نصب و راه اندازی شبکه

Installation and commissioning of network

محمد فتحی

بسم الله الرحمن الرحیم

نصب و راه اندازی شبکه

محمد فتحی

۱۳۹۲

مقدمه

Windows Server 2008 R2 دومین نسخه از ویندوز سرور ۲۰۰۸ و یکی از پرطرفدارترین محصولات در زمینه سیستم عامل شبکه است که پس از انتشار توانست به سرعت جای خود را در انواع شبکه های کوچک و بزرگ باز نماید. با توجه به اینکه اکثر شرکت ها در سرتاسر دنیا جهت مدیریت شبکه و کاربران آن از این سیستم عامل استفاده می کنند، آشنایی با پیکربندی و مدیریت آن برای متخصصین فعال در این زمینه امری ضروری خواهد بود. در این کتاب تلاش شده است به زبانی ساده و گویا، مهمترین و ضروری ترین اقدامات پیکربندی جهت استفاده از ویندوز سرور ۲۰۰۸ و R2 ۲۰۰۸ به صورت گام به گام و کاملاً مصور آموزش داده شوند.

خوانندگان عزیز پس از مطالعه این کتاب قادر خواهند بود انواع شبکه های مبتنی بر مایکروسافت را به راحتی راه اندازی نموده و به مدیریت آنها بپردازند. مواردی همچون آدرس های IPv4 و IPv6، سرویس های Active Directory، DNS، DHCP، Group Policy، File Server، Print Server، NAT، و همچنین مدیریت حساب های کاربری، گروه ها و واحدهای سازمانی از جمله مواردی هستند که به خوبی در این کتاب پوشش داده شده اند.

فهرست

سخت افزار شبکه

بررسی اجمالی سخت افزارهای شبکه

شبکه چیست؟

شبکه به بیانی ساده مجموعه‌ای از سرویس دهنده‌ها و سرویس گیرنده‌های متعددی می باشد که به یکدیگر متصل هستند. در این میان سرویس دهنده‌ها (server) نقش سرویس دهنده و خدمات دهی وسرویس گیرنده‌ها (Client) نقش سرویس گیرنده یا همان مشتری را بازی می‌کنند.

یک شبکه می تواند شامل کامپیوتر ها، چاپگرها، تلفن های همراه، و به عبارتی هر دستگاهی (node) که قابلیت اتصال به شبکه را داشته باشد بشود.

مزایای شبکه:

۱. ایجاد ارتباطات ساده تر
۲. تبادل اطلاعات ساده تر
۳. تبادل اطلاعات کم هزینه تر
۴. اشتراک اطلاعات
۵. اشتراک سخت افزار
۶. دسترسی به شبکه های گسترده تر به صورتی ساده تر
۷. مدیریت سادهتر و شامل تر بر روی نودها
۸. و...

راه اندازی یک شبکه:

برای راه اندازی یک شبکه بهینه لازم است موارد زیر را مورد بررسی قرار دهیم

- مقیاس یا نقشه محیط جهت پیاده سازی شبکه
- سرویسی که آن شبکه می خواهد ارائه دهد
- Topology مورد نظر برای پیاده سازی (توپولوژی سیاستی است که جهت پیاده سازی و نوع چینش اجزا در یک شبکه اعمال می شود)

انواع شبکه

شبکه‌ها را می‌توان به دو دسته‌ی کلی شبکه‌های محلی (LAN) و شبکه‌های بزرگ‌تر از آن (WAN) تقسیم کرد.

شبکه‌های محلی LAN (Local Area Network):

شبکه های محلی معمولا میزبان ۲ تا ۲۰کامپیوتر و در غالب Work Group می باشند. سرعت این نوع شبکه بسیار زیاد است (معمولا ۱۰۰ MB Per Sec) و می توان حجم داده های بالا را در مدت بسیار کم از طریق خطوط انتقال داد.

شبکه‌های گسترده WAN (Wide Area Network):

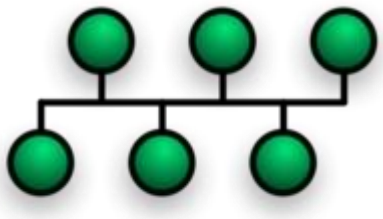
این شبکه ها بزرگتر از شبکه های LAN بوده و اغلب برای امور عمومی از آن استفاده می شود. ازجمله این شبکه ها میتوان شبکه های VAN و یا شبکه های بزرگتر مانند Internet و.. را نام برد. سرعت انتقال داده ها در این نوع شبکه ها نسبت به LAN (در کشور ایران) بسیار ناچیز می باشد. این سرعت به خاطر استفاده از خطوط ۵۶ Kb است. البته می توان با استفاده از خطوط DSL یا ISDN و یا بی سیم Wire Less سرعت این ارتباط را به اندازه ۵۱۲ Kb , ۲۵۶ Kb, ۱۲۸ Kb یا بالاتر افزایش داد.

همبندی (Topology)

توپولوژی (Topology) به معنای چگونگی پیکربندی و ایجاد اتصالات بین دستگاه‌های یک شبکه می باشد. لازم است بدانید به هر ابزار متصل به یک شبکه گره (Node) گفته می‌شود که به وسیله پیوندها (Link) به همدیگر متصل می‌گردند.

انواع همبندی شبکه

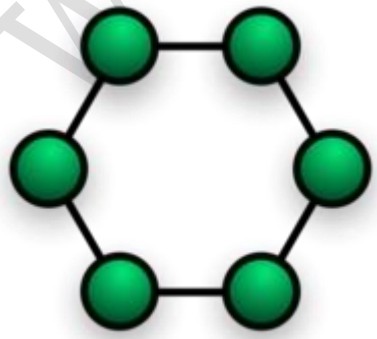
آرایش خطی یا گذرگاهی (Bus):



شبکه‌ای که از همبندی گذرگاهی استفاده می‌کند معمولاً دارای یک کابل واحد و بلند بوده که دستگاه‌های مختلف شبکه به آن متصل هستند و در هر واحد زمانی تنها یک رایانه امکان ارسال اطلاعات را دارد. در این روش کلیهٔ رایانه‌های متصل به خط، اطلاعات ارسال شده را دریافت می‌کنند ولی تنها رایانه‌ای که آدرس مقصد بسته دادهٔ متعلق به او است این اطلاعات را ذخیره می‌نماید و بقیهٔ رایانه‌ها از بسته صرف‌نظر می‌کنند.

راه اندازی این توپولوژی آسان است و به این منظور از یک رشته کابل کواکسیال (Coaxial) استفاده می شود و هر سیستم به کمک یک کانکتور به شبکه متصل می شود . ابتدا و انتهای شبکه با ترمیناتور بسته می شود. اما نگهداری از آن با مشکلاتی همچون خطایابی مشکل همراه است به همین دلیل تقریبا منسوخ شده است.

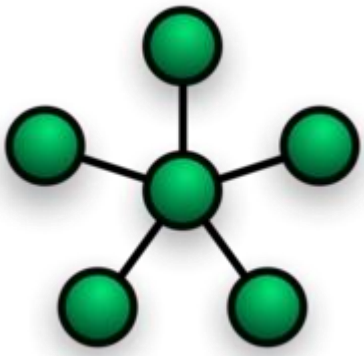
آرایش حلقوی (Ring):



این همبندی توسط شرکت آی‌بی‌ام (IBM) اختراع شد و کلیه رایانه‌ها به گونه‌ای به یکدیگر متصل هستند که مجموعه آنها یک حلقه را تشکیل می‌دهد. همیشه یک بستهٔ کوچک با نام نشانه (Token) در داخل شبکه از یک رایانه به دیگری می‌رود، زمانی که یک رایانه اطلاعاتی جهت ارسال دارد، نشانه را در اختیار گرفته و از چرخش آن داخل شبکه جلوگیری می‌کند، تا زمانیکه نشانه توسط یک رایانه نگه‌داشته شده باشد، تمام رایانه‌های شبکه پذیرای اطلاعاتی خواهند بود که رایانه مالک نشانه ارسال می‌کند.

معایب این نوع توپولوژی این است که اگر قسمتی از کابل اصلی به علتی آسیب ببیند کل شبکه از کار می افتد وعیب یابی آن بسیار وقت گیر می‌باشد واز مزایای آن میتوان به کم هزینه بودن و سادگی شبکه اشاره کرد.

آرایش ستاره‌ای (Star):



در این نوع همبندی کلیه رایانه‌ها به یک کنترل کننده‌ٔ مرکزی به نام میانگاه یا هاب (Hub) متصل می‌شوند و هرگاه رایانه‌ای بخواهد با رایانه دیگری تبادل اطلاعات کند رایانه مبدا اطلاعات را به میانگاه ارسال نموده و اطلاعات از طریق آن به رایانه مقصد انتقال می‌یابد.

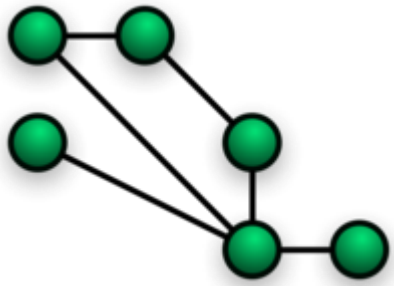
نکته:

۱. یک پیوند نقطه به نقطه را می‌توان به عنوان حالت خاصی از یک شبکه با آرایش ستاره در نظر گرفت. در نتیجه ساده‌ترین شبکه که براساس آرایش ستاره ساخته می‌شود را می‌توان یک گره که به یک گره دیگر از طریق یک پیوند نقطه یه نقطه متصل است در نظر گرفت انتخاب یک گره به عنوان میانگیر به دلخواه ممکن است.
۲. ساده‌ترین نوع شبکه براساس آرایش ستاره علاوه بر شبکه توضیح داده شده در ۱ یک میانگیر متصل به دو گره تابع می‌باشد.
۳. با وجود این که می‌توان آرایش ستاره را با استفاده از یک میانگیر یا سویچ براحتی پیاده سازی نمود اما به کار بردن یک کامپیوتر یا یک اشتراک مشترک نیز برای میانگیر کافی است. به هر حال چون در بیشتر نمایش‌های آرایش ستاره یکی از این ابزار ویژه نشان داده شده است در نتیجه ممکن است این ابهام بوجود آید که حتماً باید از یکی از این ابزار استفاده نمود در حالی که مانند مثال گفته شده در مثال دو سه کامپیوتر متصل به یکدیگر بدون استفاده از هیچ ابراز ویژه‌ای نیز خود یک شبکه با آرایش ستاره است.
۴. شبکه‌های ستاره را می‌توان بصورت پخشی با دسترسی چندگانه یا غیر پخشی با دسترسی چندگانه (NBMA)توصیف نمود که وابسته به توانایی میانگیر در ارسال سیگنال‌های موجود به تمام گره‌های تابع یا ارسال سیگنال به صورت جداگانه برای هر ارتباط است.

آرایش ستاره گسترش یافته (Wide Star):

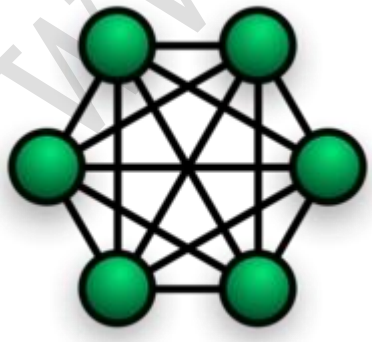
اگر بین میانگیر و گره‌ها تکرارکننده قرار دهیم تا مسافت قابل پوشش توسط میانگیر افزایش یابد به آن آرایش ستاره گسترش یافته گفته می‌شود اگر به جای تکرارکننده‌ها میانگیر قرار داده شود یک آرایش ترکیبی از ستاره-سلسله مراتبی بوجود می‌آید که در بعضی از کتاب‌ها بین این آرایش و آرایش ستاره تفاوتی قائل نمی‌گردند.

آرایش مشبک (Mesh):



در این آرایش شبکه نظم مشخصی نداشته و هر یک از رایانه‌ها به یک یا چند رایانه دیگر متصل شده‌اند. این آرایش در واقع نسخه ناقص آرایش اتصال کامل است، لذا هزینه و پیچیدگی کمتری نسبت به روش مذکور دارد.از معایب این توپولوژی میتوان به پیچیدگی و هزینهای بالای آن اشاره کرد و چون شبکه گسترده است عیب یابی ان هم نسبت سخت می‌باشد از مزایای این توپولوزی این است که اگر قسمتی از کابل قطع شود کل شبکه از کار نمی افتد و انتقال اطلاعات به صورت دوبه دو می‌باشد یعنی تمامی کامپیوترها بدون اینکه شبکه مشغول شود میتوانند به یک دیگر اطلاعات ارسال و دریافت کنند که برای اینکه از توژولوژی mesh بتوان از حداکثرنیرو استفاده کرد از دستگاهی به نام روتر یا مسیر یاب (Router) استفاده می‌شود که کار این دستگاه این است که باعث می‌شود از خطها یا مسیر هایی که خالی هستند ارسال اطلاعات انجام داد و در نتیجه این دستگاه باعث سرعت بخشیدن به ارسال اطلاعات می گردد

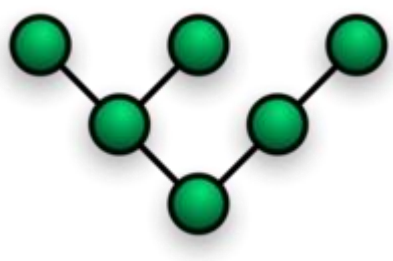
آرایش اتصال کامل (Fully Connected / Full Mesh):



در این آرایش تمام رایانه‌های شبکه مستقیما به همدیگر متصل هستند. عمده‌ترین اشکال این روش پیچیدگی و هزینه بالای این اتصالات است. مزیت این روش ارسال سریع و بیواسطه اطلاعات از هر رایانه به رایانه دیگر می‌باشد.

معمولا از این توپولوژی در سرور های بزرگ لایه ی یک (ISP Tier 1) استفاده می شود

آرایش درختی یا آرایش سلسله مراتبی (Tree) :



در آرایش درختی یک گره مرکزی (بالاترین سطح در سلسله مراتب) به دو یا چند گره در سطحی پایین تر با استفاده از یک پیوند نقطه به نقطه متصل است (به عنوان مثال در سطح دو) و گره‌های سطح دو نیز به چندین گره در سطحی پایین تر متصل هستند (برای مثال در سطح سوم). گره مرکزی تنها گرهی است که هیچ گرهی در سطحی بالاتر از خود ندارد. سلسله مراتب درخت متقارن است یعنی تعداد گره‌های متصل به هر گره در سطح پایین تر عدد ثابت "f" است. عدد "f" به عنوان عامل شاخه بندی در درخت سلسله مراتب شناخته می‌شود.

نکته:

۱. یک شبکه مبنی بر آرایش درختی فیزیکی حتماً باید حداقل سه سطح داشته باشد در غیر این صورت اگر دو سطح داشته باشد نشان دهنده آرایش ستاره است.
۲. اگر یک آرایش درختی عامل شاخه بندی برابر با یک داشته باشد این آرایش نشان دهنده آرایش خطی است.
۳. عامل شاخه بندی مستقل از تعداد کل گره هاست اگر یک گره نیاز به درگاه‌هایی برای اتصال به گره‌های دیگر داشته باشد می‌توان تعداد درگاه‌ها را بدون توجه به تعداد کل گره‌ها کاهش داد. در نتیجه تعداد درگاه‌های مورد نیاز وابسته به عامل شاخه بندی است و در نتیجه می‌توان تعداد درگاه‌ها را بدون توجه به تعداد کل گره‌ها کاهش داد.
۴. تعداد کل پیوندهای نقطه به نقطه در شبکه بر اساس آرایش درختی یکی کمتر از تعداد گره‌های شبکه می‌باشد
۵. اگر نیاز به پردازش اطلاعات توسط گره‌ها در یک آرایش درختی فیزیکی باشد گره‌های سطح بالاتر باید پردازش بیشتری نسبت به گره‌های سطح پایین تر انجام دهند

آرایش ترکیبی (Hybrid):

آرایش ترکیبی نوعی از آرایش‌های شبکه است که از همبندی یک یا چند شبکه با آرایش‌های فیزیکی متفاوت و یا همبندی چندین شبکه که دارای آرایش فیزیکی یکسان است بوجود می‌آید و آرایش فیزیکی شبکه حاصل مشابه آرایش فیزیکی شبکه‌های اولیه نمی‌باشد .

مثلاً آرایش فیزیکی شبکه‌ای که از همبندی چندین شبکه براساس آرایش فیزیکی ستاره بدست می‌آید ممکن است با توجه به نحوه اتصال شبکه‌ها به صورت ترکیبی از آرایش‌های ستاره و خطی یا ستاره و درختی باشد در حالی که اگر چندین شبکه با آرایش خطی توزیع شده به یکدیگر متصل گردند شبکه حاصل آرایش خطی توزیع شده را به خود خواهد گرفت (این توپولوژی ترکیبی است از چند شبکه با توپولوژی متفاوت که توسط یک کابل اصلی بنام Backbone (ستون فقرات) به یکدیگر مرتبط شده اند.توسط یک پل ارتباطی به نام Bridge به کابل Backbone متصل می شود.

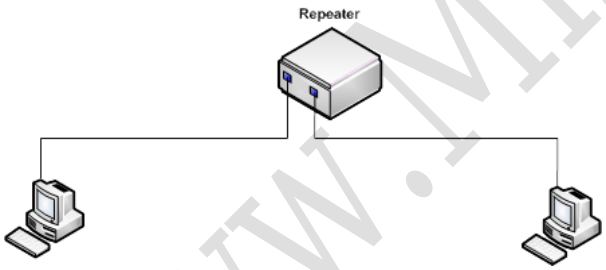
عناصر و دستگاه های شبکه

با این که هر شبکه محلی دارای ویژگی ها و خصایص منحصربفرد مختص به خود می باشد که به نوعی آن را از سایر شبکه ها متمایز می نماید ، ولی در زمان پیاده سازی و اجرای یک شبکه محلی ، اکثر آنان از استانداردها ، عناصر و دستگاه های شبکه ای مشابه ای استفاده می نمایند. در ادامه به توضیح اجمالی برخی از دستگاه های معمول مورد نیاز در شبکه خواهیم پرداخت.

از دستگاه های مورد نیاز می توان به موارد زیر اشره نمود:

- Repeater
- Hub (داخل یک شبکه LAN)
- Bridge (بین دو شبکه LAN)
- Switch (بین چند شبکه LAN)
- Router (بین شبکه های LAN و شبکه های WAN)
- Access Point
- و...

تکرارکننده (Repeater):

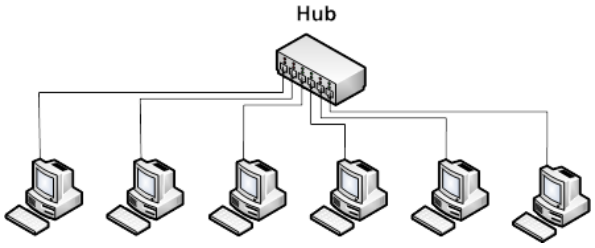


تکرارکننده دیوایسی است که برای مشکل Attenuation (سینگال در داخل کابل می تواند تا مسافت مشخصی حرکت کند و پس از طی این مسافت تضعیف شده و از بین می رود) تعبیه شده است.

وظیفه و عملکرد دستگاه Repeater این است تا این سیگنال را قبل از تضعیف و از بین رفتن دریافت نموده و بازسازی کند و به ادامه مسیر ارسال نماید. به این معنی که اگر دو کامپیوتر مانند شکل بخواهند برای یکدیگر بسته ای ارسال نمایند درحالی که از یکدیگر بسیار دور هستند، م یتوانند با بهره گیری از Repeater (که با قرار گیری در بین مسیر این دو کامپیوتر سیگنال را Retransmit یا دوباره ارسال می کند) از تضعیف سیگنال های ارسالی جلوگیری کنند. لازم است بدانید که عملکرد تکرارکننده در لایه فیزیکی از مدل(هفت لایه ای) OSI است در نتیجه این دیوایس هیچ گونه دانشی درباره آدرس مک یا آیپی ندارد . عملکرد آن فقط این است که سیگنال را دریافت و آن را دوباره ارسال کند.

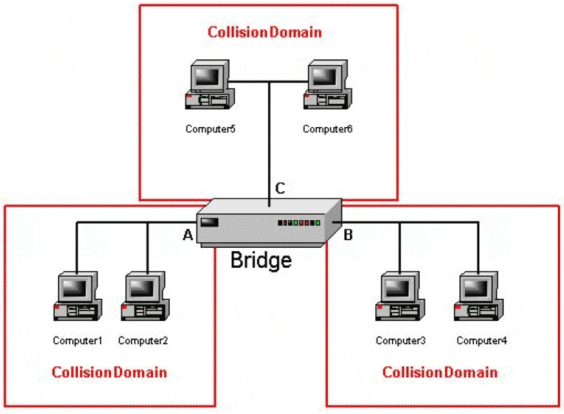
یکی از مشکلات بارز تکرارکننده این است که دستگاه مذکور هیچ دخالتی در بررسی خطا و نویز در مسیر ندارد، به این معنی که اگر سیگنالی خراب شده باشد و یا حتی بر اثر هرگونه عاملی نویز خاصی در Link ارسال شده باشد Repeater بدون هیچگونه بررسی آن سیگنال را تقویت نموده و مجدد در لینک جاری می سازد.

هاب (Hub):



در ساده ترین حالت برای ارتباط بیش از دو گره (Node) از هاب استفاده میشود. هاب مانند یک ریپیترعمل می کند با این تفاوت که چند پورتی است. به این معنی که هاب سیگنالها را دریافت نموده و آن را دوباره به تمامی پورت های منشعب شده اش ارسال می کند بنابراین می تواند این عملکرد را بین چند کامپیوتر انجام دهد. به صورت خلاصه هاب سیگنال را در یک پورت دریافت نموده و آن را بین پورت های دیگر تقسیم می کند. درست مثل یک چند راهی آب . این دیوایس نیز مانند ریپیتر در لایه فیزیکی از مدل OSI است و دانشی از آدرس مک و آی پی ندارد.

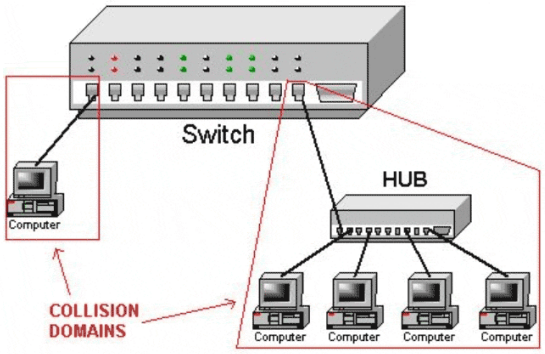
پل (Bridge):



مثل تکرار کننده دارای دو پورت است و برای اتصال گروهی ازکامپیوترها به کار می رود. تفاوت آنها در این است که پل لیستی دارد که نشان می دهد در هر سمت چه کامپیوترهایی قرار دارند و به بسته هایی که باید بطرف دیگر شبکه بروند اجازه ی عبور می دهد.

به بیانی ساده تر پل متصل کننده ی دو شبکه مختلف به یکدیگر است. یکی از فواید پل این است که نویز ها و سیگنالهای مخرب را انتقال نمی دهد.

سوئیچ (Switch):



دستگاهی است میان هاب و پل بدین معنی که مثل پل درون خود جدولی دارد که نشان می دهد چه شبکه هایی به هر پورت متصلند و بسته ها را به جایی که باید بروند می فرستد، همچنین به هاب شبیه است چون به جای دو پورت دارای چندین پورت است. ام بر خلاف هاب سیگنال ها فقط به درون پورتی که باید بروند می روند نه به تمام پورت ها. جداول و شبکه باید به قدرکافی ساده باشند چرا که فقط یک مسیر ممکن برای هر بسته وجود دارد.

