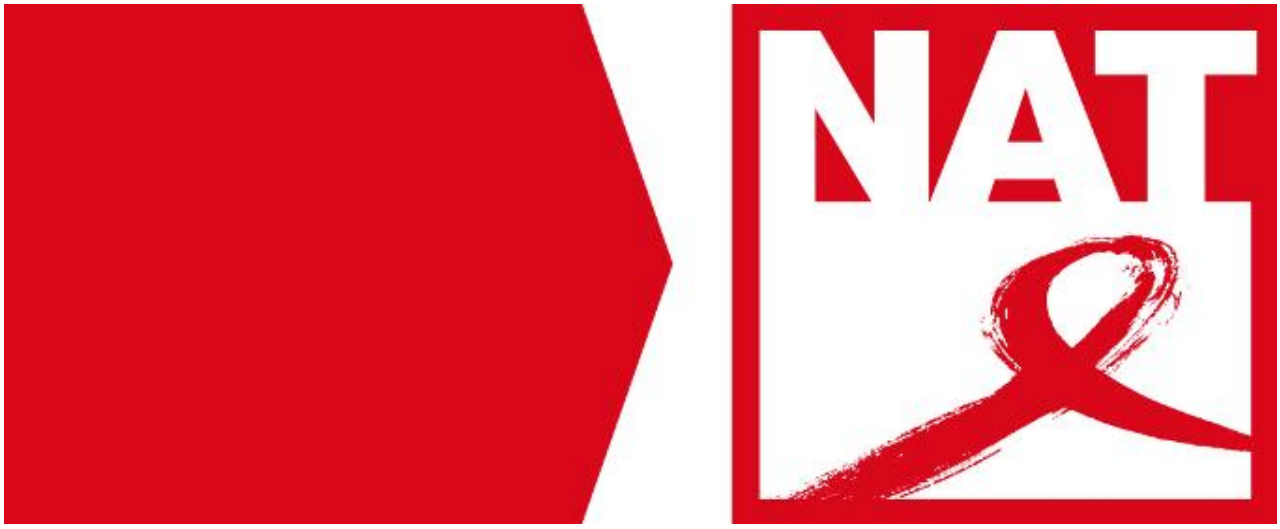


هدف اولیه NAT بدین صورت تعریف شده است که کاربران داخلی سازمان با آدرس غیر اینترنتی صرفا با تعداد محدودی آدرس اینترنتی بتوانند با شبکه اینترنت ارتباط برقرار نمایند بدون اینکه مجبور به استفاده از آدرس های Public باشند. بدین صورت که کاربران شبکه از آدرس های محدوده اختصاصی برای ارتباطات داخلی خود استفاده می کنند

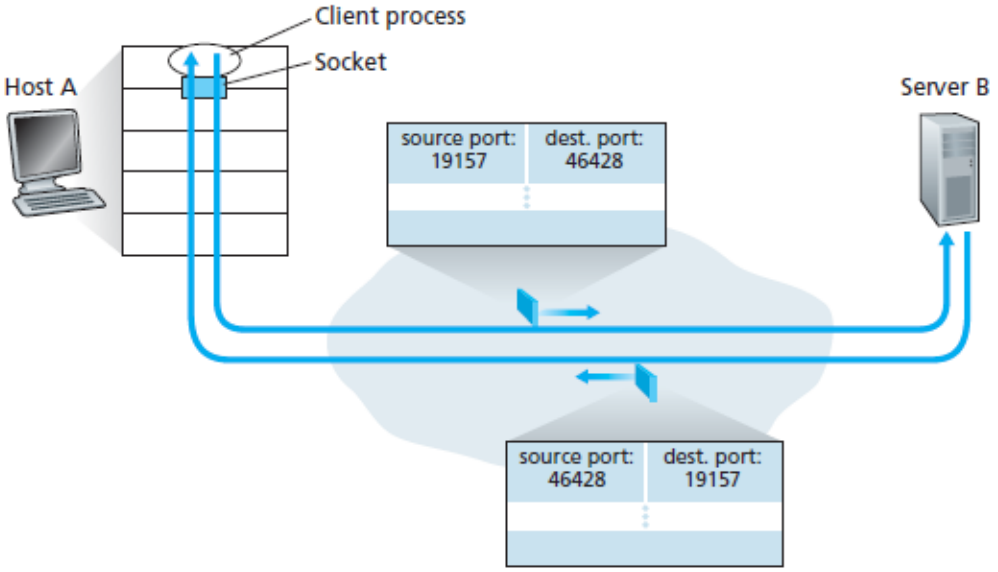
و در صورتی که بخواهند با اینترنت ارتباط برقرار کنند، تعداد زیادی کاربر صرفا از یک یا چند آدرس محدود اینترنتی به صورت اشتراکی برای اتصال به اینترنت بهره می برند. بدین ترتیب محدودیت تعداد آدرس IPV4 از بین خواهد رفت. چگونگی مکانیزم NAT را در همین فصل مورد بررسی قرار خواهیم داد.

