ بیت باقیمانده بمنظور مشخص نمودن گروههائی از کامپیوتر بوده که پیام Multicast برای آنان در نظر گرفته می شود .کلاس فوق قادر به آدرسی دهی ۲۶۸,۴۳۵,۴۵۶ (۲۲۶) کامپیوتر است

. BroadCast -پیام هائی با آدرسی از این نوع ، برای تمامی کامپیوترهای در شبکه ارسال خواهد شد .این نوع پیام ها همواره دارای آدرس زیر خواهند بود:

255.255.255.255 آدرس های رزو شده . آدرس های IP زیر بمنظور استفاده در شبکه های خصوصی :

10.x.x.x

172.16.x.x - 172.31.x.x

192.168.x.x

IP -نسخه شش . نسخه فوق برخلاف نسخه فعلی که از ۳۲ بیت بمنظور آدرس دهی استفاده می نماید ، از ۱۲۸ بیت برای آدرس دهی استفاده می کند. هر شانزده بیت بصورت مبنای شانزده نمایش داده می شود.

OSIوTCP/IP

معماری اینترنت، معماری شبکه‌ای غالب در اوایل دهه‌ی ۲۰۰۰ است .اینترنت بر پروتکل اینترنت IPاستوار است، که می‌توان آن را روی همه‌ی انواع شبکه‌های فیزیکی و تحت همه‌ی انواع برنامه‌های کاربردی به کار انداخت. استقلال پروتکل اینترنت هم از شبکه‌های فیزیکی و هم از برنامه‌های کاربردی، نقطه‌ی قوت اصلی آن است. این پروتکل حتی با فناوری‌های شبکه‌ای کاملاً جدید، مثل «شبکه‌ی محلی بیسیم» (دبلیولن] یا «سرویس رادیویی بسته‌ای عمومی» (جی‌پی‌آرِاس) و شبکه‌ی» سامانه‌ی عمومی ارتباطات همراه» (جی‌اِس‌اِم) نیز کار می‌کند. برنامه‌های جدید و بسیاری برنامه‌های دیگر که در آینده عرضه می‌شوند را می‌توان به راحتی با سرویس استاندارد پروتکل اینترنت اجرا کرد. معماری اینترنت اساساً از سال ۱۹۷۴ ثابت مانده و همچنان قدرت خود را اثبات می‌کند. بنابراین شعار قدیمی «آی‌پی ورای همه، همه چیز برروی آی‌پی» امروز بیش از هر زمان دیگری صدق میکند این مدل علا رغم محبوبیتش ایراداتی داردکه عیب‌های اصلیIP ، فضای ناکافی نشانی، عدم پشتیبانی از جایجایی فیزیکی، فقدان کیفیت متمایز سرویس، و فقدان امنیت آن می‌باشد

کار با اینترنت به پیشرفت خود ادامه می‌دهد و به عرصه‌های جدید برنامه‌های کاربردی گسترش می‌یابد .کاهش سرانه‌ی قیمت محصولات، عملاً همه‌ی برنامه‌ها را به استفاده از فناوری اصلیIP سوق خواهد داد. اگر جابجایی‌پذیری، کیفیت خدمات، و امنیت، محور اصلی خدمات اینترنت در نسل آینده باشند، در آن صورت یک سکوی عمومی جهانی خواهیم داشت تا کار الکترونیکی را بر روی آن استوار کنیم این سکوی فنی برای کار الکترونیکی امن، در حال شکل‌گرفتن است و جنبه‌های شبکه‌ای امنیت را می‌توان حل کرد. اما وقتی که با افراد و با جریان‌های پیچیده‌ی اطلاعات سروکار داریم، هیچ راه‌حل

استاندارد ساده‌ای برای امنیت کل سیستم وجود ندارد.کار زیبادی باید انجام شود. باید سازوکارهای استاندارد امنیت به‌کارگرفته شوند تا اطمینان حاصل شود که سیستم‌های اطلاعاتی مورد استفاده، امنیت جریان های اطلاعاتی را به خطر نمی‌اندازند.

هیچ روش شناخته‌شده‌ای برای اثبات امنیت کل فرایندها وجود ندارد. باید مداوماً به نظارت و به بازخورددادن به فرایندهایمان بپردازیم. همچنین بازرسی به‌وسیله‌ی یک طرف بیرونی که مسئولیتی در استقرار یا اجرای سیستم ندارد لازم است

Application	لایه کاربرد
Presentation	لایه ارائه
Session	لایه جلسه
Transport	لایه انتقال
Network	لایه شبکه
Data link	لایه پیوند داده ها
Physical	لایه فیزیکی

شکل ۱: لایه های مدلOSI

بررسی هفت لایه OSI

لایه فیزیکی

این لایه که تنها تشکیل شده از سخت افزار می باشد و قراردادهای سخت افزاری در آن اجرا می شود وظیفه انتقال نهایی اطلاعات را دارد که این انتقال یصورت سیگنال و به صورت صفرو یک می باشد

لایه پیوند داده ها

در این لایه اطلاعات ، کشف خطا و اصلاح می شوند و بدون خطا و به صورت مطمئن به سوی مقصد

ارسال می شوند .وظیفه دیگر این لایه مطمئن شدن از رسیدن اطلاعات به مقصد است که این کار توسط

بیتهای (Parity check , checksum ,crc) انجام می پذیرد .که در صورت بروز خطا مجددا اطلاعات ارسال خواهند شد.

لایه شبکه

و اما پیچیده ترین لایه یعنی لایه شبکه که در آن قراردادهای شبکه بندی تعریف شده است . وظیفه این لایه انتقال تکنولوژی برقراری ارتباط برای دیگر شبکه های مستقل است که این امر این امکان را به osiمی دهد که بتواند در زیر شبکه های مختلف فعالیت کند.

لایه انتقال

در این لایه قبل از ارسال اطلاعات یک بسته به سمت مقصد فرستاده می شود تا مقصد را برای دریافت اطلاعات آماده کند . همچنین این لایه وظیفه تکه تکه کردن بسته ها ، شماره گذاری آنها و ترتیب و نظم دهی آنها را بر عهده دارد. که البته بسته ها در طرف گیرنده دوباره در همین لایه نظم دهی و قابل استفاده برای لایه های بالاتر خواهند شد .

لایه جلسه

در این لایه بر کارهایی از قبیل زمان ارسال و دریافت بسته ها مقدار رسیده و مقدار مانده از بسته ها نظارت می شود که به مدیریت بسته ها بسیار کمک می کند.

لایه ارائه

در این لایه استانداردهای رمز نگاری و فشرده سازی اطلاعات تعریف شده است که این لایه در امنیت بسیار مهم می باشد.

لایه کاربرد :استانداردهای ارتباط بین نرم افزارهای شبکه در این لایه قرار دارد که می توان از FTAM CMIP MHS VT نام برد.

مدل شبکه ای TCP/IP(Internet protocol /Transmission Control Protocol رایج ترین مدل شبکه های کامپیوتری، مدل چهار لایه TCP/IP است که با بهره گیری از پشته پروتکل TCP/IP به تبادل داده و نظارت بر مبادلات داده می پردازد در شبکه کامپیوتری برای کاهش پیچیدگی های پیاده سازی، آن را مدل سازی میکنند که از جمله میتوان به مدل هفت لایه OSI و مدل چهار لایه TCP/IP اشاره نمود. در این مدلها، شبکه لایه بندی شده و هر لایه با استفاده از پروتکلهای خاصی به ارائه خدمات مشخصی میپردازد. مدل چهار لایه TCP/IP نسبت به OSI محبوبیت بیشتری پیدا کرده است ولی علیرغم این محبوبیت دارای نقاط ضعف و اشکالات امنیتی است که باید راهکارهای مناسبی برای آنها ارائه شود تا نفوذگران نتوانند به منابع شبکه دسترسی پیدا کرده و یا اینکه اطلاعات را بربایند .

شناسائی لایه های مدلTCP/IP ، وظایف، پروتکلها و نقاط ضعف و راهکارهای امنیتی لایه ها در تعیین سیاست امنیتی مفید است ، TCP/IPمجموعه قراردادهایی هستند که در جهت اتصال کامپیوتر ها در شبکه مورد استفاده قرار می گیرند. وبه تعریف دیگر قرارداد کنترل انتقال اطلاعات می باشد

پروتکل

لایه کاربرد	TCP لایه کاربرد
لایه کاربرد	لایه ارائه
لایه انتقال	لایه جلسه
لایه انتقال	لایه انتقال
لایه شبکه	لایه شبکه
لایه واسطه شبکه	لایه پیوند داده ها
لایه واسطه شبکه	لایه فیزیکی

مقایسه با : osi شکل۲

همانطور که از شکل پیداست TCP/IP از چهار لایه تشکیل شده که در زیر به صحبت در مورد چهار لایه TCP/IP می پردازیم

لایه واسط شبکه

در این لایه تمام استانداردهای سخت افزاری و انواع پروتکل شبکه تعریف شده که خاصیت بزرگ این لایه این موضوع می باشد که در آن می توان بین نرم افزار و سخت افزار شبکه ارتباط برقرار کرد.