با اندکی بررسی متوجه خواهید شد که سوئیچ از هاب سریعتر است چون احتیاجی نیست که هر پورت کل ترافیک ارسال و دریافت اطلاعات را متحمل شود و فقط آنچه که مخصوص خود است را دریافت می کند. البته سوئیچ از پل هم سریعتر است و درضمن گران تر از هر دوی آنها. بعضی سوئیچ ها و پل ها می توانند برای اتصال شبکه هایی که پروتکل های فیزیکی مختلفی دارند استفاده شوند. مثلا برای اتصال شبکه Ethernet یا شبکه Token ring.

هر دوی این شبکه ها می توانند به اینترنت متصل شوند. در شبکه Token ring اطلاعات به صورت نشانه (Token) هایی از یک کامپیوتر به کامپیوتر دیگر به صورت ستاره یا حلقه منتقل می شوند. این قطعات به صورت ویژه هستند و در همه ی شبکه ها استفاده نمی شوند.

مسیریاب (Router):

مسیر یاب ها Device های فوق هوشمندی هستند که از دو یا چند پورت برای ورود و خروج اطلاعات تشکیل شده اند که بوسیله ی آنها انواع مختلف شبکه ها و گره ها را به هم متل می کنند. در واقع کنترل ترافیک در اینترنت به عهده مسیریاب می باشد. مسیریاب را می توان مرتب کننده ی هوشمند بسته ها نیز نامید. همان طور که از نامش پیدا است ، بهترین مسیر را برای فرستادن قطعات به مقصد انتخاب می کند و چک می کند تا ببیند آیا بسته ها به مقصد رسیده اند یا نه. بر اساس مقصد داده ها ، بسته ها از یک مسیر یاب دیگر از طریق بهترین راه فرستاده می شوند(مسیریابی می شوند). این موضوع

باعث می شود تا به عنوان یک وسیله ی قدرتمند در شبکه های پیچیده مثل اینترنت استفاده شود در واقع می توان اینترنت را به عنوان شبکه ای از مسیر یاب ها توصیف کرد. انواع مسیر یاب ها با جداول و پروتکل های مختلفی کار می کنند (هر مسیر یاب در اینترنت باید با پروتکل TCP/IP کار کند)

اتصالات شبکه

امروزه در شبکه های کابلی برای اتصال دو یا چند گره به یکدیگر از کابل های Cat7,Cat6,Cat5 به وفور استفاده می گردد، این کابل ها از جنس مس ساخته شده و هرچه درجه خلوص مس انها بیشتر باشد دارای کیفیت بهتر و افت ولتاژ کمتری هستند .کابل های Cat6 Cat5 از چهار زوج سیم (هشت رشته سیم) به رنگ های آبی – سفید آبی، نارنجی – سفید نارنجی، سبز – سفید سبز، قهوه ای – سفید قهوه ای، تشکیل شده اند که در آنها دو رشته سیم وظیفه ارسال اطلاعات را برعهده داشته و دو رشته سیم نیز وظیفه دریافت اطلاعات، وچهار رشته بعدی فقط نقش نویز گیری را ایفا می کنند.

از جمله تفاوت های موجود مابین کابل های Cat6,Cat5 می توان به موارد زیر اشاره نمود :

- در کابل های Cat6 بین هر دو زوج سیم فویل قرار داده شده است تا امر نویز گیری بهتر انجام گیرد .
- در کابل های Cat6 قطر کابل افزایش یافته است .
- افت ولتاژ Cat6 تا حد چشم گیری پایین تر از Cat5 است .
- این نوع کابل ها (Cat6) برای مسافت های طولانی بهتر هستند .

نکته : در کابل های Cat5 حداکثر طول کابل ۱۰۰ متر می باشد.

استانداردهای اتصال سوکت به کابل مشترک برای: (Cat6 , Cat5)

برای اتصال کابل های Cat5, Cat6 به کارت شبکه از سر سیم های Rj-45 استفاده می گردد. این سر سیم ها برای کابل های Cat5 , Cat6 متفاوت می باشند.

برای اتصال سرسیم به کابل لازم است به این نکته توجه نمایید که این کابل برای چه منظوری مورد استفاده قرار خواهد گرفت:

۱. به صورت مستقیم از یک کامپیوتر به کامپیوتر دیگر
۲. با وجود واسطه هایی مانند هاب و یا سوئیچ

.به دلیل اینکه کارتهای شبکه توانایی کنترل ترافیک شبکه را ندارند برای استفاده از حالت اول باید ترافیک را با کمک کابل کنترل نمود بطوری که موقع اتصال سوکت به کامپیوتر پینی که وظیفه ارسال اطلاعات از کامپیوتر یک را دارد باید به پینی که وظیفه دریافت اطلاعات را دارد متصل گردد. بنابراین با کمی تامل متوجه خواهید شد که ترتیب سیم ها در هر دو سر کابل باید متفاوت باشد.

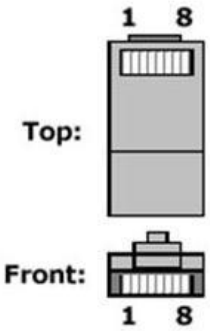
جهت چینش سیم ها در کنار هم دو استاندارد موجود می باشد:

استاندارد A: سفید سبز- سبز- سفید نارنجی - آبی - سفید آبی - نارنجی - سفید قهوه ای - قهوه ای

استاندارد B: سفید نارنجی - نارنجی - سفید سبز- آبی - سفید آبی - سبز - سفید قهوه ای - قهوه ای

نکته :

طریقه استاندارد در دست گرفتن سوکت به این صورت می باشد که وقتی آنرا در دست می گیرید



شاسی آزاد سازی آن به سمت کف دستتان باشد در این صورت اولین پین از سمت چپ را شماره ۱ می نامند

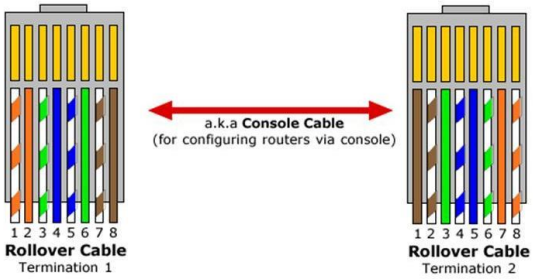
اتصال سوکت به روش مستقیم:

در اتصال سوکت به کابل برای اتصال های نوع دوم (کامپیوتر – سوئیچ– کامپیوتر) تفاوتی بین ترتیب سیم های سوکت شماره ۱ و سوکت شماره ۲ وجود ندارد و هر دو را یکسان پرس نمایید (سوییچ ها خود توانایی کنترل ترافیک شبکه را دارا می باشند

براي سوکت شماره ۱ از ترتیب زیر استفاده نمایید. از چپ به راست:

(قهوه ای – سفید قهوه ای – سبز – سفید آبی – آبی – سفید سبز – نارنجی – سفید نارنجی)

براي سوکت شماره ۲ از ترتیب زیر استفاده نمایید. از چپ به راست:



(سفید نارنجی – نارنجی – سفید سبز– آبی – سفید آبی – سبز – سفید قهوه ای – قهوه ای)

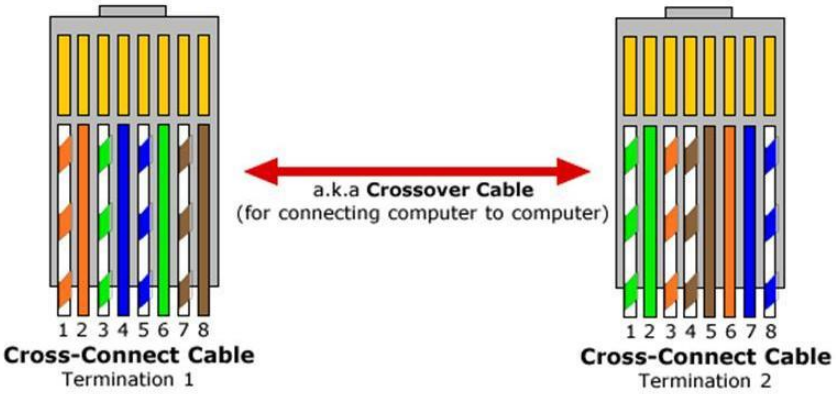
اتصال سوکت به روش کراس آور:

اگر از هاب در شبکه استفاده می کنید نیز بهتر است از این نوع اتصال سوکت که به کراس آور (Crossover)شهرت دارد بهره ببرید.

براي سوکت شماره ۱ از ترتیب زیر استفاده نمایید. از چپ به راست:

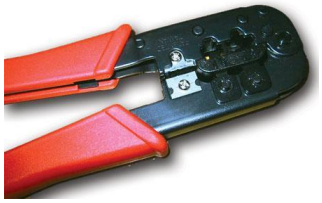
(قهوه ای – سفید قهوه ای – سبز – سفید آبی – آبی – سفید سبز – نارنجی – سفید نارنجی)

براي سوکت شماره ۲ از ترتیب زیر استفاده نمایید. از چپ به راست:



(سفید آبی – آبی – نارنجی – قهوه ای – سفید قهوه ای – سفید نارنجی – سبز – سفید سبز)

اجرای عملی اتصال سوکت به کابل مشترک برای: (Cat6 , Cat5)

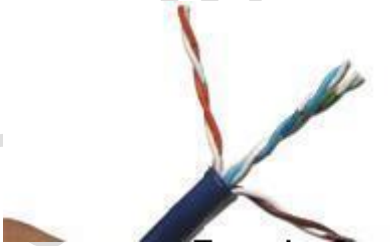


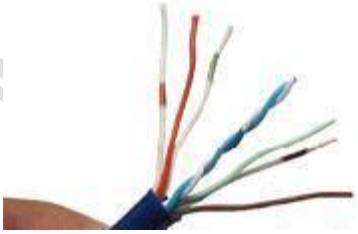
ابزار مورد نیاز:

۱. کابل شبکه Cat6 یا Cat5
۲. سیم لخت کن
۳. آچارشبکه

ابتدا با کمک سیم لخت کن بخشی از لایه ی محافظ روی کابل را در هر دو طرف و به اندازه مناسب جدا نمایید.

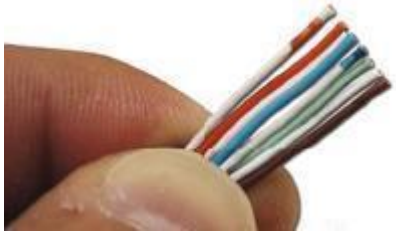






زوج های بهم تابیده شده را یک به یک از همدیگر جدا نموده و صاف نمایید.

اکنون با توجه به استاندارد هایی که در مبحث قبل به آنها اشاره شد سیم هارا مرتب فرمایید.

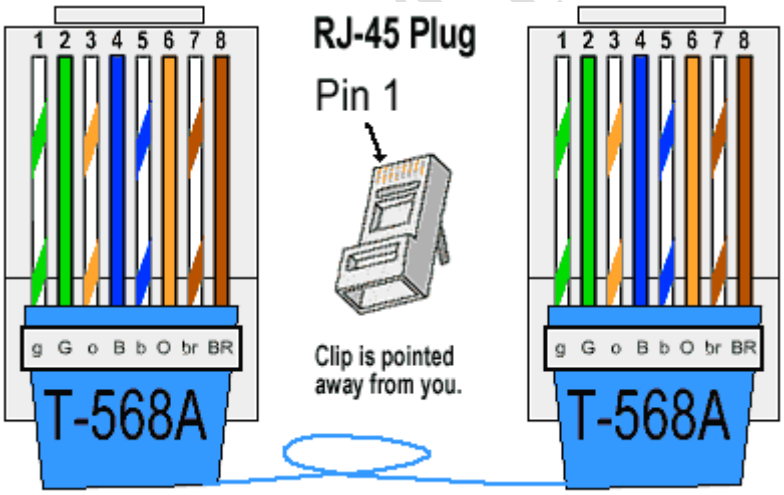



سر سیم را به اندازه مناسب (۳ سانت) و به طور ۹۰ درجه قطع نمایید تاصاف و یکدست شوند.

سپس لا توجه به توضیحات مبحث قبل سوکت را بگونه ای در دست بگیرید که ضامنش به سمت پایین باشد و بدون اینکه ترتیب سیم ها از استاندارد بهم بخورد دسته سیم را وارد سوکت نمایید.

حال به دقت سوکت را بررسی نمایید تا از مرتب، یکسان و کامل بودن سیم ها درر انتهای سوکت اطمینان داشته باشید.

در انتهای هر سوکت فلزهای تیغ مانندی موجود می باشد که بعد از پرس شدن درون سیم ها فرو



رفته و اتصال الکتریکی را برقرار می کند.

اکنون سوکت را درون آچار شبکه قرار داده و پرس نمایید.

حال یک سر کابل کامل شده و نیاز است تمامی مراحل فوق را برای سمت دیگر کابل تکرار نمایید.

یادآوری:

اگر هر دو سر کابل را با یکی از استانداردهای A یا B متصل نمایید (مستقیم) از این کابل میتون برای اتصال کامپیوتر به سویچ یا مودم یا روتر استفاده کرد.

اما اگر یکی از سوکت ها را A و سر دیگر آن را B متصل کنید اصطلاحا یک کابل کراس آور یا ضربدری ایجاد نموده اید که با کمک آن میتوانید ۲ کامپیوتر را بدون نیاز به سویچ با هم شبکه نمایید.

نرم افزار شبکه

بررسی اجمالی نرم افزارهای شبکه

معماری لایه ای در شبکه های کامپیوتری

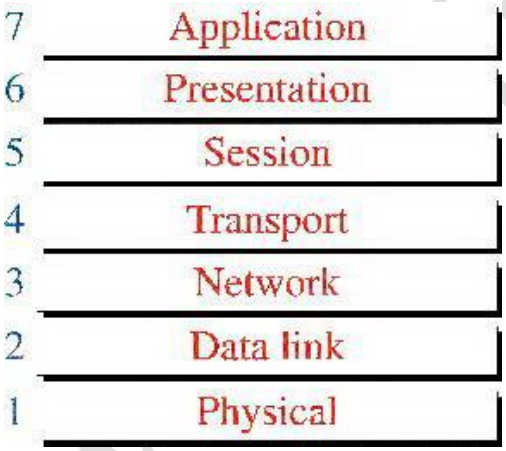
هر فعالیتی در شبکه مستلزم ارتباط بین نرم‌افزار و سخت‌افزار کامپیوتر و اجزای دیگر شبکه است. انتقال اطلاعات بین کامپیوترهای مختلف در شبکه وابسته به انتقال اطلاعات بین بخش های نرم‌افزاری و سخت‌افزاری درون هر یک از کامپیوترها است.

هر یک از فرایندهای انتقال اطلاعات را می توان به بخش‌های کوچک‌تری تقسیم کرد. هر یک از این فعالیت‌های کوچک را سیستم عامل براساس دسته‌ای از قوانین مشخص انجام می‌دهد. این قوانین را پروتکل می‌نامند. پروتکل‌ها تعیین‌کننده روش کار در ارتباط بین بخش‌های نرم‌افزاری و سخت‌افزاری شبکه هستند. بخش‌های نرم‌افزاری و سخت‌افزاری تولیدکنندگان مختلف دارای مجموعه پروتکل‌های متفاوتی می‌باشند.

استاندارد ISO

برای استانداردسازی پروتکل‌های ارتباطی، سازمان استانداردهای بین‌المللی (ISO) در سال ۱۹۸۴ اقدام به تعیین مدل مرجع OSI نمود.

مدل مرجع OSI (Open Systems Interconnection):



مدل مرجع OSI ارائه‌دهنده چارچوب طراحی محیط‌های شبکه‌ای است. در این مدل، جزئیات بخش‌های نرم افزاری و سخت افزاری برای ایجاد سهولت انتقال اطلاعات مطرح شده است و در آن کلیه فعالیت‌های شبکه‌ای در هفت لایه مدل‌سازی می‌شود. هنگام بررسی فرآیند انتقال اطلاعات بین دو کامپیوتر، مدل هفت لایه‌ای OSI روی هر یک از کامپیوترها پیاده‌سازی می‌گردد. در تحلیل این فرایندها می‌توان عملیات انتقال اطلاعات را بین لایه‌های متناظر مدل OSI واقع در کامپیوترهای مبدا و مقصد در نظر گرفت.

این تجسم از انتقال اطلاعات را انتقال مجازی (Virtual) می نامند. اما انتقال واقعی اطلاعات بین لایه‌های مجاور مدل OSI واقع در یک کامپیوتر انجام می‌شود. در کامپیوتر مبدا اطلاعات از لایه فوقانی به طرف لایه تحتانی مدل OSI حرکت کرده و از آن جا به لایه زیرین مدل OSI واقع در کامپیوتر مقصد ارسال می‌شوند. در کامپیوتر مقصد اطلاعات از لایه‌های زیرین به طرف بالاترین لایه مدل OSI حرکت می کنند.

عمل انتقال اطلاعات از یک لایه ب ه لایه دیگر در مدل OSI از طریق واسطه‌ها یا Interface ها انجام می‌شود. این واسطه ها تعیین‌کننده سرویس‌هایی هستند که هر لایه مدل OSI می تواند برای لایه مجاور فراهم آورد.

بالاترین لایه مدل OSI یا لایه هفت، لایه کاربرد یا Application است. این لایه تأمین‌کننده سرویس‌های پشتیبانی برنامه های کاربردی نظیر انتقال فایل، دسترسی به بانک اطلاعاتی و پست الکترونیکی است.

لایه شش، لایه نمایش یا Presentation است. این لایه تعیین‌کننده فرمت یا قالب انتقال داده‌ها بین کامپیوترهای واقع در شبکه است. این لایه در کامپیوتر مبدا داده‌هایی که باید انتقال داده شوند را به یک قالب میانی تبدیل می کند. این لایه در کامپیوتر مقصد اطلاعات را از قالب میانی به قالب اولیه تبدیل می کند.

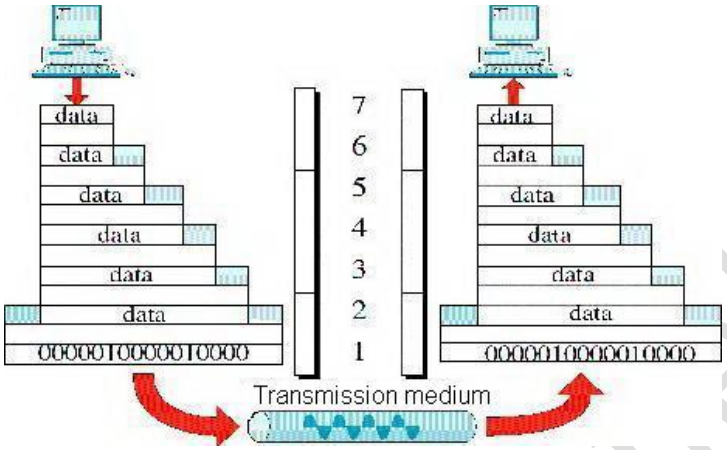
لایه پنجم در این مدل، لایه جلسه یا session است. این لایه بر برقراری اتصال بین دو برنامه کاربردی روی دو کامپیوتر مختلف واقع در شبکه نظارت دارد. همچنین تأمین کننده همزمانی فعالیت های کاربر نیز هست.

لایه چهارم یا لایه انتقال (Transmission)مسؤول ارسال و دریافت اطلاعات و کمک به رفع خطاهای ایجاد شده در طول ارتباط است. هنگامی که حین یک ارتباط خطایی بروز کند، این لایه مسؤول تکرار عملیات ارسال داده است.

لایه سوم در مدل OSI، مسؤول آدرس یا نشانی گذاری پیام‌ها و تبدیل نشانی‌های منطقی به آدرس‌های فیزیکی است. این لایه همچنین مسؤول مدیریت بر مشکلات مربوط به ترافیک شبکه نظیر کند شدن جریان اطلاعات است. این لایه، لایه شبکه یا Network نام دارد.

لایه دوم مدل OSI، لایه پیوند یا Data link است. این لایه وظیفه دارد تا اطلاعات دریافت شده از لایه شبکه را به قالبی منطقی به نام فریم (frame) تبدیل کند. در کامپیوتر مقصد این لایه همچنین مسؤول دریافت بدون خطای این فریم‌ها است.

لایه زیرین در این مدل لایه فیزیکی یا Physical است. این لایه اطلاعات را به صورت جریانی از رشته های داده ای و به صورت الکتریکی روی کابل هدایت می کند. این لایه تعریف کننده ارتباط کابل و



کارت شبکه و همچنین تعیین‌کننده تکنیک ارسال و دریافت داده ها نیز هست.

استاندارد IEEE

انجمن مهندسان برق و الکترونیک آمریکا (IEEE) برای وضع استانداردهای شبکه‌های LAN اصلاحاتی بر مدل OSI انجام داده است. این استانداردها اکنون با عنوان استاندارد IEEE 802 شناسایی می شوند.

مدل IEEE 802:

در پروژه ۸۰۲ استانداردهایی وضع شده است که در برگیرنده مشخصه‌های ارسال و دسترسی به اطلاعات از محیط فیزیکی است. این مشخصه‌ها شامل فرایندهای اتصال، حفظ و قطع ارتباط تجهیزات شبکه نیز هستند.

مشخصه های ۸۰۲ به دوازده گروه تقسیم می‌شوند که هر یک به صورت ۱,۸۰۲ تا ۱۲.۸۰۲ نام‌گذاری شده‌اند. هر یک از این گروه‌ها تعریف‌کننده استانداردهایی برای اعمال اجرایی گوناگون شبکه هستند.

مشخصات ۸۰۲ همچنین شامل اصلاحاتی بر لایه های فیزیکی و پیوند در مدل OSI نیز هست. این اصلاحات در هنگام طراحی اکثر محیط های LAN مورد استفاده قرار می‌گیرند.

کمیته پروژه ۸۰۲ با تفکیک لایه پیوند مدل OSI به دو زیرلایه، جزئیات بیشتری به مدل OSI افزوده است. این لایه‌های فرعی عبارتند از لایه LLC یا Logical link control و لایه MAC یا Media Access Control .

لایه فرعی بالایی یعنی LLC با تعریف چندین نقطه دسترسی به سرویس یا (Service Access Point SAP) بر ارتباطات لایه پیوند مدیریت می کند. SAPها نقاط اتصالی هستند که به ارتباط بین لایه‌های هفت گانه در مدل OSI کمک می کنند.

کامپیوترها از این نقاط برای انتقال اطلاعات از لایه فرعی LLC به لایه‌های بالایی بهره می گیرند.

استانداردهای انتقال اطلاعات بین لایه فرعی LLC و لایه‌های بالایی در مدل OSI، تحت عنوان IEEE 802.2 جمع آوری شده اند.

لایه فرعی MAC پایین لایه فرعی LCC قرار گرفته است. این لایه وظیفه انتقال اطلاعات را از لایه فیزیکی مدل OSI به محیط فیزیکی بر عهده دارد. این لایه مسؤول انتقال بدون خطای اطلاعات بین دو کامپیوتر واقع در شبکه نیز هست.

استانداردهای مربوط به عملکرد لایه فرعی MAC و لایه فیزیکی مدل OSI در گروه های ۸۰۲,۳، ۸۰۲,۴ و ۸۰۲,۱۲ آمده اند.

پروتکل ها

فرآیند به اشتراک گذاشتن اطلاعات نیازمند ارتباط همزمان‌شده‌ای بین کامپیوترهای شبکه است. برای ایجاد سهولت در این فرایند، برای هر یک از فعالیت‌های ارتباط شبکه‌ای، مجموعه‌ای از دستورالعمل‌ها تعریف شده است.