سوال این است که چگونه چند کاربر به صورت همزمان فقط با یک آدرس Public قادر به ارتباط با اینترنت هستند؟ در پاسخ به این سوال ابتدا لازم است تا عملکرد شماره پورت را در لایه Transport یکبار مرور نماییم.

همانطور که بخاطر دارید وقتی کاربری بخواهد با سروری ارتباط برقرار کند، یک پورت تصادفی در بازه ۱۰۲۵ تا ۶۵۵۳۵ بازاء هر session برای پورت مبدا در

نظر می گیرد. پورت مقصد نیز بر اساس سرویس انتخاب می شود که معمولا در بازه ۱ تا ۱۰۲۴ است.. به عنوان مثال اگر کاربری بخواهد از طریق browser و در قالب دو صفحه مجزا دو کلمه مختلف را در گوگل جستجو نماید، هر صفحه، session مجزایی است که شماره پورت مقصد آنها یکسان و ۸۰ در نظر گرفته می شود که نشان دهنده سرویس وب است. اما شماره پورت مبدا، بازاء هر session تصادفی و منحصربفرد در نظر گرفته می شود. ممکن است در همان زمان کاربر بخواهد ایمیل خود را نیز چک نماید که در این صورت برای session سوم، شماره پورت مبدا، عدد تصادفی منحصربفرد دیگری خواهد بود اما شماره پورت مقصد ۱۱۰ است که نشان دهنده سرویس دریافت ایمیل است. شماره پورت مبدا و مقصد و همچنین آدرس IP مبدا و مقصد در ترافیک های برگشتی از سرور به کاربر جایشان عوض می شوند و بنابرین کاربر از روی شماره پورت مقصد ترافیک های برگشتی، که همان شماره پورت مبدا ترافیک های ارسالی است، می تواند تشخیص دهد که هر بسته دریافتی به کدام session تعلق دارد.

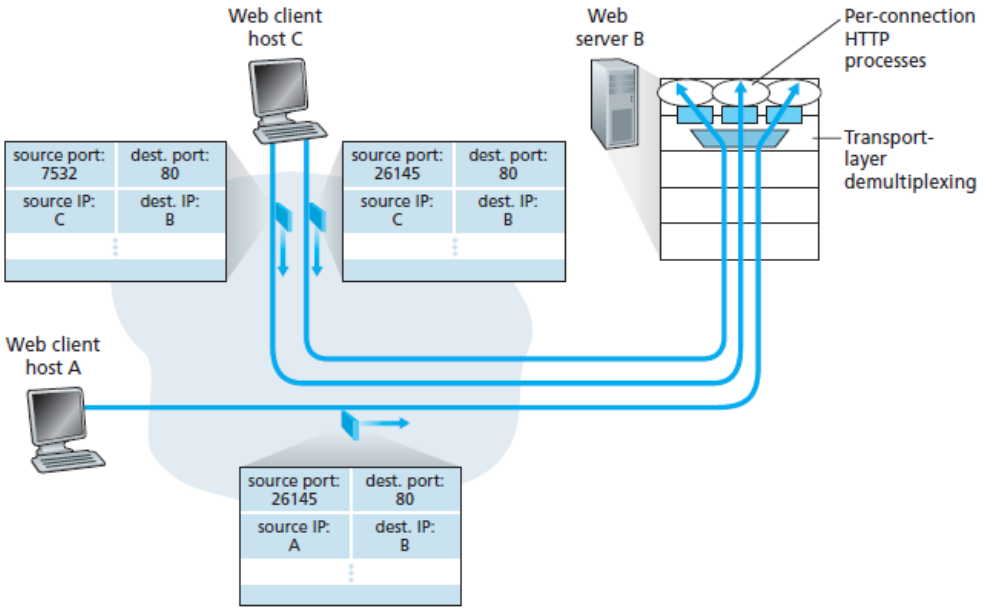
در شکل زیر کاربر A با سرور B ارتباط برقرار می کند. شماره پورت مبدا، تصادفی و معادل ۱۹۱۵۷ در نظر گرفته شده است و پورت مقصد نیز ۴۶۴۲۸ است که بر اساس نوع سروییس تعیین شده است و همواره مقدار ثابتی است. البته شماره پورت مقصد معمولا زیر ۱۰۲۴ است اما می تواند همانند این مثال در محدوده بالای ۱۰۲۴ نیز قرار داشته باشد. همانطور که در شکل مشاهده می کنید در ترافیک های برگشتی از سرور B به کاربر A جای پورت مبدا و مقصد عوض شده است و کاربر با نظاره کردن شماره پورت مقصد ترافیک های دریافتی تشخیص می دهد که ترافیک به کدام session تعلق دارد.



