شبکه TCP/IP

دانشگاه جامع علمی کاربردی

مرکز آموزش ساوجبلاغ

« هشتگرد »

مدرس : مهدی تک فلاح

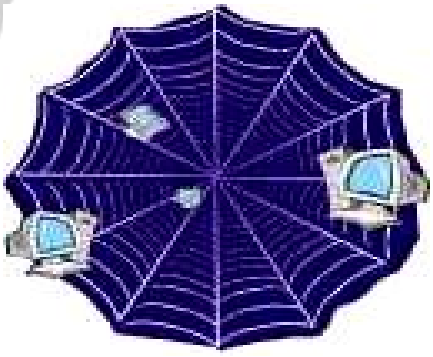
زمستان ۱۳۸۸

بسمه تعالی

مقدمه

Computer از کلمه Comput گرفته شده که به معنی محاسبه می باشد و کامپیوتر به معنی محاسبه گر می باشد.

افزایش محاسبات و نیاز به تبادل اطلاعات و ایجاد ارتباط باعث بوجود آمدن شبکه های کامپیوتری شد و با گسترش شبکه ها ، استاندارد سازی ارتباط مطرح و بحث پروتکل به میان آمد که از رایج ترین آنها OSI[1] و TCP/IP[2] می باشد.



مدل OSI « مدل مرجع ارتباطات سیستمهای باز »

مدل OSI جهت نمایش تئوری مفهوم لایه بندی شبکه بکار می رود و بصورت عملی استفاده نمی شود در صورتی که مدل TCP/IP ابتدا بصورت عملی پیاده شد و بعدها استاندارد شد این مدل در سال ۱۹۸۴ توسط ISO (سازمان بین المللی استاندارد سازی) ارائه گردید و در سال ۱۹۹۵ مورد تجدید نظر قرار گرفت. در این مدل از هفت لایه برای نمایش عملیات و مراحل مربوط به ارتباطات استفاده می گردد. هریک از لایه ها بخشی از انجام عملیات را برعهده دارند ترتیب لایه ها بصورت زیر می باشد :

[1] - Open System Interconnectio

[2] - Transmission Control Protocol / Internet Protocol

لایه های OSI

- **لایـه کاربـــــردی (Application)** ارتباط ایـن لایـه بـا سیـستم عامـل یـا برنامـه هـای کـاربردی مـی باشداکثر پروتکل ها در این لایه قرار دارند همچنین بزرگتـرین لایـه مـدل OSI اسـت از وظایف این لایه ، انتقال فایـل ، پـست الکترونیـک ، کنتـرل رایانـه از راه دور و رابـط برنامـه هـای مختلـف در شبکه می باشد.
- **لایه نمایـــــش (Presentation)** داده هـا را از لایـه Application دریافـت کـرده آنهـا رابـه شـکلی استاندارد کد گذاری می کند این عمل جهت دریافت صحیح و قابـل فهـم داده هـا در سیـستم هـا بـا سیستم عامل های مختلف بکار می رودفرمتی که در مبدا ارائه می دهـیم همـان فرمـت را در مقـصد دریافت میکنیم اطلاعات در مبدا بصورت رمـز میـشود و در مقـصد کـشف رمـز میـشود ایـن کارباعـث میشود اطلاعات به بصورت مطمئن به مقصد برسد
- **لایـه جلـســـه – نشـست (Session)** ایـن‌لایـه مـسئول فـراهم کـردن خـدمات لازم بـرای ارسـال ، مـدیریت قطعـه یـا نـشانه (Segment)، مـدیریت بـر ارتبـاط بـین کامپیوترهـا ، حـصول اطمینـان از دریافت درست ، جلوگیری از تداخل ، حفظ نوبت هنگام ترافیک و پشتیبانی است .
- **لایه انتقال (Transport)** مسئول شکستن داده هـا بـه واحـدهای کـوچکتر بنـام قطعـه(Segment) ، پـشتیبانی کنتـرل جریـان داده هـا و مراقبـت از برقـراری ارتبـاط و قطـع آن باشـدهمچنین مـسئول بررسی خطا و بازیـابی اطلاعـات بـین دسـتگاه هـای متفـاوت اسـت از وظـایف دیگـر ای لایـه هماهنگی سرعت فرستنده و گیرنده می باشد.
- **لایـه شبـکـــــه (Network)** تعیین روش ارسال داده ها برای دسـتگاه گیرنـده ، کنتـرل ترافیـک ، ترجمه آدرس منطقی بـه آدرس فیزیکـی ، یـافتن آدرس کامپیوترهـای مبـدا و مقـصد ، مـسیریابی در شبکه های بزرگ، تبدیل اطلاعات دریافتی ازلایه انتقال بـه واحـدهای کـوچکتر بنـام بـسته Packet و ارسال آنها، پروتکل های منطقی ، مسیریابی و آدرس دهی در این لایه انجـام خواهـد شـداین لایـه پیچیده ترین لایه مدلOSI است.
- **لایـه پیـــونـد داده ها (Data Link)** آماده کردن داده جهت ارسـال بـا تبـدیل داده بـه قـاب داده ، Data Frame و ارسال آن ، کنترل صحت ارسال و برطرف کـردن خطای خطوط انتقال ، همچنـین تعیین نوع شبکه و وضعیت بسته های اطلاعاتی (Packet) از وظایف این لایه مـی باشـد ایـن لایـه دو زیر لایه دارد:

۱ – LLC (Logical Link Control) :

جهت برقراری نظیر به نظیر بین فرستنده و گیرنده

- ایجاد قاب ها و کنترل خطا

۲ - MAC (MAC Address):

- کنترل آدرس فیزیکی
- کنترل نحوه دسترسی به خطوط انتقال

❖ **لایـه فیـــــزیـکـی (Physical)** نحـوه اتـصال کابل،همبنـدی ، انتقال بیـت هـا ، تایمینـگ ، طـرز کـار دستگاههای مخابراتی و خصایص فیزیکی شبکه نظیر : اتصالات ، ولتاژ و زمان را مشخص می نماید.

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 مدلTCP/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

پروتکل TCP/IP

TCP/IP، پروتکلی استاندارد برای ارتباط کامپیوترهای موجود در یک شبکه است. از این پروتکل جهت ارتباط در شبکه های بزرگ استفاده می گردد. برقراری ارتباط از طریق پروتکل های متعددی که در چهارلایه مجزا، فراهم می گردد. هر یک از پروتکل های موجود در پشته TCP/IP ، دارای وظیفه ای خاص برقراری ارتباط می باشند . در زمان ایجاد یک ارتباط ، ممکن است در یک لحظه تعداد زیادی از برنامه ها ، با یکدیگر ارتباط برقرار نمایند ای پروتکل 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 این پروتکل از محلی به محل دیگر ، با فرآیند ارسال یک نامه از نقطه ای به نقطه دیگر قابل مقایسه است .

مزایا و خصوصیات پروتکل TCP / IP عبارتند از :

- **پشتیبانی توسط انواع سیستم عامل ها** Support by all OS
- **پشتیبانی انواع شبکه ها (کوچک ، بزرگ ، پُر ترافیک و . . .)**
- **مسیر یابی** Routing
- **ارسال گروهی** Multicasting
- **پیکر بندی پیچیده** Complex Configuration
- **بستر اصلی اینترنت**
- **استفاده بصورت اتصال گرا و بدون اتصال** TCP or UDP

معایب TCP / IP

- در این مدل مفاهیم خدمات، رابطه و قرارداد بطور واضح قابل تفکیک نیست.
- مدل TCP/IP یک مدل عمومی نیست و برای تشریح هر پشته‌ای از قراردادها به جز TCP/IP مفید نیست.
- لایه میزبان شبکه که در مورد قراردادهای لایه‌ای وجود داشت، بعنوان یک لایه محسوب نمی‌شود و تنها به عنوان یک رابط (بین لایه شبکه و پیوند داده) عمل می‌کند.
- در مدل TCP/IP تمایزی بین لایه‌های فیزیکی و پیوند داده‌ها نیست. در صورتیکه این دو لایه کاملاً از هم متمایز هستند.

لایه های TCP / IP

لایه اول : لایه واسطه شبکه Network Interface

مسئول استقرار داده بر روی محیط انتقال شبکه و دریافت داده از محیط انتقال شبکه است در این لایه استانداردهای سخت افزاری و نرم افزاری و پرتکل های شبکه تعریف می شود . این لایه درگیر با مسائل سخت افزاری مرتبط با شبکه بوده و می تواند عناصر همگن و ناهمگن را به هم پیوند بزند. در این لایه تمام پروتکل های LAN ,MAN قابل استفاده هستنداین لایه 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-D4-66) بوده 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 ATM (Asynchronous Transfer Mode) ، نمونه هائی از پروتکل های موجود در این لایه می باشند . پروتکل های فوق ، نحوه ارسال داده در شبکه را مشخص می نمایند.

لایه دوم : لایه شبکه Internet

این لایه مسئول آدرس دهی ، بسته بندی و روتینگ داده ها ، هدایت از مبدا تا مقصد بسته های اطلاعاتی خاص به نام IP است .دراین لایه مسیر یاب ها از شرایط توپولوژیکی و ترافیکی شبکه اطلاعات را کسب می کند تا مسیر یاب ها به روش آسان و پویا انجام دهند .لایه فوق ، شامل چهار پروتکل اساسی است :

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

ARP(Address Resoulation Protocol) مسئول مشخص نمودن آدرس MAC آداپتور شبکه بر روی کامپیوتر مقصد است .

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

IGMP(Internet Group Managemant Protocol) مسئولیت مدیریت Multicasting در TCP/IP را برعهده دارد .

لایه سوم : لایه انتقال Transport layer

در این لایه ماشین ها ی میزبان در شبکه با هم ارتباط برقرار می کنند و به عبارت دیگر یک سرویس اتصال گرا مطمئن است برای عملیاتی مانند ارسال صوت و تصویر که سرعت مهمتر از دقت است سرویس های سریع و نا مطمئن طراحی شده است. در این سرویس لایه از رسیدن داده ها به مقصد اطلاع می یابد .

این لایه شامل دو پروتکل به شرح زیر می‌باشد:

TCP [3] **(قرار داد کنترل انتقال):** قرارداد قابل اعتماد و اتصالگرایی است که اجازه می‌دهد رشته‌ای از بایتهایی که از یک ماشین شروع به حرکت می‌کنند، بدون خطا به ماشین دیگری در لایه اینترنت تحویل شوند.

UDP [4] **(قرارداد داده گرام کاربر):** یک قرارداد غیر قابل اعتماد و بی اتصال برای کاربردهایی که در آن تحویل سریع مهمتر از تحویل صحیح می‌باشد بطور گسترده مورد استفاده قرار می‌گیرد پروتکل فوق ، امکان عرضه سریع اطلاعات بدون پذیرفتن مسئولیتی در رابطه با تضمین صحت توزیع اطلاعات را برعهده دارد

لایه چهارم : لایه کاربرد APPLICATION LAYER

لایه کاربرد در بالای لایه انتقال قرار دارد و شامل تمام قراردادهای لایه بالاتر می‌باشد. مدلهای اولیه، شامل پایانه مجازی (telnet) و انتقال فایل (FTP) و پست الکترونیکی (SMTP) بوده‌اند این لایه دارای سطح بالایی برای خلق برنامه های کاربردی ویژه و پیچیده ارائه می شود شیبه سازی ترمینال و مدیریت پست و انتقال صفحات ابر متنی و ده ها پروتکل کاربردی دیگر از سطح این لایه است 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 بمنظور ارسال فایل های صفحات وب استفاده می گردد .
- پروتکل (File Transfer Protocol) FTP از پروتکل فوق برای ارسال و دریافت فایل، استفاده می گردد

[3] - Transmission Control Protocol
[4] - User Datagram Protocol

آدرس دهی TCP/IP:

IPv4

IP4 از ۳۲ بیت ۴ قسمتی که شامل ۰ تا ۲۵۵ برای آدرس یک کامپیوتر می باشد

هر کامپیوتر قبل از وصل شدن به یک شبکه باید دارای یک IP آدرس باشد. هر بسته IP باید دارای یک آدرس قبل از اینکه بخواهد به کامپیوتر دیگری ارسال شود داشته باشداین یک IP آدرس است:۲۰۴,۱۶۸,۱۱۴,۲۷ **32 Bits = 4 Bytes**

یک IP آدرس شامل ۴ عدد می باشد. TCP/IP 4 عدد را برای آدرس یک کامپیوتر استفاده می کند. هر کامپیوتر برای آدرس دهی باید دارای ۴ عدد منحصر به فرد باشد. شماره هر عدد بین ۰ تا ۲۵۵ می باشد. عدد ها به وسیله نقاطی از یک دیگر جدا شده اند شبیه این مورد: ۱۹۲,۱۶۸,۱۰۰,۵۰.

یک بایت می تواند در بر گیرنده ۲۵۶ ارزش مختلف باشدیک آدرس TCP/IP 4 عدد بین ۰ تا ۲۵۵ می باشد

IPv6

با همگانی شدن اینترنت و شبکه های تجاری، IP موجود که ستون فقرات شبکه های TCP/IP را تشکیل می داد رو به منسوخ شدن و کهنگی می رفت.در گذشته از اینترنت برای انتقال فایل ها، نامه های الکترونیکی و دسترسی از راه دور به وسیله Telnet استفاده می شد اما امروزه در اینترنت شاهد فزونی برنامه های صوتی و تصویری ، نرم افزارهای کاربردی توانمند هستیم که باعث جلب محبوبیت و جذابیت وب شده اند. کمپانیها با ایجاد شعبه های مختلف مجموعه ای از محیط های Client/Server تحت شبکه به وجود آوردند که باعث افزایش روز افزون اینترانت ها شد، تمام این توسعه ها باعث کاهش تواناییهای شبکه های بر پایه IP شده و شبکه ها نیاز به پشتیبانی ترافیک های فوری ، کنترل انعطاف پذیری تراکم ترافیک ها و ایجاد خصوصیات امنیتی پیدا کردند، این توسعه و نیازها موجب به اتمام رسیدن طول عمر آدرس دهی های موجود طبق IPv4 شد.

خیلی زود آدرس دهی جدیدی جایگزین آدرس دهی قدیم شد که IPv6 نام گرفت. آدرس دهی Ip باعث ایجاد ارتباط سیستم ها از طریق شبکه های مختلف می شود در نتیجه کلیه ایستگاه ها و مسیریاب ها به داشتن یک آدرس ملزم می شوند تا به ایجاد ارتباط بین آن ها منتهی شود. Router (مسیر یاب) باید قادر باشد اطلاعات شبکه های مختلف را با ساختارهای مختلف انتقال داده و به مقصد مورد نظر بفرستد، این امر مستلزم فراهم آوردن سرویس های زیر می باشد:

نمای آدرس دهی : همه شبکه ها از یک ساختار هماهنگ برای آدرس دهی استفاده نمی کنند به عنوان مثال یک شبکه IEEE 802.3 با ۱۶bit or 48bit فضای آدرس دهی ، یک شبکه X.25 با ۱۲ Digit decimal آدرس دهی و...