هر دستورالعمل ارتباطی یک پروتکل یا قرارداد نام دارد. یک پروتکل تأمین‌کننده توصیه‌هایی برای برقراری ارتباط بین اجزای نرم‌افزاری و سخت‌افزاری در انجام یک فعالیت شبکه‌ای است.

هر فعالیت شبکه‌ای به چندین مرحله سیستماتیک تفکیک می‌شود. هر مرحله با استفاده از یک پروتکل منحصر به فرد، یک عمل مشخص را انجام می‌دهد.

این مراحل باید با ترتیب یکسان در تمام کامپیوترهای واقع در شبکه انجام شوند. در کامپیوتر مبدا مراحل ارسال داده از لایه بالایی شروع شده و به طرف لایه زیرین ادامه می یابد. در کامپیوتر مقصد مراحل مشابه در جهت معکوس از پایین به بالا انجام می شود.

در کامپیوتر مبدا، پروتکل‌ها اطلاعات را به قطعات کوچک شکسته، به آن‌ها آدرس‌هایی نسبت می‌دهند و قطعات حاصله یا بسته‌ها را برای ارسال از طریق کابل آماده می‌کنند.

در کامپیوتر مقصد، پروتکل‌ها داده‌ها را از بسته‌ها خارج کرده و به کمک نشانی‌های آن‌ها بخش‌های مختلف اطلاعات را با ترتیب صحیح به هم پیوند می‌دهند تا اطلاعات به صورت اولیه بازیابی شوند.

پروتکل‌های مسؤول فرآیندهای ارتباطی مختلف برای جلوگیری از تداخل و یا عملیات ناتمام، لازم است که به صورت گروهی به کار گرفته شوند. این عمل به کمک گروه‌بندی پروتکل‌های مختلف در یک معماری لایه‌ای به نام Protocol Stack یا پشته پروتکل انجام می‌گیرد.

لایه‌های پروتکل‌های گروه‌بندی شده با لایه‌های مدل OSI انطباق دارند. هر لایه در مدل OSI پروتکل مشخصی را برای انجام فعالیت‌های خود به کار می‌برد. لایه‌های زیرین در پشته پروتکل‌ها تعیین‌کننده راهنمایی برای اتصال اجزای شبکه از تولیدکنندگان مختلف به یکدیگر است.

لایه‌های بالایی در پشته پروتکل‌ها تعیین‌کننده مشخصه‌های جلسات ارتباطی برای برنامه‌های کاربردی می‌باشند. پروتکل‌ها براساس آن که به کدام لایه از مدل OSI متعلق باشند، سه نوع طبقه‌بندی می‌شوند. پروتکل‌های مربوط به سه لایه بالایی مدل OSI به پروتکل های Application یا کاربرد معروف هستند. پروتکل‌های لایه Applicationتأمین‌کننده سرویس‌های شبکه در ارتباطات بین برنامه‌های کاربردی با یکدیگر هستند. این سرویس‌ها شامل انتقال فایل، چاپ، ارسال پیام و سرویس‌های بانک اطلاعاتی هستند.

پروتکل‌های لایه نمایش یا Presentation وظیفه قالب‌بندی و نمایش اطلاعات را قبل از ارسال برعهده دارند. پروتکل‌های لایه جلسه یا Session اطلاعات مربوط به جریان ترافیک را به داده‌ها اضافه می‌کنند.

پروتکل‌های نوع دوم که به پروتکل‌های انتقال (Transport) معروف هستند، منطبق بر لایه انتقال مدل OSI هستند. این پروتکل‌ها اطلاعات مربوط به ارسال بدون خطا یا در واقع تصحیح خطا را به داده‌ها می افزایند.

وظایف سه لایه زیرین مدل OSI بر عهده پروتکل های شبکه است. پروتکل‌های لایه شبکه تأمین‌کننده فرایندهای آدرس‌دهی و مسیریابی اطلاعات هستند. پروتکل‌های لایه Data Link اطلاعات مربوط به بررسی و کشف خطا را به داده‌ها اضافه می‌کنند و به درخواست‌های ارسال مجدد اطلاعات پاسخ می‌گویند.

پروتکل‌های لایه فیزیکی تعیین‌کننده استانداردهای ارتباطی در محیط مشخصی هستند.

پروتکل های مشترک

پروتکل های Application:

تولیدکنندگان نرم‌افزار مختلف از پروتکل‌های متفاوتی استفاده می‌کنند. برای انتخاب مناسب‌ترین پروتکل برای شبکه خودتان لازم است تا مزایای چند پروتکل متداول را بشناسید.

در این جا به معرفی مزیت‌های به کارگیری چند پروتکل کاربردی می‌پردازیم.

از پروتکل DLS یا Data Link Control می‌توان در محیط‌های شبکه‌ای که نیاز به کارآیی بالایی دارند استفاده نمود. از این پروتکل می‌توان در شبکه‌هایی که در آن‌ها لایه شبکه وجود ندارد نیز استفاده کرد. در چنین وضعیتی این پروتکل اطلاعات را از برنامه کاربردی مستقیماً به لایه Data Link منتقل می‌کند. این پروتکل در نقش لایه شبکه نیز ظاهر می‌شود و دارای عملکردهایی نظیر کنترل جریان داده، تصحیح خطا و acknowledge نیز می‌باشد.

پروتکل NFS (Network File System) برای به اشتراک گذاشتن فایل بین کامپیوترها در یک شبکه براساس سیستم عامل یونیکس به کار می رود. از این پروتکل برای انتقال داده بین شبکه نیز استفاده می‌شود. پروتکل NFS فقط به کاربرانی اجازه ورود به شبکه را می دهد که دارای اسم رمز معتبر باشند. کاربری که از طرف مدیر شبکه شناسایی نشده باشد، اجازه دسترسی به شبکه را نخواهد داشت. پروتکل NFS دارای نسخه‌هایی برای سیستم عامل‌هایی غیر از یونیکس نیز هست. سیستم عامل‌هایی از قبیل داس، ویندوزNT و OS2.

پروتکل NetBIOS (Network Basic Input / Output System)، از جمله پروتکل‌های بسیار متداول است. از این پروتکل برای یافتن گره‌های شبکه براساس نام آن استفاده می‌شود. این پروتکل از سیستم نامگذاری (Naming System) کمک می‌گیرد.

پروتکل NetBIOS، پروتکل استاندارد شرکت IBM برای توسعه برنامه‌های کاربردی در شبکه‌های سازگار با IBM است. این پروتکل، یک پروتکل لایه جلسه یا Session است که به‌صورت یک واسطه بین دو شبکه عمل می‌کند. NetBIOS به‌صورت گسترده‌ای به عنوان استانداردی برای واسطه‌های شبکه‌ها در صنعت پذیرفته شده است. این پروتکل تأمین‌کننده ابزارهای لازم یک برنامه برای برقراری ارتباط با برنامه‌های دیگردر شبکه است.

AppleTalk مجموعه پروتکل دیگری است که به کامپیوترهای مکینتاش قابلیت به اشتراک گذاشتن فایل ها و چاپگرها را در شبکه می دهد.

پروتکل (AFP) AppleTalk Filing Protocol با ترجمه فرامین محلی سیستم فایل به قالب پذیرفته شده سرویس فایل شبکه، به اشتراک گذاشتن فایل را امکان پذیر می سازد.

پروتکل‌های Name Binding و Printer Access با استفاده از برنامه کاربردی AppleShare، به اشتراک گذاشتن چاپگر را در محیط شبکه اپل فراهم می‌کنند.

پروتکل‌های Transport:

پروتکل‌های انتقال به دو طبقه تقسیم می‌شوند. این طبقه بندی‌ها عبارتند از:

Transmission Control Protocol (TCP) و Sequential Packet Exchange (SPX) . از پروتکل TCP برای اتصال دو شبکه متفاوت به یکدیگر استفاده می‌شود.

در واقع این پروتکل برای ارتباط دو سیستم عامل غیریکسان به کار می رود.

پروتکل TCP واسطه‌ای بین دو شبکه متفاوت فراهم می‌آورد تا بتوانند با استفاده از یک زبان مشترک به تبادل داده بپردازند. این پروتکل در صنعت نرم‌افزار بسیار متداول بوده و توسط شرکت‌های متعددی برای سکوهای متفاوت، از PC تا Mainframe ها عرضه می شود.

TCP رشته‌ای از داده‌ها را از پروتکل‌های بالاتر مثل لایه انتقال دریافت کرده و این رشته داده ای را به قطعه‌هایی

(Segments) شکسته و به هر یک از این بخش‌ها یک شماره ترتیبی نسبت می‌دهد. این شماره‌های ترتیبی تضمین‌کننده دریافت صحیح و با ترتیب داده‌ها هستند.

نوع دوم پروتکل انتقال، پروتکل SPX است. این پروتکل توسط شرکت ناول (Novell) عرضه شده و روشی قابل اطمینان برای انتقال داده‌ها ارائه می کند.

این پروتکل برای بررسی انتقال صحیح داده ها، محاسباتی بر روی داده‌ها در کامپیوتر مبدا و مقصد انجام می‌دهد. برای یک فرآیند انتقال صحیح مقادیر محاسبه شده در کامپیوتر مبدا قبل از ارسال باید با مقادیر محاسبه شده در کامپیوتر مقصد پس از دریافت داده‌ها، یکسان باشند. SPX قابلیت ردیابی انتقال صحیح داده ها را نیز دارد. در این پروتکل اگر Segment یا قطعه داده‌ای در زمان مشخص به مقصد نرسد و یا از کامپیوتر مقصد در این مورد سیگنالی دریافت نگردد، آن قطعه از داده‌ها مجدداً ارسال خواهد شد. اگر انتقال مجدد نیز به مقصد نرسید، این پروتکل پیام‌های هشدار مربوط به از کارافتادگی شبکه را صادر می‌کند.

پروتکل‌های انتقال علاوه بر TCP و SPX در برگیرنده پروتکل های NetBEUI و NWLink نیز هستند.

پروتکل NetBEUI یا NetBIOS Extended User Interface از نظر حجم ، پروتکلی کوچک است که قابلیت انتقال بسیار سریع را در محیط‌های شبکه فراهم می کند. این پروتکل با تمام انواع شبکه های مایکروسافت سازگار است.

پروتکل NWLink نیز توسط شرکت مایکروسافت ارائه شده است. از این پروتکل علاوه بر پروتکل انتقال برای ارتباط چندین شبکه LAN و تشکیل شبکه‌های بزرگ‌تر استفاده می‌شود.

مفاهیم بنیادین

آدرس مک MAC (Media Access Control)

MAC Address مخفف عبارت Media Access Control Address به معنای "زیرلایه کنترل دسترسی به رسانه" بوده و یک آدرس فیزیکی ۶ یا ۸ بایتی است که توسط سازنده‌های کارت‌های واسط شبکه (قطعات سخت افزاری که امکان اتصال کامپیوترها به یکدیگر یا به یک شبکه را می‌دهند.) بر روی حافظه آن (اغلب بر روی ROM - حافظه فقط خواندنی) ذخیره می‌کنند. آدرس مک معمولاً آدرس فیزیکی (Physical Address) نیز خوانده می‌شود.

تمامی دستگاه‌هایی که به هر طریقی به یک شبکه متصل می‌شوند (از جمله تلفن‌های هوشمند، مودم‌های خانگی، لپ تاپ‌ها و...) دارای یک مک آدرس جداگانه هستند. به این ترتیب در یک شبکه داده‌ها به مقصد و واسط شبکه مشخص ارسال می‌شوند.

تفاوت شاخصی که یک آدرس MAC با یک آدرس IP دارد در این است که آدرس IP در پروتکل TCP/IPدر یک لایه نرم افزاری تعیین می‌شود درحالی که آدرس MAC در لایه سخت افزاری بوده و به عبارت ساده تر یک آدرس فیزیکی از پیش تعیین شده بر روی کارت واسط شبکه است.

به عبارت ساده تر آدرس مک مثل یک آدرس خانه ثابت است (البته آدرس مک بعضاً قابلیت تغییر را دارد). این خانه درواقع همان رابط شبکه ما است. حال فرض کنید که در یک شهر با محدوده مشخص (شبکه) قرار داریم و یک نفر (از داخل شبکه) می‌خواهم پیغامی (پاکت‌های داده) را برای ما ارسال کند. فرد برای انجام این کار باید آدرس خانه مورد نظر را در دست داشته باشد. به این ترتیب پاکت‌های داده نیز برای انتقال در درون یک شبکه نیاز به آدرس‌های مک کارت‌های شبکه دارند.

انواع آدرس گذاری MAC:

آدرس MAC نیز دارای استانداردهای مختلفی است که به دلیل نیاز به دامنه گسترده تری از آدرس‌ها طراحی شده اند. سه استاندارد آدرس گذاری مک عبارت اند از MAC-48 ، EUI-۴۸ و EUI-۶۴ که در هر سه مورد مقدار عددی نشان دهنده طول آدرس مک (در همان ساختار) بر اساس تعداد بیت‌ها است. این ساختارهای آدرس گذاری توسط مؤسسه مهندسان برق و الکترونیک (IEEE) طراحی شده اند.

برای مثال در ساختار آدرس گذاری MAC-48 می‌توان در هر آدرس از ۴۸ بیت (یا ۶ بایت) استفاده کرد. به این ترتیب با محاسبه ۲ به توان ۴۸ می‌توان ۲۸۱۴۷۴۹۷۶۷۱۰۶۵۶ آدرس مختلف را در این

ساختار استفاده کرد. به همین ترتیب در ساختار EUI-64 که شامل ۶۴ بیت (۸ بایت) است، می‌توان ۱۸۴۴۶۷۴۴۰۷۳۷۰۹۵۵۱۶۱۶ آدرس مختلف را استفاده کرد. با توجه به این که این مقدار بسیار زیاد است، استفاده از ساختار EUI-64 زیاد رایج نبوده و در شبکه‌های بسیار گسترده (مانند شبکه‌ای که از IPv6 استفاده می کند) استفاده می شود.

آدرس گذاری MAC-48 بسیار رایج بوده و در تکنولوژی‌هایی مانند موارد زیر برای مشخص کردن رابط‌های شبکه مورد استفاده قرار می‌گیرد:

- بی سیم (Wireless)
- بلوتوث (Bluetooth)
- اترنت (Ethernet)
- اکثر شبکه‌هایی که برپایه استاندارد IEEE 802 هستند.

ساختار آدرس MAC:

مک آدرس در ساختارهای MAC-48 و EUI-48 تقریباً یکسان بوده و در آن آدرس مک توسط کاراکترهای هگزادسیمال (Hexadecimal) به صورت جفتی نشان داده می‌شود. هر دو ساختار ۶ بایتی اند بنابراین آدرس مک ما نیز ۶ بخش خواهد بود که هر بایت توسط یک جفت کاراکتر هگزادسیمال نشان داده می‌شود. هر بخش توسط یکی از کاراکترهای دونقطه (:) یا خط تیره (-) و گاهاً نقطه (.) از یکدیگر جدا می‌شوند. برای مثال، عبارت زیر نشان دهنده یک آدرس مک ۴۸ بایتی است:

D0-DF-9A-C8-9F-6B

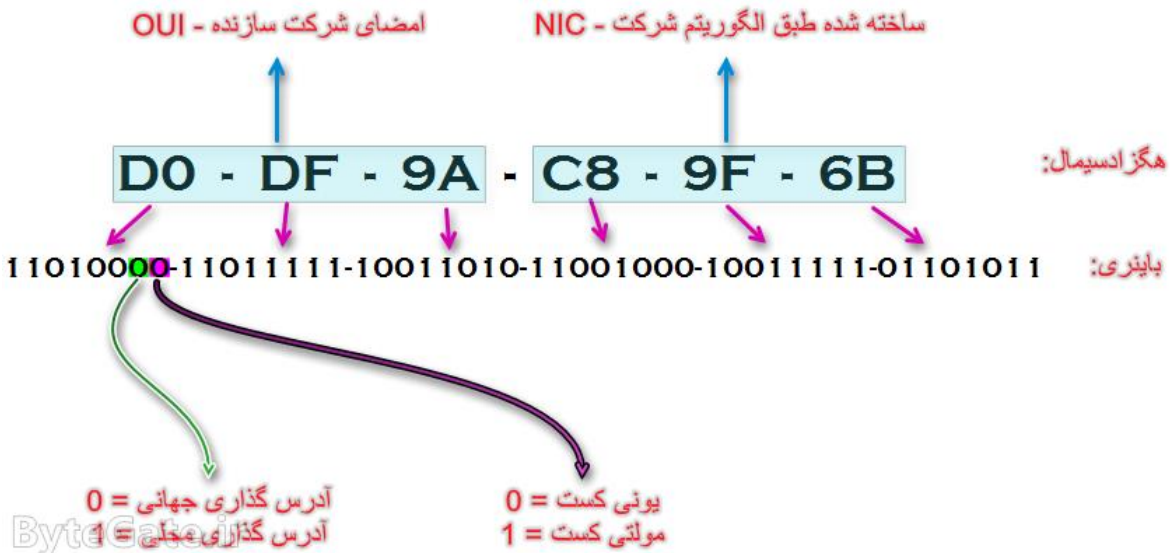
آدرس دهی مک به صورت کلی به دو نوع محلی (Locally) و جهانی (Universally) تقسیم می‌شوند. در نوع محلی (Locally administered addresses) به صورت کامل آدرس مک توسط مدیر شبکه تعیین می‌شود و در نوع جهانی (Universally administered addresses) این آدرس از پیش توسط شرکت سازنده تعیین می‌شود. محلی یا جهانی بودن آدرس از طریق هفتمین بیت بایت اول تشخیص داده می‌شود. برای مثال بایت اول ما به صورت هگزادسیمال D0 هست که تبدیل شده آن به باینری ۱۱۰۱۰۰۰۰ می‌شود که در آن هفتمین بیت ما ۰ به معنای جهانی (ثبت شده توسط شرکت) است. درصورتی که هفتمین بیت بایت اول ۱ باشد، به این معناست که آدرس مک ما به صورت محلی (تعیین شده توسط مدیر شبکه) است. تمامی کارت‌های شبکه که توسط شرکت‌ها ساخته می‌شوند بیت هفتم بایت اول آن‌ها بر روی صفر تنظیم می‌شود.

در حالت Universally administered addresses ، سه بخش اول در هر مک آدرس استاندارد به صورت قراردادی مشخص کننده شرکت تولید کننده آن واسط شبکه است تا از ادغام آدرس‌های

مک شرکت‌های مختلف با یکدیگر جلوگیری شود؛ به این امضاء) OUI مخفف عبارت Organizationally Unique Identifier)نیز گفته می‌شود. برای مثال در عبارت بالا سه بخش اول یعنی "D0-DF-9A" نشان دهنده شرکت Liteon Technology Corporation است.

آخرین بیت در اولین بایت نیز نشان دهنده Unicast یا Multicast بودن رابط شبکه است. این سوئیچ به رابط شبکه اطلاع می‌دهد که وضعیت دریافتی پاکت‌ها به چه صورت باشد. در یونی کست رابط پاکت را یکبار دریافت می‌کند اما در مولتی کست با توجه به پیکربندی‌های انجام شده، پاکت را شناسایی کرده و دریافت می‌کند.

سه بایت (در MAC-48 و EUI-48) یا پنج بایت (در EUI-64) بعدی نیز با توجه به شیوههای



مختلفی که شرکت‌ها برای نام گذاری استفاده می‌کنند، تعیین می‌شود. این بایت‌ها نیز از ادغام مک آدرس‌های مختلف یک شرکت جلوگیری می‌کند.

تغییر آدرس MAC:

امروزه آدرس مک دیگر چیز ثابتی نیست و توسط برخی از برنامه‌ها در سیستم عامل‌هایی مانند ویندوز و بخصوص لینوکس قابل تغییر هستند. به این ترتیب هیچ یک از بیت‌های شناسایی و آدرس‌های مک دیگر قابل اعتماد نبوده و بعضی از متدهای امنیتی مانند فیلترینگ آدرس مک را زیر سوال می‌برد.

آدرس آی پی IP (Internet Protocol)

یک عدد ۳۲ بیتی (bit) است که پس از اتصال به شبکه (... , LAN , Internet) به هر نود تعلق می‌گیرد. شکل کلی IP را می توان به صورت xxx.xxx.xxx.xxx در نظر گرفت که با هر بار اتصال به اینترنت به صورت Dial Up این عدد تغییر می کند. به عنوان مثال در حال حاضر IP ما ۲۱۳,۱۵۵,۵۵,۱۰۴ است اما در اتصال بعدی ممکن است این عدد به ۲۱۳,۱۵۵,۵۵,۲۰ تغییر کند.

کاربرد آدرس IP:

IP به عنوان یک شناسنامه در شبکه است و کاربردهای بسیاری دارد .برای توصیف کامل IP نیاز به شرح TCP/IP است که بعدا به آن اشاره خواهیم کرد. همان طور که در جامعه شناسنامه وسیله ای برای احراز هویت ماست و بدون آن جزو آن جامعه محسوب نمی شویم ، IP نیز وسیله ای برای شناسایی ما در شبکه است و امکان اتصال به شبکه بدون آن وجود ندارد. به طور مثال هنگامی که در شبکه مشغول چت (Chat) هستیم ، کامپیوتر ما دارای یک IP می باشد. و جملاتی را که تایپ می کنیم به وسیله مسیر یابها (Router) مسیر یابی (Routing) شده و به کامپیوتر شخص مقابل میرسند و متنی را هم که شخص مقابل تایپ میکند روی IP ما فرستاده می شود.

البته لازم به ذکر است مثال فوق یک نمونه ی بسیار بسیار ساده از اتفاقاتی است که در شبکه رخ می دهد،کما اینکه توضیح ریزتر مسئله از موضوع درس این مبحث خارج است.

دستیابی به آدرس IP:

برای بدست آوردن IP خود در سیستم عامل ویندوز کافی است به محیط Command Prompt رفته و عبارت " IPCONFIG " را تایپ نمایید. به طور مثال پس از اجرای دستور به نتایج زیر می رسید :

Windows IP Configuration 0 Ethernet adapter:

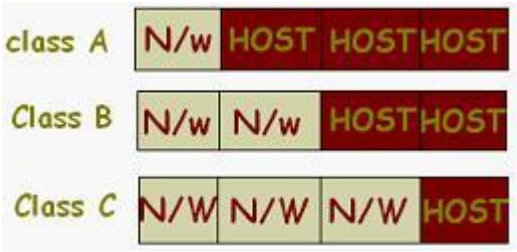
IP Address. . . . . : 213.155.55.232

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 213.155.55.232

فعلا تنها به سطر IP Address که مشخص شده است توجه کنید سایرموارد(Default Gateway, Subnet Mask) بعدا بررسی خواهد شد. ملاحظه می کنید که IP ما ۲۱۳,۱۵۵,۵۵,۲۳۲ است.

کلاس های استاندارد آدرس 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 که به شرح آنها می پردازیم .

هر آدرس IP به دو قسمت Net و Host تقسیم می‌شو د. قسمت Net بیانگر آدرس شبکه‌ای است که آدرس به آن تعلق دارد و Host هر آدرس در شبکه Net را مشخص می‌کند. ترتیب مورد استفاده برای تخصیص Net و Host به یک آدرس IP، بستگی به کلاس (Class) آن آدرس دارد.

کلاس A:

این نوع کلاس بیشتر برای تخصیص IP در شبکه‌های بزرگ مورد استفاده قرار می‌گیرد. اکتت اول این کلاس‌ها از ۱ تا ۱۲۶ متفاوت می‌باشد. از باقی اکتت‌ها برای Host استفاده می‌شود. حدود نیمی از ترکیب‌های موجود برای تمام آدرس‌های IP، در این کلاس قرار می‌گیرند. اولین رقم این آدرس‌ها در مبنای دو نیز با ۰ شروع می‌شود.