عملکرد شماره پورت در لایه Transport

توجه کنید که در پروتکل های لایه Transport شماره پورت مبدا به ازاء هر session در یک کاربر منحصربفرد است اما دو کاربر مختلف ممکن است همزمان از شماره پورت های یکسان برای پورت مبدا استفاده کنند. بدیهی است که یکسان بودن شماره پورت مبدا روی دو session که به دو کاربر متفاوت مرتبط است، هیچ مشکلی ایجاد نمی کند زیرا آدرس IP دو ترافیک متفاوت است و روی دو کامپیوتر مختلف دریافت می شود.

در شکل زیر دو session از کاربر C و یک session از کاربر A به سرور B ایجاد شده است. اما اگر توجه کنید شماره پورت مبدا یکی از session های کاربر C با شماره پورت مبدا session مربوط به کاربر A یکسان است اما در عین حال هیچ مشکلی ایجاد نمی شود زیرا ترافیک های برگشتی این دو session آدرس IP مقصد متفاوتی دارند و روی دو کامپیوتر مختلف دریافت می شوند.



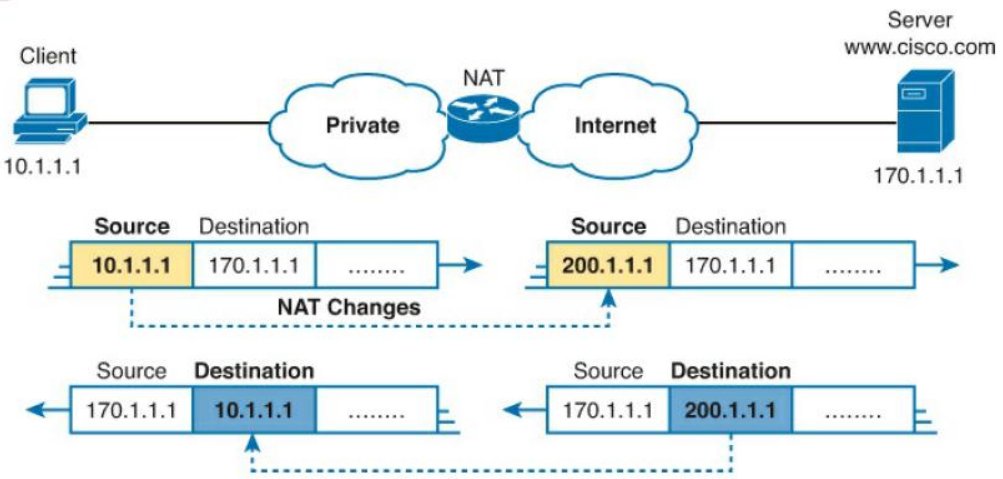
پورت مبدا به ازاء هر session در سطح کامپیوتر منحصربفرد است نه در سطح شبکه