بزرگترین اندازه بسته های اطلاعاتی : بسته های اطلاعاتی یک شبکه ممکن است به قسمتهای کوچک تر تقسیم شده تا قابل انتقال به شبکه های دیگر باشد « به این عمل fragmentation می گویند» به عنوان مثال بزرگترین اندازه بسته های اطلاعاتی برای شبکه های Ethernet 1500بایت می باشد برای شبکه های X.25 1000 است در این صورت مسیریاب باید برای انتقال اطلاعات از شبکه های Ethernet به شبکه های X.25 بسته های اطلاعات را به ۲ قسمت تقسیم کند.

رابط های شبکه (Interfaces) :ارتباط دهنده های سخت افزاری و نرم افزاری در شبکه های مختلف متفاوت می باشد که مسیریاب باید قدرت تشخیص این اختلافات را داشته باشد.

قابلیت اطمینان : سرویسهای مختلف یک شبکه ممکن است از ابتدا تا انتها به صورت یک سرویس قابل اعتماد در یک حلقه مجازی تا یک سرویس غیر قابل اعتماد قابل تغییر باشند. عملکرد یک مسریاب نباید وابسته به قابلیت اعتماد یک شبکه باشد.

در نتیجه این IP مطمئن نیست چون درستی رسیدن اطلاعات را تضمین نمی کند و مسوولیت سالم رسیدن بسته های اطلاعاتی را به پروتکل لایه بالایی (TCP) می سپارد به این شکل Error recovery توسط TCP صورت می پذیرد این امر تا حد زیادی قابلیت انعطاف پذیری را فراهم می آورد.

وقتی اینترنت روزبه روز رشد کرد و نقایص IPv4 بیشتر آشکار شد برای پاسخ به نیازهای جدید می بایست راهی اندیشیده می شد درنتیجه این درخواست ها IETF ..... در سال ۱۹۹۲ اولین طرح خود را به عنوان IP جدید ارائه داد که پس از طراحی نهایی در سال ۱۹۹۴ بیرون آمد که بعد از آن تغییراتی روی آن داده شد و بالاخره IPv6 نام گرفت. پیشبرد IPv6 بیشتر به خاطر نداشتن محدودیت های آدرس دهی در IPv4 می باشد که البته این IP جدید علاوه بر آن قابلیت های دیگری هم دارد که به شرح آنها خواهیم پرداخت که با ۳۲ بیت فضای آدرس دهی تنها ۲ به توان ۳۲ آدرس مختلف می توان ایجاد کرد که حدود ۴ میلیارد آدرس است این فضای آدرس دهی در اینترنت روبه رشد فضای محدودی است از سال ۱۹۸۰ به بعد دریافتن که دیگر این مقدار فضا جواب گوی نیازها نیست و در سال ۱۹۹۰ این مشکل به طور آشکار نمایان شد. دلایل نامناسبی ۳۲ بیت فضای آدرس دهی به شرح زیر می باشد:

دوساختار از IP Address شامل Net ID و Host ID که راحت و مناسب است اما با فضای آدرس دهی محدود. یک مرتبه که به شبکه خود تعدادی از آدرسها را اختصاص می دهید برای همه شبکه های میزبان نیز می توانید از این آدرسهای استفاده کنید. فضای آدرس دهی برای آن شبکه ممکن است به صورت گسترده ای استفاده شود البته بدون اینکه شما نگران از دست دادن کارایی آن باشید.

شبکه ها به سرعت رو به افزایش هستند. اغلب سازمان ها چندین Lan دارند. شبکه های بی سیم به تدریج نقش اساسی یافته اند همچنین رشد اینترنت درسالهای آتی رو به انفجار است.

افزایش استفاده از TCP/Ip در مناطق جدید خواستار IP های خاص (unique ip address) می باشد. برای داشتن این آدرس ها Ipv6 از **۱۲۸ بیت** فضای آدرس دهی در عوض ۳۲ بیت استفاده می کند و این امر فضای آدرس دهی را از ۲ به توان ۳۲ به ۲ به توان ۹۶ می رساند که البته امن تر و مطمئن تر نیز می باشد.

IPv6 Header : هدر Ipv6 با طول ثابت ۴۰ octet در مقایسه با هدر Ipv4 با طول ۲۰ octet

آینده IP

اگر به پیش بینی هایی که در رابطه با مصرف آدرس ها به عمل آمده است توجه کنیم، می بینیم که براساس این پیش بینی ها زمان اتمام آدرس های IPV4 در سال ۲۰۲۰ خواهد بود که همه آدرس هایی که در اختیار IANA قرار دارد به اتمام خواهد رسید و در سال ۲۰۲۲ آدرس های موجود در دفاتر ثبت منطقه ای تمام خواهد شد و نهایتاً این آدرس ها در سال ۲۰۲۸ که در اختیار دفاتر ثبت محلی قراردارند تمام خواهد شد و در این سال امکان ورود تجهیزات جدید به شبکه مقدور نخواهد بود و باید برای این سال چاره اندیشی کرد.

متخصصان صنعت IT بر این باورند که با راه اندازی سیستم آدرس دهی IPV6 این مشکل حل شده و امکان اضافه کردن آدرس های جدید در شبکه فراهم و مشکل کاربران نیز مرتفع خواهد شد

پورت PORT

پورت ها را می توان به دروازه هایی برای ورود و خروج اطلاعات تشبیه کرد که کامپیوتر با استفاده از آنها اطلاعات را دریافت و یا به بیرون انتقال می دهد.

Port Number

عددی که امکان ارسال بسته هایIP به یک فرآیند خاص از یکی از کامپیوترهای متصل به اینترنت را فراهم می کند.برخی از این شماره ها که تحت عنوان شماره های شناخته شده مطرح هستند به طور دائمی اختصاص می یابند مجموعا 65535 شماره پورت برای استفادهTCP/IP در دسترس است همین تعداد نیز برایUDP موجود می باشد

انواع پورت ها :

۱ – پورتهای سخت افزاری
۲– پورت های نرم افزاری

Port سخت افزاری

پرت های سخت افزاری به پورتهایی گفته می شود که لوازم جانبی کامپیوتر مثل : صفحه کلید، ماوس ، مانیتور ، چاپگر ، اسکنر و .. به وسیله آنها به کامپیوتر متصل می شوند. برای هک کردن یک کامپیوتر اغلب از Port های نرم افزاری استفاده می کنیم

Port های نرم افزاری

پورتهای نرم افزاری به پورتهایی گفته میشود که در شبکه های کامپیوتری از آنها برای دریافت و یا ارسال داده ها از روی یک کامپیوتر به کامپیوتر دیگر استفاده می شود. تعداد پورتهای نرم افزاری ۶۵۵۳۵ تا است و هر کدام مخصوص سرویس خاصی در شبکه می باشد.
به عنوان مثال Port شماره ۸۰ برای دیدن صفحات وب به کار می رود ، Port شماره ۱۱۰ برای دریافت E-Mail و ....

پورت مشخصه ای برای یک برنامه و در یک کامپیوتر خاص است .پورت با یکی از پروتکل های لایه "حمل TCP "و یا UDP مرتبط و پورت TCP و یا پورت UDP ، نامیده می شود. پورت می تواند عددی بین صفر تا 65535 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

دسترسی به پورت ها

هر پورت زبان خاص خودش را دارد که ما با استفاده از دستوراتی که برای هر پورت در نظر گرفته شده با آن صحبت می کنیم بعضی مواقع این دستورات در سیستم عامل های مختلف (Windows,Linux,..) با هم تفاوت هایی دارند اما اساس کار آنها یکسان است.

به عنوان مثال برای دیدن صفحات وب یک سایت (یا به عبارت دیگر سرویس گرفتن از سرور وب آن) باید پورت مربوط به آن را بدانیم . شماره این پورت ۸۰ است پس ما باید با سرور وب (Web Server) یک ارتباط از روی پورت ۸۰ برقرار کرده و شروع به صحبت کردن با این پورت کنیم.

فرض می کنیم که ارتباط ما در حال حاضر از طریق خط فرمان با پورت ۸۰ برقرار شده، پس به صحبت با این پورت می پردازیم . به عنوان مثال به Web Server درخواست صفحه اصلی یا همان home Page را به صورت زیر می دهیم GET /index.html http/1.0

مثال بالا نمونه ساده ای از صحبت کردن با یک پورت بود.

حتما متوجه شده اید که اگر بخواهیم به روش بالا صفحات یک سایت را مرور کنیم هم وقت زیادی تلف می شود و هم اینکه نتیجه کار برای ما سودی ندارد زیرا تنها کدهای HTML صفحه نمایش داده می شوند و هیچ گونه شکل گرافیکی در خروجی وجود ندارد!!!!

برای رفع این مشکل نرم افزارهایی به وجود آمده است که پورت ها توسط آنها هدایت می شود. یعنی کار بر هیچ گونه دستوری را به طور مستقیم برروی پورت ارسال نمی کند. در واقع این نرم افزارها رابط بین کاربر و پورت مورد نظر هستند و با دریافت و درخواست از کاربر آن را به صورت قابل فهم برای پورت ترجمه و آن را ارسال می کنند. پس از ارسال درخواست پاسخی که به صورت کد است از طریق همان پورت برروی کامپیوتر ها ارسال می شوند. پاسخ پورت نیز توسط همان نرم افزار برای ما ترجمه شده و برروی صفحه نمایش نقش می بندد.

ما می خواستیم . صفحه اصلی یک وب سایت را نگاه کنیم اما پاسخ برای ما قابل فهم نبود و زمان زیادی را نیز طلب می کردحالا اگر از سیستم عامل ویندوز استفاده می کنید Internet Explorer یا (IE) خود را باز کنید.

شما میتوانید از نرم افزارهای مورد علاقه تان برای این کار استفاده کنید اما این نکته همیشه ثابت است که درخواست برروی پورت ۸۰ فرستاده می شود. حتما می دانید که با وارد کردن نام یک سایت در Bar Address به راحتی می توانید صفحه اصلی آن را ببینید و تنها با یک کلیک به صفحات دیگر انتقال پیدا کنید .

حالا یک بار برای خودتان کارهایی را که IE برای نمایش دادن یک وب سایت به شما انجام می دهد را توضیح دهید تا آن را به خاطر بسپارید.

ضمنا توجه داشته باشید که این مهم تنها پورت ۸۰ شما را شامل نمی شود بلکه هر داده ای که وارد کامپیوتر می شود باید توسط نرم افزار یا خود سیستم عامل ترجمه شود تا به صورت قابل فهم در آید.

مفهوم Port های باز و بسته چیست ؟

Port باز به Port ی گفته می شود . که بتوان با آن ارتباط برقرار کرد و از روی آن اطلاعاتی گرفته و یا برروی آن داده ای ارسال کنیم.

Port بسته : به پورتی گفته می شود که نتوانیم با آن ارتباط برقرار کنیم و در نتیجه از ارسال و دریافت داده برروی آن باز بمانیم .

برای اینکه مفاهیم بالا را بهتر متوجه شوید مثال زیر را که به بیان ساده بیان شده را با دقت بخوانید:

همان طور که گفته شد برای استفاده از سرویس های مختلف در اینترنت از Port های مختلف که هریک مخصوص یک سرویس هستند استفاده می شود .به عنوان مثال من یک POP3 Mailbox دارم. اگر بخواهم e-mail هایم رو بخوانم باید به سرور میل (mail server) وصل بشویم.

برای خواندن e-mail هایی که داخل POP Box من هستند باید از Port ۱۱۰ استفاده کنیم ، پس تا یک ارتباط با Mail server Port ۱۱۰ برقرار نکنیم نمی توانیم e-mail های موجود در آن را بخوانم. همان طور که گفته شد از نرم افزارهای مختلف برای این کار استفاده میتوان کرد.

پس قرار بر این شد که من یک درخواست روی پورت 110 mail server ای که از آن آدرس ایمیل دارم بدم تا بتوانم ایمیل هایم را بخوانم. خوب ، من یه در خواست به mail server می دهم و بعد از برقراری ارتباط به mail server ایمیلهایم را میخوانم.

حالا اگر در خواست دادم و سرور در خواست من رو قبول نکرد چی؟

این به این معناست که پورت ۱۱۰ سرور برای پاسخگویی آمادگی ندارد و این یعنی خواندن ایمیل تعطیله چون پورت ۱۱۰ بسته است.

از مثال بالا نتیجه می گیریم که اگر بخواهیم از یک سرور و یا حتی یک کامپیوتر خانگی اطلاعات بگیریم و یا روی آن اطلاعات بفرستیم باید پورت مربوط به درخواست ما باز باشد و به درخواست ما جواب بدهد.

آشنایی با پورت های مختلف :

برای این که با پورت های مختلف آشنا و ذهنیتی از یک پورت لیست داشته باشید کل پورتهای شبکه را در زیر لیست می کنیم

```
echo            7/udp
discard          9/tcp sink null
discard          9/udp sink null
systat          11/tcp users #Active users
systat           11/tcp users #Active users
daytime          13/tcp
daytime          13/udp
qotd            17/tcp quote #Quote of the day
qotd            17/udp quote #Quote of the day
chargen          19/tcp ttytst source #Character generator
chargen          19/udp ttytst source #Character generator
ftp-data        20/tcp #FTP, data
ftp             21/tcp #FTP. control
telnet          23/tcp
smtp            25/tcp mail #Simple Mail Transfer Protocol
time            37/tcp timserver
time            37/udp timserver
rlp              39/udp resource #Resource Location Protocol
nameserver      42/tcp name #Host Name Server
nameserver      42/udp name #Host Name Server
nicname         43/tcp whois
```

```
domain          53/tcp #Domain Name Server
domain          53/udp #Domain Name Server
bootps          67/udp dhcps #Bootstrap Protocol Server
bootpc          68/udp dhcpc #Bootstrap Protocol Client
tftp            69/udp #Trivial File Transfer
gopher          70/tcp
finger          79/tcp
http            80/tcp www www-http #World Wide Web
kerberos        88/tcp krb5 kerberos-sec #Kerberos
kerberos        88/udp krb5 kerberos-sec #Kerberos
hostname        101/tcp hostnames #NIC Host Name Server
iso-tsap        102/tcp #ISO-TSAP Class 0
rtelnet         107/tcp #Remote Telnet Service
pop2            109/tcp postoffice #Post Office Protocol - Version 2
pop3            110/tcp #Post Office Protocol - Version 3
sunrpc          111/tcp rpcbind portmap #SUN Remote Procedure Call
sunrpc          111/udp rpcbind portmap #SUN Remote Procedure Call
auth            113/tcp ident tap #Identification Protocol
uucp-path       117/tcp
nntp            119/tcp usenet #Network News Transfer Protocol
ntp             123/udp #Network Time Protocol
epmap           135/tcp loc-srv #DCE endpoint resolution
epmap           135/udp loc-srv #DCE endpoint resolution
netbios-ns      137/tcp nbname #NETBIOS Name Service
netbios-ns      137/udp nbname #NETBIOS Name Service
netbios-dgm     138/udp nbdatagram #NETBIOS Datagram Service
netbios-ssn     139/tcp nbsession #NETBIOS Session Service
imap            143/tcp imap4 #Internet Message Access Protocol
pcmail-srv      158/tcp #PCMail Server
snmp            161/udp #SNMP
snmptrap        162/udp snmp-trap #SNMP trap
print-srv       170/tcp #Network PostScript
bgp             179/tcp #Border Gateway Protocol
irc             194/tcp #Internet Relay Chat Protocol
ipx             213/udp #IPX over IP
ldap            389/tcp #Lightweight Directory Access Protocol
https           443/tcp MCom
https           443/udp MCom
microsoft-ds    445/tcp

microsoft-ds    445/udp
kpasswd         464/tcp # Kerberos (v5)
kpasswd         464/udp # Kerberos (v5)
isakmp          500/udp ike #Internet Key Exchange
exec            512/tcp #Remote Process Execution
biff            512/udp comsat
login           513/tcp #Remote Login
who             513/udp whod
cmd             514/tcp shell
syslog          514/udp
printer         515/tcp spooler
talk            517/udp
ntalk           518/udp
efs             520/tcp #Extended File Name Server
router          520/udp route routed
timed           525/udp timeserver
tempo           526/tcp newdate
courier         530/tcp rpc
conference      531/tcp chat
netnews         532/tcp readnews
netwall         533/udp #For emergency broadcasts
uucp            540/tcp uucpd
klogin          543/tcp #Kerberos login
```

kshell	544/tcp krcmd #Kerberos remote shell
new-rwho	550/udp new-who
remotefs	556/tcp rfs rfs_server
rmonitor	560/udp rmonitord
monitor	561/udp
ldaps	636/tcp sldap #LDAP over TLS/SSL
doom	666/tcp #Doom Id Software
doom	666/udp #Doom Id Software
kerberos-adm	749/tcp #Kerberos administration
kerberos-adm	749/udp #Kerberos administration
kerberos-iv	750/udp #Kerberos version IV
kpop	1109/tcp #Kerberos POP
phone	1167/udp #Conference calling
ms-sql-s	1433/tcp #Microsoft-SQL-Server
ms-sql-s	1433/udp #Microsoft-SQL-Server
ms-sql-m	1434/tcp #Microsoft-SQL-Monitor
ms-sql-m	1434/udp #Microsoft-SQL-Monitor
wins	1512/tcp #Microsoft Windows Internet Name Service
wins	1512/udp #Microsoft Windows Internet Name Service
ingreslock	1524/tcp ingres
l2tp	1701/udp #Layer Two Tunneling Protocol
pptp	1723/tcp #Point-to-point tunnelling protocol
radius	1813/udp #RADIUS accounting protocol
nfsd	2053/tcp #Kerberos de-multiplexor
man	9535/tcp #Remote Man Server