Network ID (bit): 00000000.00000000. 00000000. 00000000
Broadcast ID (bit): 01111111.11111111. 11111111. 11111111
Subnet Mask (bit): 01111111.00000000. 00000000. 00000000
First ID (bit): 00000000.00000000. 00000000. 00000001
Last ID (bit): 01111111.11111111. 11111111. 11111110

کلاس B:

معمولاً شبکه‌های متوسط از این نوع کلاس بهره می‌برند. آدرس‌هایی که اولین اکتت آن‌ها از ۱۲۸ تا ۱۹۱ تغییر می‌کند عضو این کلاس هستند. اکتت دوم این آدرس‌ها نیز برای تعیین Net، و دو اکتت دیگر برای مشخص کردن آدرس Host مورد استفاده قرار می‌گیرد. اولین رقم اولین اکتت این آدرس‌ها در مبنای دو ۱ و رقم دوم ۰ است.

Network ID (bit): 10000000.00000000. 00000000. 00000000
Broadcast ID (bit): 10111111.11111111. 11111111. 11111111
Subnet Mask (bit): 10111111.11111111. 00000000. 00000000
First ID (bit): 10000000.00000000. 00000000. 00000001
Last ID (bit): 10111111.11111111. 11111111. 11111110

کلاس C:

شبکه‌های کوچک می‌توانند از این کلاس استفاده کنند. آدرس‌های که اکتت اول آن‌ها از ۱۹۲ تا ۲۲۳ است در این کلاس قرار می‌گیرند. اکتت‌های اول تا سوم برای معین کردن آدرس Net و باقی برای تخصیص آدرس به Host مورد استفاده قرار می‌گیرد. این آدرس‌ها در مبنای دو دارای اولین رقم ۱ دومین رقم ۱ و سومین رقم ۰ است.

Network ID (bit): 11000000.00000000. 00000000. 00000000
Broadcast ID (bit): 11011111.11111111. 11111111. 11111111
Subnet Mask (bit): 11011111.11111111. 11111111. 00000000
First ID (bit): 11000000.00000000. 00000000. 00000001
Last ID (bit): 11011111.11111111. 11111111. 11111110

کلاس D:

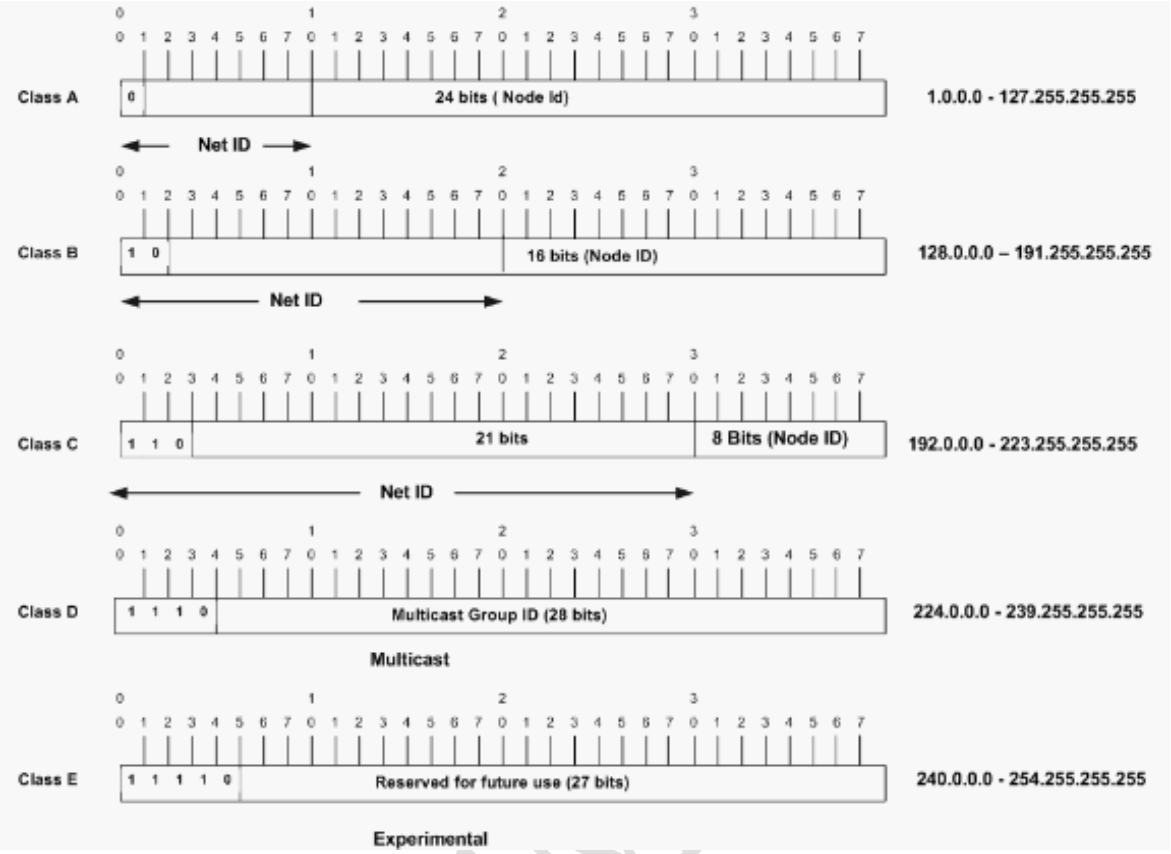
از این کلاس برای Multicast استفاده می‌شود و کمی با کلاس‌ها و آدرس‌ها قبلی تفاوت دارد. اولین، دومین و سومین بیت این آدرس‌ها با ۱ و چهارمین بیت با صفر شروع می‌شود. ۲۸ بیت بعدی برای مشخص کردن آدرس مقصد پیغام‌های Multicast مورد استفاده قرار می‌گیرد

Network ID (bit): 11100000.00000000. 00000000. 00000000
Broadcast ID (bit): 11101111.11111111. 11111111. 11111111
Subnet Mask (bit): 11101111.11111111. 11111111. 00000000
First ID (bit): 11100000.00000000. 00000000. 00000001
Last ID (bit): 11101111.11111111. 11111111. 11111110

کلاس E:

این کلاس شباهتی زیادی به کلاس D دارد و بیشتر در موارد آزمایشی مورد استفاده قرار می‌گیرد. تنها تفاوت آن با کلاس D این است که بیت چهارم آن از ۱ شروع می‌شود.

Network ID (bit): 11110000.00000000. 00000000. 00000000
Broadcast ID (bit): 11111111.11111111. 11111111. 11111111
Subnet Mask (bit): 11111111.11111111. 11111111. 00000000
First ID (bit): 11110000.00000000. 00000000. 00000001
Last ID (bit): 11111111.11111111. 11111111. 11111110



تحلیل آدرس IP

همان طور که گفته شد IP یک عدد ۳۲ بیتی است. هم اکنون این گفته را کاملتر شرح داده و مطلب را بازتر می کنیم/ درک این قسمت از مطلب نیازمند دانستن مفاهیم Bit و Byte است . این در حقیقت واحدهای اندازه گیری حافظه کامپیوتر هستند که در پایین آنها را شرح می دهیم :

BIT: به کوچکترین واحد اندازه گیری حافظه کامپیوتری می گویند.

Byte: به مجموع ۸ بیت ، یک بایت می گویند. بنابر این نتیجه می گیریم ۳۲ بیت همان ۴ بایت در مبنای اعشاری (مبنای ۱۰) است و برای این که کامپیوتر اعداد را در مبنای ۲ در نظر می گیرد آن را به صورت Binary (مبنای ۲) می نویسیم.

آی پی Loopback:

آدرس ۱۲۷.۰.۰.۱ برای عملیاتی به نام Loopback استفاده می‌شود. Loopback زمانی انجام می‌شود که یکی از کامپیوترهای میزبان بسته‌ای را برای خودش می‌فرستد. کاربرد این متد در رفع مشکل و تست اتصالات شبکه است.

Subnet Mask:

برای بدست آوردن آدرس Subnet Mask لازم است تمامی بیت های Net را یک وبیت های host را صفر نمایید.

Broadcast:

زمانی که تمامی بیت های سمت Host آدرس آی پی را یک نمایید آدرس Broadcast آن شبکه را بدست آورده اید که می توانید از این طریق پیغام‌هایی که لازم است برای تمام اعضای شبکه فرستاده شود را ارسال نمایید.

آی پی های Valid و Invalid:

IP های Valid بر خلاف آنچه تصور می شود معتبر در شبکه مورد نظر می باشند و ممکن است در شبکه دومی معتبر نباشد مثلا دو شبکه داشته باشیم که کلاینت A در شبکه اول دارای IP بصورت ۱۹۲,۱۶۸,۲۲۶,۱ باشد بنابراین این IP تنها در شبکه A معتبر است و در شبکه دومی شاید این IP به کلاینت دیگری متصل باشد.

آی پی های Public و Private:

IP های Public بر خلاف Valid در کل اینترنت معتبر است مثل IP های سایت های گوگل و.. که در هر جای دنیا، آن IP به سایت گوگل بر می گردد. این دسته از IP ها در شرکت (ANAI Authority Numbers Assigned Internet) ثبت می باشند. Private address برای تعیین شبکه های محلی استفاده می شود و برای استفاده از آنها احتیاج به هیچ مجوزی نیست.

چگونه می توان تشخیص داد ای پی عمومی است یا خصوصی ؟

برای IP های خصوصی یک رنج موجود می باشد اگر IP در آن رنج بود خصوصی است در غیر اینصورت IP عمومی است.

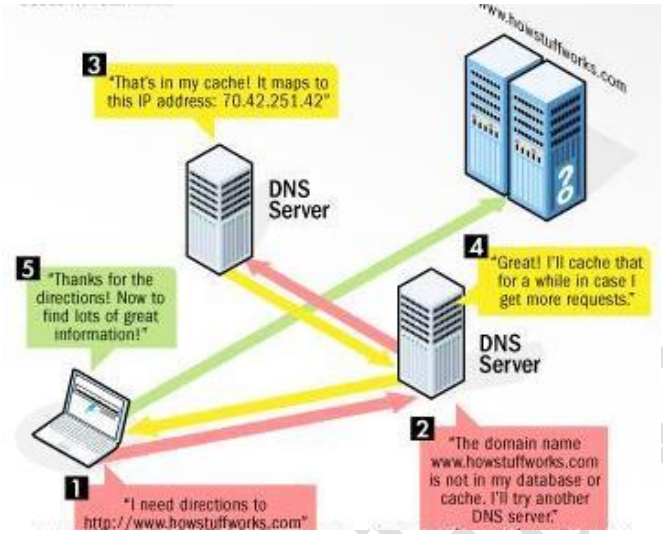
PRIVATE IP ADDRESS		
IP Class	Host IP from	Host IP To
Class A	۱۰.۰.۰.۰	۱۰.۲۵۵.۲۵۵.۲۵۵
Class B	۱۷۲.۱۶.۰.۰	۱۷۲.۳۱.۲۵۵.۲۵۵
Class C	۱۹۲.۱۶۸.۰.۰	۱۹۲.۱۶۸.۲۵۵.۲۵۵

سرویس DNS (Domain Name System)

همانطور که می دانید کلیه آدرس ها در شبکه بر مبنای IP Address است بدین معنی که جهت ورود به سایتی باید از آدرس آن سایت یا IP مربوط به آن اطلاع داشت، اما آیا واقعا ما IP مربوط به همه ی سایت هایی را که مرتب به آنها مراجعه می کنیم را حفظ هستیم؟ مثلا شما هر روز از سایت گوگل استفاده می کنید اما هر بار برای وارد شدن به گوگل به جای نوشتن google.com ، آدرس ۱۷۳,۱۹۴,۳۲,۳۳ که یکی از IP های گوگل است را در نوار آدرس می نویسید؟ خوب در این صورت ما باید بی نهایت IP رو برای وارد شدن به سایت ها حفظ کنیم ! و استفاده از اینترنت تنها برای تعداد محدودی از افراد امکانپذیر می شد ! در اینجاست که اهمیت سرویس DNS مشخص می شود.در واقع DNS، IPها را به اسم سایت ها و بالعکس ، اسامی سایت ها را به IP های آنها تبدیل می کند.یعنی شما زمانی که در نوار آدرس مرورگر خود مثلا Itpro.ir را تایپ می کنید، DNSفورا IP مربوط به این سایت را پیدا می کند و از طریق IPآن ، وارد Itpro.ir می شود .

حال این DNS Server چیست و در کجا قرار دارد؟ DSN Serverنوع به خصوصی از کامپیوتر است که معمولا به صورت پیشفرض ،شرکت ارائه دهنده ی اینترنت یا همان ISP ، IPهای DNS Serverرا در اختیار کاربران خود قرار می دهد و گاهی چون این سرویسی که در اختیار مشتریان خود قرار می دهد سرعت و کیفیت پایینی دارد سبب کند شدن سرعت در گرفتن اطلاعات می شود.از اینرو تغییر DNS پیش فرض ISP با یک DNS با کیفیت، راه حل مناسبی است.البته برای بهبود عملکرد DNS،هر کاربر پس از وارد شدن به سایتی برای اولین بار و تبدیل hostname آن سایت به IP اش ، آن IP در cache ی که مختص DNS است نگهداری می شود تا در صورتی که کاربر مجددا بخواهد از آن سایت استفاده کند،برای به دست آوردن IP ، به DNS Server مراجعه نشود و این سرعت را در شبکه بالا میبرد.

DNS Server ،اطلاعات مربوط به DNS را در تعدادی فایل که در هارددیسک سرور ذخیره می شوند،نگهداری می کند و این فایل ها مرتب به روزرسانی یا update می شوند که این باعث بهبود عملکرد و افزایش سرعت در به دست آوردن IP ها و اسامی سایت ها می شود.بدین صورت که زمانی که



شما برای اولین بار نام سایتی را وارد می کنید و DNS ، IPآن را به دست می آورد ،این IP در حافظه ی سرور آن باقی می ماند تا دفعه ی بعدکه شما خواستید مجددا از آن سایت استفاده کنید ،با داشتن IP آن در Cache مربوط به) DNS یا حافظه ی سرور)،بالا آمدن سایت سریعتر انجام شود.به شکل زیر توجه کنید

در این شکل کاربر قصد وارد شدن به سایت www.howstuffworks.com را دارد. پس از وارد کردن hostname در مرورگر خود،درخواستش به نزدیکترین DNS ارسال می شود DNS Server. در مرحله ۲ می گوید که "من IP متناظر با این hostname را در cache خود ندارم پس اجازه بده از یک سرور دیگر برایت بگیرم ".سپس درخواست به Server DNS در مرحله ۳ ارسال می شود IP .مورد نظر ما آنجا وجود دارد.درمحله ی بعد این IP ابتدا در cache مربوط به DNS مرحله ی ۲ ذخیره می شود تا در دفعات بعدی اگر کاربر مجددا خواست از این سایت استفاده کند ، دسترسی به این IP با یک مرحله کمتر انجام شود و سپس IP برای کاربر ارسال و کاربر می تواند وارد سایت مورد نظر خود شود .

DNSاز دو قسمت تشکیل شده است :Forward lookup zone و Reverse lookup zone که هر کدام وظیفه ی خاصی دارند.در Forward lookup zone ، IP ها به اسامی تبدیل می شوند و در Reverse lookup zone اسامی به IP ها ترجمه می گردند.

سرویس DHCP (Dynamic Host Configuration Protocol)

DHCP یکی از سرویس های بیسار مهم و پرکاربرد کامپیوتری می باشد که امکان تعریف IP address ، آدرس subnet mask، default gateway و آدرس DNS و دیگر تنظیمات برای هر سیستم را به طور اتوماتیک فراهم آورده است.

به عنوان مثال زمانی که یک PC می خواهد به اینترنت وصل شود، تقاضای IP آدرس خود را به صورت Broadcast درون شبکه ارسال می کند، اولین DHCP server ی که درخواستش را گرفت به آن PC یک IP برای دسترسی به اینترنت اختصاص می دهد. PC، IP یی که DHCP server

برایش ارسال کرده دریافت می کند و می پذیرد و در پاسخ به DHCP server ، یک پیغام قبول درخواست ارسال می کند.DHCP server با گرفتن این پیغام یک acknowledgement را به همراه دیگر آدرس ها و تنظیمات مورد نیاز PC (subnet mask address، DNS و ..) برایش ارسال می نماید. این پروسه که طی ۴ مرحله انجام می شود به صورت زیر می باشد:

همانطور که مشاهده می کنید در مرحله ی اول PC یا Discover با ارسال یک broadcast به جستجوی یک DHCP Server می پردازد. در مرحله ی دوم که به آن offer نیز می گویند، DHCP با معرفی خود به PC ، یک آدرس IP به آن می دهد. در مرحله ی سوم PC ، Request آن IP را می پذیرد و از DHCP تقاضای IP های دیگر برای دیگر تنظیماتش می کند.در مرحله ی آخر DHCP acknowledgement با ارسال acknowledge اطلاعات دریافت شده را تایید و دیگر اطلاعات مورد نیاز PC را برایش ارسال می کند. لازم به ذکر است که این سرویس از پورتهای ۶۸ و ۶۹ استفاده می نماید.

ساب‌نتیگ Subnetting

در این حالت با استفاده از یکی از آدرس های کلاس A یا B یا C ما میتوانیم به بیش از یک NET ID دست پیدا کرده و در همان آدرس با طبقه بندی بیش از یک Subnet ارتباطات را از هم جدا کنیم، به عنوان مثال شما پس از استفاده از Net Id 192.168.100.0 در کلاس C فقط میتوانید در یک طبقه بندی بین آدرس های ۱۹۲,۱۶۸,۱۰۰,۱ ~ ۱۹۲,۱۶۸,۱۰۰,۲۵۴ آدرس دهی کرده و ارتباطات مسقیم را پیاده سازی نمائید. حال انکه فرض کنید شما میخواهید با خرد کردن رنج آدرس های فوق از ارتباط بین دو نود ۱۹۲,۱۶۸,۱۰۰,۱۳۰ و ۱۹۲,۱۶۸,۱۰۰,۱۰ به صورت مستقیم جلوگیری کرده و با عبور ترافیک آنها به صورت غیر مستقیم با استفاده از روتر اطلاعات جابجا شده بین آنها را کنترل نمائید برای رسیدن به هدف بالا میبایست با استفاده از IP Subnetting یک رنج آدرس کلاس C را به دوطبقه بندی تقسیم کرده و ارتباط مستقیم بین طبقه بندی اول و دوم را قطع نمائید. برای شروع عملیات Subnetting ما تعدادی بیت یک به استاندارد Subnet mask اضافه می نمائیم:

۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰ ۲۵۵.۲۵۵.۰.۰

۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۰۰۰.۰۰۰۰۰۰۰۰ ۲۵۵.۲۵۵.۲۴۸.۰

----------|YYYYY|----------

Y=Subnetting ID

مثال ۱:

شبکه آدرس دهی بر اساس آدرس ۱۹۲,۱۶۸,۱۰۰,۰ را به دو شبکه منطقی تقسیم کرده و رنج هریک را محاسبه نمائید. با استفاده از فرمول زیر تعداد بیت هائی که می بایست به subnet mask اضافه نمود را بدست آورید:

(#Subnetting bit)>=#subnet) ۲^ تعداد شبکه مورد نیاز در تقسیم)

y=1 <= ۲=<y^۲ تعداد بیت برای Subnetting ID

۱	IP Address	۱۹۲.	۱۶۸.	۱۰۰.	۰	
۲	Default Subnet Mask ((Decimal	۲۵۵.	۲۵۵.	۲۵۵.	۰	
۳	Default Subnet Mask: Binary	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	۰۰۰۰۰۰۰۰	= ۲۵۵.۲۵۵.۲۵۵.۰
۴	Subnetted Subnet Mask: Binary	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	۱۰۰۰۰۰۰۰	=۲۵۵.۲۵۵.۲۵۵.۱۲۸

۵	Default IP NetID	۱۱۰۰۰۰۰۰.	۱۰۱۰۱۰۰۰.	۰۱۱۰۰۱۰۰.		
۶	Subnetted IP NetID	۱۱۰۰۰۰۰۰.	۱۰۱۰۱۰۰۰.	۰۱۱۰۰۱۰۰.	V	
					V=0 or 1	
۷	NetID Range01	۱۱۰۰۰۰۰۰.	۱۰۱۰۱۰۰۰.	۰۱۱۰۰۱۰۰.	۰	
۸	NetID Range02	۱۱۰۰۰۰۰۰.	۱۰۱۰۱۰۰۰.	۰۱۱۰۰۱۰۰.	۱	
۹	Range01	۱۱۰۰۰۰۰۰.	۱۰۱۰۱۰۰۰.	۰۱۱۰۰۱۰۰.	۰۰۰۰۰۰۰۰	۱۹۲.۱۶۸.۱۰۰.۰
۱۰		۱۱۰۰۰۰۰۰.	۱۰۱۰۱۰۰۰.	۰۱۱۰۰۱۰۰.	۰۱۱۱۱۱۱۱	۱۹۲.۱۶۸.۱۰۰.۱۲۷
۱۱	Range02	۱۱۰۰۰۰۰۰.	۱۰۱۰۱۰۰۰.	۰۱۱۰۰۱۰۰.	۱۰۰۰۰۰۰۰	۱۹۲.۱۶۸.۱۰۰.۱۲۸
۱۲		۱۱۰۰۰۰۰۰.	۱۰۱۰۱۰۰۰.	۰۱۱۰۰۱۰۰.	۱۱۱۱۱۱۱۱	۱۹۲.۱۶۸.۱۰۰.۲۵۵

در نتیجه از ۲۴/۱۹۲,۱۶۸,۱۰۰,۰ به ۲۵/۱۹۲,۱۶۸,۱۰۰,۰ و ۲۵/۱۹۲,۱۶۸,۱۰۰,۱۲۸ تبدیل می شود ﴿عدد ۲۴/ و ۲۵/ ، CIDR نام دارد (در ادامه بدان می پردازیم) و نشان دهنده تعداد بیت های استفاده شده در Subnet می باشد ۲۵/ یعنی ۳ تا ۸ تا که همان ۳ octet اول است و یک بیت هم از octet آخر که می شود ۲۵ که در مقدار دهدهی subnet جای همه یک می گذاریم)

در اصل مدل IP فوق یعنی ۱۹۲,۱۶۸,۱۰۰,۰ (سطر اول فوق) از نوع کلاس C می باشدکه دارای Subnet پیش فرض ۲۵۵,۲۵۵,۲۵۵,۰ است (سطر دوم) لذا از سه قسمت اول subnet 24 بیت (۳ تا ۸ بیت) و چون به دو قسمت قرار است تقسیم گردد طبق فرمول y=1 <= ۲=<y^۲ یک بیت دیگر نیز نیاز است که این بیت از قسمت چهارم استفاه می شود که این یک بیت ۲۵ ام نیز دارای ارزش یک می گردد لذا Subnet مورد نیاز برابر می گردد با ۲۵۵,۲۵۵,۲۵۵,۱۲۸ (سطر سوم) (بخش آخر ۱۰۰۰۰۰۰۰معادل است با ۱*۱۲۸+۰*۶۴+۰*۳۲+۰*۱۶+۰*۸+۰*۴+۰*۲+۰*۱ = ۱۲۸- اگر دو بیت بود می شد ۱۱۰۰۰۰۰۰ که معادل است با ۱۲۸+۶۴=۱۹۲ و الی آخر) -

در مر حله بعد و اخر رنج IP های مورد نیاز با استفاده از تعداد بیت متغیر مورد نیاز و بر اساس IP اصلی بدست می آید که مثلا در اینجا که یک بیت اول از Octet آخر آن نیز (همان یک بیت که گفته شد برای تغییرات بدان نیازمندیم) بین ۰ و ۱ متغیر است (اگر دو بیت نیاز بود آن دو بیت بین ۰ و ۱ تغییر می کند که حالات ۰۰ – ۰۱ – ۱۰ – ۱۱ را شامل می گردد.) پس رنج IPامی شد سطر های ۷ یا ۸ و حد اقل و حداکثر هرکدام نیز با قرار دادن تمام بیت ها با ارزش ۰ و تمام بیت های مابقی با ارزش ۱ بدست می آید (سطر۹ و ۱۰ برای رنج اول و حالت xxxxxxx۰ از Octet آخر و سطر ۱۱ و ۱۲ برای حالت xxxxxxx۱ از octet آخر).