لایه شبکه

در این لایه پروتکل IP آدرس دهی و تنظیم می شود .(توضیحات در قسمت (IP و همچنین دیگر پروتکل ها مانند ARP,ICMP,BOOTP که در این میان نقش هیچکدام به اندازه IP , ICMP مهم نیست در کل وظیفه این لایه دادن اطلاعات در مورد شبکه و آدرس دهی در آن می باشد که مسیر یابها از آن بسیار استفاده میکنند

لایه انتقال

ابتدایی ترین وظیف این لایه آگاهی از وضعیت بسته ها می باشد که بسیار مهم نیز هست. و در مرحله بعد وظیفه این لایه انتقال اطلاعاتی می باشد که نیاز به امنیت ندارند و سرعت برای آنها مهم تر است

لایه کاربرد:

این لایه دارای امکانات زیادی برای هنر نمایی متخصصان می باشد . در این لایه برنامه های کاربردی قرار دارند و در کل این لایه لایه ی نرم افزارهای شبکه می باشد و همچنین لایه پروتکل های نرم افزاری نیز می باشد

از مهم ترین نکات در خصوص این لایه قرارداشتن : انتقال فایل (FTP) و مدیریت پست (SMTP) و بقیه برنامه های کاربردی می باشد.

پروتکل اینترنتIP

یکی از مهمترین قسمتهای TCP/IP و شاید بتوان گفت مهمترین قسمت آن زیرا تقریبا شما برای هر کاری نیاز به آن خواهید داشت IP. یک آدرس عددی است که برای ارتباط با شبکه به هر ماشینی در شبکه اختصاص داده می شود (چون IP برای وسایلی از قبیل ROUTER و MODEM و LAN و ... استفاده می شود ما اصطلاحا به جای نام بردن تک تک آنها همه را ماشین می نامیم(IP»شما نسبت به نوع اتصال شما متغییر و یا ثابت می باشد« .

وظیفه IP چیست ؟

وظیفه پروتکل IP حمل و تردد بسته های حاوی اطلاعات و همچنین مسیر یابی آنها از مبدا تا مقصد است

اساس کار پروتکل IP چیست ؟

IPپس از دریافت اطلاعات از TCP شروع به قطعه قطعه کردن آن به قطعه های کوچک به اسم FRAGMENTمی نماید، پس از این مرحله برای هر FRAGMENT یک بسته IP می سازد که حاوی اطلاعات مورد نیاز بسته برای حرکت در طول شبکه می باشد و بسته IP را به بسته TCP اضافه می کند

و شروع به ارسال بسته های تیکه تیکه شده (FRAGMENT)می نماید حال مسیر یابها بر اساس تنظیمات قسمت IP بسته ها را به مقصد خود هدایت می کنند و آن را داخل زیر شبکه ها هدایت می کنند

خصوصیاتIP

بسته IP حد اکثر ۶۴ کیلوبایت فضا را اشغال خواهد کرد و بیشتر از آن نمی تواند باشد ولی موضوع جالب اینجاست که در حالت عادی حجم بسته حدود ۱۶۰۰ بایت بیشتر نمی شود IPدر تمامی سیستم های عامل با ساختار استانداردی که دارد به درستی کار می کنند و نیاز به هیچ نوع سخت افزار ندارد.

نکاتی جالب در مورد IP

آدرس های ویژه

این آدرسها نمونه های از آدرس های IP خاص هستند که از قبل برای مقاصد خاصی در نظر گرفته شده اند و در تعریف شبکه نمی توان از آنها به عنوان IP برای ماشینها استفاده کرد.

0.0.0.0

از این آدرس در مواردی استفاده می شود که ماشین میزبان از IP خود بی اطلاع است .البته اگر از این آدرس به عنوان آدرس فرستنده استفاده شود هیچ جوابی برای فرستنده پس فرستاده نمی شود.

HostId.0

این آدرس برای زمانی است که از آدرس خود در زیرشبکه بی اطلاع باشیم

255.255.255.255

از این آدرس برای ارسال پیامهای به صورت عمومی و فراگیر در شبکه استفاده می شود البته با استفاده از این آدرس میتوان در زیر شبکه خود پیام فراگیر ارسال کرد.

NetId.255

از این آدرس برای ارسال پیامهای فراگیر در دیگر شبکه ها از خارج از آنها استفاده می شود .البته این سرویس تقریبا در بیشتر اوقات از سوی مدیران شبکه غیر فعال می شود.

مقایسه دو پروتکل در بخش های مختلف امنیتی

در ادامه، حملات، سرویس ها و مکانیزم ها و تجهیزات امنیتی در لایه های مختلف در قالب جداول 1-2-3-4با یکدیگر مقایسه می شوند و همانطور که در جداول مذکور نشان داده شده است می توان نتیجه گرفت که بیشترین حملات به ترتیب در لایه IP,TCP ، کاربرد و میزبان به شبکه است و سرویس ها و مکانیزم ها بیشتر در لایه IP به چشم می خورد و تجهیزات امنیتی با بهره گیری از مکانیزم های مختلف بیشتر در لایه TCP , IP و کاربرد ، کاربری دارند.

در جدول ۵تجهیزات امنیتی از نظر پارامترهای مختلف با یکدیگر مقایسه می شوند و مورد ارزیابی قرار می گیرند، استفاده از تجهیزات سخت افزاری نظیر فایروال، سوئیچ ها و مسیریابهای مدیریت پذیر، گران است و هزینه پشتیبانی آنها نیز بالاست و از پیچیدگی نسبتا بالایی برخوردارند. در تجهیزات نرم افزاری نیز هزینه پشتیبانی بدلیل لزوم Update مرتب ، بالا است ولی هزینه استقرار و پیچیدگی پائین است

جدول ۱. مقایسه تهدیدات امنیتی در لایه های چهارگانهTCP/IP

تهدید /لایه	Host to Network	IP	TCP	Application
Trojan,Virus,Worm				*
SQL-Injection				*
TCP/IP Spoofing		*	*	
Session Hijacking			*	*
Port Scan			*	*
Physical Attacks	*			
Phishing			*	*
Password Attacks				*
Packet Sniffing		*	*	
Dos/DDos Attacks		*	*	*

Network Layer Attacks		*		
Application Layer Attacks				*
Buffer Over Flow Attacks		*	*	*
Replay	*	*	*	*
Traffic Analysis	*	*	*	
Message Modification	*	*	*	

جدول ۲. اهراف امنیتی در منابع شبکه

منابع / اهداف	شبکه				کاربران شبکه
	سخت افزارها	نرم افزارها	اطلاعات	ارتباطات	
محرمانگی			*	*	
صحت	*	*	*	*	
قابلیت دسترسی	*	*	*	*	
محافظت فیزیکی	*		❊	❊	
تشخیص هویت					*
صدور اختیارات					*
حریم خصوصی					*✓
آگاهی رسانی امنیتی					

جدول ۳. سرویس های امنیتی در لایه های مختلفTCP/IP

سرویس/لایه	Host to Network	IP	TCP	Application
محرمانگی	*	*	*	*
تایید هویت	*	*	*	*
رد انکار				*
کنترل جامعیت و صحت		*	*	

جدول ۴. مکانیزم های امنیتی مربوط به لایه های مختلفTCP/IP

مکانیزم/لایه	Host to Network	IP	TCP	Application
رمزنگاری	*	*	*	*
امضائ دیجیتال		*	*	*
کنترل دستیابی		*	*	*
درستی و صحت داده		*	*	*
کنترل مسیریابی		*		
رد انکار سندیت		*		*

جدول ۵. مقایسه تجهیزات امنیتی در لایه های چهارگانهTCP/IP

تجهیزات امنیتی/لایه	Host to Network	IP	TCP	Application
حفاظت فیزیکی	*			
رمزنگاری	*	*	*	*
IP Sec		*		
SSL			*	
Firewall		*	*	*
AntiVirus				*
AAA Server	*	*	*	*
VPN	*	*	*	*
PGP				*
IDS/IPS		*	*	*