پروتکل DHCP[5] یکی از سرویس های پایه شبکه می باشد

آدرس های IP یکی از مهمترین اجزای شبکه های کامپیوتری در دنیای امروز می باشند که در لایه سوم از مدل مرجع OSI کار می کنند و در حال حاضر از ورژن چهار آن در سراسر دنیا به طرز گسترده ای استفاده می شود و کارشناسان و متخصصین در حال تحقیق و توسعه آن و آماده سازی ورژن شش آن می باشند در شبکه هایی که بستر آن مایکروسافت می باشد به سه طریق مختلف امکان آدرس دهی IP وجود دارد :

◈ **Static IP Addressing**

در این روش که معمولا در شبکه های کوچک کاربرد دارند آدرس دهی توسط یک فرد یا مدیر شبکه انجام می پذیرد. در این روش برای آدرس دهی به هر رایانه می بایست به تنظیمات شبکه آن رایانه رفت و تغییرات لازم را اعمال نمود.

◈ **APIPA**

در این روش که مخفف Automatic Private IP Addressing می باشد و یکی از پروتکل هایی می باشد که توسط سیستم عامل XP و جهت کاربر پسند کردن این سیستم عامل توسط شرکت مایکروسافت ارائه می گردد.در این روش اگر آدرسی به صورت دستی یا Static برای کلاینت های ۹۸ و ۲۰۰۰ و Xp پیدا نشود و DHCP Server نیز در شبکه ما موجود نباشد سیستم عامل به صورت خودکار یک آدرس IP برای رایانه ما در نظر می گیرد ، این آدرس آی پی از رنج ۱۶۹,۲۵۴ x.y.یک IP انتخاب میکنند ضمن اینکه قبل از استفاده از آن ، آنرا Broadcast میکنند تا احیانا کلاینت دیگری در حال استفاده از آن IP

[5] - Dynamic Host Configuration Protocol

نباشد. با این حال هر ۵ دقیقه یک بار به تلاش خود مبنی بر گرفتن IP از DHCP ادامه میدهد که توسط شرکت مایکروسافت بدین منظور رزرو شده است و در حقیقت از آدرس های خصوصی یا Private می باشد. مایکروسافت این پروتکل را به منظور سهولت کار، کاربران ابداع نمود تا در شبکه های خانگی و شبکه های اداری کوچک تنها با اتصال کابل ها کاربران بدون نیاز به تنظیمات آدرس دهی از بستر شبکه استفاده نمایند.

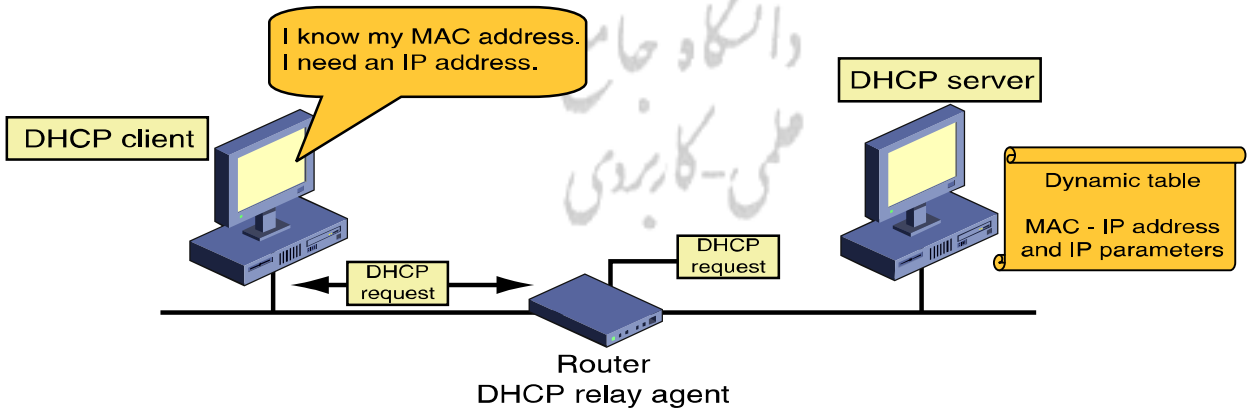
◈ Dynamic Host Control Protocol (DHCP)

در این روش که در شبکه های Medium To Large کاربرد ویژه ای دارد، یک سرور به منظور خدمات دهی به ایستگاه های کاربری در نظر گرفته می شود و وظیفه این سرویس دهنده یا سرور اختصاص آدرس آی پی به ایستگاه های کاربری و مدیریت آدرس ها می باشد . پیکربندی این سرور در پلاتفرم های مختلف از جمله لینوکس و مایکروسافت به مدیر شبکه این امکان را می دهد که بر اساس سیاست های سازمان پلان IP Addressing سازمان را تدوین نموده و ایستگاه های کاربری این امکان را می دهد که بدون دخالت مدیر شبکه و به صورت اتو ماتیک پیکر بندی مربوط به آدرس دهی آی پی آنها از طریق DHCP Serverانجام میپذیرد. استفاده از DHCP Server در شبکه ها ضمن ساده نمودن کار مدیر شبکه امکان مدیریت متمرکز آدرس دهی را نیز امکان پذیر می سازد.

DHCP همه ی سرویس‌های BootP بعلاوه تعدادی کاربرد مهم دیگر را ارائه می‌دهد یک خاصیت مهم در DHCP این است که آدرس‌ها می‌توانند بصورت پویا به یک سیستم داده شوند.

آدرس IP که با استفاده از دستور ifconfig یا بوسیلهBootP ، به یک سیستم تخصیص می یابد، به صورت دائم برای آن در نظر گرفته می شود و سیستم دیگری در شبکه نمی تواند آنرا اختیار کند. اما DHCP آدرس را برای یک مدت زمانی مشخص به کلاینت اجاره می‌دهد و بعد از اتمام دوران اجاره، می‌تواند آن آدرس را به کلاینت‌های دیگر اجاره دهد.

مزیت استفاده از آدرس‌دهی پویا، استفاده بهینه از تعداد کم آدرس است. آدرس‌های بلا استفاده برای استفاده سایر کلاینت‌ها آزاد می‌شود. آدرس دهی پویا بوسیلهDHCP ، مانند همه چیزهای دیگر بدون نقص نیست. از آنجاییکه DNS از آدرس‌هایی که توسط DHCP تخصیص می‌یابد اطلاعی ندارد در نتیجه کامپیوترهای خارج از شبکه داخلی نمی‌توانند سیستمی را که از طریقDHCP ، آدرس دریافت کرده را پیدا کنند در نتیجه این سیستم نمی‌تواند به سایر سیستمهای راه دور سرویس ارائه دهد. این یک نقص است ولی باعث اختلال در شبکه نمی‌شود.



از آنجاییکه اولا فقط سرورها باید به سایر سیستم‌ها سرویس ارائه دهند، می‌توان پیکر بندی شبکه آنها را بصورت دستی تنظیم نمود. دوما اینکه تعداد سرورها نسبت به مجموع تعداد سیستم‌ها کمتر است. در نتیجه هزینه و حجم پیکربندی سرورها به نسبت کمتر است. پس نتیجه می‌گیریم که سیستم‌های رومیزی نامزدهای خوبی برای پیکربندی توسط DHCP هستند. اما تکنیکهایی برای انطباق آدرس‌های DHCP و DNS با استفاده از Dynamic DNS (DDNS) وجود دارد که برای توضیحات بیشتر به مقالات DNS مراجعه شود

چگونگی کارکرد DHCP

زمانیکه یک کاربر کامپیوتر خود را راه اندازی می کند سیستم عامل آن بعد از بالا آمدن جهت دریافت IP مراحل زیر را انجام می دهد :

1 - DHCP Discover
2 - DHCP Offer
3 – DHCP Request
4 - DHCP Ack

۱ – کلاینت ها در زمان بوت شدن سیستم یا شروع مجدد سرویس یا با استفاده از دستور ipconfig /renew شروع به پخش پیغام هایی به نام DHCP Discover بصورت همگانی (broadcast) می کنند و در این پیغام ها درخواست IP خود را برای DHCP سرور های در محل به آدرس ۲۵۵,۲۵۵,۲۵۵,۲۵۵ ارسال میکند و IP خود او نیز ۰,۰,۰,۰ در نظر میگیرد..

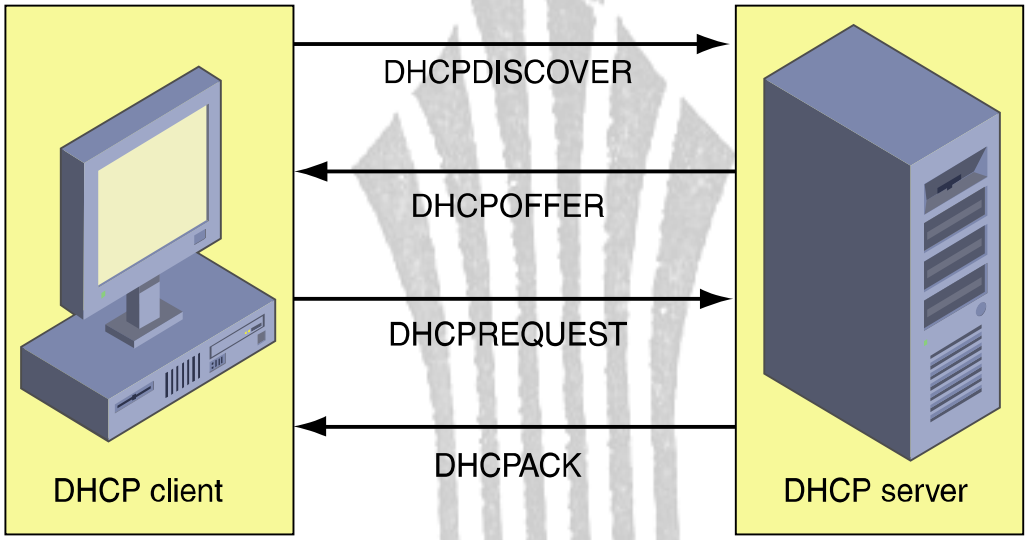
۲ – سروهای DHCP که این پیغام را دریافت می کنند در جوب پیغامی بنام DHCP Offer برای کلاینت ارسال می کنند و IP مورد نظر خود را به کلاینت پیشنهاد می دهند در این مرحله تمام DHCP Server هائیکه Broadcast انجام شده در مرحله اول را دریافت میکنند از IP Range تعریف شده بر روی خود یک IP انتخاب نموده و به همراه مدت زمانی که قرار است آنIP را در اختیار Client قرار دهد و آنرا به شکل زیر ارسال میکند.

Source IP=IP of DHCP Server
Destination MAC Address=Client Destination IP=255.255.255.255

۳ – کلاینت که ممکن است از چندین سرور پیشنهاد IP داشته باشد معمولا به سریعترین پیشنهاد با پیغامی بنام DHCP Request درخواست IP می کند.کلاینت درخواست کننده پس از دریافت DHCP Offer ها اولین DHCP Offer را انتخاب نموده و آنرا توسط یک Packet در شبکه Broadcast میکند و در آن Packet آدرسDHCP Server که Offer او قبول شده است مشخص مینماید.

۴- پس از آنکه کلاینت به DHCP Server که Offer اوقبول شده DHCP Request را فرستاد در صورتیکه هنوز IP که Offer شده در Range او وجود داشته باشد و توسط Admin حذف نشده باشد DHCP Server تایید خود را مبنی بر اختصاص IP به Client اعلام میکندو با یک پیغام DHCP ACK با این درخواست موافقت می کند ولی اگر IP توسط Admin از Range مربوطه حذف شده باشد DHCP به کلاینت درخواست کننده پیغام DHCP Nackرا ارسال میکند و کلاینت مجبور میشود که تمام مراحل را دوباره طی کند.