باید توجه داشت که اولین آدرس نشانی شبکه و آخرین نشانی همه پخشی (Broadcast) شبکه مورد نظر است که با تر کیب منطقی حالت باینری هر آدرس شبکه با subnet مربوط ان بدست می آید.

یکی از IP های شبکه اصلی	۰	۱۰۰.	۱۶۸.	۱۹۲.	IP Address
	۰	۲۵۵.	۲۵۵.	۲۵۵.	Default Subnet Mask (Decimal)
	۰۰۰۰۰۰۰۰	۰۱۱۰۰۱۰۰.	۱۰۱۰۱۰۰۰.	۱۱۰۰۰۰۰۰.	IP Address (Binary
	۰۰۰۰۰۰۰۰	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	Default Subnet Mask (Binary)
	۰۰۰۰۰۰۰۰	۰۱۱۰۰۱۰۰.	۱۰۱۰۱۰۰۰.	۱۱۰۰۰۰۰۰.	IP AND Subnet
نتیجه: NET IP Address=192.168.100.0 , Broadcast IP Address=192.168.100.255					
شبکه تفکیک شده اول					
یکی از IP های شبکه اول	۵۰	۱۰۰.	۱۶۸.	۱۹۲.	IP Address (Subnet 1 ۲)
	۱۲۸	۲۵۵.	۲۵۵.	۲۵۵.	Default Subnet Mask (Decimal)
	۰۰۱۱۰۰۱۰	۰۱۱۰۰۱۰۰.	۱۰۱۰۱۰۰۰.	۱۱۰۰۰۰۰۰.	IP Address (Binary
	۱۰۰۰۰۰۰۰	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	Default Subnet Mask (Binary)
	۰۰۰۰۰۰۰۰	۰۱۱۰۰۱۰۰.	۱۰۱۰۱۰۰۰.	۱۱۰۰۰۰۰۰.	IP AND Subnet
نتیجه: NET IP Address=192.168.100.0 , Broadcast IP Address=192.168.100.127					
یکی از IP های شبکه دوم	۱۷۰	۱۰۰.	۱۶۸.	۱۹۲.	IP Address (Subnet 1 ۲)
	۱۲۸	۲۵۵.	۲۵۵.	۲۵۵.	Default Subnet Mask (Decimal)
	۱۰۱۰۱۰۱۰	۰۱۱۰۰۱۰۰.	۱۰۱۰۱۰۰۰.	۱۱۰۰۰۰۰۰.	IP Address (Binary
	۱۰۰۰۰۰۰۰	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	۱۱۱۱۱۱۱۱.	Default Subnet Mask (Binary)
	۱۰۰۰۰۰۰۰	۰۱۱۰۰۱۰۰.	۱۰۱۰۱۰۰۰.	۱۱۰۰۰۰۰۰.	IP AND Subnet
نتیجه: NET IP Address=192.168.100.128 , Broadcast IP Address=192.168.100.255					
تعریف اعمال منطقی AND	0 AND 1=0 / 0 AND 0= 0 / 1 AND 1 =1 / ۱ □□□ ۰ = ۰				
تعریف اعمال منطقی OR	0 OR 1=1 / 0 OR 0= 0 / 1 OR 1 =1 / ۱ □□ ۰ = ۱				
تعریف اعمال منطقی XOR	0 XOR 1=1 / 0 XOR 0= 0 / 1 XOR 1 =0 / ۱ □□□ ۰ = ۱				

مثال ۲:

تقسیم یک شبکه بفرم کلی ۲۴/۱۹۲,۱۶۸,۲۲۶,۰ به ۶ شبکه مستقل که یکدیگر را Pingنکنند (همدیگر را نبینند)

در این مورد با توجه به اینکه ۲^۳>۶ است لذا به ۳ بیت اضافی نیازمندیم و چون کلاس آدرس اصلی از نوع Cاست لذا subnetاصلی ۲۵۵,۲۵۵,۲۵۵,۰می باشدپس subnet جدید عبارتست از :

۲۵۵.۲۵۵.۲۵۵.۲۲۴ (۱۲۸+۶۴+۳۲=۲۲۴) = ۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۰۰۰۰۰

لذا رنج IPهای جدید بصورت زیر بدست می آید

با ۳ بیت می توان ۸ حالت بر اساس ۰ و ۱ داشت ۰۰۰-۰۰۱-۰۱۰-۰۱۱-۱۰۰-۱۰۱-۱۱۰-۱۱۱ لذا بر اساس IP داده شده داریم:

IP = 11000000.10101000.11100010.00000000 =192.168.226.0 اصلی

(۱۹۲.۱۶۸.۲۲۶.۰ ---۱۹۲.۱۶۸.۲۲۶.۳۱) ۱۱۰۰۰۰۰۰.۱۰۱۰۱۰۰۰.۱۱۱۰۰۰۱۰.۰۰۰۰۰۰۰۰ =۱۹۲.۱۶۸.۲۲۶.۰/۲۷

(۱۹۲.۱۶۸.۲۲۶.۳۲ ---۱۹۲.۱۶۸.۲۲۶.۶۳) ۱۱۰۰۰۰۰۰.۱۰۱۰۱۰۰۰.۱۱۱۰۰۰۱۰.۰۰۱۰۰۰۰۰ =۱۹۲.۱۶۸.۲۲۶.۳۲/۲۷

(۱۹۲.۱۶۸.۲۲۶.۶۴ ---۱۹۲.۱۶۸.۲۲۶.۹۵) ۱۱۰۰۰۰۰۰.۱۰۱۰۱۰۰۰.۱۱۱۰۰۰۱۰.۰۱۰۰۰۰۰۰ =۱۹۲.۱۶۸.۲۲۶.۶۴/۲۷

(۱۹۲.۱۶۸.۲۲۶.۹۶ ---۱۹۲.۱۶۸.۲۲۶.۱۲۷) ۱۱۰۰۰۰۰۰.۱۰۱۰۱۰۰۰.۱۱۱۰۰۰۱۰.۰۱۱۰۰۰۰۰ =۱۹۲.۱۶۸.۲۲۶.۹۶/۲۷

(۱۹۲.۱۶۸.۲۲۶.۱۲۸ ---۱۹۲.۱۶۸.۲۲۶.۱۵۹) ۱۱۰۰۰۰۰۰.۱۰۱۰۱۰۰۰.۱۱۱۰۰۰۱۰.۱۰۰۰۰۰۰۰ =۱۹۲.۱۶۸.۲۲۶.۱۲۸/۲۷

(۱۹۲.۱۶۸.۲۲۶.۱۶۰ ---۱۹۲.۱۶۸.۲۲۶.۱۹۱) ۱۱۰۰۰۰۰۰.۱۰۱۰۱۰۰۰.۱۱۱۰۰۰۱۰.۱۰۱۰۰۰۰۰ =۱۹۲.۱۶۸.۲۲۶.۱۶۰/۲۷

(۱۹۲.۱۶۸.۲۲۶.۱۹۲ ---۱۹۲.۱۶۸.۲۲۶.۲۲۳) ۱۱۰۰۰۰۰۰.۱۰۱۰۱۰۰۰.۱۱۱۰۰۰۱۰.۱۱۰۰۰۰۰۰ =۱۹۲.۱۶۸.۲۲۶.۱۹۲/۲۷

(۱۹۲.۱۶۸.۲۲۶.۲۲۴ ---۱۹۲.۱۶۸.۲۲۶.۲۵۵) ۱۱۰۰۰۰۰۰.۱۰۱۰۱۰۰۰.۱۱۱۰۰۰۱۰.۱۱۱۰۰۰۰۰ =۱۹۲.۱۶۸.۲۲۶.۲۲۴/۲۷

که ۶ قسمت اول بکار این مثال می آید و دوتای آخر اضافی می ماند.

دستورات شبکه در CMD (Command Prompt)

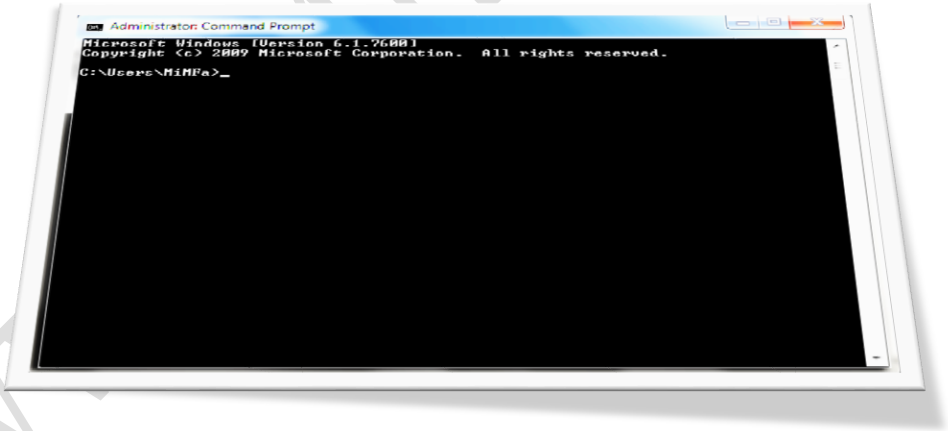
سیستم عامل ها امروزه برای آسان کردن انجام کارها برخلاف گذشته که فقط دارای رابط کاربری متنی بودند از یک رابط کاربری گرافیکی (Graphic User Interface / GUI) نیز استفاده می کنند که کار با آن برای هرکس آسان و قابل انجام است.

اما رابطهای متنی هنوز در سیستم عاملها باقی مانده و بسیاری از کارها در آن انجام داده می شود. در رابطهای متنی مانند Terminal در لینوکس و CMD در ویندوز کاربران به جای استفاده از اشیا باید از دستور نویسی استفاده کنند که شاید حرفه ای تر و در بعضی مواقع مخصوصا جهت انجام برخی کارهای خاص شبکه ای، برخلاف ظاهر، بسیار آسانتر باشد.

برای وارد شدن به محیط CMD از دو روش متداول می توان استفاده نمود:

روش اول: به منوی Start/All Programs/Accessories رفته و سپس Command Prompt را اجرا کنید.

روش دوم: کلیدهای Win+R را زده تا وارد Run شوید سپس در کادر متنی cmd را تایپ کرده و



با زدن OK برنامه خط فرمان اجرا خواهد شد.

دراین درس ما فرض را براین می گیریم که شما با اصل برنامه CMD آشنایی کافی دارید.

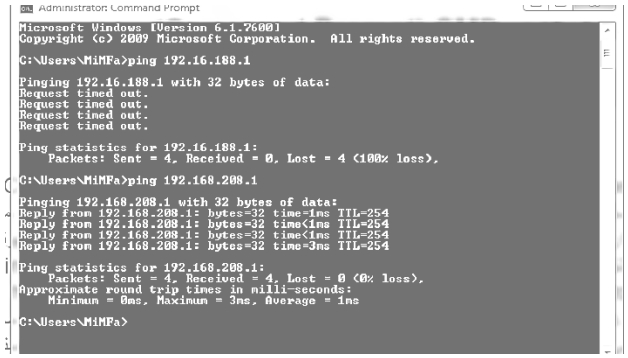
برخی از دستورات شبکه در CMD:

- دستور ARP : این دستور در بیشتر موارد برای چک کردن وضعیت ارتباطات اترنت و IP در شبکه استفاده می شود .

- دستور IPConfig : برای انجام تنظیمات و چک کردن کلیه کارت های شبکه استفاده می شود .
- دستور Netstat : خلاصه ای از وضعیت اتصالات شبکه و وضعیت سوکت های را نشان می دهد.
- دستور NSLookup : برای چک کردن نام دامین (domain) و اطلاعات IP یک سرور استفاده می شود .
- دستور PING : این دستور با ارسال چندین بسته (packet) تست ، ارتباط شبکه ای بین چند نقطه را تست می کند .
- دستور PS: لیست تمام پردازشهای موجود بر روی سرور را نشان می دهد .
- دستور Route : تمامی routing table های موجود بر روی سرور را نشان می دهد .
- دستور Shred : حذف نمودن ایمن فایل ها بوسیله چندین بار بازنویسی اطلاعات بر روی دیسک بصورتی که قابل بازیابی نباشند
- دستور Tracert : تست کردن مسیر گذر کردن یک بسته (packet) از یک مبدا به یک مقصد .

در ادامه به توضیح برخی از این دستورات خواهیم پرداخت.

دستور PING



دستور Ping یا Packet Internet Group از ساده ترین و کاربردی ترین ابزارهای خطایابی قابل دسترس TCP/IP است. این کامند برای تست اتصال یک دستگاه یا سیستم به سیستم های دیگر و تایید فعال بودن سیستم مقصد استفاده می شود.همچنین برای بررسی برقراری ارتباط با یک host در شبکه نیز از این کامند استفاده می شود.زمانی که بین دو کامپیوتر مشکل برقراری اتصال وجود داشته باشد،استفاده از این کامند اولین قدم در پیدا کردن هرگونه خطا در این زمینه است. Ping از پروتکل ICMP یا Internet Control Message Protocol برای بررسی برقراری اتصال با یک host یا remote host استفاده می کند.درواقع این کامند با ارسال درخواست (request) به مقصد،منتظر پاسخ (reply) می ماند و دریافت پاسخ از مقصد به معنی وجود ارتباط می باشد. د رمواردی که در برقراری اتصال به اینترنت دچار مشکل هستیم باید مراحل زیر را با استفاده از دستور ping طی کنیم .طی کردن این موارد باعث می شود متوجه شویم گره کار در کدام قسمت است.

اجرای دستور PING:

ابتدا برقراری اتصال سیستم خود را با شبکه از طریق ping 127.0.0.1 چک می کنیم.در صورتی که به درخواست ما (request) پاسخ داده شود (reply) پس مشکل از سیستم ما نمی باشد.

Ping IP Address of local host

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

سپس شبکه داخلی را تست می کنیم. برای این منظور یکی از کامپیوترهای دیگری که در شبکه محلی ما (local network) قرار دارد را ping می کنیم.

Ping IP Address of local network

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time<4ms TTL=64

Reply from 192.168.0.2: bytes=32 time<4ms TTL=64

Reply from 192.168.0.2: bytes=32 time<4ms TTL=64

Reply from 192.168.0.2: bytes=32 time<4ms TTL=64

Ping statistics for 192.168.0.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

اگر در مرحله ی قبل نیز مشکلی نداشتیم default gateway را ping می کنیم .اینکار را با کامند زیر انجام می دهیم.با این کامند اتصال default gateway را با اینترنت بررسی می کنیم .در صورتی که از این کامند پاسخی (reply) گرفتیم پس در برقراری اتصال default gateway با اینترنت مشکلی نداریم.

Ping IP Address of default gateway

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<4ms TTL=64

Reply from 192.168.0.1: bytes=32 time<4ms TTL=64

Reply from 192.168.0.1: bytes=32 time<4ms TTL=64

Reply from 192.168.0.1: bytes=32 time<4ms TTL=64

Ping statistics for 192.168.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

در مرحله ی آخر برای بررسی برقراری ارتباط ، یک remote host (یا مثلا یک سایت مثل سایت yahoo.com) را ping می کنیم تا برقراری ارتباط با روترهای در مسیر را چک کنیم.

Ping IP Address of remote host

Pinging itpro.ir [62.193.15.162] with 32 bytes of data:

Reply from 62.193.15.162: bytes=32 time=150ms TTL=116

Reply from 62.193.15.162: bytes=32 time=153ms TTL=116

Reply from 62.193.15.162: bytes=32 time=149ms TTL=116

Reply from 62.193.15.162: bytes=32 time=154ms TTL=116

Ping statistics for 62.193.15.162:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 406ms, Maximum = 457ms, Average = 423ms

در طی این چهار مرحله می توان قدم به قدم صحت برقراری ارتباط را در هر سطح چک کرد و بدین صورت مشکل شبکه را خطایابی نمود.

سوئیچ های دستور PING:

دستور ping ،زیرمجموعه های (switch) زیادی دارد .با وارد کردن عبارت ping/? در command prompt ،کلیه ی زیرمجموعه ی این کامند را می توان مشاهده کرد. که در اینجا به چند نمونه از آن اشاره :

a- : تبدیل آدرس IP به نام آن

f- : با نوشتن این عبارت ،از قطعه قطعه کردن بسته های ارسالی توسط روترها و getway ها ، جلوگیری می شود.

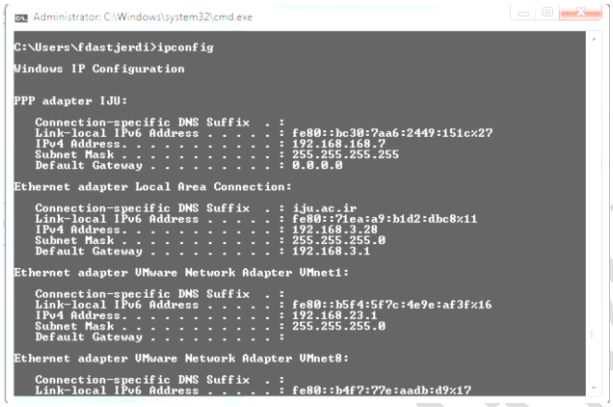
i- : تعیین مقدار یا ظرفیت داده های ارسالی در یک packet ،این مقدار به صورت پیش فرض ۳۲ بایت است و حداکثر تا ۶۵۵۰۰ بایت می تواند ظرفیت داشته باشد.

n count- : تعیین تعداد درخواستهای ارسالی که به صورت پیش فرض ۴ است.

دستور HPING

همانطور که گفته شد دستور ping از پروتکل ICMP استفاده می کند،پس در مواردی که پورتهای این پروتکل در فایروال بسته باشد استفاده از این دستور امکانپذیر نمی باشد ! انواع دیگری از این دستور وجود دارد که قابلیت ها و انعطاف پذیری بیشتری در استفاده از این دستور را به ما می دهد مانند Hping و ورژن جدیدترش Hping2 . Hping2 بیشتر مورد استفاده قرار می گیرد چرا که در این کامند به جای استفاده از پروتکل ICMP ،از پروتکل TCP استفاده می شود.پس دیگر نگرانی در استفاده از این کامند وجود نخواهد داشت چرا که هر زمان که خواستید می توانید از این کامند استفاده نمایید.

دستورIPConfig



Ipconfig یکی دیگر از دستورات کاربردی شبکه در سیستم عمل ویندوز است که برای نمایش اطلاعات مربوط به پروتکل TCP/IP استفاده می شود. با استفاده از این دستور شما می توانید تنظیمات دیگری که مربوط به IP می باشند را مشاهده فرمایید مانند اطلاع از نوع سرور DNS مورد استفاده. با این دستور می توانید MAC address یا همان آدرس فیزیکی مربوط به کارت شبکه ی خود را نیز مشاهده نمایید.اگر بیش از یک کارت شبکه موجود باشد،این دستور اطلاعات مربوط به هر کارت شبکه را به طور جداگانه نمایش می دهد .اگر از این کامند به تنهایی و بدون سوئیچ استفاده نمایید، اطلاعات نمایش داده به شما شامل IP Address ، subnet mask و default getway می باشد اما اگر ipconfig را با سوئیچ /all استفاده فرمایید، تمامی اطلاعات و تنظیمات موجود پروتکل TCP / IP نمایش داده می شود. در ادامه مثالی از کاربرد دستور ipconfig بدون سویچ های اضافی را مشاهده می فرمایید.