انچه در مطالب فوق گفته شد چکیده توضیحاتی در مورد مدل شبکه های کامپیوتری است که همانطور که در ابتدا بیان شد دارای ایراداتی است که مهمترین انها عدم امنیت است و اشاره شد کـه ارائـه یـک الگوریتم امنیتی ثابت ممکن نیست هر مدیر امنیتی در هر سازمان یا شبکه با توجه به اطلاعاتی کـه از سیستم شبکه خود دارد باید به تنظیم یک سیاست امنیتی کامل و جامع بپردازد

بعـضی از معـروف‌تـرین و پـر اسـتفاده‌تـرین پروتکـل‌هـای موجـود در اینترنـت عبـارت‌انـد از:

* IP
* Internet Protocol Suite
* TCP
* UDP
* DNS
* SLIP
* ICMP
* IMAP
* SMTP

* HTTP
* HTTPS
* SSH
* Telnet
* FTP
* LDAP

بعضی از سرویس‌های پراستفاده و محبوب در اینترنت که بر اساس این پروتکل‌ها کار می‌کنند عبارت‌اند از :پست الکترونیک، USENet ، اشتراک گذاری فایل، World Wide Web، Gopher ، session access، finger،WAIS،) IRCچت اینترنتی(، MUDها. از همه این سرویس‌ها پست الکترونیکی و وب از همه بیشتر استفاده می‌شوند و حتی سرویس‌های زیادی نیز بر اساس آنها ساخته شده‌اند مانند mailing list و وب لاگ. بطور معمول، اغلب مردم اینترنت را با سرویس‌های مشهور آن یعنی وب و پست الکترونیک می‌شناسند. اینترنت همچنین توانایی سرویس‌دهی هم‌زمان یا زنده را نیز فراهم آورده‌است مانند رادیو تحت وب و Webcast که قابل دسترسی در هر نقطه‌ای از دنیا هستند.

بعضی دیگر از سرویس‌های پر استفاده و محبوب در اینترنت به این روش ساخته نشده‌اند بلکه بر اساس سیستم‌های خاص خود ساخته شده‌اند مانند IRC :، AIM،ICQ، CDDBو.Gnutella.

تحلیل‌ها و اظهار نظرات زیادی در مورد اینترنت و ساختار آن وجود دارد. برای مثال اینکه سیستم Internet IP routingسیستم مسیر یابی توسط پروتکل IP در اینترنت و پیوندهای موجود در وب می‌توانند نمونه‌هایی از شبکه‌های قابل گسترش باشند. برای استفاده از سرویس SSH در ویندوز می‌توان از برنامه Putty استفاده کرد.

دیتاگرام IP

دیتاگرام های IP

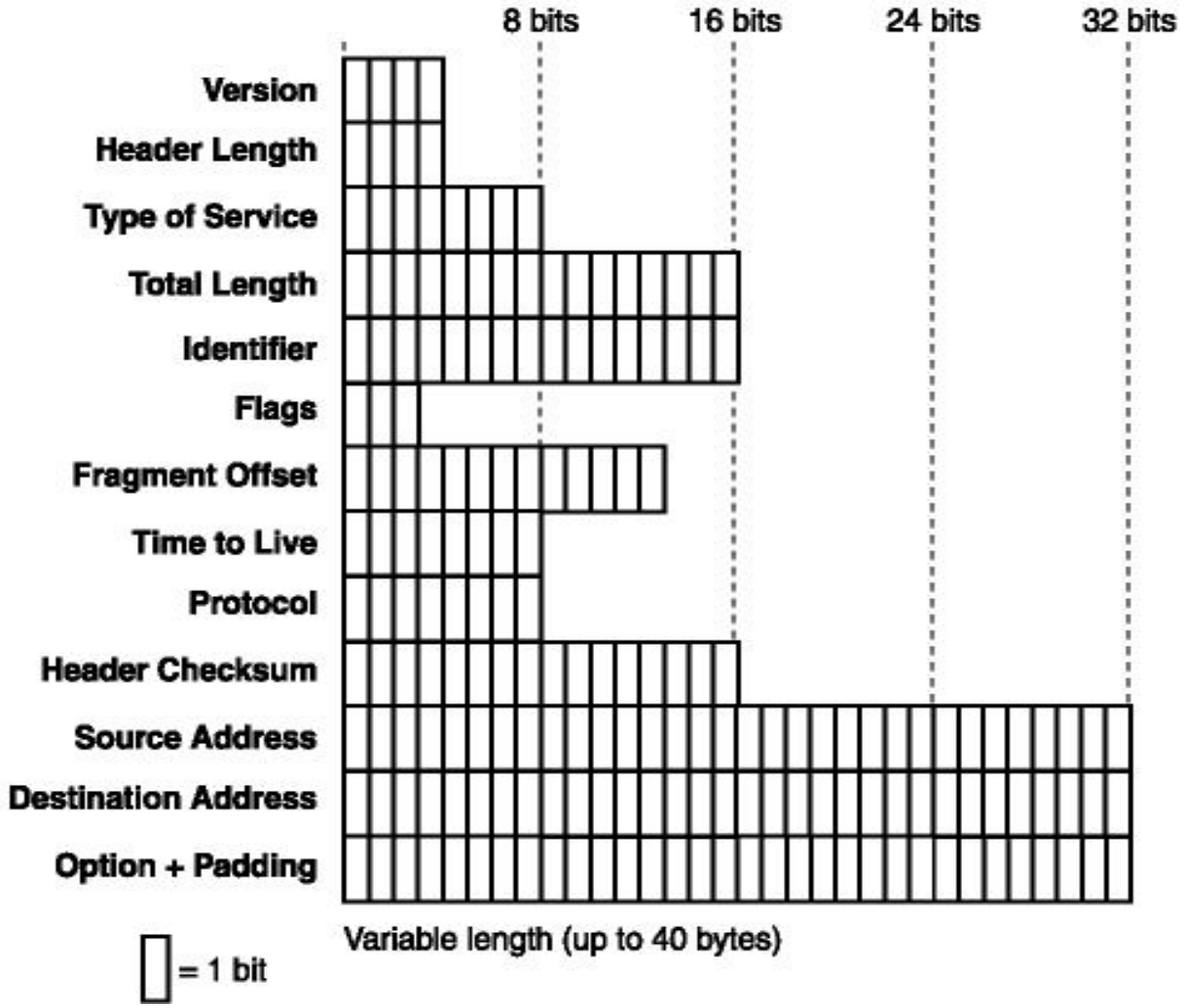
دو جزء اصلی در دیتاگرام IP وجود دارد. Header و Payload. مانند پکت هایی که در لایه رابط شبکه ساخته میشوند، وقتی IP مورد استفاده قرار میگیرد تا دیتاگرام تشکیل شود، ساختاری وجود دارد که پکت میتواند به کمک آن توسط هر ساخت TCP/IP شناخته شود. بدین ترتیب هر کامپیوتری با هر سیستم عاملی میتواند با کامپیوتر دیگر ارتباط برقرار کند و این زمانی ممکن میشود که هر دو از نسخه یکسانی از مجموعه پرتکلهای TCP/IP استفاده کنند.

چون TCP/IP یک پروتکل استاندارد صنعتی است و هر نمونه ای از آن میتواند اطلاعات سرآیند دیتاگرام IP را کدگشایی کند و هر هکر و کراکری میتواند همین اطلاعات را بدست آورده و مثلث CIA را به خطر بیاندازد.

بررسی سرآیند IP

قسمت سرآیند از یک پکت IP شامل اطلاعاتی است که برای بدست آوردن خصوصیات پکت IP، آدرس های مبداء و مقصد و اینکه آیا دیتاگرام چند تکه است یا نه و پروتکل آن، مورد استفاده قرار میگیرد.

با اینکه اندازه سرآیند IP متغیر است، ولی این نیز بصورت استاندارد صنعتی تعریف شده است. پس هکر و کراکر میتواند پکتی را روی شبکه بدست آورد و اطلاعات را بخواند. شناخت اطلاعاتی که در پکت IP ارائه میشود به شما کمک میکند تا نحوه یکپارچگی اطلاعات ارسالی قابل سوء استفاده در شبکه محلی یا اینترنت را درک کنید. شکل زیر نشانگر یک سرآیند دیتاگرام IP است. هر قسمت نیز دارای توضیح مختصری است.



4) Version بیت) : بخش Version برای شناسایی نسخه IP استفاده شده در پکت مورد استفاده قرار میگیرد.