شکل زیر مراحل بالا را بخوبی نشان می دهد:

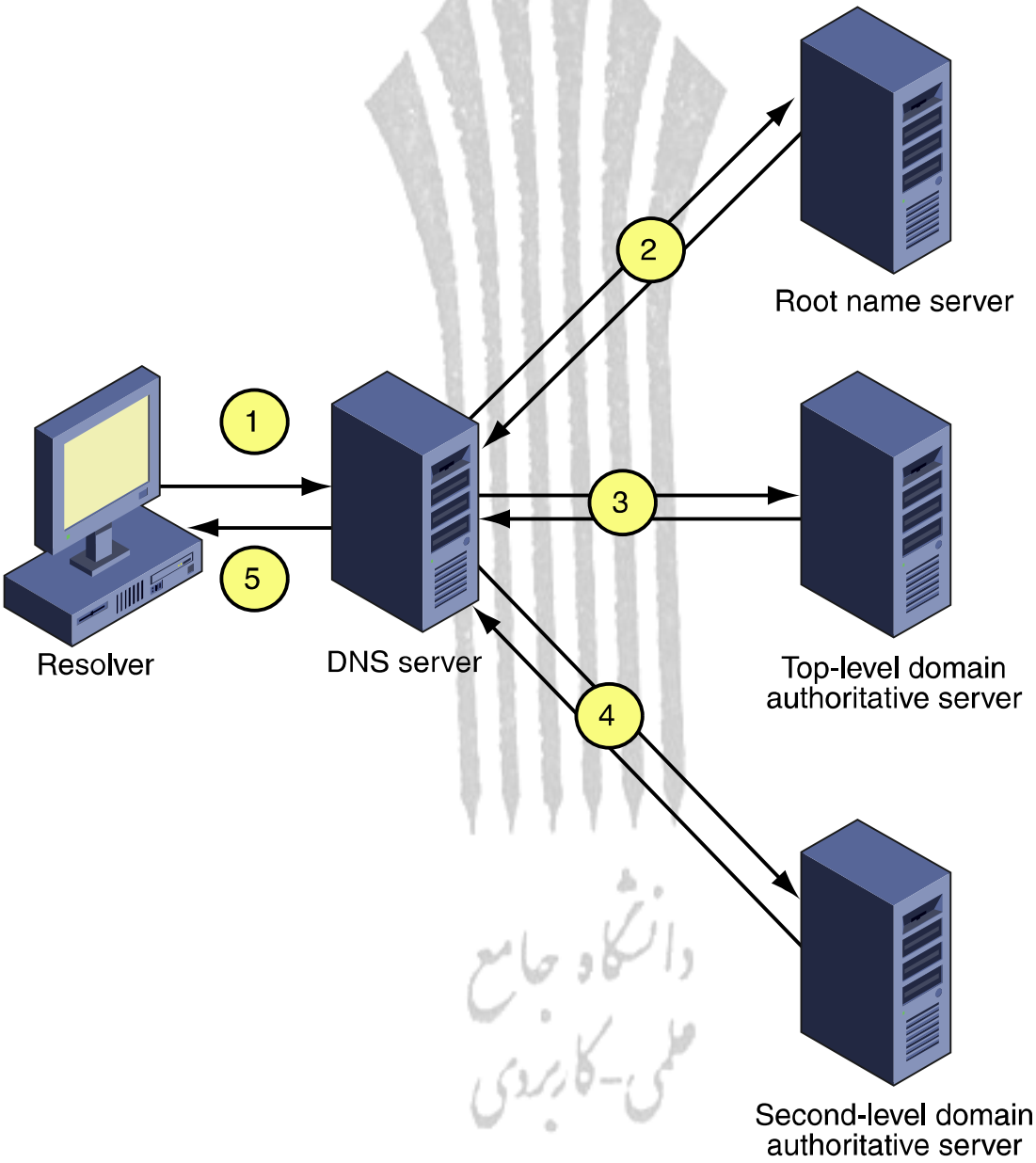


اگر DHCP در شبکه موجود نباشدکلاینت پس از ارسال DHCP Discover یک ثانیه منتظر جواب می ایستد اگر جوابی دریافت نکرد ۳بار دیگر به فاصله زمانی ۹ و ۱۳ و ۱۶ ثانیه دوباره Broadcast میکند اگر باز هم جوابی نگرفت هر ۵ دقیقه یک بار به کار خود ادامه میدهد

DNS (Domain Name Server)

سرویسی است جهت تبدیل IP به نام و بالعکس

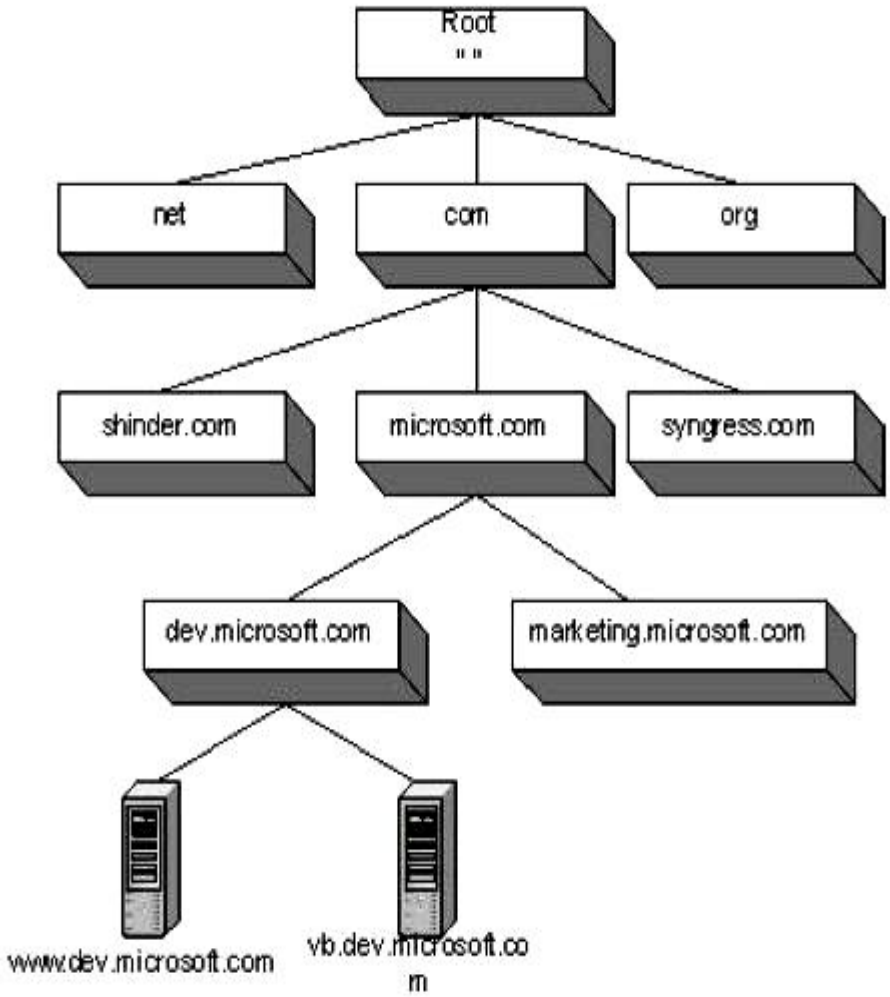
از آنجا که به خاطر سپردن IP مشکل می باشد بکار می رود ضمنا IP و NAME منحصر بفرد هستند



DNS NameSpace

همانگونه که اشاره گردید DNS از یک ساختار سلسله مراتبی برای سیستم نامگذاری خود استفاده می نماید. با توجه به ماهیت سلسله مراتبی بودن ساختار فوق، چندین کامپیوتر می توانند دارای اسامی یکسان بر روی یک شبکه بوده و هیچگونه نگرانی از عدم ارسال پیام ها وجود نخواهد داشت. ویژگی فوق درست نقطه مخالف سیستم نامگذاری NetBIOS است . در مدل فوق قادر به انتخاب دو نام یکسان برای دو کامپیوتر موجود بر روی یک شبکه یکسان نخواهیم نبود.

بالاترین سطح در DNS با نام Root Domain نامیده شده و اغلب بصورت یک "." و یا یک فضای خالی "" نشان داده می شود. بلافاصله پس از ریشه با اسامی موجود در دامنه بالاترین سطح (Top Level) برخورد خواهیم کرد. دامنه های .edu , .org , .net , Com نمونه هائی از این نوع می باشند. سازمانهائی که تمایل به داشتن یک وب سایت بر روی اینترنت دارند، می بایست یک دامنه را که بعنوان عضوی از اسامی حوزه Top Level می باشد را برای خود اختیار نماید. هر یک از حوزه های سطح بالا دارای کاربردهای خاصی می باشند مثلا" سازمان های اقتصادی در حوزه .com و موسسات آموزشی در حوزه .edu و ... domain خود را ثبت خواهند نمود.شکل زیر ساختار سلسله مراتبی DNS را نشان می دهد.



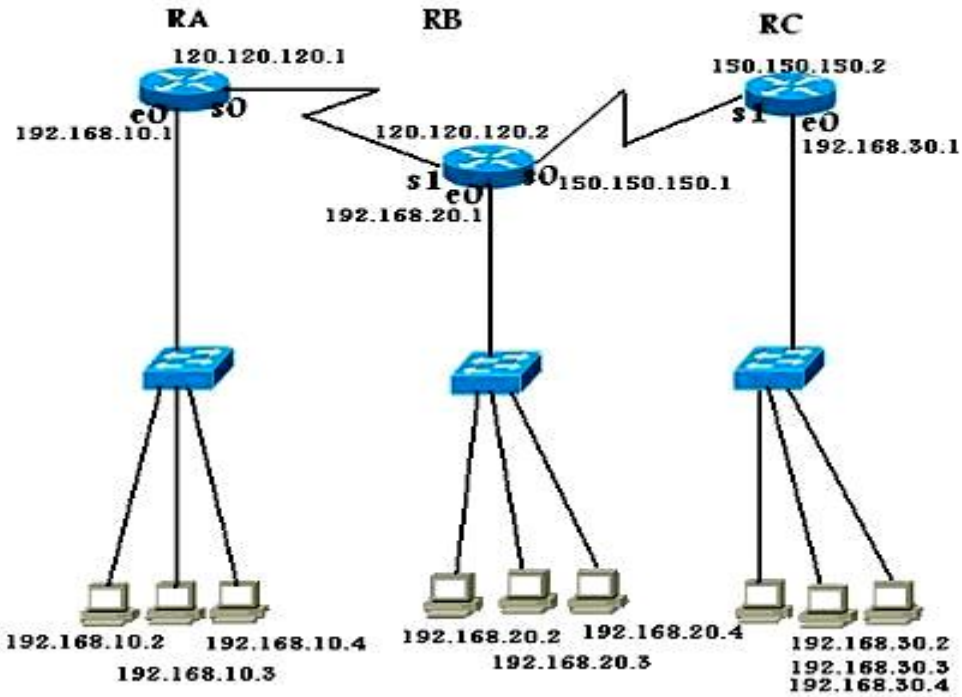
Dns شامل بخشهای زیر است

- The DNS namespace : ZONE , DOMAIN
- TREE
- FORREST
- HOST : Records

Subnet Mask

Subnet Mask عددی است که در واقع تعداد بیت (Bit) های Host ID و Net ID را مشخص می کند و در کلاسهای مختلف متفاوت است . اکنون Subnet Mask های استاندارد را در کلاس های مختلف مورد بررسی قرار می دهیم.

Subnet Mask در کلاسهای مختلف :



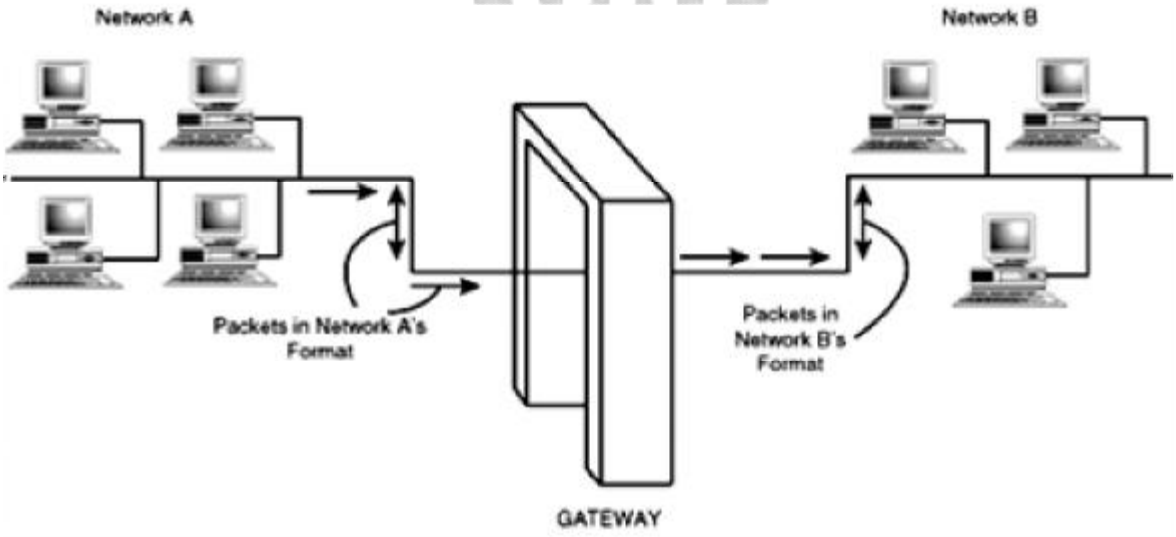
Mask Subnet در کلاس A به صورت ۲۵۵,۰,۰,۰ است.NetID، دارای هشت بیت است و بقیه بیت ا مربوط به HostID می شوند.

Subnet Mask در کلاس B به صورت ۲۵۵,۲۵۵,۰,۰ است و در کلاس C به صورت ۲۵۵,۲۵۵,۲۵۵,۰ می باشد.دقت داشته باشید که این Subnet Mask ها مربوط به سرویس دهندها هستند. به عنوان مثال Subnet Mask ، با عدد ۲۵۵,۲۵۵,۲۵۵,۰ مربوط به سرویس دهنده ای (Server) است که از IP کلاس C برای سرویس دادن به مشتری هایش (Client) استفاده میکند نه به ما که یک Host بر روی آن هستیم.

Subnet Mask یک Client که روی IP کلاس C است ۲۵۵,۲۵۵,۲۵۵,۲۵۵ است ، یعنی هیچ بیتی برای Host ندارد. اگر این مطلب را متوجه شده باشید به راحتی می توانید Subnet Mask را در

دروازه Gateway

به هر ابزاری که ارتباط میان چند شبکه محلی (LAN) و یک شبکه گسترده (WAN) را فراهم آورد در اصطلاح Gateway گفته می شود. برای مثال گاه یک Proxy server این مهم را فراهم می آورد که در چنین مواقعی این Proxy sever مفهوم کلی یک دروازه (Gateway) را تداعی می نماید آنچه بیش از همه مهم است محل فعالیتGateway می باشد که در لایه دوم شبکه Data link layer فعالیت دارد . همانطور که گفته شد در این لایه دستگاهها با سخت افزار کار می کنند در شبکه ها از Gatewayبه عنوان مفسر یا کلمپایلر پروتکل (protocol) استفاده می شود. باید توجه داشت که استفاده از ابزارهای ارتباطی همیشه برای گسترش و ایجاد WAN نیست گاهیً مدیران و طراحان شبکه با بکار گیری این ابزارها قصد تبدیل پروتکل (Protocol) های شبکه را به یکدیگر دارند. به عنوان نمونه برای اتصال دو شبکه با پروتکل های متفاوت مثل IPX Netwar شبکه ای با منابع IP می توان از gateway بهره برد.