اجرای دستور IPConfig:

```
ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix:

   IPv4 Address. . . . . : 192.168.1.3

   Subnet Mask . . . . . : 255.255.255.0

   Default Gateway . . . . . : 192.168.1.1

Ethernet adapter VMware Network Adapter VMnet1:
```

```
   Connection-specific DNS Suffix :
   Link-local IPv6 Address . . . . . : fe80::d826:ecc1:b3f5:755
   IPv4 Address. . . . . . . . . . . : 192.168.179.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway. . . . . .
Ethernet adapter VMware Network Adapter VMnet8:
   Connection-specific DNS Suffix:
   Link-local IPv6 Address . . . . . : fe80::49c3:c9db:dbd4:a87
   IPv4 Address. . . . . . . . . . . : 192.168.94.1
```

سویچ های دستور IPConfig:

Ipconfig /all : اجرای این دستور در command prompt خروجی مانند خروجی زیر را به کاربر نمایش می دهد.همانطور که مشاهده می کنید hostname ، IP address، MAC address، DNS Serverو IP address مربوط به DHCP server که به سیستم شما IP addressمی دهد نیز نمایش داده شده است . در ادامه مثالی از کاربرد این دستور با استفاده از سویچ /allرا مشاهده می فرمایید :

```
ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : V
   Primary Dns Suffix. . . . . .
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
Wireless LAN adapter Wireless Network Connection:
   Connection-specific DNS Suffix: .
   Description . . . . . . . . . . . : Atheros AR9287 Wireless Network Adapte
   Physical Address. . . . . . . . . : 78-DD-٠٨-D-CA-0C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred(
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained . . . . . . . . . . : الخميس, أوت ١٦, ٢٠١٢ ٠٩:٢٣:٥١ ق.ظ
   Lease Expires . . . . . . . . . . : الجمعة, أوت ١٧, ٢٠١٢ ٠٩:٢٤:٠٢ ق.ظ
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

DNS Servers . . . . . : 192.168.1.1

NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix: .

Description . . . . . : VMware Virtual Ethernet Adapter for VM

Physical Address. . . . . : 00-50-۵۶-□۰-۰۰-۰۱

DHCP Enabled. . . . . : No

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::d826:ecc1:b3f5:۷۵۵□٪۱۸(□□□□rred

IPv4 Address. . . . . : 192.168.179.1(Preferred(

Subnet Mask . . . . . : 255.255.255.0

Default Gateway: . . . . . .

DHCPv6 IAID . . . . . : 637554774

DHCPv6 Client DUID. . . . . : 00-0۱-۰۰-۰۱-۱۴-۴□-۴۶-۵۷-۵۴-۴۲-۴۹-□۹-۳□

DNS Servers . . . . . : fec0:0:0:ffff::1%1

fec0:0:0:ffff::2%1

fec0:0:0:ffff::3%1

NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix: .

Description . . . . . : VMware Virtual Ethernet Adapter for VM 8

Physical Address. . . . . : 00-50-۵۶-□۰-۰۰-۰۸

DHCP Enabled. . . . . : No

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::49c3:c9db:dbd4:a879%19(Preferred

IPv4 Address. . . . . : 192.168.94.1(Preferred(

Subnet Mask . . . . . : 255.255.255.0

Default Gateway: . . . . . .

DHCPv6 IAID . . . . . : 654331990

DHCPv6 Client DUID. . . . . : 00-0۱-۰۰-۰۱-۱۴-۴□-۴۶-۵۷-۵۴-۴۲-۴۹-□۹-۳□

DNS Servers . . . . . : fec0:0:0:ffff::1%1

fec0:0:0:ffff::2%1

fec0:0:0:ffff::3%1

NetBIOS over Tcpip. . . . . : Enabled

یکی از ویژگی های ipconfig ارائه قابلیت هایی در خصوص DHCP می باشد.

ipconfig با سوئیچ های release و renew ، به کاربر اجازه ی کنترل عملکرد DHCP را می دهد.سوئیچ release/، آی پی های اختصاص داده شده به سیستم شده را آزاد می کند .درواقع به صورت پیش فرض ،این سوئیچ همه ی IP های اختصاص داده شده به سیستم را از همه ی کارت شبکه های یک سیستم، که برای DHCP استفاده می شوند، آزاد می کند. با مشخص کردن نام کارت شبکه بعد از ذکر سوئیچ ، تغییرات تنها بر روی کارت شبکه تعیین شده، اعمال می گردد. این سوئیچ زمانی که شما با DHCP مشکل پیدا کرده اید بسیار کاربرد دارد، مانند اینکه متوجه شده اید که آدرسی که دریافت می کنید، از DHCP server اشتباهی می باشد یا زمانی که در IP یی که دریافت کرده اید ناسازگاری یا ناهماهنگی وجود دارد.

سوئیچrenew/ به DHCP server درخواستی می فرستد و تقاضای IP جدید می کند.مانند سوئیچ قبلی ، می توان نام یک کارت شبکه خاص را برای گرفتن IP جدید،در ادامه ی renew/ افزود.این زمانی که یک کارت شبکه برای گرفتن یک IP جدید از DHCP ،راه اندازی شده باشد جواب می دهد.

Ipconfig سوئیچ هایی برای خطایابی DNS نیز ارائه می دهد.این سوئیچ ها عبارتند از :

ipconfig /flushdns

ipconfig /displaydns

ipconfig /flushdns: زمانی که dns یک hostname را به IP تبدیل می کند،برای مدت زمانی نتیجه ی این تبدیل را در cache خود ذخیره می کند که اگر کاربر مجددا قصد استفاده از آن آدرس را داشت،برای تبدیل مجدد آن نیازی به مراجعه ی دوباره به سرور DNS نباشد.حال اگر مشکلی در DNS cache وجود داشته باشد ، برای پاک کردن این cache می توان از این سوئیچ استفاده کرد.ipconfig / displaydns:برای مشاهده محتویات cache DNS از این سوئیچ استفاده می کنیم. لازم به ذکر است که Ifconfig دستور معادل ipconfig در لینوکس است. در ادامه مثالی از استفاده از این دو سویچ مهم در رفع اشکال را مشاهده خواهید نمود.

استفاده از ipconfig /displaydns برای مشاهده کش DNS

```
ipconfig /displaydns
Windows IP Configuration

    parsgo.com
    ----------------------------------------
    Record Name . . . . .  parsgo.com
    Record Type . . . . . : 5
```

Time To Live . . . . : 206

Data Length . . . . . : 8

Section . . . . . : Answer

CNAME Record . . . . : mail.parsgo.com

Myadmin.void.search.com

Name does not exist

mail.google.com

Record Name . . . . . : mail.google.com

Record Type . . . . . : 5

Time To Live . . . . : 87

Data Length . . . . . : 8

Section . . . . . : Answer

CNAME Record . . . . : googlemail.l.google.com

vaiogatenotifications2.sony-europe.com

Name does not exist

استفاده از دستور ipconfig /registerdns برای ثبت اطلاعات نام کامپیوتر در dns سرور :

ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has b

een initiated. Any errors will be reported in the Event Viewer in 15 minutes.

استفاده از دستور ipconfig /release برای رها کردن آدرس IP کنونی :

ipconfig /release

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

Media State . . . . . : Media disconnected

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix: .

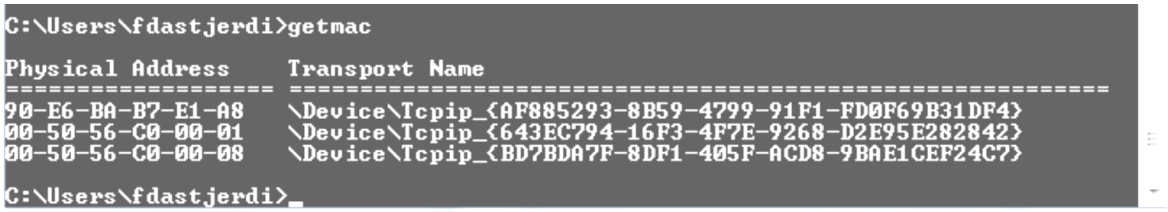
IP Address. . . . . : 0.0.0.0

Subnet Mask . . . . . : 0.0.0.0

Default Gateway: . . . . . .

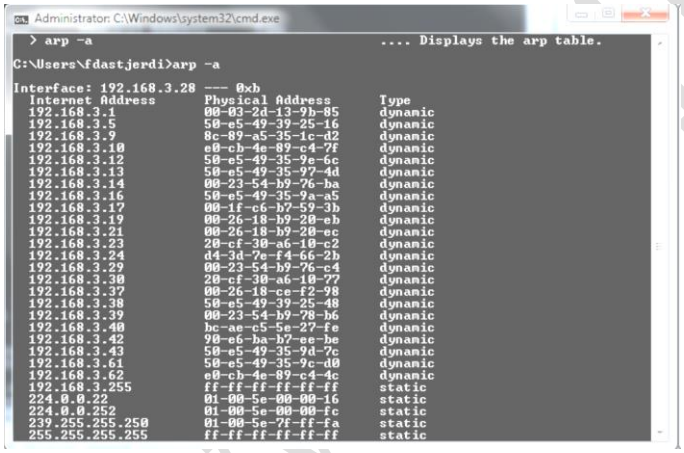
دستور GetMAC

یکی دیگر از روش های بدست آوردن آدرس مک سیستم مورد نظر وارد نمودن دستور Getmac می باشد که از آن طریق لیستی از آدرس های مک هر کدام از Interface های خروجی دستگاه اعم از



وایرلس، LAN و ... را برای شما نمایش می دهد. نکتها قابل توجه این است که این دستور از وضعیت Connevted یا Disconnected آن درگاه نیز شما را مطلع می سازد.

دستورARP



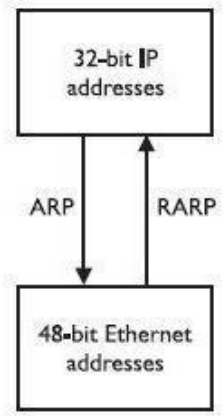
همانطور که در مطالب فوق اشاره شد، کارت شبکه یک آدرس سخت افزاری دارد که بر روی آن حک شده است. زمانیکه یک سیستم با سیستم دیگری می خواهد ارتباط برقرار نماید، باید از IP مربوط به hostسیستم مقابل مطلع باشد. این روالی است که با آن آشنا شده اید. اما در پشت پرده اتفاق دیگری می افتد، در واقع سیستم باید برای دریافت و ارسال داده از آدرس سخت افزاری یا همان MAC Address استفاده نماید. حال سوالی که پیش می آید این است که یک سیستم از کجا آدرس MAC سیستم های دیگر که می خواهد از طریق شبکه با آنها ارتباط برقرار کند را پیدا می نماید؟پاسخ چیزی جز ARP نمی باشد. در واقع ARP یا Address Resolution Protocol برای تبدیل آدرس های منطقی TCP/IP به آدرس های فیزیکی MAC طراحی شده است.حال این پروسه، یعنی تبدیل آدرس منطقی (از لایه ی ۳ به آدرس MAC در لایه ی ۲) که از طریق ارسالbroadcasting در داخل شبکه انجام می شود. بدین صورت عمل می کند که گویا کامپیوتر ارسال کننده در داخل شبکه فریاد می زند که " این آدرس IPمتعلق به چی کسی است؟ من آدرس MAC تورا نیاز دارم ! ".

Broadcast به داخل شبکه فرستاده می شود و همه ی host ها و data های broadcast را دریافت می نماید. سپس host ی که آدرس IP ارسال شده متعلق به او می باشد در پاسخ ، آدرس MACخود را می فرستد.در نهایت این پروسه با در اختیار قرار دادن آدرس MAC به کامپیوتری که برای ارسال داده های خود نیازمند آن آدرس بود کامل می شود.

ARP قوانین این پروتکل را برای انتقال و تبدیل آدرس (از لایه ی ۳ به لایه ی ۲ و همچنین از لایه ی ۲ به لایه ی ۳ (که همان ARP معکوس است) برقرار نگه می دارد.

(ARP) تبدیل آدرس ۳۲ بیتی IP به آدرس ۴۸ بیتی MAC

(RARP) تبدیل آدرس ۴۸ بیتی MAC به آدرس ۳۲ بیتی IP



این جدول با عنوان cache ARP شناخته می شود و برای نگهداری هر آدرس MAC تبدیل شده به IP متناظرش استفاده می شود. Cache ARP یکی از مهمترین قسمتهای این پروتکل است اما از آنجا که سایز آن محدود است ورودی ها باید به صورت دوره ای پاک شوند. این پروسه همچنین هر گونه تلاش ناموفق برای برقراری ارتباط با کامپیوترهایی که دیگر استفاده نمی شوند را پاک می نماید. به طور کلی ۲ نوع ورودی به cache وجود دارد:

Static Cache & Dynamic Cache

ورودی های static ورودی هایی هستند که توسط ARP وارد جدول می شوند و از cache حذف نخواهند شد اما ورودی هایی که به صورت اتوماتیک از طریق broadcast وارد جدول می شوند (در مواردی که برای پیدا کردن IP مورد نظر ، سیستم در شبکه ما نبوده و برای پیدا کردن آن از router ها ، getway ها و switch های مختلفی باید عبور کنند و IP همه آنها جداگانه در cache ذخیره می شود) و به آنها ورودی های dynamic گفته می شود و از cache پاک خواهند شد .

سوئیچ های دستور ARP:

تمام ورودی ها به ARP cache می توانند مشاهده، اضافه و حذف شوند.برای برطرف کردن مشکلات مربوط به این آدرس ها می توانید از ARP cache استفاده نمایید. برای مشاهده ی ARP cacheاز کامند arp -a یا arp -g استفاده نمایید. حال اگر نیاز باشد ARP cache را فقط برای IPهای خاصی استفاده نمایید از کامند arp -a <IP Address> بهره ببرید. برای حذف ARP cache، از کامند arp -d و برای اضافه کردن از arp -s استفاده می شود. بعضی از کامپیوتر ها، کارت های شبکه چند منظوره (multiple NICs) دارند که ARP cache آدرس های مربوط به هر کارت را به طور جداگانه ای نگهداری می کند. لذا برای مشاهده ی ARP cache مربوط به یک کارت شبکه نیز میتوانید از دستور arp -a –n <interface> استفاده فرمایید.

اجرای دستورَARP:

```
arp -a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           1۰-□۶-۱f-e9-aa-4۱     □□□□□□□□
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-0۰-۵□-۰۰-۰۰-۱۶     static
  224.0.0.252           0۱-۰۰-۵□-۰۰-۰۰-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
Interface: 192.168.179.1 --- 0x12
  Internet Address      Physical Address      Type
  192.168.179.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            0۱-۰۰-۵□-۰۰-۰۰-۱۶     static
  224.0.0.252           0۱-۰۰-۵□-۰۰-۰۰-fc     static
Interface: 192.168.94.1 --- 0x13
  Internet Address      Physical Address      Type
  192.168.94.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            0۱-۰۰-۵□-۰۰-۰۰-۱۶     static
  224.0.0.252           0۱-۰۰-۵□-۰۰-۰۰-fc     static
```

دستور NSLookup

NSLookup ابزاری مفید جهت خطایابی، تست و رفع اشکال مشکلات مربوط به DNS می باشد. با استفاده از این فرمان در فضای CMD، نام host و IP آدرس DNS سیستم نمایان می شود.

درصورتی که DNS ، fail شود یا اطلاعات نادرست ارائه دهد، سرعت برقراری ارتباط در شبکه کاهش می یابد و client ها دچار مشکل می شوند چرا که همانطور که در مورد عملکرد DNS در مبحث پیشین بیان شد، Clientها دیگر نمی توانند از طریق اسامی سایت وارد آنها شوند. در شبکه های برمبنای ویندوز،اکتیودایرکتوری ها (که درآینده مفصلا به انها خواهیم پرداخت) به DNS نیازمندند در واقع به عبارتی اگرDNS ، fail شود اکتیودایرکتوری و domain نیز fail خواهند شد NSLookup .، انواع رکوردها در DNS Server را بررسی می نماید و برای خطایابی در عدم اتصال سیستم به سیستم های دیگر استفاده می شود. در صورتی که رکورد اشتباهی در DNS Server وجود داشته باشد یا اصلا رکوردی وجود نداشته باشد، جهت بررسی مشکل می توان از این کامند استفاده نمود. در صورتی که با Ping، IP مربوط به سرور مورد نظر را توانستید از آن Reply بگیرید اما از طریق Ping نام آن سرور را نتوانستید کسب نمایید، اطمینان داشته باشید که مشکل از DNS می باشد.

به طور کلی NSLookup دو حالت دارد:

Interactive & Noninteractive

در حالت interactive ، به سادگی تنها دستور NSlookup را در command prompt تایپ می نمایید. این حالت زمانی استفاده می شود که در پایگاه داده DNS سیستم قصد دارید بیشتر از یک مورد را بررسی نمایید. به بیانی ساده تر زمانی که دستور NSlookup را در command promptتایپ می کنید، ابتدا نام وIP مربوط به DNS Server ی که سیستم استفاده می کند نشان داده می شود، سپس در سطر بعدی ، خط فاصله ی چشمک زن، منتظر وارد کردن دستور بعدی NSLookup می ماند و تا زمانی که کلید exit یا ctrl + c را نزنید این انتظار ادامه پیدا خواهد کرد. حال فرض کنید جهت از انتظار در آوردن این خط فاصله ی چشمک زن ، Parsgo.com را تایپ نمایید، دراین صورت کلیه ی IP های مربوط به این سایت، و همچنین مجددا IP مربوط به DNS Serverی که استفاده می کنید را مشاهده خواهید فرمود.

اما در حالتnoninteractive ، تنها یک دستور NSLookup تایپ نمی شود، بلکه گزینه های دیگری نیز در ادامه ی آن تایپ می شود. به عنوان مثال اگر برای حل مشکل خود به دنبال یک IP بخصوص می باشید، می توانید پس از تایپ NSlookup ، نام سایتی که به دنبال IP آن هستید را تایپ کنید یا باالعکس یعنی اگر IP را دارید و به دنبال نام سایت هستید نیز می توانید از این حالت استفاده فرمایید.

سویچ های دستورNSLookup:

Ls: این سوئیچ اطلاعات را برای DNS domain به صورت لیست در می آورد.

Server : سرور DNS را تبدیل به سرور به خصوصی که کاربر می خواهد می کند .

[Ser port] : پورتی که توسط DNS استفاده می شود را تغییر می دهد .

[Set retry] : تعداد ورودی ها را مشخص می کند .

[Set type] : نوع اطلاعاتی که بررسی می شود را تغییر می دهد

جهت مشاهده سایر سوئیچ های این کامند به صورت کامل می توانید از سوئیچ help یا /? استفاده نمایید.

دستور NETSTAT

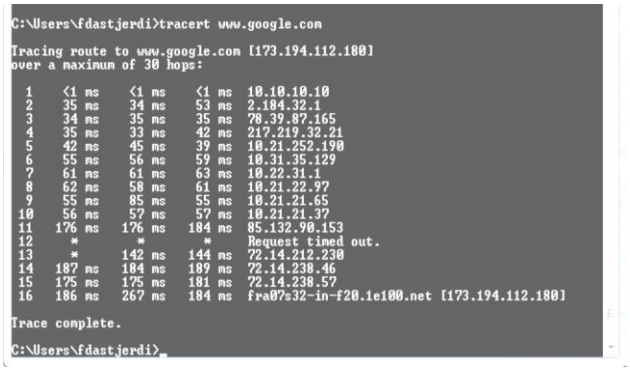
یکی دیگر از دستوراتی که برای خطایابی TCP/IP استفاده می شود netstat می باشد..این دستور وضعیت پروتکل و کلیه ی ارتباطات و تنظیمات در حال حاضر TCPIP ی شبکه ، کلیه ی پورتهایی که در حال استفاده هستند و همچنین جداول مسیریابی (routing table) را نشان می دهد. در واقع این کامند کلیه ی ورودی ها و خروجی ها به کامپیوتر شما را کنترل و بررسی می نماید. netstat اطلاعات مربوط به هر session ، کارت شبکه ، و اینکه اینها به چه صورت درحال استفاده هستند را نشان می دهد.

به صورت پیش فرض اطلاعاتی که netstat به شما می دهد شامل انواع پروتکل هایی که در آن زمان استفاده می کنید ، local address ها واطلاعات مربوط به پورتها یی که استفاده می کنند، remote address ها و اطلاعات مربوط به پورتهایی که آنها نیز استفاده می کنند و در نهایت وضعیت جاری را نمایش می دهد.همانطور که پیداست این اطلاعات مشخص می کنند که چه ارتباطاتی برقرار و چه عملیاتی

```
>
C:\Users\fdastjerdi>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49888        activate:49889         ESTABLISHED
  TCP    127.0.0.1:49889        activate:49888         ESTABLISHED
  TCP    127.0.0.1:51716        activate:12882         TIME_WAIT
  TCP    127.0.0.1:51725        activate:12882         TIME_WAIT
  TCP    192.168.3.28:50634     10.10.10.10:pptp       ESTABLISHED
  TCP    192.168.168.7:2492     blugro2relay:2492      ESTABLISHED
  TCP    192.168.168.7:51724    111.111.111.111:http   SYN_SENT

C:\Users\fdastjerdi>_
```

در حال انجام است و در زمان جاری کدام پورتهای سیستم باز و در حال تبادل اطلاعات و برقراری session هستند.در واقع ترافیک شبکه را کنترل می کند و به شما می گوید که به طور کلی در شبکه چه خبر است.

دستور Tracert



Tracert کامندی است که تنها برای انجام یک وظیفه ی اساسی طراحی شده است و آن نیز تعیین مسیری است که بسته های داده برای رسیدن به مقصد طی می کنند.این دستور با دستور ping متفاوت است.درواقع ping به شما می گوید که آدرسی که آن را ping کرده اید فعال یا run است یا خیر و برقراری ارتباط را بررسی می کند اما tracert تک تک روترهایی را که بسته های داده در مسیر با آن برخورد خواهند داشت را برای کاربر نشان می دهد.در واقع زمانی که بسته های داده به مقصد نمی رسند و یا زمان پاسخ دستور ping زمانی نامعقول و طولانی باشد از این دستور استفاده می کنیم.لازم به ذکر است که این کامند هم همانطور که پیشتر ذکر کردم، همانند کامند ping از پروتکل ICMP استفاده می کند .

این کامند به شما کمک می کند تا تعداد شبکه ها یا هاب های بین شما و کامپیوتر مقصد را بدانید.برای درک بهتر کاربرد این دستور یک مثال میزنم: فرض کنید که data packet ها یا همان بسته های داده از دفتر نمایندگی شرکتی در آبادان تا دفتر نمایندگی آن شرکت در تهران به طور معمول ۱۳ هاب را طی می کنند اما یک روز کاربران از سرعت پایین شبکه شاکی می شوند،زمانی که شما از این دستور استفاده می کنید متوجه می شوید که تعداد هاب ها به ۲۰ عدد افزایش یافته است که این بدان معناست که بسته ها مسیر دیگری را برای رسیدن به مقصد طی می کنند و این ممکن است به این علت باشد که مسیری که بسته ها به صورت معمول طی می کرده اند down شده باشد و بسته های داده ی شما برای رسیدن به مقصد مجبورند مسیر دیگری را طی کنند.درواقع در یک شرکت اگرهم شما برای داشتن یک شبکه ی خوب ، از تجهیزات خوب نیز استفاده کنید،اما به محض اینکه داده های شما وارد دنیای وسیع اینترنت شدند کسی نمی تواند تصمیم بگیرد که داده ها چه مسیری را برای رسیدن به مقصد طی کنند.به عبارتی پروسه ی مسیریابی یک پروسه ی پویا است اما با استفاده از این کامند می توانید متوجه شوید که مشکل در شبکه شما از کجا یا کدام روتر است .برای خطایابی مشکل به وجود آمده می توانید ازاین دستور بدین صورت استفاده کنید :

```
Tracert <hostname>

Tracert <ipaddress>
```

اگرچه این دستور نمی تواند علت رخ دادن مشکل را کشف کند اما میتواند نقطه ای را که مشکل در آنجا رخ داده است را پیدا کند،سپس دارندگان روترهای معیوب نسبت به برطرف کردن مشکل اقدام می کنند.استفاده از tracert ممکن است در ابتدا کمی گیج کننده باشد.زمانی که یک hostname یا یک

ipaddressرا tracert می کنیم اطلاعات مربوط به هاب ها در ۵ ستون نمایش داده می شود.در ستون اول ،تعداد هاب هایی که بسته ها رد می کنند را نشان می دهند.در ۳ ستون بعدی ،مدت زمانی که رسیدن بسته ها به روتر ها را نشان می دهد و در ستون آخر لیست کامل domain name هر روتر نشان داده می شود .

سوئیچ های دستور Tracert:

d- این سوئیچ مانع از تبدیل IP ها به hostname ها می شود.بدون استفاده از این سوئیچ برنامه همچنان کار می کند منتها با تبدیل IP مربوط به هر هاب به hostname آن که این عمل سرعت انجام پروسه را پایین می آورد.

h- با استفاده از این سوئیچ می توان حداکثر تعداد هاب های یک روتر را تعیین کرد.به صورت پیش فرض تعداد هاب هایی که بسته ها برای رسیدن به remote host رد می کنند ۳۰ عدد می باشد.اما در برخی موارد که لازم است این تعداد محدود شوند می توان از این سوئیچ استفاده کرد.

w- مدت زمانی را (براساس میلی ثانیه) که طول می کشد تا یک برنامه منتظر پاسخ بماند را تعیین می کند. در مواقعی که مشکل پهنای باند داریم ، کم یا زیاد کردن این مدت زمان می تواند به ما کمک کند.

j- بدون استفاده از این سوئیچ،بسته ها از مسیری که به صورت پیش فرض برایشان در نظر گرفته شده عیور می کنند.زمانی که از این سوئیچ استفاده می کنید، tarcert همان مسیری را که برایش تعریف شده دنبال می کند و به کامپیوتر شما برمی گردد.به این option که Loose Source Rooting Optionمی گویند و کامند آن به صورت زیر اجرا می شود.