4) Internet Header Length بیت) : بخش طول سرآیند اینترنت معرف سرآیند IP بزرگتر است. این بخش مشخص کننده طول سرآیند بصورت کلمات ۳۲ بیتی (بلوک های ۴ بایتی) استو به محل شروع Payload اشاره میکند. سرآیند طول بایت ها را بصورت عددی معرفی میکند و عدد قابل قبول آن در محدوده ۵ تا ۱۵ است. یعنی طول سرآیند باید در محدوده ۲۰ تا ۶۰ بایت باشد.

8) Type Of Service بیت) : بخش نوع سرویس پارامترهایی را برای نوع سرویس درخواستی تعریف میکند. سطوح سرویس که بصورت پکت قابل درخواستند از کامپیوتر مبداء به کامپیوتر مقصد حرکت میکنند و شامل سطوح اهمیت، تاخیر، عبور و قابلیت اطمینان میباشند.

16) Totla Length بیت) : این بخش مربوط به طول کلی دیتاگرام (به بایت) است و شامل Header و Payload است. وقتی تعریف RFC یک دیتاگرام IP را مطالعه میکنید (RFC791) متوجه خواهید شد که این بخش بصورت مبنای ۸ اندازه گیری میشود. یک اکتت ۸ بیت طول دارد که یک بایت است. حداکثر اندازه یک دیتاگرام IP قابل قبول ۶۵۵۳۵ بایت است که اندازه پیشنهادی در RFC 576 بایت است که میتوان به کمک آن یک سرآیند ۶۴ بایتی و Payload 512 بایتی داشت.

16) Identifier بیت) : این مقدار توسط فرستنده تعیین میشود و برای بازسازی پراکندگی دیتاگرام های IP در مقصد مورد استفاده قرار میگیرد.

3) Flags بیت) : این بیت ها برای نشان دادن پراکندگی دیتاگرام مورد استفاده قرار میگیرند و اگر چنین باشد، نشان میدهند که آیا این تکه، تکه آخر است. پراکندگی را در فصول بعد با جزئیات بیشتری بررسی خواهیم کرد.

13) Fragment Offset بیت) : این بخش مشخص میکند که تکه موجود به کدام بخش دیتاگرام تعلق دارد. این مقدار با گام های ۸ بایتی (۶۴ بیت) اندازه گیری میشود و اولین تکه همیشه دارای آفست صفر است، چون اولین تکه در سری است. اطلاعات تکه و آفست تکه بسیار مهمند زیرا دیتاگرام ها همیشه به ترتیب به مقصد نمی رسند.

8) Time To Live بیت) : قسمت طول عمر (TTL) نشانگر حداکثر تعداد اتصالاتی است که یک پکت قادر به عبور از آنهاست تا به کامپیوتر مقصد برسد. کامپیوتر مبداء حداکثر TTL را تعیین میکند و سپس هر روتری که پکت را بدست میگیرد آنرا یک واحد کاهش میدهد و سپس پکت را هدایت میکند. اگر کاهش TTL قبل از رسیدن به مقصد صفر شود، پکت ندید گرفته میشود و در اصطلاح می میرد.

8) Protocol بیت) : این بخش نشانگر پروتکل مورد استفاده در لایه انتقال از سیستم چهار لایه ای DARPA است. برای مثال، اگر دیتاگرام یک پکت TCP باشد، این قسمت مقدار ۶ را خواهد داشت. اگر پکت UDP باشد، این بخش ۱۷ خواهد بود.

16) Header Checksum بیت) : سرجمع سرآیند برای فراهم آوردن یکپارچگی سطح بیتی اطلاعات سرآیند مورد استفاده قرار میگیرد. این سرجمع فقط برای سرآیند IP است و بخش Payload دیتاگرام را شامل نمیشود. کامپیوتر مبداء سرجمع اولیه قبل از ارسال پکت، محاسبه میکند. هر روتری که پکت را دریافت میکند، سرجمع را کنترل میکند، TTL را کاهش داده، سرجمع جدیدی محاسبه میکند و سپس پکت را ارسال میکند. اگر سرجمع در هر روتری بین کامپیوترهای مبداء و مقصد نادرست باشد، دیتاگرام ندید گرفته میشود.

32) Source IP Address بیت) : آدرس IP کامپیوتر مبداء است.

32) Destination IP Address بیت) : آدرس IP کامپیوتر مقصد است.

IP Option and Padding (متغیر) : این بخش اختیاری است و میتواند طولهای متفاوتی داشته باشد. اگر این بخش مورد استفاده قرار گیرد، باید با گامهای ۳۲ بیتی افزایش پیدا کند. بدین ترتیب اگر دیتاگرام دارای گزینه اختیاری باشد (۸ بیتی تعریف میشود)، ۲۴ بیت اضافی (صفر) باید بعنوان لایه

گذاری اضافه شود. پس گزینه اضافه شده ۳۲ بیتی میشود. هر گزینه بصورت ۸ بیتی تعریف میشود و دارای سه بخش است : یک پرچم کپی شده یک بیتی، کلاس خصیصه ۲ بیتی و شماره خصیصه ۵ بیتی. اطلاعات بیشتر در مورد خصیصه ها را میتوانید در این آدرس بدست آورید.

مدل مرجع تی‌سی‌پی/آی‌پی

یکی از اولین اهداف آرپانت ارتباط یکپارچهٔ شبکه‌های کامپیوتری بود که بالاخره توسط مدل TCP/IP در سال ۱۹۸۵ محقق شد. TCP/IP مخفف Transmission Control Protocol/Internet Protocol می‌باشد.با اینکه پروتکل فوق کند و مستلزم استفاده از منابع زیادی است، ولی بدلیل مزایای بالای آن نظیر: قابلیت روتینگ، حمایت در اغلب پلات فورم‌ها و سیستم‌های عامل همچنان در زمینه استفاده از پروتکل‌ها حرف اول را می‌زند. این مدل برخلاف مدل مرجع OSI که هفت لایه داشت، دارای چهار لایه به قرار زیر است:

لایه اینترنت

این لایه معادل لایه شبکه در مدل مرجع OSI می‌باشد که دارای وظایف زیر است:

- اجازه دادن به بسته‌ها جهت ارسال از روی شبکه به سمت مقصد.
- به مقصد رساندن بسته‌های IP دار.
- مسیر یابی

لایه انتقال

این لایه مکالمه عناصر همتا را برعهده می‌گیرد و طبق دو پروتکل زیر عمل می‌کند:

- TCP: داده‌ها را در مبدا بسته بسته می‌کند و در مقصد به هم می‌چسباند. در اصل این پروتکل که اتصال گرا می‌باشد وظیفه کنترل جریان با قابلیت اعتماد بالا را دارد.
- UDP: این پروتکل غیر متصل می‌باشد و برخلاف TCP از سرعت بالا تری برخوردار است، اما قابلیت اعتماد آن کمتر است.

لایه کاربرد

پروتوکل‌های سطح بالا مثل ,HTTP,SMB,NFS,MIME,TFTP، TELNET، FTP، SMTP، DNS، NNTP و غیره در این لایه قرار دارد.

لایه میزبان به شبکه

مدل TCP/IP در باره این لایه سکوت اختیار کرده، و تنها می‌توان گفت که وظیفه اصلی این لایه اتصال میزبان به شبکه‌است.

مفاهیم اولیه پروتکل TCP/IP (بخش اول)

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 می گیرد.

معرفی پروتکل TCP/IP

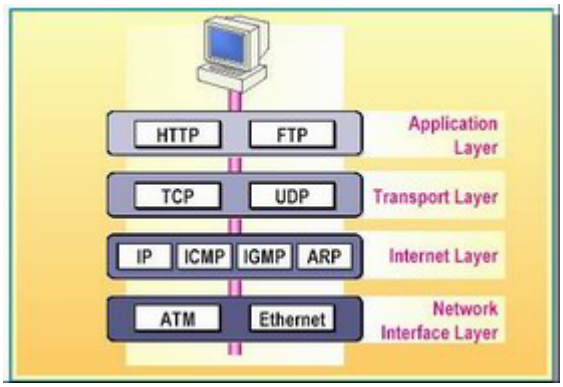
TCP/IP ، پروتکلی استاندارد برای ارتباط کامپیوترهای موجود در یک شبکه مبتنی بر ویندوز ۲۰۰۰ است. از پروتکل فوق، بمنظور ارتباط در شبکه های بزرگ استفاده می گردد. برقراری ارتباط از طریق پروتکل های متعددی که در چهارلایه مجزا سازماندهی شده اند ، میسر می گردد. هر یک از پروتکل های موجود در پشته TCP/IP ، دارای 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 تحقـق عملیـات فوق با رویکردی مستقل نسبت به محیط انتقال ، انجام خواهد شد .