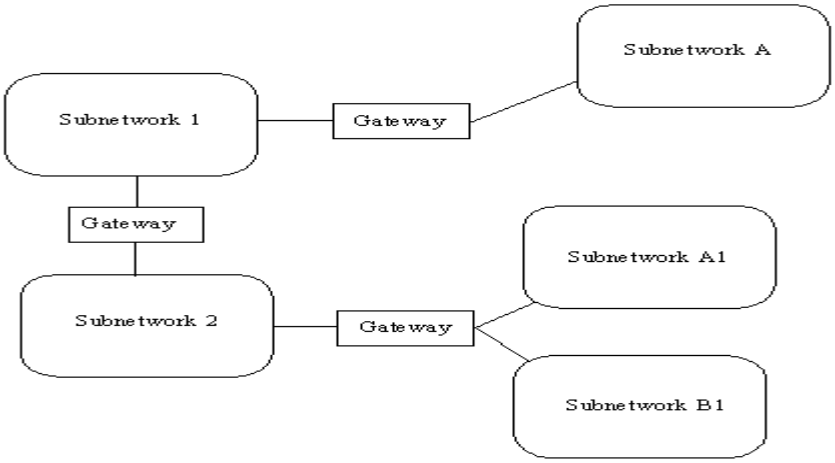
زمانی که دو یا چند شبکه به یکدیگر متصل می شوند،از Gateway استفاده می شود. Gateway ماشینی است که به عنوان رابط بین چند شبکه عمل می کند و اطلاعات را بر اساس نشانی های ip آن ها به شبکه های مربوطه هدایت و مسیردهی می کند. زمانی که قرار باشد یک سیستم لینوکسی به عنوان Gateway کار کند،باید چند تغییر در تنظیمات فایل های configuration شبکه اعمال شود. برای آنکه بتوان از سرویس های یک سیستم دیگر به عنوان Gateway استفاده کرد،باید به جدول مسیریابی،اطلاعاتی از Gateway قرار باشد شبکه ای را به اینترنت متصل سازد کاربران فقط قادر خواهند بود که اطلاعات را به سیستم ها ی مقصد در شبکه دوم ارسال کنند و قابلیت دریافت اطلاعات از آن سیستم ها وجود نخواهد داشت. برای حل این مسئله لازم است که در جداول مسیریابی سیستم های شبکه دوم تنظیماتی انجام شود. اگر قصد استفاده از سیستم محلی خود را به عنوان ارتباط دهنده دو شبکه داشته باشید،باید سیستم خود را به دو کارت شبکه (یا دو اتصال PPP و یا SLIP) مجهز کنید. فرض کنید که قصد استفاده از سیستم خود را برای اتصال دو شبکه به نام های Small-net و big-net

داشته باشیم و شرایط سخت افزاری این کار فراهم شده باشد. نخستین گام آن است که رابط های اترنت کارت های شبکه هر یک با نشانی های خودشان تنظیم شوند.

merlin.big-net.com merlin-iface1 ۱۶۳,۱۲,۳۴,۳۶

merlin-iface2 merlin.small-net.com ۱۴۷,۱۲۳,۱۲,۱

در این مثال فرض شده است که سیستم شما در هر دو شبکه دارای نام merlin است که کاملا" قانونی است در مورد فوق اسامی رابط ها نیز به جهت سهولت قید شده اند. پس از این مرحله باید از فرمان ifconfig برای برقراری ارتباط بین رابط ها و اسامی های به کار رفته در فایل \etc\hosts استفاده کنیم: merlin-iface1 ifconfig eth1merlin-iface2 ifconfig eth 0



در انتها لازم است که جدول مسیریابی را تغییر دهیم. برای این کار از دستورات زیر به صورت مشخص شده باید استفاده کنیم: Route add small-net Route add big-net زمانی که این مراحل به درستی انجام شوند، می توانید از سیستم خود به عنوان یک Gateway برای برقراری ارتباط بین دو شبکه استفاده کنید.

دستور تایپ	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 Pars23:** Connection-specific DNS Suffix . : IP Address. . . . . : 10.1.1.216 Subnet Mask . . . . . : 255.255.255.255 Default Gateway . . . . . : 10.1.1.216

BootP

از پروتکل BOOTP برای راه اندازی ایستگاههای بدون دیسک استفاده می‌شود. این پروتکل می‌تواند به غیر از آدرس IP ایستگاه بدون دیسک، اطلاعات اضافه‌تری را مانند آدرس IP مسیریاب پیش‌فرض ، الگوی زیر شبکه و ... را به ایستگاهها ارایه دهد.

DHCP

مشکل جدی پروتکل BOOTP اینست که جدول نگاشت آدرسهای IP را باید بصورت دستی تنظیم و پیکربندی شود. پروتکل DHCP این امکان را می‌دهد که آدرسهای IP را هم بصورت خودکار و هم بصورت دستی تنظیم نمود.

RARP

پروتکل RARP عکس عمل ARP را انجام می‌دهد. یعنی آدرس فیزیکی را گرفته و آدرس IP متناظر با آن را برمی‌گرداند.

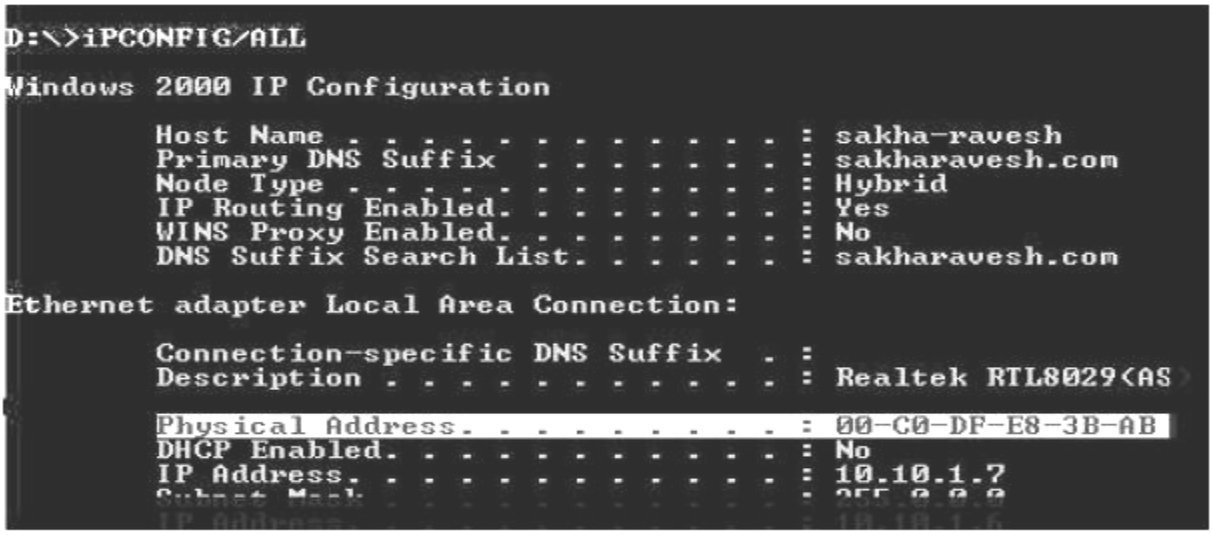
در این پروتکل هم می‌توان آدرسهای فیزیکی ماشینهای مختلف را بصورت فراگیر روی شبکه پخش کرد یا آدرس IP یک ماشین در تصویر حافظه جاسازی شود.

Gateway :

یک عضو در شبکه می باشد که به مثابه یک ورودی به شبکه ای دیگر است . طبق این تعریف ISP شما که باعث برقراری ارتباط شما با اینترنت می شود یک Gateway است. Gateway می تواند سخت افزاری یا نرم افزاری باشد و وظیفه اصلی آن تبدیل پروتوکل ها به یکدیگر است. مثلا اگر شما در یک LAN از پروتوکلی خاص استفاده می کنید، برای اتصال به اینترنت احتیاج به Gateway دارید تا این پروتوکل را به پروتوکل مورد استفاده در اینترنت تبدیل کند. Gateway همچنین به عنوان یک Proxy Server یا Firewall عمل می کند

ARP

همانطور که می‌دانیم آدرسهای فیزیکی توسط لایه پیوند داده دریافت و فهمیده می‌شوند. ولی این لایه از آدرسهای IP چیزی نمی‌داند. این پروتکل برای ترجمه آدرسهای IP به آدرسهای فیزیکی(MAC) بکار می‌رود.



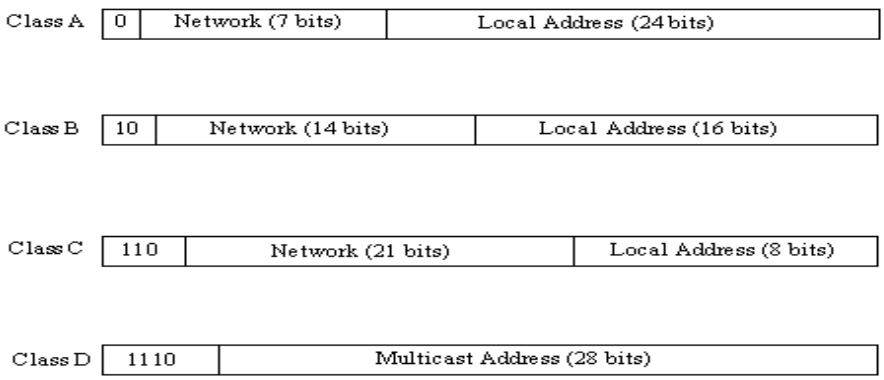
سایر سوئیچ های دستور ipconfig : با استفاده از دستور ipconfig و برخی سوئیچ های آن (release ,renew) ، می توان اطلاعات مربوط به پیکربندی TCP/IP ارائه شده توسط سرویس دهنده DHCP را که در اختیار یک سرویس گیرنده قرار داده شده است را آزاد و یا آنان را مجددا" از سرویس دهنده درخواست نمود . فرآیند فوق به منظور 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 :

سوئیچ	عملکرد
/ release [adapter]	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 MyLan1)
/renew [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)
/ flushdn	حذف محتویات Dns Resolver Cache
/ registerdn	Refresh نمودن تمامی اطلاعات تولید شده توسط DHCP برای آداپتور و ریجستر نمودن اسامی Dns

انواع کلاس بندی در TCP / IP

آدرسهای IP به پنج کلاس A,B,C,D,E تقسیم می شوند. از بین این کلاسها تنها کلاسهای A,B,C کاربرد دارند

IP از دو قسمت Net ID و Host ID تشکیل شده است و مقادیر بیت ها در این دو قسمت در کلاسهای مختلف IP متفاوت است .Net ID در واقع شناسه شبکه و Host ID شناسه میزبان در IP است .



کلاس : A

Net ID هشت بیت است و Host ID آن ۲۴ بیت که مجموعا ۳۲ بیت می شود . این کلاس می تواند ۱۶,۷۷۷,۲۱۴ میزبان (Host) داشته باشد یعنی ۱۶,۷۷۷,۲۱۴ IP که زیر مجموعه آن قرار می گیرند. به عنوان مثال 112.10.57.13 : یک IP کلاس A است. این کلاس برای پایگاهای بزرگ اینترنتی و آژانس های ستون فقرات اینترنت بکار می رود در این کلاس OCTET ابتدای آدرس ها از ۱ تا ۱۲۶ می باشد یعنی در این کلاس بیت با ارزش همیشه صفر است

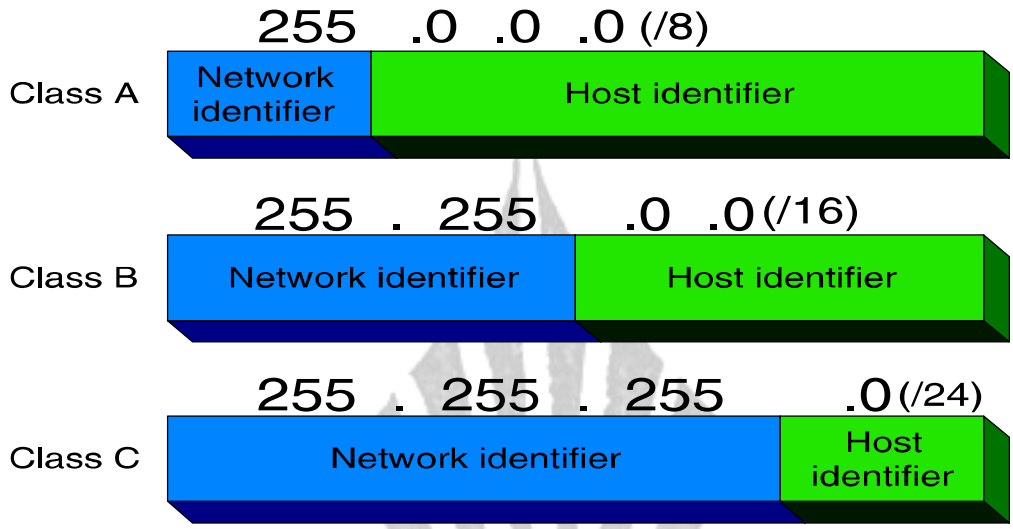
کلاس : B

NetID از هشت بیت به شانزده بیت افزایش می یابد و فضا را برای host ID کمتر می کند، به همین دلیل IP های زیر مجموعه آن به ۶۵,۵۳۴ کاهش می یابد در این کلاس OCTET ابتدای آدرس ها از ۱۲۸ تا ۱۹۱ می باشد یعنی در این کلاس بیت با ارزش همیشه ۱۰ است.

کلاس : C

NetID باز هم بزرگتر شده و از ۱۶ بیت در کلاس B به بیست و چهار افزایش می یابد و Host ID به کوچکترین مقدار خود یعنی هشت بیت می رسد. این کلاس تنها ۲۵۴ کامپیوتر میزبان را پشتیبانی می

کندبرای میزبانها بکار می رود در این کلاس OCTET ابتدای آدرس ها از ۱۹۲ تا ۲۲۳ می باشد یعنی در این کلاس بیت با ارزش همیشه ۱۱۰ است.



کلاس D :

جهت Multicasting بکار می رود این کلاس تنها ۱۶ کامپیوتر میزبان را پشتیبانی می در این کلاس OCTET ابتدای آدرس ها از ۲۲۴ تا ۲۳۹ می باشد یعنی در این کلاس بیت با ارزش همیشه ۱۱۱۰ است

کلاس E :

جهت موارد تجربی بکار می رود در این کلاس OCTET ابتدای آدرس ها از ۲۴۰ می باشد یعنی در این کلاس بیت با ارزش همیشه ۱۱۱۱ است

تعریف پروتکـل : مجموعـه قـوانین نـرم افـزاری جهـت بـالا بـردن بهـره وری از امکانـات سـخت افـزاری و برقراری سرویس در شبکه یا مجموعه قوانین لازم بمنظور قانونمند نمودن نحوه ارتباطات در شبکه ها

پروتکل های پشته ای

یک پروتکل پشته ای ، شامل مجموعه ای از پروتکل ها است که با یکدیگر فعالیت نموده تـا امکـان انجـام یک عملیات خاص را برای سخت افزار و یا نرم افزار فـراهم نماینـد. پروتکـل TCP/IP نمونـه ای از پروتکـل های پشته ای است . پروتکل فوق از چهار لایه استفاده می نماید.

انواع پروتکل های شبکه (Protocol Network) :

۱- پروتکل NET BEUI :

این پروتکل برای محصولات مایکروسافت استفاده می شود و موارد زیر کاربرد دارد :
اگر در شبکه تعداد کامپیوترها حداکثر ۲۰ تا ۲۰۰ عدد بود.

- در شبکه های Domain با وجود استفاده از TCP/IP ، پروتکل NET BEUI پیشنهاد نمی شود.
- این پروتکل قابلیت Route کردن یا مسیریابی را ندارد و همچنین هیچ گونه تنظیماتی ندارد.

Name NetBIOS فرمت قدیمی مایکروسافت می باشد که این اسم از ۱۶ کاراکتر تشکیل می شود که ۱۵ تای ابتدایی آن را کاربر انتخاب می کند و آخرین کاراکتر را خود سیستم با توجه به سرویس های مختلف اضافه می کند.

۲- DLC :

این پروتکل مخصوص محصولات IBM می باشد و در واقع مواقعی که پرینترها بخواهند با یکدیگر ارتباط شبکه ای برقرار کنند استفاده می شود. بعضی از پرینترها به صورت مستقل دارای کارت شبکه هستند و برای استفاده از چنین پرینترهایی باید پروتکل فوق بر روی آنها نصب شود.