```
Tracert -j <hop list>
```

tarcert ابزار سودمندی است که علت در دسترس نبودن یک remote host را مشخص می کند.این کامند در ویندوز استفاده می شود.کامند معادل آن در لینوکس traceroutمی باشد.جدول

Tracert Switch	Definition
-d	Does not resolve address to computer names.
-h	Specifies maximum number of hops.
-j	Specifies loose source route along host-list.
-w	Specifies time in milliseconds to wait for reply.
target_name	Specifies target computer.

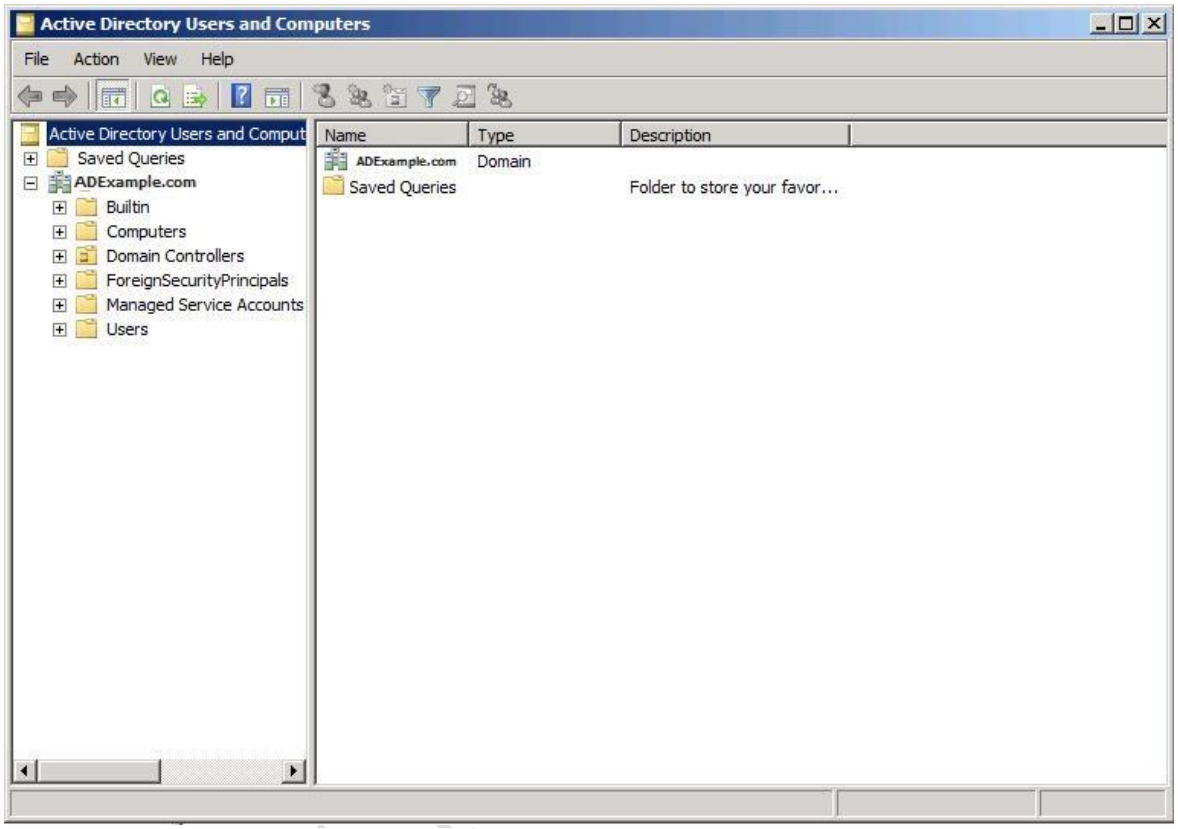
سوئیچ های tracert را در زیر می توانید مشاهده کنید .

سیستم عامل شبکه

مبحث این کتاب: Windows Server 2008 R2

اکتیو دایرکتوری (Active Directory)

اکتیو دایرکتوری از فناوری‌های شرکت مایکروسافت برای مدیریت منابع شبکه و در اساس یک بانک اطلاعاتی مجتمع توزیع پذیر است که برای سرویس‌دهنده های بر مبنای ویندوز سرور تهیه گردیده است.



تصویر شماره ۱شمای کلی از اکتیو دایرکتوری

بدون اکتیو دایرکتوری برای مدیریت منابع نیازمند مدیریت تک به تک آنها بصورت منفرد می باشیم در حالی که با اکتیو دایرکتوری مدیریت منابع شبکه بصورت مجتمع صورت می پذیرد. در ادامه با نصب و کار با اکتیو دایرکتوری تحت ویندوز سرور ۲۰۰۸ آشنا خواهید شد.

در مهندسی نرم افزار، Directory یک راه حل هدایت کردن نام به مقدار است. به عنوان یک مثال ساده، می توان یک یک دیکشنری را یک دایرکتوری در نظر گرفت که در آن معنای یک لغت (اسم) به معانی واژه (مقدار) مربوط شده است. در یک دفترچه تلفن، اسامی اشخاص (نام-گره) به شماره تلفن های آن ها (مقدار-اطلاعات) مرتبط می شود و در DNS، نام DNS به IP address ها مرتبط می شوند. به عبارت دیگر می توان گفت؛ یک سرویس دایرکتوری تقریبا مشابه یک دیتابیس است.

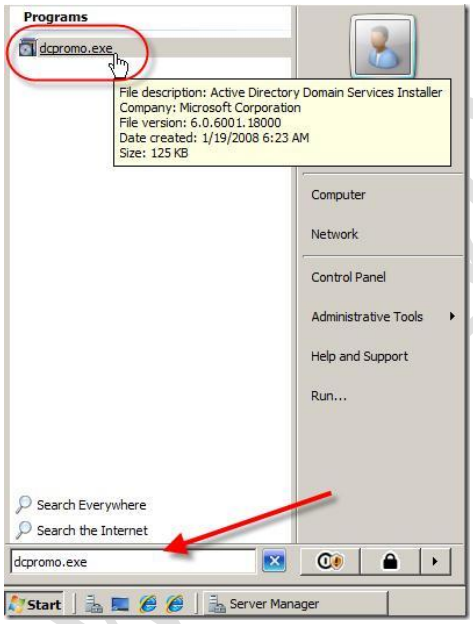
در یک دایرکتوری اشیائی که به نوعی مرتبط اند، ذخیره می شوند و از طریق صفاتشان قابل دسترسی اند. در سرویس های مختلف و در سیستم عامل های مختلف، از یک سرویس دایرکتوری استفاده می شود. در سرویس دایرکتوری اطلاعات به صورت سلسه مراتبی نگه داری می شود همچنین سرویس دایرکتوری

تمامی اطلاعات لازم را نگه داری می کند. با توجه به ارتباط میان اشیاء، دسترسی از طریق صفات و نگه داری تمامی اطلاعات لازم، مدیریت اطلاعات مرکزی و آسان تر می شود. بدیهی است عمکرد سرویس های دایرکتوری که در سرویس های مختلف استفاده می گردد، متفاوت است. با توجه به اهمیت این سرویس، باید مکانیسم های امنیتی و مدیریتی دیگر برای اثر بخشی، یکپارچگی و حفظ حریم خصوصی اتخاذ شود که در نتیجه باید از پروتکل ها و سرویس های دیگری نیز در کنار سرویس دایرکتوری استفاده شود.

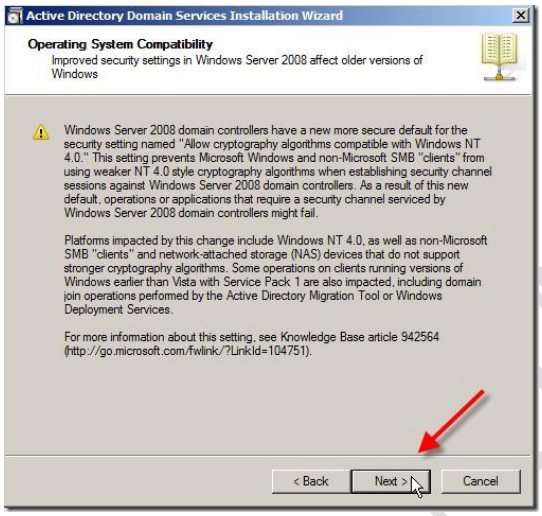
در اینجا Directory Services عاملی برای Identity and Access یا IDA را فراهم می آورد. راهکار های IDA، راهکارهایی هستند که به سازمان ها کمک می کنند تا کاربرانشان را مدیریت کنند و حقوق دسترسی آن ها به منابع را معین کنند. مایکروسافت مجموعه ای از راهکار های مختلف را جهت IDA ارائه می دهد که مشهورترین آن ها Active Directory Domain Services است. اکتیو دایرکتوری دامین سرویسز در ۱۹۹۹ دیده شد و برای اولین بار همراه با ویندوز ۲۰۰۰ ارائه شد. پیش تر مایکروسافت نام NTDS را برای این سرویس انتخاب کرده بود.

نصب Active Directory در ویندوز سرور۲۰۰۸:

۱. در قسمت Run و یا جلوی خط فرمان CMD دستور dcpromo را تایپ می کنیم.در تصویر با باز نمودن Start Menu و Search به راحتی dcpromo را باز می نماییم.



۲. در این قسمت گزینه Advanced Mode Installation را انتخاب می کنیم. وسپس بر روی دکمه Next کلیک فرمایید.



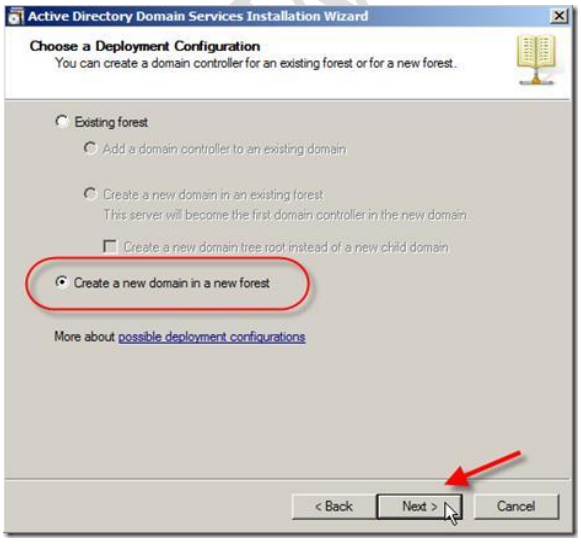
۳. بر روی دکمه Next کلیک فرمایید. (در این مرحله تذکراتی در خصوص سازگاری با سیستم عامل های قبلی داده می شود که کم و بیش در مطلب پیش نیاز و حوزه عملکرد در موردش بحث شد. برای اطلاعات بیشتر به وب سایت مایکروسافت مراجعه فرمایید. اما به صورت کلی بدانید از ویندوز NT در دامین کنترلر های ویندوز سرور ۲۰۰۸ به دلیل پشتیبانی نکردن از الگوریتم های رمزنگاری قدیمی مورد استفاده ویندوز NT پشتیبانی نمی شود. پس چنانچه از این نسخه از ویندوز در شبکه خود هنوز استفاده می کنید، از ادامه مراحل خودداری کنید.)

۴. مشخص کردن ساختار جنگل و ساختار درختی:

در این قدم لازم است جایگاه سرور در ساختار منطقی مشخص گردد. گزینه های در دسترس عبارت اند از:

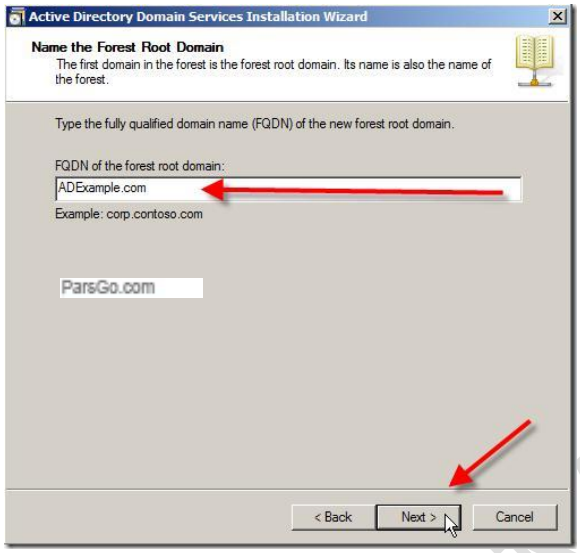
- Create a new Domain in a new forest (ساخت یک دامین جدید در یک جنگل جدید.):
  - در اینجا چون هیچ Forest از پیش وجود ندارد این گزینه را انتخاب می کنیم.
  - Existing Forest (در یک جنگل موجود):
  - Add a Domain Controller to an existing domain (افزودن یک دامین کنترلر به یک دامین):
  - یک Additional Domain Controller ایجاد می کند. برای اطمینان از Availability سرویس معمولا در یک دامین از بیش از یک دامین کنترلر استفاده می گردد تا اگر یک سرور با مشکلی رو به رو شد، سرور دوم پاسخ گوی کلاینت ها باشد.
  - Create new domain in an existing forest (ساخت یک دامین جدید در یک جنگل موجود):
  - این گزینه یک دامین فرزند (Child Domain) جدید در یک جنگل ایجاد می کند.
  - Create a new domain tree instead of a new child domain (ایجاد یک Tree Root):
  - با این گزینه یک درخت جدید در جنگل ایجاد می شود که Tree Root دامینی است که در اینجا ایجاد می شود.

۵. با توجه به گزینه ای که در اینجا انتخاب می شود، مراحل بعدی می تواند متمایز از آنچه در فوق ذکر شد باشد. در اینجا صرفا قصد داریم یک دامین جدید در یک Forest جدید ایجاد نماییم. نکته قابل توجه آن است که برای ایجاد هر کدام موارد فوق باید دسترسی های لازم را در اختیار داشته باشید. به عنوان مثال چنانچه گزینه ی create a new domain in an existing forest را انتخاب کنید یا به عبارتی یک Child Domain ایجاد کنید، لازم است یک Credential

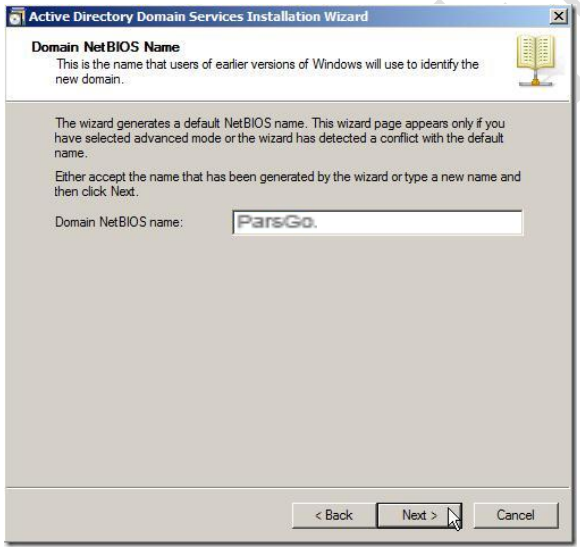


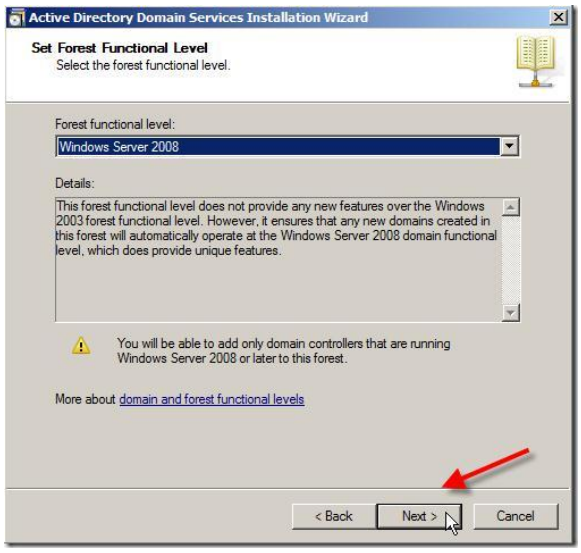
مناسب که یک اکانت عضو گروه Enterprise Administrators است فرآهم آورید. به عنوان مثال دیگری، برای ایجاد یک Read-Only Domain Controller داشتن مجوز دسترسی Domain Administrator کفایت می کند. همچنین لازم است نام DNS جایی که قصد راه اندازی مورد جدید را در آن داریم وارد کنیم. این نام باید یک نام معتبر روی یک Forest موجود باشد.

۶. در این مرحله باید نام Forest Root Domain را وارد نماییم. به مواردی که پیش تر تذکر داده شد توجه فرمایید. در اینجا از نام ParsGo.com استفاده می نماییم.

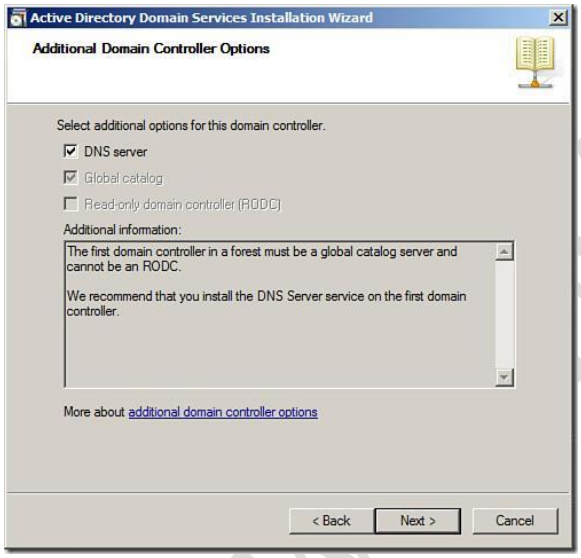