لایه های پروتکل TCP/IP

TCP/IP ، فرآیندهای لازم بمنظور برقراری ارتبـاط را سـازماندهی و در ایـن راسـتا از پروتکـل هـای متعددی در پشته TCP/IP استفاده می گردد. بمنظور افزایش کارآئی در تحقق فرآیند های مورد نظر، پروتکل ها در لایه های متفاوتی، سازماندهی شده اند . اطلاعات مربـوط بـه آدرس دهـی در انتهـا قـرار گرفته و بدین ترتیب کامپیوترهای موجود در شبکه قادر به بررسی آن با سرعت مطلوب خواهند بود. در این راستا، صرفا" کامپیوتری که بعنوان کامپیوتر مقصد معرفی شده است ، امکـان بـاز نمـودن بـسته اطلاعاتی و انجام پردازش های لازم بر روی آن را دارا خواهد بود. TCP/IP ، از یک مدل ارتباطی چهار لایه بمنظور ارسال اطلاعات از محلی به محل دیگر استفاده می نمایـد: Application ,Transport Internet, و Interface Network ، لایه های موجود در پروتکل TCP/IP می باشند.هـر یـک از پروتکل های وابسته به پشته TCP/IP ، با توجه به رسالت خود ، در یکی از لایه های فوق، قرار مـی گیرند.



لایه Application

لایه Application ، بالاترین لایه در پشته TCP/IP است .تمامی برنامه و ابزارهای کاربردی در این لایه ، با استفاده از لایه فوق، قادر به دستتیابی به شبکه خواهند بود. پروتکل های موجود در این لایه بمنظور فرمت دهی و مبادله اطلاعات کاربران استفاده می گردند . HTTP و FTP دو نمونه از پروتکل ها ی موجود در این لایه می باشند .

- پروتکل Hypertext Transfer Protocol(HTTP) . از پروتکل فوق ، بمنظور ارسال فایل های صفحات وب مربوط به وب ، استفاده می گردد .
- پروتکل File Transfer Protocol(FTP) . از پروتکل فوق برای ارسال و دریافت فایل، استفاده می گردد .

لایه Transport

لایه " حمل " ، قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به لایه Application (لایه بالای خود) و یا لایه اینترنت (لایه پایین خود) را بر عهده دارد. لایه فوق ، همچنین مشخصه منحصربفردی از برنامه ای که داده را عرضه نموده است ، مشخص می نماید. این لایه دارای دو پروتکل اساسی است که نحوه توزیع داده را کنترل می نمایند.

- Transmission Control Protocol(TCP) . پروتکل فوق ، مسئول تضمین صحت توزیع اطلاعات است .
- User Datagram Protocol UDP) . پروتکل فوق ، امکان عرضه سریع اطلاعات بدون پذیرفتن مسئولیتی در رابطه با تضمین صحت توزیع اطلاعات را برعهده دارد .

لایه اینترنت

لایه "اینترنت"، مسئول آدرس دهی ، بسته بندی و روتینگ داده ها ، است. لایه فوق ، شامل چهار پروتکل اساسی است :

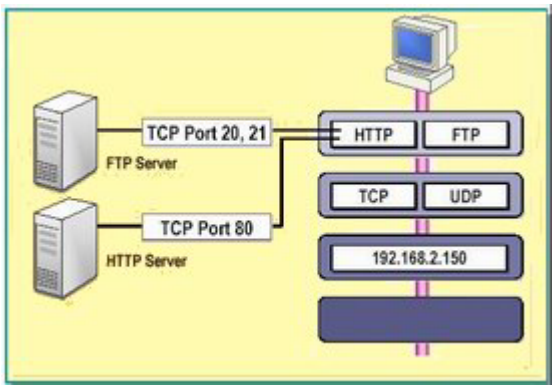
- Internet Protocol(IP) . پروتکل فوق ، مسئول آدرسی داده ها بمنظور ارسال بـه مقـصد مورد نظر است .
- Address Resoulation Protocol ARP) . پروتکـل فـوق ، مـسئول مـشخص نمـودن آدرس Media Access Control MAC) آداپتور شبکه بر روی کامپیوتر مقصد است.
- Internet Control Message Protocol(ICMP) . پروتکل فوق ، مـسئول ارائـه توابـع عیب یابی و گزارش خطاء در صورت عدم توزیع صحیح اطلاعات است .
- Internet Group Protocol Managemant IGMP) . پروتکل فوق ، مسئول مدیریت Multicasting در TCP/IP را برعهده دارد.

لایه Network Interface

لایه " اینترفیس شبکه " ، مسئول استقرار داده بر روی محیط انتقال شـبکه و دریافـت داده از محـیط انتقال شبکه است . لایه فوق ، شامل دستگاه های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه اسـت . کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده (نظیر : B5-50-04-22-D4-66) بوده که آدرس MAC ، نامیده می شود. لایه " اینترفیس شبکه " ، شامل پروتکل هـای مبتنـی بـر نرم افزار مشابه لایه های قبل ، نمی باشـد. پروتکـل هـای Ethernet و ATM)Asynchronous Transfer Mode) ، نمونه هائی از پروتکل های موجود در این لایه می باشند . پروتکل هـای فـوق ، نحوه ارسال داده در شبکه را مشخص می نمایند.

مشخص نمودن برنامه ها

در شبکه های کامپیوتری ، برنامه ها ی متعددی در یک زمان با یکـدیگر مـرتبط مـی گردنـد. زمانیکـه چندین برنامه بر روی یک کامپیوتر فعال می گردند ، TCP/IP ، می بایست از روشـی بمنظـور تمـایز یک برنامه از برنامه دیگر، استفاده نماید. بدین منظور ، از یـک سـوکت (Socket) بمنظـور مـشخص نمودن یک برنامه خاص ، استفاده می گردد.



آدرس IP

برقراری ارتباط در یک شبکه ، مستلزم مشخص شدن آدرس کامپیوترهای مبداء و مقصد است (شـرط اولیه بمنظور برقراری ارتباط بین دو نقطه ، مشخص بودن آدرس نقاط درگیر در ارتباط است) . آدرس هر یک از دستگاه های درگیر در فرآیند ارتباط ، توسط یک عدد منحصربفرد که IP نامیده می شود ، مشخص می گردند. آدرس فوق به هریک از کامپیوترهای موجود در شبکه نسبت داده می شـود . IP : **۱۰.۱,۱,۱۰** ، نمونه ای در این زمینه است .

پورت TCP/UDP

پورت مشخصه ای برای یک برنامه و در یک کامپیوتر خاص است .پورت با یکـی از پروتکـل هـای لایـه "حمل" (TCP و یا UDP) مرتبط و پورت TCP و یا پورت UDP ، نامیده می شـود. پـورت مـی تواند عددی بین صفر تا ۶۵۵۳۵ را شامل شود. پورت ها برای برنامـه هـای TCP/IP سـمت سـرویس دهنده ، بعنوان پورت های "شناخته شده " نامیده شده و به اعداد کمتر از ۱۰۲۴ ختم و رزو می شوند تا هیچگونه تعارض و برخوردی با سایر برنامه ها بوجود نیاید. مـثلا" برنامـه سـرویس دهنـده FTP از پورت TCP بیست و یا بیست ویک استفاده می نماید.

سوکت (Socket)

سوکت ، ترکیبی از یک آدرس IP و پورت TCP ویا پورت UDP است . یـک برنامـه ، سـوکتی را بـا مشخص نمودن آدرس IP مربوط به کامپیوتر و نوع سرویس (TCP برای تضمین توزیع اطلاعات و یـا

UDP) و پورتی که نشاندهنده برنامه است، مشخص می نماید. آدرس IP موجود در سوکت ، امکان آدرس دهی کامپیوتر مقصد را فراهم و پورت مربوطه ، برنامه ای را که داده ها برای آن ارسال می گردد را مشخص می نماید.

در بخش دوم این مقاله به تشریح هر یک از پروتکل های موجود در پشته TCP/IP، خواهیم پرداخت .