۳- پروتکل Apple Talk :

برای ارتباط با کامپیوترهای Macintosh Apple از این پروتکل باید استفاده کنیم.

٤- پروتکل Network Monitor Driver :

این پروتکل در مواقعی که بخواهیم Packet ها را از روی کابل گرفته و یا به اصطلاح Capture کنیم و بر روی کامپیوتر خود منتقل کنیم باید چنین پروتکلی بر روی کامپیوتر ما نصب باشد. (برای سرقت کردن اطلاعات)

٥- پروتکل NW Link IPX/ SPX / Net Bios Compatible Tranport Protocol :

پروتکل IPX/SPX محصول شرکت ناول می باشد. مایکروسافت برای اینکه محصولات خود را سازگار با محصولات ناول بکند پروتکلی تحت عنوان NWLink عرضه کرده است. این پروتکل معادل پروتکل IPX/SPX در ناول می باشد و برای اینکه بتوانیم با کامپیوترهای ناول ارتباط برقرار کنیم ، نصب پروتکل فوق الزامی است.

انواع پروتکل های TCP / IP

TCP/IP،شامل شش پروتکل اساسی است که عبارتند از :

- **TCP**
- **UDP**
- **IP**
- **ARP**
- **ICMP**
- **IGMP**

لایه دسترسی به شبکه در اینترنت : (Network Access)

پایین ترین لایه مدل TCP/IP یا Network Access که شامل کنترل و مدیریت رسانه فیزیکی و پروتکلهای انتقال فریم می باشد و هیچ تعریف مشخصی نداشته و به دلیل تنوع فراوان تجهیزات و پروتکلها در این لایه بسیار انعطاف پذیر می باشد . سخت افزارها یا کانالهای ارائه سرویس در این لایه می توانند خطوط تلفن ، سیم زوج تابیده STP و UDP و کابلهای هم محور کواکسیال ، فیبرهای نوری ، کانالهای رادیویی و کانالهای ماهواره ای و غیره باشند تمام این کانالها دارای مفهومی به نام پهنای باند (Band With) می باشند Band With دریک مفهوم ساده و غیر دقیق ؛ پهنای باند هر کانال را می توان توانایی و ظرفیت آن کانال در ارسال اطلاعات با نرخ بیت بر ثانیه (Bit/s) تعریف نمود . بسیاری از کاربران شبکه اینترنت بوسیله مودم و خط تلفن معمولی (Modem/Dial up) به اینترنت متصل می شوند . این کاربران برای برقراری ارتباط با اینترنت نیاز به یک تامین کننده ارتباط یا (ISP Internet Service Provider)دارند . این تامین کنندگان ارتباط نیز خود به شکلی به اینترنت متصل هستند . در اکثر موارد ارتباط بین کاربران و سرویس دهنده و همچنین ارتباط بین سرویس دهنده بزرگتر ، ارتباطی نقطه به نقطه یا Point to Point می باشد . بنابراین پروتکلهای برقراری ارتباط نقطه به نقطه در استفاده از اینترنت کاربرد فراوانی دارد . در ادامه به بررسی دو پروتکل PPP و SLIP به عنوان نمونه ای از این پروتکلها می پردازیم :

پروتکل : SLIP یک ایستگاه ارسال اطلاعات را با فرستادن رشته ۰ XC0به ایستگاه مقابل اعلام می دارد . همچنین خاتمه ارسال اطلاعات نیز با همین رشته مشخص می شود . در این پروتکل هیچگونه کشف خطایی گنجانده نشده و کشف خطا به لایه بالاتر واگذارشده است . همچنین در فریم مربوط SLIP فقط پروتکل) IP بسته (IP قرارمی گیرد . از دیگر نقاط ضعف SLIP این است که ایستگاههای کاری باید دارای IP ثابت باشند که معمولا در اینترنت چنین نیست و به دلیل این ساختار در این پروتکل مشکل امنیتی وجود دارد که باعث می شود تا هر ایستگاهی که ارتباط برقرار نماید ماشین معتبر شناخته شود .

پروتکل : PPP این پروتکل دارای ساختار فریم زیر می باشد :

1 – 1 Byte FLAG (ابتدای فریم)
2– 1 Byte ADDRESS
3 – 1 Byte CONTROL
4 – 1 OR 2 Byte PROTOCOL
5 – Variable Byte PAY LOAD
6 – 2 OR 4 Byte CHECK SUM
7 – 1 Byte FLAG (انتهای فریم)

در هنگام اتصال با مودم ابتدا لازم است یک سری پارامترها بین مبدا و مقصد انتقال یابد و پس از انتقال این پارامترهای کنترلی ارسال اطلاعات آغاز می شود . این پارامترهای کنترلی به دو رشته NCP و LCP تقسیم می شوند :

LCPها (Link Control Protocol) پارامترهای کنترل PPP را بصورت توافقی بین طرفین و تا هنگام قطع ارتباط مشخص می نمایند . پس از تنظیمLCP ها ، NCPها (Network Control Protocol) تنظیم خواهند شد که بوسیله آنها پارامترهای مربوط به لایه بالاتر انتقال داده شده وتنظیم می گردند ؛ به مجموعه این مراحل فاز مذاکره یا Negotiation phase می گویند . پس از این فاز واحدهای دریافتی از لایه بالاتر در قسمت PAY LOAD قرار گرفته و انتقال داده می شود . در هنگام قطع ارتباط نیز یک سری NCPو LCP رد و بدل می شوند و سپس ارتباط قطع می شود . به عنوان مثال در هنگام رد و بدلNCP ها یک سرویس دهنده به میزبان خود IP اختصاص می دهد .

لایه اینترنت :Network

یادآور می شویم که مفهوم مسیریابی در شبکه اینترنت و سایر شبکه های WAN انتقال اطلاعات بین شبکه های مختلف و یا در حالت کلی بین شبکه های مختلف با توپولوژیها و استانداردهای مختلف می باشد . در شبکه های مختلف قالب فریمهای انتقالی با یکدیگر متفاوت بوده و بنابراین اطلاعات یک شبکه با فریم همان شبکه نمی تواند از مرز شبکه خارج شود . همچنین یادآور می شویم که در لایه اول مدل TCP/IP آدرسهای مورد استفاده برای انتقال فریمها MAC آدرسها یا آدرسهای سخت افزاری نام داشتند و برای یک شبکه خاص منحصر به فرد بوده اند .

بی نظمی در شبکه های مختلف و تنوع توپولوژی و پروتکلها و همچنین روشهای آدرس دهی ایجاب می کند که برای برقراری ارتباط بین تمام کامپیوترها و تمام شبکه ها در اینترنت اصول مشترک و استانداردی بوجود آید . برای انجام این عمل در اولین مرحله بوجود آوردن آدرسهای منحصر بفرد و استاندارد با ساختار خاص در نظر گرفته و طراحی شود . مرحله اول IP Address : آدرسهای جهانی منحصر بفرد در اینترنت مرحله دوم ایجاد ساختار بسته ای است که برای کلیه شبکه ها استاندارد و قابل انتقال باشد ؛ در واقع باید بسته ای در نظر گرفته شود که به راحتی بتواند در طول اینترنت و بر روی شبکه های مختلف به راحتی حرکت کند . در مدل TCP/IP به واحد اطلاعاتی که درون فیلد داده هر فریم قرار می گیرد بسته IP از

شبکه ای به شبکه دیگر به راحتی و با قرار گرفتن در فریمها انتقال داده می شود . در واقع می توان گفت وجه تشابه کلیه کامپیوترهای موجود در اینترنت داشتن یک آدرس منحصر بفرد و پشتیبانی پروتکل TCP/IPمی باشد . { مرحله دوم IP Pocket : بسته استاندارد }

۲ – پروتکلهای لایه Transport

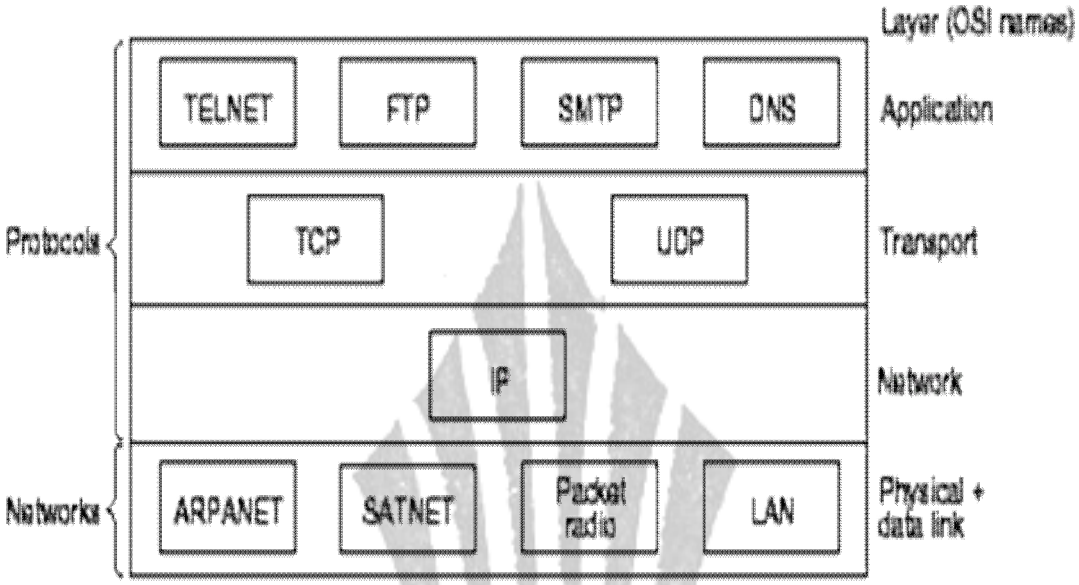
TCP -Transmission Control Protocol و UDP-User Datagram Protocol

پروتکلیTCP/IP که بر روند تجزیه پیامها به بسته های قابل ارسال باIP و بازگرداندن بسته های دریافتی به حالت اول و بررسی درستی آنها نظارت داردTCP.که یک پروتکل اتصال گرای قابل اطمینان است(قابل اطمینان از جهت تضمین تحویل بدون خطا) با لایه Transport مدل مرجعOSI متناظر است

TCP این پروتکل امکان ایجاد ارتباطات قابل اطمینان و اتصال گرا را فراهم می نماید. برخی از وظایف مربوط به این پروتکل به قرار زیر می باشد :

- **شکستن و تقسیم بندی داده ها و پشته های دریافتی از لایه بالاتر به بسته های** TCP **و ساخت مجدد پشته ها از بسته های** TCP **در مقصد .**
- **حصول اطمینان از رسیدن بسته ها به مقصد .**
- **بازبینی بسته ها و مرتب کردن آنها و کنترل خطا**
- **کنترل جریان داده ها**

UDP این پروتکل برای فراهم آوردن مکانیزمی جهت کاهش و کم کردن سرریز داده ها در انتقال اطلاعات بکار می رود و معمولا برای ارتباطاتی که نیاز به قابلیت اطمینان ندارند استفاده می شود.داده های تحویلی به لایه کاربرد توسط برنامه های کاربردی قابل دریافت می باشد این برنامه ها می توانند با استفاده ازAPI ها (Application Program Interface) مستقیما با لایه انتقال ارتباط برقرار کنند UDP پیامهای یک برنامه کاربردی را به بسته های قابل ارسال از طریقIP تبدیل می کند اما چندان قابل اطمینان نیست چرا که پیش ازانتقال مسیر بین فرستنده و گیرنده را تعیین نمی کند و درستی تحویل پیامها را نیز بررسی نمی کند پروتکلی در سطح لایه "حمل" بوده که برنامه مقصد در شبکه را مشخص نموده و از نوع بدون اتصال است . پروتکل فوق، امکان توزیع اطلاعات با سرعت مناسب را ارائه ولی در رابطه با تضمین صحت ارسال اطلاعات ، سطح مطلوبی از اطمینان را بوجود نمی آورد UDP . در رابطه با داده های دریافتی توسط مقصد ، به Acknowledgment نیازی نداشته و در صورت بروز اشکال و یا خرابی در داده های ارسال شده ، تلاش مضاعفی بمنظور ارسال مجدد داده ها ، انجام نخواهد شد . این بدان معنی است که داده هائی کمتر ارسال می گردد ولی هیچیک از داده های دریافتی و صحت تسلسل بسته های اطلاعاتی ، تضمین نمی گردد .از پروتکل فوق ، بمنظور انتقال اطلاعات به چندین کامپیوتر با استفاده از Broadcast و یا Multicast ، استفاده بعمل می آید . پروتکل UDP ، در مواردیکه حجم اندکی از اطلاعات ارسال و یا اطلاعات دارای اهمیت بالائی نمی بانشد ، نیز استفاده می گردد .استفاده از پروتکل UDP در مواردی همچون Multicasting Streaming media، و یا انتشار لیستی از اسامی کامپیوترها که بمنظور ارتباطات محلی استفاده می گردندبمنظور استفاده از UDP ، برنامه مبداء می بایست پورت UDP خود را مشخص نماید دقیقا" مشابه عملیاتی که می بایست کامپیوتر مقصد انجام دهد . لازم به یادآوری است که پورت های UDP از پورت های TCP مجزا و متمایز می باشند



پروتکلهای لایه Internet

IP -Internet Protocol
ICMP-Internet Control Message Protocol
ARP-Address Resolution Protocol
RARP -Reverse Address Resolution Protocol

پروتکل IP -Internet Protocol

لایه IP یک واحد اطلاعات را از لایه بالاتر تحویل می گیرد . این واحد اطلاعات Data Gramنام دارد اگر طول Data Gram بزرگ باشد لایه IP آن را به واحدهای کوچکتر بنام قطعه تقسیم می نماید ، پس با استفاده از قطعه و اضافه کردن Header یا سربار به آن (سرآیند) بسته IP را تشکیل می دهد . در هر بسته IP که آدرس مبدا و مقصد در آن موجود می باشد Header بسته توسط مسیریابها پردازش شده وبسته به سمت مقصد هدایت می شود . طول یک بسته IP می تواند حداکثر ۶۴ کیلو بایت باشد ؛ اما معمولا بسته های IP با طولی حدود ۱۵۰۰ بایت تشکیل می شود به دلیل اینکه اکثر استانداردهای شبکه در لایه پایین تر طول فریم در همین حدود دارد و تشکیل بسته IP با این طول باعث می شود حتی الامکان یک بسته IP بین مبدا و مقصد شکسته نشده و به واحدهای کوچکتر تقسیم نشود . در این پروتکل به قطعات ساخته شده از یک دیاگرام شماره ترتیب تخصیص داده می شود تا در مقصد بسته های IP مجددا به ترتیب چیده شده و قطعه اصلی تشکیل شود . در کنار پروتکل IP پروتکلهای دیگری مانند ICMP : ، ARP، RARP، RIPو غیره وجود دارد که پروتکل IP را در عملکرد بهتر ، مسیریابی صحیح ، مدیریت خطاهای احتمالی و مواردی از این قبیل کمک می کند.