۷. در این مرحله با زدن Next ویزارد چک می کند تا این نام قبلا در شبکه موجود نباشد. پس از چند ثانیه، چنانچه موجود نباشد، نام NetBIOS از شما پرسیده خواهد شد که به صورت پیش فرض بخش اول نامی است که در بالا انتخاب فرموده اید. توصیه می شود این نام را تغییر ندهید.





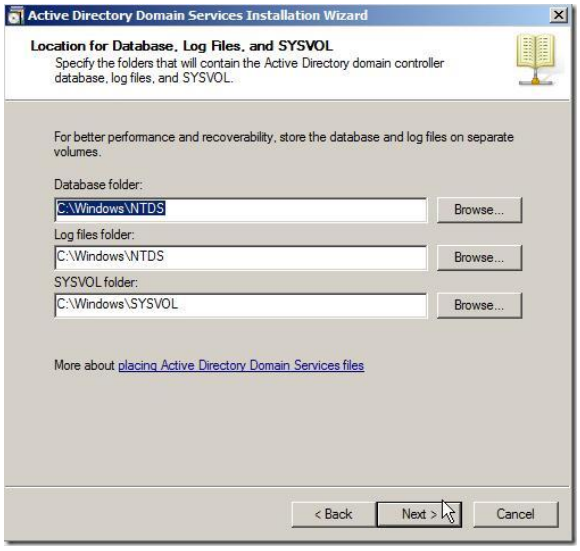
۸. با زدن Next در این مرحله باید Forest Functional Level و Domain Functional Level را انتخاب کنید . همانطور که ذکر شده اینجا Windows Server 2008 R2 را با فرض عدم وجود DCهای با نسخه ی پایین تر ویندوز انتخاب می شود. در صورتی که DC ای داشته باشیم که روی ویندوز سرور ۲۰۰۳ نصب شده باشد باید Functional Level را روی Windows Server 2003 تنظیم کرد.



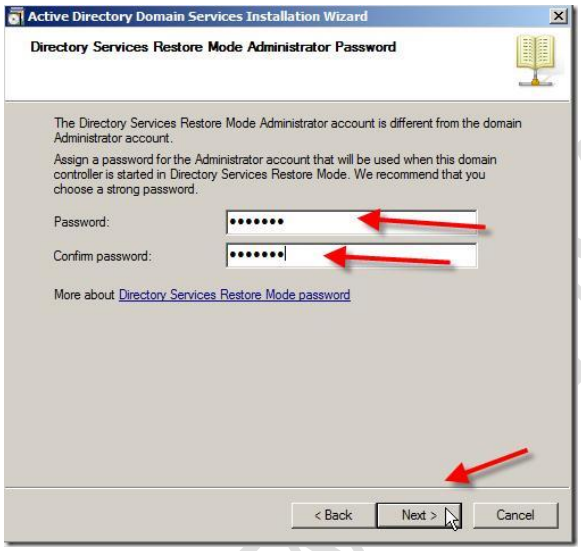
۹. در این مرحله باید تنظیمات اضافی را اعمال نمود. به صورت پیش فرض DNS Server انتخاب شده است. چنانچه اولین دامین کنترلر نباشد شما می توانید تنظیمات Global Catalog) GC) و Read-only Domain Controller را اعمال کنید. اما از آنجایی که در اینجا در حال نصب اولین دامین کنترلر هستیم، این موارد غیر قابل تغییرمی باشند.

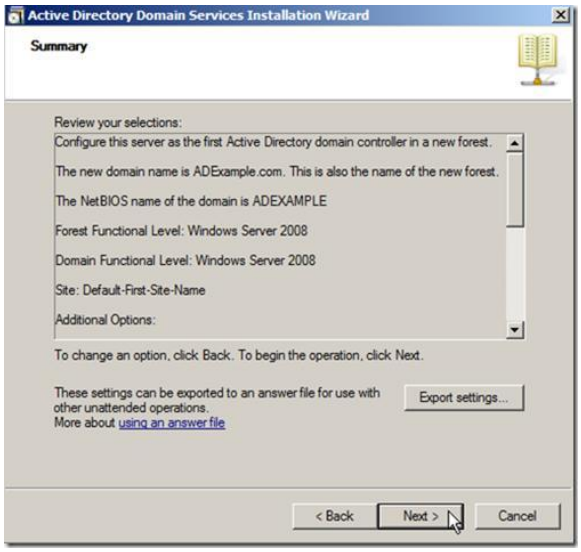
۱۰. در صورت انتخاب DNS Server در این مرحله پیام هشداری دریافت می کنید مبنی بر اینکه امکان ساخت Delegation برای DNS Zone وجود ندارد زیرا Parent Zone قابل دسترسی نیست یا از Windows DNS Server استفاده نمی کند. از آنجایی که در حال نصب اولین دامین در جنگل جدید هسیتم، با زدن Yes پیغام را تایید می نمایید.

۱۱. سپس جای فلدر های ذخیره سازی اطلاعات اکتیو دایرکتوری را معین می نمایید.(لزومی به تغییر این قسمت نمی باشد)



۱۲. در این مرحله باید کلمه عبوری برای Directory Services Restore Mode انتخاب کنید. توصیه می شود این کلمه عبور با کلمه عبور خودتان متمایز باشد و یادآوری آن ساده باشد هر چند امنیت آن اهمیت بسیاری دارد. البته راهی برای تعویض این کلمه عبور وجود است که در آینده آن را ذکر خواهیم کرد. در وضعیت Directory Services Restore Mode سرویس اکتیو دایرکتوری به صورت آفلاین می شود و در برخی عملیات کاربرد بسیاری دارد .





۱۳. در این مرحله خلاصه ای از تنظیمات مشخص شده را می توانید مشاهده کنید. آن ها را بازبینی کنید تا مشکلی موجود نباشد. نکته جدید دیگری همانطوری که در تصویر زیرمشاهده می کنید وجود دارد دکمه Export settings است. همانطوری که درنصب به روش Unattended توضیح داده شد ، با این گزینه می توانید یک answer file برای نصب اکتیو دایرکتوری های دیگری با همین تنظیمات استفاده نمایید.

۱۴. با زدن Next انجام نصب را تایید می کنید. این مراحل قدری طول می کشد و پس از پایان نیاز است تا کامپیوتر ریستارت "Restart" شود. یکی از کمک های مایکروسافت به شما مدیر شبکه گزینه Reboot on completion می باشد که به پس از پایان مراحل نصب سیستم را به صورت اتوماتیک Restart می نماید.

۱۵. لازم به ذکر است که چنانچه این سرور شما سرویس های دیگری را به شبکه ارائه می دهد، باید در زمان بندی معین و اعلام قبلی به کاربران سرور را ریستارت فرمایید.

نکته :

سرور اکتیو دایرکتوری حتما باید روی یوزر Administrator پسورد داشته باشد که این پسورد با پسورد ریکاوری اکتیو دایرکتوری باید متفاوت باشد.

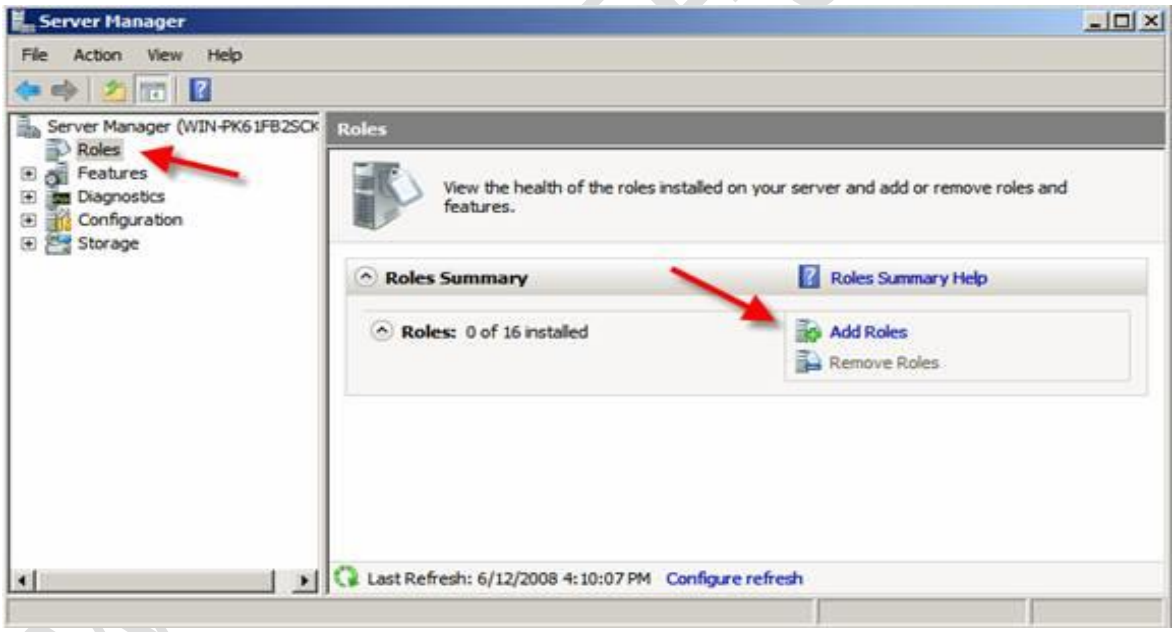
دی اچ سی پی سرور (Dynamic Host Configuration Protocol)(DHCP)

وظیفه DHCP تنظیم کردن TCP/IP کامپیوتر کاربران می باشد.در این حالت کامپیوتر کاربران به صورت اتوماتیک از DHCP Server آی پی می گیرند، کاربرد DHCP بیشتر برای مراکزی است که تعداد کلاینتهای (کاربران کامپیوتر) آنها زیاد باشد و یا دسترسی به تمامی کلاینت ها برای مدیر شبکه (ISP) دشوار باشد.

سرویس DHCP این امکان را به مدیر شبکه می دهد تا تمامی تنظیمات و آدرسهای مورد نیاز که باید به سرویس گیرنده ها تعلق گیرد را در Server به صورت متمرکز انجام دهد و این سرور هم، آدرسهای مذکور را به کامپیوترهای فاقد آدرس ارسال و در اختیار آنها قرار دهد.

نصب DHCP SERVER در ویندوز سرور۲۰۰۸:

۱. ابتد از طریق منوی Start وارد Server Manager شده و سپس گزینه Role و متعاقبا گزینه

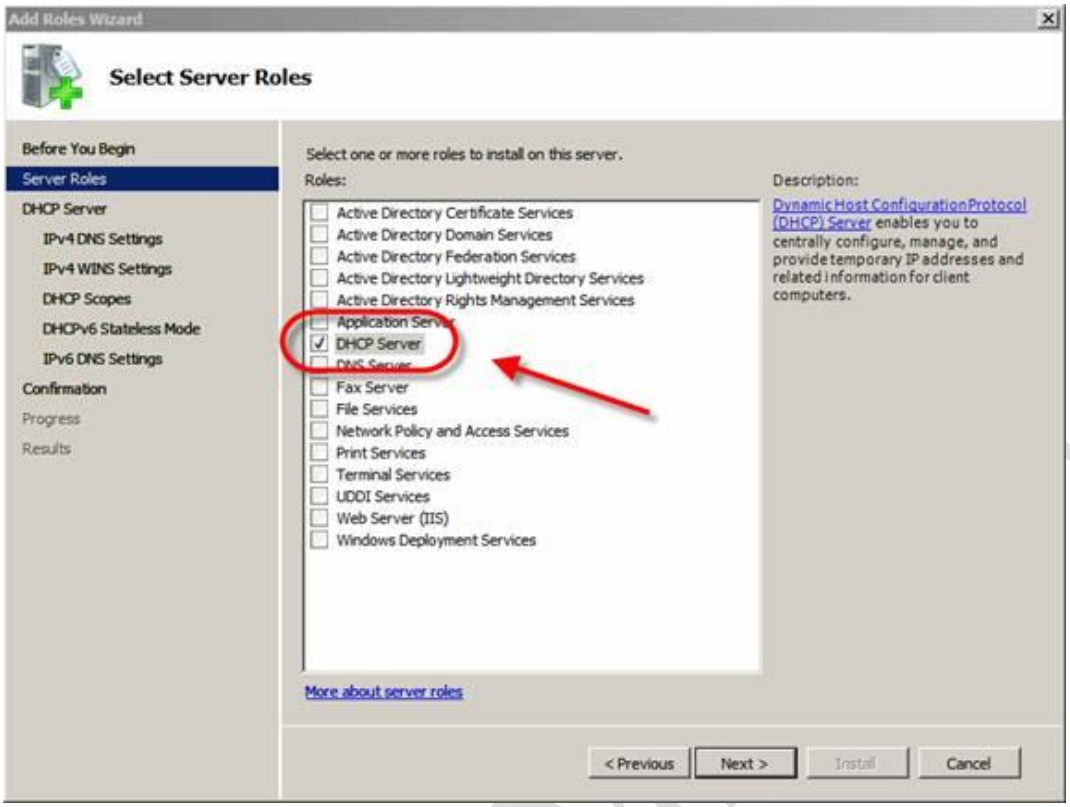


ی Add Role را انتخاب نمایید.

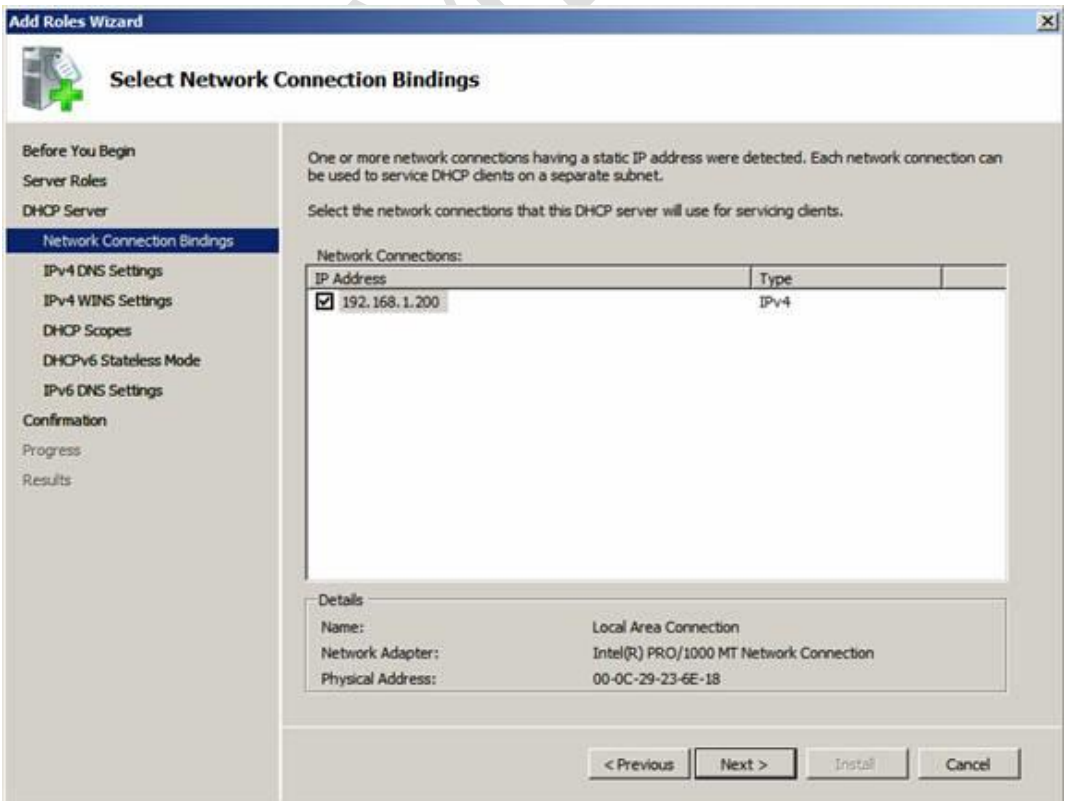
۲. سپس پنجره ای باز می شود بنام Select Server Role که ما سرویس مورد نظر را تیک می زنیم و گزینه next را انتخاب می کنیم.

۳. نکته : در نسخه Web edition ویندوز سرور امکان نصب DHCP وجود ندارد.

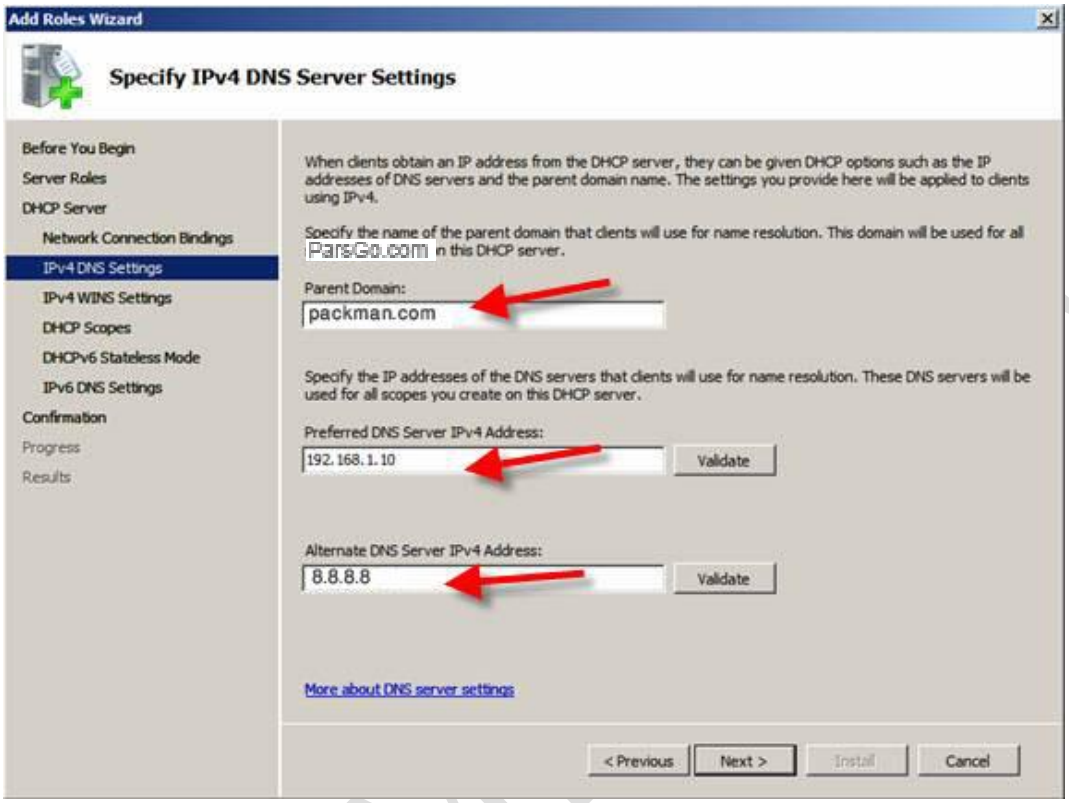
۴. در این بخش گزینه ی DHCP Server را تیک زده و Next را می زنیم.



۵. Network Connection Binding: این مرحله را نیز بدون هیچگونه تغییری ادامه می دهیم.

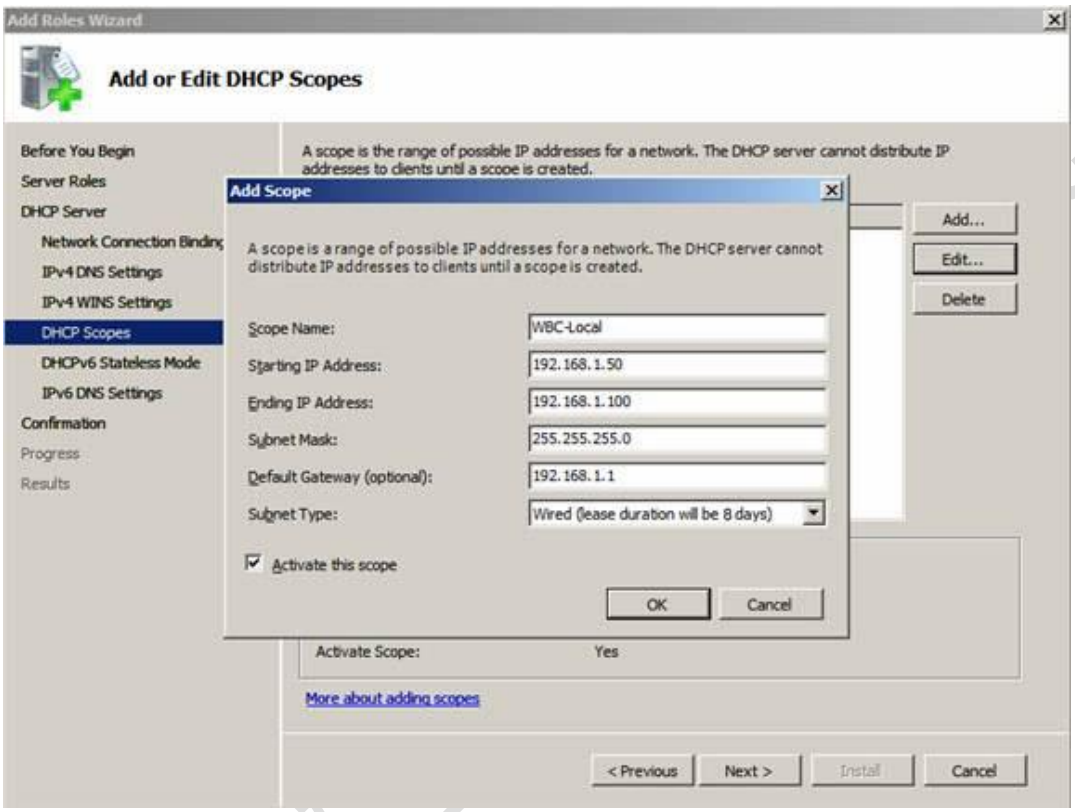


۶. Ipv4 Dns Setting: در قسمت اول اسم دامین را واردمی نمایید،(همان نامی که در اکتیو دایرکتوری انتخاب نموده ایم) ParsGo.com و در قسمت دوم IP Dns Server را می دهیم و در قسمت سوم Ip Global مثل ۸,۸,۸,۸ می دهیم.



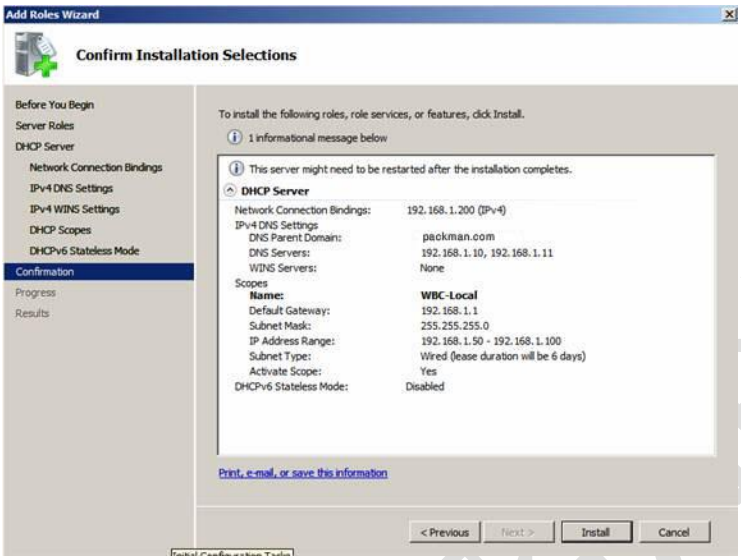
۷. Ipv4 Wins Setting: در این مرحله گزینه اول را انتخاب نمایید. .چون ما winsserverنداریم.

۸. DHCP SCOPES: با انتخاب گزینه add پنجره ای باز می شود که در قسمت اول نام حوزه یا قلمرو را تعریف می کنیم ودر قسمت بعدی رنج IP را در محدوده تعریف شده طوری انتخاب می کنیم که تکراری نباشد و در قسمت Subnet type به صورت پیش فرض هر ۸ روز یکبار IP چک می شود و یا تغییر می کند. قسمت Active This Scope اگر تیک داشته باشد،از زمان فعال شدن IP می دهد.

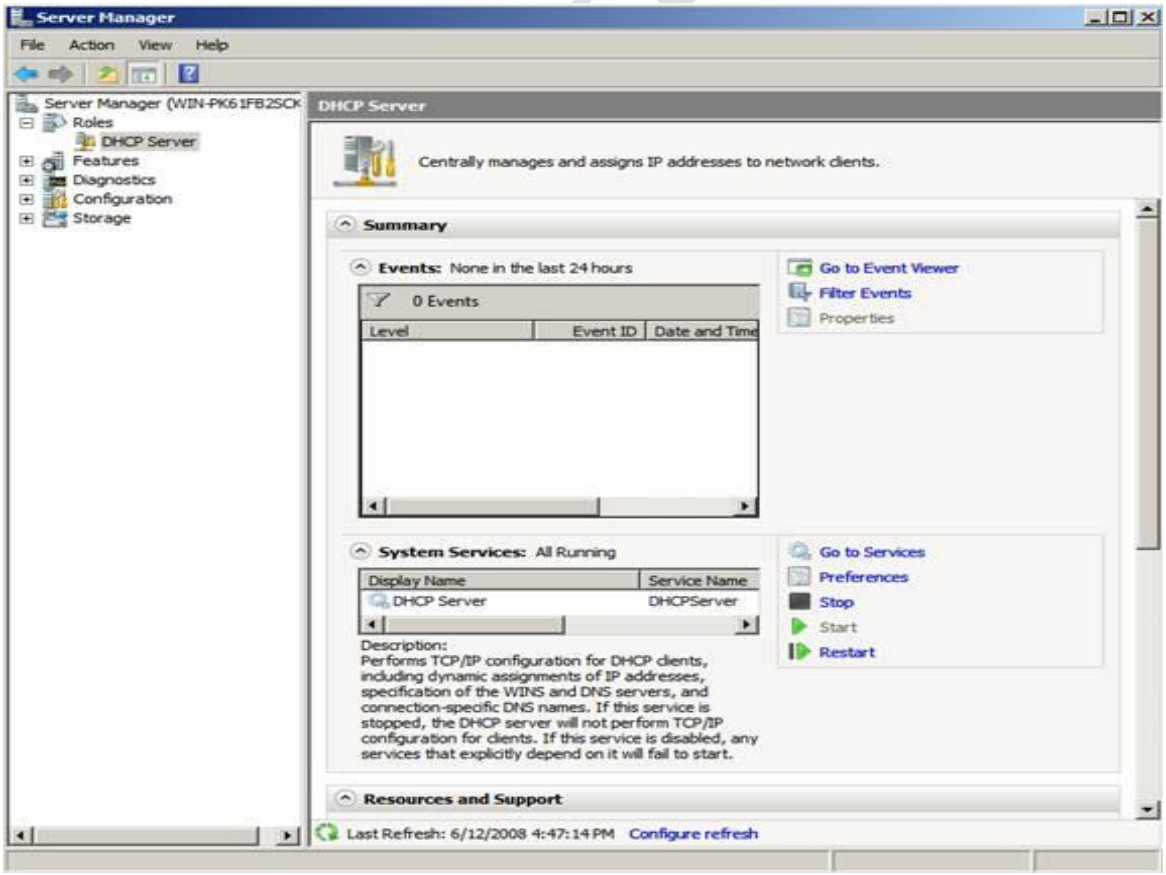


۹. در مرحله بعدی بخاطر اینکه نیاز به تنظیم کردن IP Ver6 نداریم ، گزینه Disable DHCPv6 را انتخاب نمایید و Next را می زنید.

۱۰. در آخرین مرحله پنجره ای به صورت زیر باز می شود که در آن خلاصه ای از کلیه تنظیمات انجام داده شده باز می شود.در این مرحله گزینه Install را می زنیم تا این سرویس نصب شود.

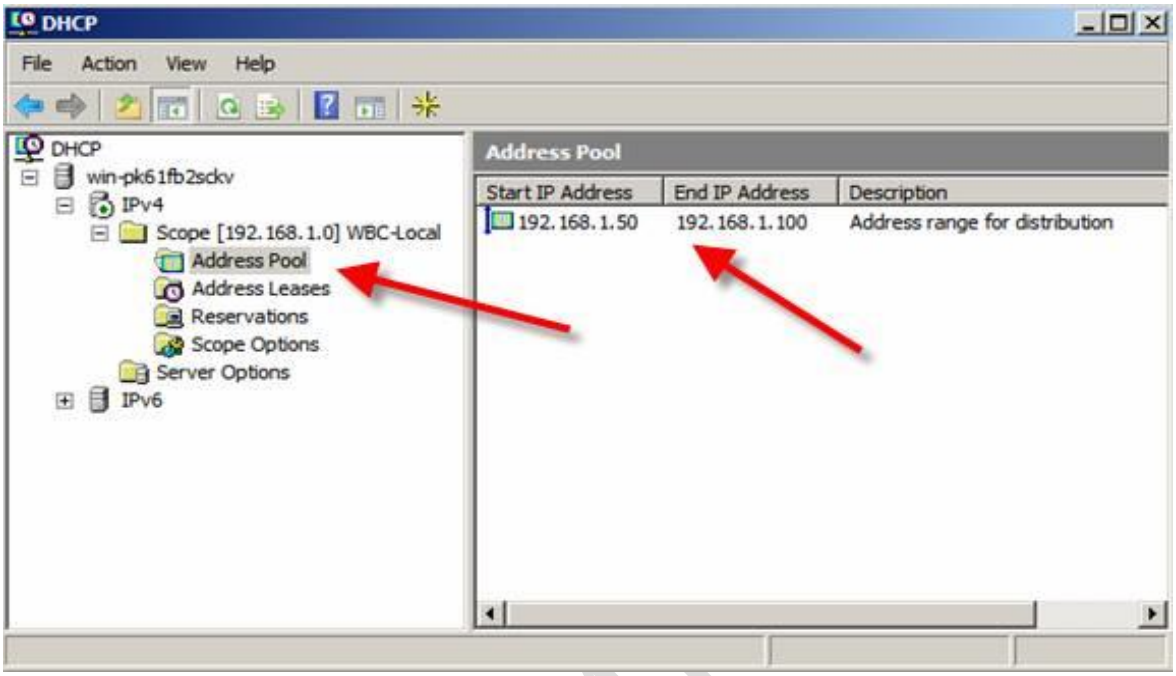


در قسمت Roles مشاهده می فرمایید که سرویس DHCP Server اضافه شده است همچنین



می توانید از طریق منوی Start/Administrative tools وارد قسمت DHCP شوید.

DHCP Server را باز نموده و وارد IPV4 شوید و Scope ساخته شده را انتخاب نمایید. مشاهده می فرمایید که داخل آن محدوده IP که تعریف نموده اید نمایش داده می شود و همچنین در



قسمت Scope Option نام Domain و همچنین IP DNS Server نمایش داده می شود.

تصویر شماره ۲ محیط دی اچ سی پی سرور

Installation and commissioning of network

www.MiMFa.net
Info@mimfa.net

MiMFa Production