مقایسه مدلهای OSI و TCP/IP

مدل مرجع OSI و مدل مرجع TCP/IP نقاط مشترک زیادی دارند. هر دوی آنها مبتنی بر مجموعه ای از پرتوکل های مستقل هستند، و عملکرد لایه ها نیز تا حدی شبیه یکدیگر است. مدل OSI ثابت کرده که بهترین ابزار برای توصیف شبکه های کامپیوتری است. اما پروتکل های TCP/IP در مقیاس وسیعی مورد استفاده قرار می گیرد. این دو مدل تفاوت هایی با هم دارند که در زیر به برخی از آنها اشاره می کنیم:

- در مدل TCP/IP تفاوت سرویس ها، واسط ها و پروتکل ها واضح و مشخص نمی باشد.
- پروتکلهای OSI بهتر از TCP/IP مخفی شده است.
- قبل از ایجاد مدل OSI پروتکلهای آن طراحی و ابداع شد. در نتیجه این مدل وابستگی و تعامل خاصی با هیچ مجموعه پروتکلی ندارد. اما در TCP/IP مسئله برعکس بود و این خود باعث شده که مدل TCP/IP تنها برای شبکه های تحت خود مناسب باشد.
- مدل OSI دارای هفت لایه است اما مدل TCP/IP ، چهار لایه دارد و از لایه ارائه و لایه نشست خبری نیست.
- لایه شبکه در مدل OSI اتصال گرا و غیر مستقیم است و لایه انتقال آن تنها اتصال گرا است اما در TCP/IP لایه شبکه الزاما غیر متصل و لایه انتقال آن اتصال گرا(TCP) یا غیر متصل(UDP) است.

مشکلات مدل OSI

- **زمان نامناسب**: استاندارد گذاری در زمان مناسبی انجام نشد(برخلاف فرضیه ملاقات فیل ها). در واقع OSI کامل ارائه شد TCP/IP محبوبیت بسیاری پیدا کرده بود.
- **تکنولوژی نا مناسب**: مدل ها و پروتکل های آن ناقص و معیوب است، پیاده سازی آن دشوار و غیر قابل فهم است و عملکرد ها در لایه های مختلف تکرار شده .
- **پیاده سازی نامناسب**: بسیار حجیم، سنگین و کند است.
- **سیاست های نامناسب**: این پیش فکر وجود داشت که OSI استانداردی دولتی است.

مشکلات مدل TCP/IP

- مفاهیم سرویس، واسط و پروتکل به روشنی از هم تفکیک نشده است.
- مدلی کامل و کلی به شمار نمی رود.
- با در نظر گرفتن مفاهیم شبکه لایه، میزبان به شبکه اساسا لایه ای واقعی نیست.
- برخی از پروتکل های آن خوب طراحی نشده است.

مقدمه ای بر TCP/IP

از آنجایی که در دنیای مجازی اینترنت و به خصوص دنیای امنیت یکی از مهمترین قسمتها بخش پایه شبکه و بخصوص TCP/IP می باشد ما بر آن شدیم تا در این سری مقالات در خصوص TCP/IP و تا حدودی osi مختصری بپردازیم پیشاپیش هر قصور و کمبودی را به بزرگواری خودتان بر این شاگرد ناچیز ببخشید .

از آنجایی که در دنیای مجازی اینترنت و به خصوص دنیای امنیت یکی از مهمترین قسمتها بخش پایه شبکه و بخصوص TCP/IP می باشد ما بر آن شدیم تا در این سری مقالات در خصوص TCP/IP و

تا حدودی osi مختصری بپردازیم پیشاپیش هر قصور و کمبودی را به بزرگواری خودتان بر این شاگرد ناچیز ببخشید .

OSI چیست ؟

OSI (Open System Interconnection) یک مدل مرجع برای ارتباط بین دو کامپیوتر می باشد که در سال ۱۹۸۰ طراحی گردیده است. هر چند امروزه تغییراتی درآن به وجود آمده اما هنوز هم کاربردهای فراوانی در جاهای مختلف اینترنت و به خصوص در پایه های شبکه دارد.

این مدل بر اساس لایه بندی قراردادهای برقراری ارتباط که همزمان روی دو سیستم مرتبط اجرا شده اند پایه ریزی شده است که این امر بسیار سرعت و دقت ارتباط را افزایش می دهد و این قراردادها بصورت طبقه طبقه در هفت لایه تنظیم شده اند که در زیر بررسی خواهند شد. (شکل ۱)

مدل مرجع osi	
لایه کاربرد	Application
لایه ارائه	Presentation
لایه جلسه	Session
لایه انتقال	Transport
لایه شبکه	Network
لایه پیوند داده ها	Data link
لایه فیزیکی	Physical
شکل ۱: لایه های مدل OSI	

بررسی هفت لایه OSI :

لایه فیزیکی :

این لایه که تنها تشکیل شده از سخت افزار می باشد و قراردادهای سخت افزاری در آن اجرا مـی شـود وظیفه انتقال نهایی اطلاعات را دارد که این انتقال یصورت سیگنال و به صورت صفرو یک می باشد

لایه پیوند داده ها :

در این لایه اطلاعات ، کشف خطا و اصلاح می شوند و بدون خطا و به صورت مطمئن بـه سـوی مقـصد ارسال می شوند .وظیفه دیگر این لایه مطمئن شدن از رسیدن اطلاعات به مقصد اسـت کـه ایـن کـار توسط بیتهای (Parity check , checksum ,crc) انجام می پذیرد .که در صـورت بـروز خطـا مجددا اطلاعات ارسال خواهند شد .

لایه شبکه :

و اما پیچیده ترین لایه یعنی لایه شبکه که در آن قراردادهای شبکه بندی تعریف شـده اسـت . وظیفـه این لایه انتقال تکنولوژی برقراری ارتباط برای دیگر شبکه های مستقل است که این امر این امکان را به osi می دهد که بتواند در زیر شبکه های مختلف فعالیت کند .

لایه انتقال :

در این لایه قبل از ارسال اطلاعات یک بسته به سمت مقـصد فرسـتاده مـی شـود تـا مقـصد را بـرای دریافت اطلاعات آماده کند . همچنین این لایه وظیفه تکه تکه کردن بسته ها ، شماره گـذاری آنهـا و ترتیب و نظم دهی آنها را بر عهده دارد. که البته بسته ها در طرف گیرنده دوباره در همین لایـه نظـم دهی و قابل استفاده برای لایه های بالاتر خواهند شد.

لایه جلسه :

در این لایه بر کارهایی از قبیل زمان ارسال و دریافت بسته ها مقدار رسیده و مقدار مانـده از بـسته هـا نظارت می شود که به مدیریت بسته ها بسیار کمک می کند .

لایه ارائه :

در این لایه استانداردهای رمز نگاری و فشرده سازی اطلاعات تعریف شده است که این لایـه در امنیـت بسیار مهم می باشد .

لایه کاربرد :استانداردهای ارتباط بین نرم افزارهای شبکه در این لایه قرار دارد که می توان از :

نام برد FTAM CMIP MHS VT

Internet protocol /Transmission Control Protocol » TCP/IP

TCP/IP چیست ؟

TCP/IP مجموعه قراردادهایی هستند که در جهت اتصال کامپیوتر ها در شبکه مورد اسـتفاده قـرار می گیرند. وبه تعریف دیگر قرارداد کنترل انتقال اطلاعات می باشد .

مقایسه با osi: (شکل۲)

مدل مرجع osi	مدل چهار لایه TCP/IP
لایه کاربرد	لایه کاربرد
لایه ارائه	
لایه جلسه	لایه انتقال
لایه انتقال	
لایه شبکه	لایه شبکه
لایه پیوند داده ها	لایه واسطه شبکه
لایه فیزیکي	

همانطور که از شکل پیداست TCP/IP از چهار لایه تشکیل شده که در زیر به صحبت در مورد چهـار لایه TCP/IP می پردازیم .

لایه واسط شبکه :

در این لایه تمام استانداردهای سخت افزاری و انواع پروتکل شبکه تعریف شده که خاصیت بـزرگ ایـن لایه این موضوع می باشد که در آن می توان بین نرم افزار و سخت افزار شبکه ارتباط برقرار کرد.

لایه شبکه :

در این لایه پروتکل IP آدرس دهی و تنظیم می شود .(توضیحات در قـسمت IP) و همچنـین دیگـر پروتکل ها مانند ARP,ICMP,BOOTP که در این میان نقش هیچکـدام بـه انـدازه IP , ICMP مهم نیست در کل وظیفه این لایه دادن اطلاعات در مورد شبکه و آدرس دهی در آن می باشد که مسیر یابها از آن بسیار استفاده می کنند .

لایه انتقال :

ابتدایی ترین وظیف این لایه آگاهی از وضعیت بسته ها می باشد که بسیار مهم نیز هست .

و در مرحله بعد وظیفه این لایه انتقال اطلاعاتی می باشد که نیاز به امنیت ندارند و سـرعت بـرای آنهـا مهم تر است

لایه کاربرد :

این لایه دارای امکانات زیادی برای هنر نمایی متخصصان می باشد.