پروتکل ICMP

امکانات لازم در خصوص اشکال زدائی و گزارش خطاء در رابطه با بسته های اطلاعاتی غیرقابل توزیع را فراهم می نماید. با استفاده از ICMP ، کامپیوترها و روترها که از IP بمنظور ارتباطات استفاده می نمایند ، قادر به گزارش خطاء و مبادله اطلاعاتی محدود در رابطه وضعیت بوجود آمده می باشند. مثلا" در صورتیکه IP ، قادر به توزیع یک بسته اطلاعاتی به مقصد مورد نظر نباشد ، ICMP یک پیام مبتنی بر غیرقابل دسترس بودن را برای کامپیوتر مبداء ارسال می دارد . با اینکه پروتکل IP بمنظور انتقال داده بین روترهای متعدد استفاده می گردد ، ولی ICMP به نمایندگی از TCP/IP ، مسئول ارائه گزارش خطاء و یا پیام های کنترلی است . تلاش ICMP ، در این جهت نیست که پروتکل IP را بعنوان یک پروتکل مطمئن مطرح نماید ، چون پیام های ICMP دارای هیچگونه محتویاتی مبنی بر اعلام وصول پیام (Acknowledgment) بسته اطلاعاتی نمی باشند . ICMP ، صرفا" سعی در گزارش خطاء و ارائه فیدبک های لازم در رابطه با تحقق یک وضعیت خاص را می نماید مدیریت لیست اعضاء برای Multicasting IP ، در یک شبکه TCP/IP را بر عهده دارد . IP Multicasting، فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرندگان که گروه multicat نامیده می شوند ؛ ارسال می گردد . IGMP لیست اعضاء را نگهداری می نماید .

مدیریت Multicasting IP

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

پروتکل ARP Address Resolution Protocol

مسئولیت مسئله " نام به آدرس" را در رابطه با بسته های اطلاعاتی خروجی (Outgoing) ، برعهده دارد . ماحصل فرآیند فوق ، Mapping آدرس IP به آدرسMAC ، مربوطه است . کارت شبکه از آدرس MAC ، بمنظور تشخیص تعلق یک بسته اطلاعاتی به کامپیوتر مربوطه ، استفاده می نمایند . بدون آدرس های MAC ، کارت های شبکه ، دانش لازم در خصوص ارسال بسته های اطلاعاتی به لایه بالاتر بمنظور پردازش های مربوطه را دارا نخواهند بود . همزمان با رسیدن بسته های اطلاعاتی به لایه IP بمنظور ارسال در شبکه ، آدرس های MAC مبداء و مقصد به آن اضافه می گردد .

ARP ، از جدولی خاص بمنظور ذخیره سازی آدرس های IP و MAC مربوطه ، استفاده می نماید. محلی از حافظه که جدول فوق در آنجا ذخیره می گردد ، Cache ARP نامیده می شود. ARP Cache هر کامپیوتر شامل mapping لازم برای کامپیوترها و روترهائی است که صرفا" بر روی یک سگمنت مشابه قرار دارند. پروتکل ARP ، آدرس IP مقصد هر یک از بسته های اطلاعاتی خروجی را با ARP Cache مقایسه تا

آدرس MAC مقصد مورد نظر را بدست آورد . در صورتیکه موردی پیدا گردد ، آدرس MAC از Cache بازیابی می گردد . در غیر اینصورت ؛ ARP درخواستی را برای کامپیوتری که مالکیت IP را برعهده دارد ، Broadcast نموده و از وی می خواهد که آدرس MAC خود را اعلام نماید .

کامپیوتر مورد نظر (با IP مربوطه) ، در ابتدا آدرس MAC کامپیوتر ارسال کننده درخواست را به Cache خود اضافه نموده و در ادامه پاسخ لازم را از طریق ارسال آدرس MAC خود ، به متقاضی خواهد داد . زمانیکه پاسخ ARP توسط درخواست کننده ، دریافت گردید ، در ابتدا با استناد به اطلاعات جدید دریافتی، Cache مربوطه بهنگام و در ادامه بسته اطلاعاتی به مقصد کامپیوتر مورد نظر ارسال می گردد . در صورتیکه مقصد یک بسته اطلاعاتی ، سگمنتی دیگر باشد ، ARP ، آدرس MAC را به روتر مسئول در سگمنت مربوطه ، تعمیم خواهد داد (در مقابل آدرس مربوط به کامپیوتر مقصد) . روتر ، در ادامه مسئول یافتن آدرس MAC مقصد و یا Forwarding بسته اطلاعاتی برای روتر دیگر است .

RARP-Reverse Address Resolution Protocol

یک پروتکل برای تعیین نشانیIP یک گره در یک شبکه محلی که به اینترنت متصل است این کار زمانی که تنها نشانی سخت افزاری معلوم است انجام می شود

CSMA/CD -Carrier Sense Multiple Access With Collision Detection

پروتکلی در شبکه ها که شرایطی را که دو یا چند گره اقدام به ارسال همزمان نموده و سبب به وجود آمدن تصادم می شوند مدیریت میکند.در این پروتکل گره های موجود در شبکه بر خط شبکه نظارت نموده و تنها زمانی اقدام به ارسال داده ها می کنند که خط مشغول نباشد.اگر گره دیگری از خط استفاده نماید و سبب به وجود آمدن تصادم شود هر دو گره ارسال داده ها را متوقف خواهند کرد.برای اجتناب از تصادم هر دو گره مدتی صبر نموده(مدت زمانی که گره هادر انتظار می مانند تصادفی است) و سپس اقدام به ارسال مجدد می کنند

سرویس های TCP / IP

الف) Telnet شبیه سازی پایانه ارتباطی : با استفاده از این پروتکل می توان یک ارتباط راه دور بین دو میزبان برقرار نمود و ترمینال یا پایانه را برای دو میزبان شبیه سازی می کند .
این ترمینال راه دور کلیه امکانات یک ترمینال محلی را در اختیار قرارمی دهد .

ب) FTP (File Transport Protocol) انتقال فایل : با استفاده از این پروتکل کاربر قادر خواهد بود از راه دور از راه دور فایلها را از میزبانی به میزبان دیگر انتقال دهد .

ج) POP3 (post of protocol 3) و SMTP(Simple Mail Transfer protocol) مدیریت پست الکترونیک : این پروتکل استانداردی برای ارسال و دریافت پست الکترونیک برروی اینترنت می باشد .

د) HTTP(Hyper Text Transfer Protocol) انتقال صفحات وب : ازاین پروتکل برای انتقال ابرمتنها بر روی اینترنت استفاده می شود . این متنها بر روی میزبانها به وسیله مرورگرها (Explorer) قابل نمایش

هستند . با استفاده از این پروتکل می توان متن ، صدا ، تصویر ، تصاویر متحرک ، موسیقی و فیلم را بر روی شبکه انتقال داد .

ه) NNTP (Network news Transfer protocol) دسترسی به گروههای خبری

و) RDP (Remote Desktop protocol) همان Telnetگرافیکی است

ز) SNMP (Simple Network Management protocol) مدیریت شبکه

ح) SNTP (Simple Network Time protocol) ساعت دقیق در شبکه های مالی و پرسنلی

لایه ارتباطات اینترنتی

لایه ارتباطات اینترنتی مسئول ایجاد ارتباط بین میزبانها است ، بدون توجه به لایه دسترسی به شبکه ای که بکار گرفته شده است . این لایه می بایست قادر به ارتباط برقرار کردن بین میزبانهای شبکه محلی و شبکه های گسترده باشد . بنابراین در این لایه باید یک آدرس بندی و پروتکل ارتباطی قابل مسیردهی داشته باشیم . لایه ارتباطات اینترنتی از IP برای آدرس دهی و انتقال داده ها استفاده می کند . بنابراین این لایه غیر اتصالی است و متناظر با لایه شبکه (Netwoek Layer) مدل OSI است . بعلاوه لایه ارتباطات اینترنتی مسئول فراهم آوردن همه اطلاعات لازم برای لایه دسترسی به شبکه به منظور فرستادن فریمهایش به مقصد محلی است (یا مقصد میزبان دیگری یا مسیریاب) . بنابراین ، این لایه باید پروتکل (Address Resolution Protocol) ARP را هم در بر داشته باشد . پروتکل دیگری به نام RARP (Reverse Address Resoulation Protocol)برای آدرس دهی ایستگاههای بدون دیسکت (diskless)نیز وجود دارد که براین لایه تکیه دارد .

بعلاوه این لایه می بایست قادر به مسیریابی داده ها از طریق Internetwork به مقصدهای خود باشد . بنابراین ، این لایه دربرگیرنده پروتکل RIP (Routing Informatio Protocol) نیز می باشد که می تواند از ابزارهای روی شبکه پرس وجو هایی انجام دهد تا تعیین کند که بسته ها به یک مقصد مشخص چگونه باید مسیریابی شوند.

همچنین لایه ارتباطات اینترنت شامل قابلیتهایی برای میزبانها به منظور تبادل اطلاعات درباره مشکلات یا خطا ها در شبکه می باشد . پروتکلی که این ویژگی را پیاده سازی می کند ، ICMP (Internet Control Message Protocol)نام دارد و در نهایت ، لایه ارتباطات اینترنتی ویژگی Multicast را دربردارد ویژگی که کار ارسال اطلاعات به چندین مقصد میزبان را در هر لحظه خواهیم داشت

این فرآیند توسط پروتکل (Internet Group Management Protocol) پشتیبانی می شود .

لایه ارتباطات میزبان به میزبان : لایه ارتباطات میزبان به میزبان سرویسهای مورد نیاز برای ایجاد ارتباطات قابل اعتماد بین میزبانهای شبکه را پیاده سازی می کند و مطابق با لایه حمل و قسمتی از لایه جلسه مدل OSIاست و در ضمن در برگیرنده قسمتی از کارهای لایه های نمایش و کاربردی نیز می باشد . لایه میزبان به میزبان شامل دو پروتکل است . اولین آن TCP (Transimission Control Protocol) می باشد

TCP . توانائی برقراری سرویس ارتباط گرا بین میزبانها را فراهم می کند. آن شامل ویژگیهای زیر می باشد

- قسمت بندی داده ها به بسته (Packets)
- ساخت رشته های داده از بسته ها
- دریافت تائید
- سرویس های سوکت برای ایجاد چندین ارتباط با چندین پورت روی میزبانهای دور
- بازبینی بسته و کنترل خطا
- کنترل جریان انتقال داده
- مرتب سازی و ترتیب بندی بسته

سرویس های TCP سرویس های ارتباط گرای قابل اعتمادی با قابلیت کشف خطا ها و مشکلات را فراهم می کنند .

لایه Transport

یکی از پروتکل های استاندارد TCP/IP است که امکان توزیع و عرضه اطلاعات (سرویس ها) بین صرفا" دو کامپیوتر ، با ضریب اعتماد بالا را فراهم می نماید. چنین ارتباطی (فقط بین دو نقطه) ، Unicast نامیده می شود . در ارتباطات با رویکرد اتصال گرا ، می بایست قبل از ارسال داده ، ارتباط بین دو کامپیوتر برقرار گردد . پس از برقراری ارتباط ، امکان ارسال اطلاعات برای صرفا" اتصال ایجاد شده ، فراهم می گردد . ارتباطات از این نوع ، بسیار مطمئن می باشند ، علت این امر به تضمین توزیع اطلاعات برای مقصد مورد نظر برمی گردد . بر روی کامپیوتر مبداء ، TCP داده هائی که می بایست ارسال گردند را در بسته های اطلاعاتی (Packet) سازماندهی می نماید. در کامپیوتر مقصد ، TCP ، بسته های اطلاعاتی را تشخیص و داده های اولیه را مجددا" ایجاد خواهد کرد .

نحوه ارسال اطلاعات در TCP

TCP ، بمنظور افزایش کارائی ، بسته های اطلاعاتی را بصورت گروهی ارسال می نماید . TCP ، یک عدد سریال (موقعیت یک بسته اطلاعاتی نسبت به تمام بسته اطلاعاتی ارسالی) را به هریک از بسته ها نسبت داده و از Acknowledgment بمنظور اطمینان از دریافت گروهی از بسته های اطلاعاتی ارسال شده ، استفاده می نماید. در صورتیکه کامپیوتر مقصد ، در مدت زمان مشخصی نسبت به اعلام وصول بسته های اطلاعاتی ، اقدام ننماید ، کامپیوتر مبداء ، مجددا" اقدام به ارسال اطلاعات می نماید. علاوه برافزودن یک دنباله عددی و Acknowledgment به یک بسته اطلاعاتی ، TCP اطلاعات مربوط به پورت مرتبط با برنامه ها ی مبداء و مقصد را نیز به بسته اطلاعاتی اضافه می نماید. کامپیوتر مبداء ، از پورت کامپیوتر مقصد بمنظور هدایت صحیح بسته های اطلاعاتی به برنامه مناسب بر روی کامپیوتر مقصد ، استفاده می نماید. کامپیوتر مقصد از پورت کامپیوتر مبداء بمنظور برگرداندن اطلاعات به برنامه ارسال کننده در کامپیوتر مبداء ، استفاده خواهد کرد .

هر یک از کامپیوترهائی که تمایل به استفاده از پروتکل TCP بمنظور ارسال اطلاعات دارند ، می بایست قبل از مبادله اطلاعات ، یک اتصال بین خود ایجاد نمایند . اتصال فوق ، از نوع مجازی بوده و Session نامیده می شود .دو کامپیوتر درگیر در ارتباط ، با استفاده از TCP و بکمک فرآیندی با نام : Three-Way handshake ، با یکدیگر مرتبط و هر یک پایبند به رعایت اصول مشخص شده در الگوریتم مربوطه خواهند بود ابتدا کامپیوتر مبداء ، اتصال مربوطه را از طریق ارسال اطلاعات مربوط به Session ، مقداردهی اولیه می نماید در ادامه کامپیوتر مقصد ، به اطلاعات Session ارسال شده ، پاسخ مناسب را خواهد داد در پایان کامپیوتر مبداء ، از شرح واقعه بکمک Acknowledgment ارسال شده توسط کامپیوتر مقصد ، آگاهی پیدا خواهد کرد .

عملیات انجام شده توسط IP

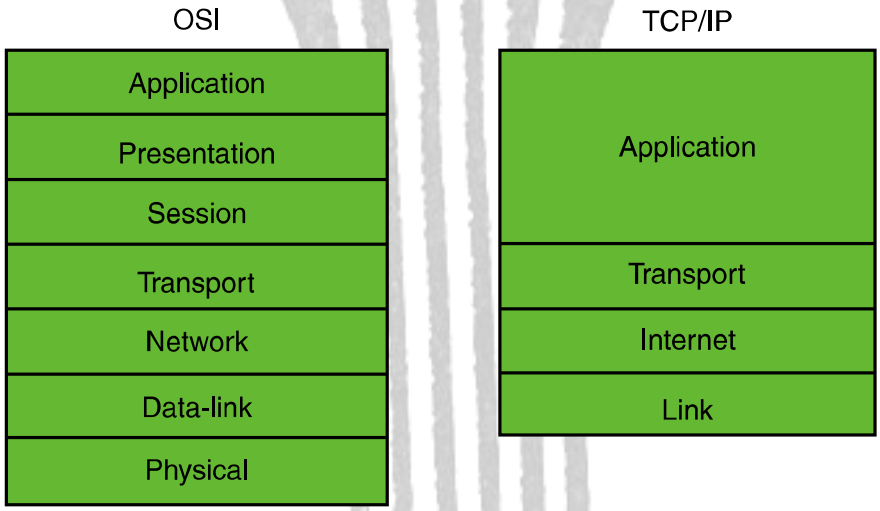
می توان IP را بعنوان مکانی در نظر گرفت که عملیات مرتب سازی و توزیع بسته های اطلاعاتی در آن محل ، صورت می پذیرد. بسته ها ی اطلاعاتی توسط یکی از پروتکل های لایه حمل (TCP و یا UDP) و یا از طریق لایه " اینترفیس شبکه " ، برای IP ارسال می گردند . اولین وظیفه IP ، روتینگ بسته های اطلاعاتی بمنظور ارسال به مقصد نهائی است . هر بسته اطلاعاتی ، شامل آدرس IP مبداء (فرستنده) و آدرس IP مقصد (گیرنده) می باشد. در صورتیکه IP ، آدرس مقصدی را مشخص نماید که در همان سگمنت موجود باشد ، بسته اطلاعاتی مستقیما" برای کامپیوتر مورد نظر ارسال می گردد . در صورتیکه آدرس مقصد در همان سگمنت نباشد ، IP، می بایست از یک روتر استفاده و اطلاعات را برای آن ارسال نماید.یکی دیگر از وظایف IP ، ایجاد اطمینان از عدم وجود یک بسته اطلاعاتی (بلاتکلیف !) در شبکه است . بدین منظور محدودیت زمانی خاصی در رابطه با مدت زمان حرکت بسته اطلاعاتی در طول شبکه ، در نظر گرفته می شود .عملیات فوق، توسط نسبت دادن یک مقدار (TTL(Time To Live به هر یک از بسته های اطلاعاتی صورت می پذیرد TTL .، حداکثر مدت زمانی را که بسته اطلاعاتی قادر به حرکت در طول شبکه است را مشخص می نماید .

