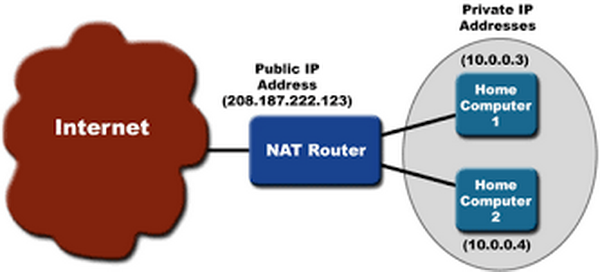
الف:

همان‎گونه که از نام آنها مشخص است، تفاوت اصلی بین آی‌پی عمومی‎ و آی‌پی خصوصی در شبکه‎ای است که آنها استفاده می‎کنند. آی‌پی‌‎های عمومی‎ که در تمام اینترنت یکتا هستند، به دستگاه‌ها اجازه می‎دهند تا به اینترنت متصل شوند. برای مديريت یکتایی آنها، واگذاری آنها از طریق یک سازمان و به صورت متمرکز سازماندهی و انجام می‎شود. آدرس‌های آی‌پی خصوصی در شبکه‎های خصوصی استفاده می‎شوند که یا به اینترنت متصل نیستند و یا از طریق NAT به اینترنت متصل می‎شوند.

آدرس آی‌پی عمومی‎ به صورت جهانی و در کل اینترنت یکتا و منحصر به فرد است. در استاندارد محدوده آدرس‌های آی‌پی مشخصی برای استفاده در شبکه‎های خصوصی در نظر گرفته شده است. هر آی‌پی که به عنوان آی‌پی خصوصی رزرو نشده باشد را می‎توان به عنوان آی‌پی عمومی‎ استفاده کرد. یک شبکه آی‌پی باید برای هر کدام از دستگاه‌های خود از یک آی‌پی منحصر به فرد استفاده کند. از آنجا که اینترنت هم یک شبکه آی‌پی است، برای جلوگیری از استفاده شدن یک آی‌پی یکسان برای چند دستگاه مختلف باید آدرس‌های آی‌پی به درستی نگهداری شوند. این مدیریت آدرس‌های آی‌پی توسط سازمانی به نام Internet Assigned Numbers Authority یا به اختصار IANA انجام می‎شود و آنها هستند که محدوده‎های آی‌پی را به سازمان‎های مختلف اختصاص ميدهند.



**NAT چیست؟**

NAT یا Network Address Translation پروتکلی است برای تبدیل آدرس های IP غیر معتبر به آدرس های معتبر برای استفاده کاربران از اینترنت که در لایه ۳ مدل OSI کار می کند.  
این امکان زمانی مورد استفاده قرار میگیرد که در یک شبکه کاربرانی که دارای آدرس های معتبر نیستند نیاز به برقراری ارتباط با اینترنت را دارند.

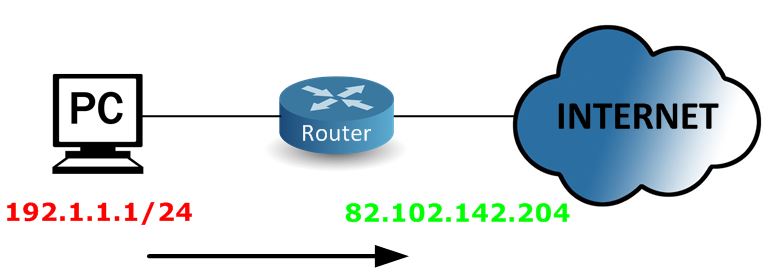
این پروتکل تعداد آدرس های غیر معتبر را که از یک طرف به یک اینترفیس سرور NAT متصل است را در قالب یک آدرس معتبر(Encapsulation) به سمت اینترفیس خروجی که به اینترنت متصل است ارسال می کند.  
به زبان ساده زمانی از این سرویس استفاده می کنیم که تعدادی کامپیوتر را بخواهیم از طریق یک ارتباط اینترنت به اینترنت متصل نمائیم. برای راه اندازی این سرویس روی ویندوز سرور ۲۰۰۳ نیازمند ۲ کارت شبکه بر روی کامپیوتر سرور که یکی از آنها به شبکه داخلی و دیگری به طریقی شبکه اینترنت متصل باشد ، هستیم.

NAT یکی از ابزارهای قدرتمند دنیای IT است که دقیقا همان کاری را انجام می دهد که از اسم آن بر می آید,به وسیله NAT میتوانیم آدرسهای یک شبکه را به یک شبکه دیگر ترجمه کنیم.

NAT تقریبا در تمامی سیستم عاملها و روتر ها قابل انجام است که هر کدام شیوه و روش خود را دارند.  
برای همه متخصصین واضح است که قوی ترین روتر های دنیا Cisco هستند و تقریبا ۸۰ درصد از بستر اینترنت بر روی دستگا های Cisco بنا شده اند. در این آموزش به توضیح مراحل انجام NAT به صورت عملی بر روی سخت افزارهای سیسکو می پردازیم.

از کاربردهای NAT می توان به موارد زیر اشاره کرد:

ترجمه IP های Private به Public یا بلعکس  
تغییر مرکز سرویس دهنده اینترنت بدون نیاز به تغییر IP ها داخلی  
حفاظت از یک شبکه حساس در مقابل برخی حملات خارجی  
تغییر پورت مقصد پکتها برای کاربران داخلی به صورت



آيپي دهي اتوماتيك چگونه صورت ميگيرد.

در این روش دستگاهی تحت عنوان Dynamic Host Configuration Protocol در شبکه قرار می گیرد که وظیفه آی پی دهی به صورت خودکار به کامپیوتر های شبکه را برعهده می گیرد . برای درک بهتر فرض کنیم که ما در شبکه خود یک سرور DHCP داریم که یک رنج آی پی به او تعلق می گیرد و کلاینت ها به صورت دینامیک به سرور DHCP می گویند که من به یک آی پی نیاز دارم و DHCP یک آی پی از رنج در نظر گرفته شده را به او می دهد .  
این روش معمولترین روش آی پی دهی به کلاینت ها در شبکه می باشد . شما به عنوان مدیر شبکه یک سرور DHCP را پیکربندی می کنید و یک رنج آی پی خاص برای او تعریف می کنید و کلاینت ها به نیاز خود می رسند . حال فرض کنید که کامپیوتر شما به صورت دستی آی پی دهی نشده است و روی حالت دریافت اتوماتیک آی پی قرار دارد . به DHCP درخواستی برای دریافت آی پی ارسال می کند ولی دستگاه DHCP به هر دلیل در دسترس نیست . چه اتفاقی رخ می دهد ؟ آیا کامپیوتر شما بدون آی پی خواهد ماند ؟ خیر . سیستم عامل , با استفاده از روش APIPA شروع به آی پی دهی به کامپیوتر های درون شبکه میکند .APIPA مخفف کلمه Automatic Private IP Addressing می باشد که در این روش با استفاده از رنج آی پی 169.254.0.0 که به این منظور رزرو شده است سیستم ها آی پی دریافت می کنند .