در این لایه برنامه های کاربردی قرار دارند و در کل این لایه لایه ی نرم افزارهـای شـبکه مـی باشـد و همچنین لایه پروتکل های نرم افزاری نیز می باشد .

از مهم ترین نکات در خصوص این لایه قرارداشتن : انتقال فایل (FTP) و مـدیریت پـست (SMTP) و بقیه برنامه های کاربردی می باشد .

پروتکل اینترنت IP

حتما همه شما عزیزان واقف به این موضوع هستید که IPیکی از مهمترین قسمتهای TCP/IP و شاید بتوان گفت مهمترین قسمت آن زیرا تقریبا شما برای هر کاری نیاز به آن خواهید داشت لذا بسیار ضروری و حیاتی می باشد که شما اطلاعات خود را در زمینه این مهم افزون کنید .

IPیک آدرس عددی است که برای ارتباط با شبکه به هر ماشینی در شبکه اختصاص داده می شود (چون IPبرای وسایلی از قبیل ROUTERو MODEM و LAN و ... استفاده می شود ما اصطلاحا به جای نام بردن تک تک آنها همه را ماشین می نامیم)

« IP شما نسبت به نوع اتصال شما متغییر و یا ثابت می باشد. »

وظیفه IPچیست ؟

وظیفه پروتکل IP حمل و تردد بسته های حاوی اطلاعات و همچنین مسیر یابی آنها از مبدا تا مقصد است

اساس کار پروتکل IPچیست ؟

IP پس از دریافت اطلاعات از TCP شروع به قطعه قطعه کردن آن به قطعه های کوچک به اسم FRAGMENT می نماید، پس از این مرحله برای هر FRAGMENT یک بسته IP می سازد که حاوی اطلاعات مورد نیاز بسته برای حرکت در طول شبکه می باشد و بسته IP را به بسته TCP اضافه می کند

و شروع به ارسال بسته های تیکه تیکه شده(FRAGMENT) می نماید حال مسیر یابها بر اساس تنظیمات قسمت IP بسته ها را به مقصد خود هدایت می کنند و آن را داخل زیر شبکه ها هدایت می کنند

خصوصیات IP :

بسته IP حد اکثر ۶۴ کیلوبایت فضا را اشغال خواهد کرد و بیشتر از آن نمی تواند باشد ولی موضوع جالب اینجاست که در حالت عادی حجم بسته حدود ۱۶۰۰ بایت بیشتر نمی شود

« بعدها یک حمله do's بر مبنای همین موضوع طراحی شد »

IPدر تمامی سیستم های عامل با ساختار استانداردی که دارد به درستی کار می کنند و نیاز به هیچ نوع سخت افزار ندارد .

بررسی ساختار بسته ساخته شده توسط پروتکل IP

بسته IP ساخته شده از تعدادی فیلد مجزا می باشد که هر کدام اطلاعاتی را در خود دارند که در زمان مورد نیاز این اطلاعات از داخل بسته ها استخراج می شود و مورد استفاده قرار می گیرد این اطلاعات شامل مواردی مثل :آدرس IP فرستنده . آدرس IP گیرنده و ..... می باشد

بررسی فیلدها :

فیلد version:

وظیفه مشخص کردن نوع پروتکل IP را بر عهده دارد (در حال حاضر از دو version ۴و۶ استفاده می شود)

اندازه فیلد :چهار بیت

فیلد :IHL

وظیفه این فیلد نگهداری اندازه قسمت بالایی بسته در خود می باشد که از آن برای تعیین مرز بین اطلاعات و محتویات بسته IP استفاده می شود .

اندازه فیلد : ۴ بیت

فیلد TYPE OF SERVICE:

دراین فیلد نوع سرویس انتقال تعیین می شود : ((کم سرعت و مطمئن))و ((پر سرعت و نامطمئن))

اندازه فیلد : هشت بایت

فیلد TOTAL LENGTH :

در این فیلد اندازه کل بسته IP قرار دارد که شامل قسمت سر آیند و ناحیه داده می باشد که همانطور که گفته شد می تواند ۶۵۵۳۵ بایت باشد .

اندازه فیلد : ۱۶ بیت

فیلد FRAGMENT OFFSET :

این قیلد خود به سه بخش تقسیم می شود :

۱- بیت DF(DON'T FRAGMENT): اگر این بیت ۱ باشد هیچ مسیر یابی حق شکستن این بسته را ندارد

۲- بیت MF(MORE FEAGMENT): اگر این بیت ۰ بود به این معنی می باشد که این قطعه آخرین قطه ارسال شده می باشد

۳- FRAGMENT OFFSET

در این قسمت شماره قطعه های شکسته شده قرار دارد و چون اندازه این فیلد ۱۳ بیت می باشد اطلاعات می توانند تا ۸۱۹۲ قطعه شکسته شوند (اندازه هر قطعه به غیر از قطعه آخری باید ضریبی از ۸ باشد)

فیلد TIME TO LIVE:

همانطور که می دانید در این فیلد زمان سرگردانی بسته مشخص می شود و این به معنی می باشد که این بسته می تواند از چند مسیر یاب عبورکند که حداکثر آن ۲۵۵می باشد . این فیلد یک نعمت بزرگ می باشد

اندازه فیلد :۸ بیت

فیلد PROTOCOL:

در این فیلد شماره پروتکلی که قرار است بسته به آن برسد مشخص می شود

فیلد : HEADER CHECKSUM:

وظیف کشف خطا را بر عهده دارد

فیلد SOURCE ADDRESS :

این فیلد فیلد بسیار مهمی می باشد چون در آن آدرس مبدا موجود می باشد برنامه های فیلترنیگ و فایروالها بسیار از این فیلد استفاده می کنند .

فیلد DESTINATION ADDRESS:

در این فیلد هم آدرس IP مقصد موجود می باشد

فیلد OPTION :

این فیلد یک فیلد خالی می باشد که در آن هر توضیحاتی به صورت دلخواه می توان نوشت

فیلد PAYLOAD:

در این فیلد داده ها بین لایه های مختلف رد و بدل می شود البته این امر از لایه های بالا به سمت لایه های پائینتر صورت می گیرد

نکاتی جالب در مورد IP

آدرس های ویژه :

این آدرسها نمونه های از آدرس های IP خاص هستند که از قبل برای مقاصد خاصی در نظر گرفته شده اند و در تعریف شبکه نمی توان از آنها به عنوان IP برای ماشینها استفاده کرد .

0.0.0.0

از این آدرس در مواردی استفاده می شود که ماشین میزبان از IP خود بی اطلاع است .البته اگر از این آدرس به عنوان آدرس فرستنده استفاده شود هیچ جوابی برای فرستنده پس فرستاده نمی شود

HostId.0

این آدرس برای زمانی است که از آدرس خود در زیرشبکه بی اطلاع باشیم

255.255.255.255

از این آدرس برای ارسال پیامهای به صورت عمومی و فراگیر در شبکه استفاده می شود البته با استفاده از این آدرس می توان در زیر شبکه خود پیام فراگیر ارسال کرد .

NetId.255

از این آدرس برای ارسال پیامهای فراگیر در دیگر شبکه ها از خارج از آنها استفاده می شود .البته این سرویس تقریبا در بیشتر اوقات از سوی مدیران شبکه غیر فعال می شود .

در مقالات بعدی به بررسی TCPخواهیم پرداخت

اشکال زدائی شبکه های مبتنی بر TCP/IP (بخش دوم)

ipconfig ، یکی از دستورات مفید به منظور بررسی وضعیت پیکربندی TCP/IP در کامپیوترهای سرویس دهنده و یا سرویس گیرنده ای است که بر روی آنان ویندوز نصب شده است . در یونیکس و لینوکس از دستور ifconfig در این رابطه استفاده می شود . در سیستم هائی که بر روی آنان ویندوز x۹ و یا ME نصب شده است ، می توان از دستور winipcfg استفاده نمود .

استفاده از ipconfig

برای استفاده از دستور فوق، کافی است نام آن را از طریق پنجره command prompt تایپ نمود . عملکرد ipconfig و اطلاعاتی که در اثر اجرای آن نمایش داده خواهد شد به نوع سوئیچ استفاده شده ، بستگی دارد .