نقطه ضعف پروتکل TCP

جهت برقراری یک ارتباط TCP احتیاج به انجام یک فرآیندی می باشد که طی آن دستگاهی که قصد برقراری ارتباط با یک کامپیوتر هدف را دارد بسته Tcp با تنظیم بیت SYN=1 به سمت کامپیوتر مقصد می فرستد و در جواب ؛ کامپیوتر مقصد یک بسته با بیتهای SYN=1 و ACK=1 خواهد فرستاد و در نهایت ارتباط برقرار می گردد. همچنین گزینه ای بنام Sequence Number نیز در این ارتباط تعریف می گردد تا توالی بسته ها در مقصد مشخص باشد. رنج Sequence Number به گزینه دیگری بنام Window که در حقیقب مقدار فضای بافر اختصاص داده شده به ارتباط Tcp را مشخص می نماید ؛ بستگی دارد و در واقع تفاضل دو Sequence Number پی در پی در یک کامپیوتر از مقدار فضایWindow ای که در طرف دیگر تعیین شده نمی تواند بیشتر باشد. در پایان نیز جهت خاتمه ارتباط ؛ یک بسته با تنظیم بیت RST=1 به کامپیوتر مقابل فرستاده می شود و ارتباط قطع می گردد .

در این نقطه ضعف هکر با استفاده از یک بسته TCP/IP که آدرس IP و شماره پورت آن جعلی و برابر با شماره IP و پورت کامپیوتر هدف می باشد و نیز بیت RST آن برابر ۱ تنظیم شده است ؛ این بسته را به سمت کامپیوتر یا روتری که کامپیوتر قربانی با آن در ارتباط است می فرستد که باعث گمراه شدن آن و قطع ارتباط کامپیوتر قربانی با آن می شود .نکته ماجرا در تعیین Sequence Number صحیح جهت گمراه کردن کامپیوتر یا دستگاه مقصد می باشد. در گذشته چنین کاری تقریباً غیر ممکن می نمود اما شواهد حاکی از چیز دیگریست . مسئله اینجاست که هنگام فرستادن یک بسته Tcp با بیت RST=1 ؛ مقدار Sequence Numberمی تواند هر عددی در محدوده رنج گزینه Window باشد و به همین دلیل حدس زدن آن برای هکر بسیار راحتتر می باشد که در نهایت هکر را قادر به بستن ارتباط کامپیوتر هدف(که می تواند یک سرور باشد) با دستگاهی که سرور با آن یک ارتباط برقرار کرده است (مثل روتر) می نماید.

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 پروتکل 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 استTCPپیچیده تر 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 .

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 فیزیکی	

خلاصه

پس از برقراری ارتباط ، امکان ارسال اطلاعات برای صرفا" اتصال ایجاد شده ، فراهم می گردد . ارتباطات از این نوع ، بسیار مطمئن می باشند ، علت این امر به تضمین توزیع اطلاعات برای مقصد مورد نظر برمی گردد . بر روی کامپیوتر مبداء ، TCP داده هائی که می بایست ارسال گردند را در بسته های اطلاعاتی (Packet) سازماندهی می نماید. در کامپیوتر مقصد ، TCP ، بسته های اطلاعاتی را تشخیص و داده های اولیه را مجددا" ایجاد خواهد کرد . ارسال اطلاعات با استفاده از TCP TCP ، بمنظور افزایش کارائی ، بسته های اطلاعاتی را بصورت گروهی ارسال می نماید . TCP ، یک عدد سریال (موقعیت یک بسته اطلاعاتی نسبت به تمام بسته اطلاعاتی ارسالی) را به هریک از بسته ها نسبت داده و از Acknowledgment بمنظور اطمینان از دریافت گروهی از بسته های اطلاعاتی ارسال شده ، استفاده می نماید. در صورتیکه کامپیوتر مقصد ، در مدت زمان مشخصی نسبت به اعلام وصول بسته های اطلاعاتی ، اقدام ننماید ، کامپیوتر مبداء ، مجددا" اقدام به ارسال اطلاعات می نماید. علاوه برافزودن یک دنباله عددی و Acknowledgment به یک بسته اطلاعاتی ، TCP اطلاعات مربوط به پورت مرتبط با برنامه ها ی مبداء و مقصد را نیز به بسته اطلاعاتی اضافه می نماید. کامپیوتر مبداء ، از پورت کامپیوتر مقصد بمنظور هدایت صحیح بسته های اطلاعاتی به برنامه مناسب بر روی کامپیوتر مقصد ، استفاده می نماید. کامپیوتر مقصد از پورت کامپیوتر مبداء بمنظور برگرداندن اطلاعات به برنامه ارسال کننده در کامپیوتر مبداء ، استفاده خواهد کرد . هر یک از کامپیوترهائی که تمایل به استفاده از پروتکل TCP بمنظور ارسال اطلاعات دارند ، می بایست قبل از مبادله اطلاعات ، یک اتصال بین خود ایجاد نمایند . اتصال فوق ، از نوع مجازی بوده و Session نامیده می شود .دو کامپیوتر درگیر در ارتباط ، با استفاده از TCP و بکمک فرآیندی با نام : Three-Way handshake ، با یکدیگر مرتبط و هر یک پایبند به رعایت اصول مشخص شده در الگوریتم مربوطه خواهند بود . فرآیند فوق ، در سه مرحله صورت می پذیرد : مرحله اول : کامپیوتر مبداء ، اتصال مربوطه را از طریق ارسال اطلاعات مربوط به Session ، مقداردهی اولیه می نماید (عدد مربوط به موقعیت یک بسته اطلاعاتی بین تمام بسته های اطلاعاتی و اندازه مربوط به بسته اطلاعاتی) مرحله دوم : کامپیوتر مقصد ، به اطلاعات Session ارسال شده ، پاسخ مناسب را خواهد داد . کامپیوتر مبداء ، از شرح واقعه بکمک Acknowledgment ارسال شده توسط کامپیوتر مقصد ، آگاهی پیدا خواهد کرد . پروتکل UDP : لایه User Datagram Protocol (Transport UDP) ، پروتکلی در سطح لایه "حمل" بوده که برنامه مقصد در شبکه را مشخص نموده و از نوع بدون اتصال است . پروتکل فوق، امکان توزیع اطلاعات با سرعت

مناسب را ارائه ولی در رابطه با تضمین صحت ارسال اطلاعات ، سطح مطلوبی از اطمینان را بوجود نمی آورد . UDP در رابطه با داده های دریافتی توسط مقصد ، به Acknowledgment نیازی نداشته و در صورت بروز اشکال و یا خرابی در داده های ارسال شده ، تلاش مضاعفی بمنظور ارسال مجدد داده ها ، انجام نخواهد شد . این بدان معنی است که داده هائی کمتر ارسال می گردد ولی هیچیک از داده های دریافتی و صحت تسلسل بسته های اطلاعاتی ، تضمین نمی گردد .از پروتکل فوق ، بمنظور انتقال اطلاعات به چندین کامپیوتر با استفاده از Broadcast و یا Multicast ، استفاده بعمل می آید . پروتکل UDP ، در مواردیکه حجم اندکی از اطلاعات ارسال و یا اطلاعات دارای اهمیت بالائی نمی باشد ، نیز استفاده می گردد. استفاده از پروتکل UDP در مواردی همچون Multicasting Streaming media ، (نظیر یک ویدئو کنفرانس زنده) و یا انتشار لیستی از اسامی کامپیوترها که بمنظور ارتباطات محلی استفاده می گردند ، متداول است . بمنظور استفاده از UDP ، برنامه مبداء می بایست پورت UDP خود را مشخص نماید دقیقا" مشابه عملیاتی که می بایست کامپیوتر مقصد انجام دهد . لازم به یادآوری است که پورت های UDP از پورت های TCP مجزا و متمایز می باشند (حتی اگر دارای شماره پورت یکسان باشند). پروتکل IP : لایه Internet Protocol (Internet IP) ، امکان مشخص نمودن محل کامپیوتر مقصد در یک شبکه ارتباطی را فراهم می نماید. IP ، یک پروتکل بدون اتصال و غیرمطمئن بوده که اولین مسئولیت آن آدرس دهی بسته های اطلاعاتی و روتینگ بین کامپیوترهای موجود در شبکه است . با اینکه IP همواره سعی در توزیع یک بسته اطلاعاتی می نماید ، ممکن است یک بسته اطلاعاتی در زمان ارسال گرفتار مسائل متعددی نظیر : گم شدن ، خرابی ، عدم توزیع با اولویت مناسب ، تکرار در ارسال و یا تاخیر، گردند.در چنین مواردی ، پروتکل IP تلاشی بمنظور حل مشکلات فوق را انجام نخواهد داد (ارسال مجدد اطلاعات درخواستی) .آگاهی از وصول بسته اطلاعاتی در مقصد و بازیافت بسته های اطلاعاتی گم شده ، مسئولیتی است که بر عهده یک لایه بالاتر نظیر TCP و یا برنامه ارسال کننده اطلاعات ، واگذار می گردد . عملیات انجام شده توسط IP می توان IP را بعنوان مکانی در نظر گرفت که عملیات مرتب سازی و توزیع بسته های اطلاعاتی در آن محل ، صورت می پذیرد .بسته ها ی اطلاعاتی توسط یکی از پروتکل های لایه حمل (TCP و یا UDP) و یا از طریق لایه " اینترفیس شبکه " ، برای IP ارسال می گردند . اولین وظیفه IP ، روتینگ بسته های اطلاعاتی بمنظور ارسال به مقصد نهائی است . هر بسته اطلاعاتی ، شامل آدرس IP مبداء (فرستنده) و آدرس IP مقصد (گیرنده) می باشد. در صورتیکه IP ، آدرس مقصدی را مشخص نماید که در همان سگمنت موجود باشد ، بسته اطلاعاتی مستقیما" برای کامپیوتر مورد نظر ارسال می گردد . در صورتیکه آدرس مقصد در همان سگمنت نباشد ، IP ، می بایست از یک روتر استفاده و اطلاعات را برای آن ارسال نماید.یکی دیگر از وظایف IP ، ایجاد اطمینان از عدم وجود یک بسته اطلاعاتی (بلاتکلیف !) در شبکه است . بدین منظور محدودیت زمانی خاصی در رابطه با مدت زمان حرکت بسته اطلاعاتی در طول شبکه ، در نظر گرفته می شود .عملیات فوق، توسط نسبت دادن یک مقدار Time To Live(TTL) به هر یک از بسته های اطلاعاتی صورت می پذیرد. TTL ، حداکثر مدت زمانی را که بسته اطلاعاتی قادر به حرکت در طول شبکه است را مشخص می نماید(قبل از اینکه بسته اطلاعاتی کنار گذاشته شود) . پروتکل ICMP : لایه Internet Control Message Protocol (Internet ICMP) ، امکانات لازم در خصوص اشکال زدائی و گزارش خطاء در رابطه با بسته های اطلاعاتی غیرقابل توزیع را فراهم می نماید. با استفاده از ICMP ، کامپیوترها و روترها که از IP بمنظور ارتباطات استفاده می نمایند ، قادر به گزارش خطاء و مبادله اطلاعاتی محدود در رابطه وضعیت بوجود آمده می باشند. مثلا" در صورتیکه IP ، قادر به توزیع یک بسته اطلاعاتی به مقصد مورد نظر نباشد ، ICMP یک پیام مبتنی بر غیرقابل دسترس بودن را برای کامپیوتر مبداء ارسال می دارد . با اینکه پروتکل IP بمنظور انتقال داده بین روترهای متعدد استفاده می گردد ، ولی ICMP به نمایندگی از TCP/IP ، مسئول ارائه گزارش خطاء و یا پیام های کنترلی است . تلاش ICMP ، در این جهت نیست که پروتکل IP را بعنوان یک پروتکل مطمئن مطرح نماید ، چون پیام های ICMP دارای هیچگونه محتویاتی مبنی بر اعلام وصول پیام (Acknowledgment) بسته اطلاعاتی نمی باشند . ICMP ، صرفا" سعی در گزارش خطاء و ارائه فیدبک های لازم در رابطه با تحقق یک وضعیت خاص را می نماید . پروتکل IGMP : لایه Internet Group (Internet IGMP)

Managment Protocol) ، پروتکلی است که مدیریت لیست اعضاء برای IP Multicasting ، در یک شبکه TCP/IP را بر عهده دارد . IP Multicasting، فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرندگان که گروه multicat نامیده می شوند ؛ ارسال می گردد . IGMP لیست اعضاء را نگهداری می نماید .
پروتکل ARP : لایه Address Resolution (Protocol Internet ARP) ، پروتکلی است که مسئولیت مسئله " نام به آدرس" را در رابطه با بسته های اطلاعاتی خروجی (Outgoing) ، برعهده دارد . ماحصل فرآیند فوق ، Mapping آدرس IP به آدرسMedia Access Control(MAC) ، مربوطه است . کارت شبکه از آدرس MAC ، بمنظور تشخیص تعلق یک بسته اطلاعاتی به کامپیوتر مربوطه ، استفاده می نمایند . بدون آدرس های MAC ، کارت های شبکه ، دانش لازم در خصوص ارسال بسته های اطلاعاتی به لایه بالاتر بمنظور پردازش های مربوطه را دارا نخواهند بود . همزمان با رسیدن بسته های اطلاعاتی به لایه IP بمنظور ارسال در شبکه ، آدرس های MAC مبداء و مقصد به آن اضافه می گردد . ARP ، از جدولی خاص بمنظور ذخیره سازی آدرس های IP و MAC مربوطه ، استفاده می نماید. محلی از حافظه که جدول فوق در آنجا ذخیره می گردد ، ARP Cache نامیده می شود. ARP Cache هر کامپیوتر شامل mapping لازم برای کامپیوترها و روترهائی است که صرفا" بر روی یک سگمنت مشابه قرار دارند.

موفق باشید