استفاده از ipconfig بدون سوئیچ ،اطلاعات پیکربندی TCP/IP در ارتباط با هر یک از آداپتورهای موجود بر روی سیستم را نمایش خواهد داد:

- آدرس IP
- Mask Subnet
- gateway Default
- اطلاعات سرویس دهنده DNS
- Domain

تایپ دستور	خروجی
C:\>ipconfig	**Ethernet adapter MyLan1:** Connection-specific DNS Suffix . : IP Address. . . . . : 10.10.1.1 Subnet Mask . . . . . : 255.0.0.0 Default Gateway . . . . . : **PPP adapter My ISP:** Connection-specific DNS Suffix . : IP Address. . . . . : 10.1.1.216 Subnet Mask . . . . . : 255.255.255.255 Default Gateway . . . . . : 10.1.1.216

دستور فوق ، اطلاعات مربوط به اتصالات از نوع PPP که از آنان در Dialup و VPN استفاده می شود را نیز نمایش خواهد داد .

استفاده از ipconfig به همراه سوئیچ all ، علاوه بر نمایش اطلاعات اشاره شده در بخش قبل ، اطلاعات دیگری را نیز نمایش خواهد داد :

- آدرس سخت افزاری کارت شبکه (آدرس MAC)
- اطلاعات مربوط به DHCP

تایپ دستور	خروجی
C:\>ipconfig /all	**Windows 2000 IP Configuration** Host Name . . . . . : srco Primary DNS Suffix . . . . . : srco.ir Node Type . . . . . : Broadcast IP Routing Enabled. . . . . : No WINS Proxy Enabled. . . . . : No DNS Suffix Search List. . . . . : srco.ir **Ethernet adapter MyLan1:** Connection-specific DNS Suffix . : Description . . . . . : D-Link DFE-680TX CardBus PC Card Physical Address. . . . . : 00-50-BA-79-DB-6A DHCP Enabled. . . . . : No IP Address. . . . . : 10.10.1.1 Subnet Mask . . . . . : 255.0.0.0 Default Gateway . . . . . : DNS Servers . . . . . : 127.0.0.1 **PPP adapter My ISP:** Connection-specific DNS Suffix . : Description . . . . . : WAN (PPP/SLIP) Interface Physical Address. . . . . : 00-53-45-00-00-00 DHCP Enabled. . . . . : No IP Address. . . . . : 10.1.1.216 Subnet Mask . . . . . : 255.255.255.255 Default Gateway . . . . . .: 10.1.1.216 DNS Servers . . . . . : x1.y1.z1.w1 x2.y2.z2.w2

سایر سوئیچ های دستور ipconfig : با استفاده از دستور ipconfig و برخی سوئیچ های آن (release ,renew) ، می توان اطلاعات مربوط به پیکربندی TCP/IP ارائه شده توسط سرویس دهنده DHCP را که در اختیار یک سرویس گیرنده قرار داده شده است را آزاد و یا آنان را مجددا" از سرویس دهنده درخواست نمود . فرآیند فوق به منظور تشخیص عملکرد صحیح سرویس دهنده DHCP در شبکه بسیار مفید و کارساز است . (آیا سرویس دهنده DHCP وظایف خود را به خوبی انجام می دهد ؟ آیا یک سرویس گیرنده قادر به برقراری ارتباط با سرویس دهنده DHCP به منظور درخواست و دریافت اطلاعات پیکربندی TCP/IP می باشد ؟) . دستور ipconfig دارای سوئیچ های مفید متعددی است که می توان با توجه به نوع خواسته خود از آنان استفاده نمود :

عملکرد	سوئیچ
آدرس IP پیکربندی شده توسط DHCP را آزاد می نماید . در صورتی که سوئیچ فوق را به تنهائی و بدون مشخص نمودن adapter تایپ نمائیم،پیکربندی IP برای تمامی آداپتورهای موجود بر روی کامپیوتر، آزاد می گردد. در صورتی که قصد آزاد سازی اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم ، می بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد . (مثلا" ipconfig / release MyLan)	/release [adapter]
یک آدرس IP را بر اساس اطلاعات جدیدی که از طریق DHCP دریافت می نماید ، پیکربندی مجدد می نماید . در صورتی که سوئیچ فوق را به تنهائی و بدون مشخص نمودن adapter تایپ نمائیم،پیکربندی IP تمامی آداپتورهای موجود بر روی کامپیوتر، مجددا" انجام خواهد شد. در صورتی که قصد ایجاد مجدد اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم ، می بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد. (مثلا" ipconfig / renew MyLan1)	/renew [adapter]
حذف محتویات Dns Resolver Cache	/flushdn
Refresh نمودن تمامی اطلاعات تولید شده توسط DHCP برای آداپتور و ریجستر نمودن اسامی Dns	/registerdn
نمایش محتویات Dns Resolver Cache	/d isplaydns
نمایش تمامی ID DHCP Class مجاز برای آداپتور	/ showclassid [adapter]
تغییر ID DHCP Class	/setclassid [adapter] [classidtoset]

توضیحات :

- تشخیص نام آداپتور : نام آداپتور را می توان با کلیک (click Right) بـر روی Network Neighborhood و انتخـاب گزینـه properties، از طریـق پنجـره Network and Connections Dial-up مشاهده نمود (اسامی آدپتورها ، نام آیکون ها می باشند) .
- مفهوم DNS Cache : زمانی که یک سیستم ، ترجمه (تبدیل نـام host بـه آدرس) را از طریق یک سرویس دهنده DNS دریافت می نماید ، برای مدت زمـان کوتـاهی آن را در یـک Cache ذخیره می نماید . در صورتی کـه مجـددا" از نـام اسـتفاده شـود ، پـشته TCP/IP محتویات Cache را به منظور یافتن رکورد درخواستی بررسی می نماید . بدین ترتیب امکـان پاسخگوئی سریعتر به درخواست ترجمه نسبت به حالتی کـه در خواسـت بـرای یـک سـرویس دهنده DNS ارسال می شود ، فراهم می گردد . با توجه به این که اندازه Cache نمی توانـد از یک میزان منطقی و تعریف شده تجاوز نماید ، هر رکورد موجود در Cache پـس از مـدت زمانی خاص حذف می گردد. در صورت اعمال هرگونه تغییرات در DNS (مـثلا" تغییـر یـک رکورد DNS) ، می توان بـا اسـتفاده از دسـتور ipconfig/flushdns تمـامی رکوردهـای موجود در cache را حذف نمود . بـدین ترتیـب در صـورت درخواسـت یـک نـام host ، بـا سرویس دهنده DNS مشورت می گردد و نتایج مجددا" در Cache ذخیـره خواهنـد شـد . دستور ipconfig / displaydns ، محتویات cache را نمایش خواهد داد. از اطلاعاتی که نمایش داده می شود ، می توان به منظور تشخیص این موضوع که آیا برای ترجمه نام به آدرس از Cache و یا سرویس دهنده DNS استفاده شده است ، کمک گرفت .
- موارد استفاده از دستور Ipconfig : از دستور فوق در مواردی که قصد تشخیص این موضـوع را داریم که آیا سرویس دهنده DNS و DHCP در شبکه به درستی وظـایف خـود را انجـام می دهند ، استفاده می شود(علاوه بـر مـشاهده اطلاعـات پیکربنـدی TCP/IP) . مـثلا" بـا استفاده از سوئیچ های release و renew ، می توان براحتی تشخیص داد که آیا در زمینـه

دریافت اطلاعات پیکربندی از یک سرویس دهنده DHCP مشکل خاصی وجود دارد .از سوئیچ های مرتبط با DNS می توان به منظور اعمال تغییرات پیکربندی ، بهنگام سازی cache محلی و یا ریجستر نمودن اطلاعات پیکربندی جدید با یک سرویس دهنده DNS ، استفاده نمود .

- امکانات جانبی به همراه دستور ipconfig : با استفاده از سوئیچ all / اطلاعات متنوعی در رابطه با پیکربندی TCP/IP نمایش داده خواهد شد . در صورتی که حجم اطلاعات بگونه ای است که می بایست صفحه را scroll نمود ، می توان از |More به همراه دستور ipconfig استفاده نمود . در صورت تمایل می توان خروجی دستور ipconfig را در مقابل ارسال بر روی دستگاه استاندارد خروجی (صفحه نمایشگر) ، در یک فایل ذخیره نمود تا امکان بررسی سریعتر نتایج و رفع مشکل فراهم گردد.
- (test1.txt < ipconfg /all)

همانگونه که اشاره گردید در سیتم هائی که از لینوکس و یا یونیکس استفاده می نمایند ، از دستور ifconfig استفاده می گردد. از دستور فوق برای نمایش اطلاعات پیکربندی IP و اعمال تغییرات لازم استفاده می شود .