حال مجددا سوال ابتدای این بخش را تکرار می کنیم. چطور چندین کاربر با بکارگیری تکنولوژی NAT به صورت همزمان و با یک آدرس اینترنتی یکسان می توانند به اینترنت متصل شوند؟ در پاسخ به این سوال موقعی که ترافیک کاربران از دروازه شبکه سازمان به اینترنت ارسال می شوند، آدرس IP مبدا همه ترافیک های داخل به بیرون به یک آدرس یکسان که همان آدرس اینترنتی است، نگاشت می شوند. بدیهی است که در این شرایط ترافیک های برگشتی قابل تفکیک نخواهند بود تا به دست کاربر مورد نظر برسند زیرا آدرس مقصد هم ترافیک های برگشتی یکسان و همان آدرس نگاشت شده خواهد بود. برای رفع این مشکل نه تنها نسبت به تغییر آدرس مبدا ترافیک های داخل به بیرون اقدام می شود، بلکه شماره پورت مبدا نیز تغییر داده می شود. بدین صورت که تمام ترافیک هایی که شماره پورت مبدا آنها در سطح شبکه (نه در سطح کاربر) منحصربفرد نیستند، تغییر داده شده و به یک شماره پورت منحصربفرد تغییر می کنند. البته تغییر

آدرس IP و همچنین شماره پورت مبدا در جایی در روتر مرزی سازمان ثبت می شود. در چنین شرایطی ترافیک های برگشتی کل شبکه به ازاء هر session شماره پورت مقصد منحصربفردی خواهند داشت که قابلیت تفکیک ترافیک ها و session را فراهم می کند. بعد از تشخیص و تفکیک session، آدرس IP و همچنین شماره پورت به حالت اولیه باز گردانده شده و تحویل کاربر نهایی می شود. بدین ترتیب فقط با یک آدرس اینترنتی حداکثر به تعداد شماره پورت، session همزمان می توانند از سازمان به اینترنت ارتباط برقرار نمایند. بدیهی است که اگر بیش از یک آدرس اینترنتی در اختیار داشته باشیم، به همین نسبت تعداد session های بیشتری از سازمان به اینترنت قابل انتقال خواهد بود.

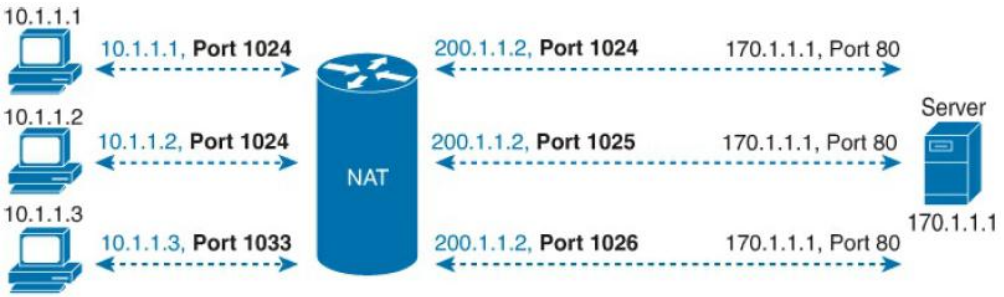
شکل زیر تغییر آدرس مبدا را زمانی که ترافیک از داخل به خارج سازمان منتقل می شود را نشان داده است و اینکه مشخصات این ترافیک (آدرس IP) بعد از برگشت از اینترنت مجددا به حالت قبلی باز می گردد. این دقیقا کاری است که در تکنولوژی NAT صورت می گیرد. در این شکل وقتی ترافیک با آدرس مبدا غیر اینترنتی ۱۰.۱.۱.۱، از داخل به خارج سازمان منتقل می گردد، به آدرس ۲۰۰.۱.۱.۱ تغییر داده می شود. آدرس مقصد ترافیک برگشتی مجددا از ۲۰۰.۱.۱.۱ به ۱۰.۱.۱.۱ برگردانده می شود.

اما نکته مهم در این تکنولوژی این است که چندین کاربر بتوانند همزمان با یک آدرس IP اینترنتی به شبکه اینترنت متصل شوند که در شکل بعدی تشریح شده است.



مکانیزم NAT Source

در شکل زیر سه کاربر مختلف با آدرس های غیر اینترنتی ۱۰.۱.۱.۱، ۱۰.۱.۱.۲ و ۱۰.۱.۱.۳ همزمان قصد دارند وارد اینترنت شوند. اگر دقت کنید آدرس پورت مبدا دو کاربر اول و دوم نیز تصادفا یکسان انتخاب شده است که کاملا طبیعی است. در مرز شبکه وقتی ترافیک ها از داخل به خارج منتقل می گردند، آدرس مبدا همه آنها به آدرس یکسان ۲۰۰.۱.۱.۲ تغییر داده می شوند. از آنجایی که در چنین شرایطی نمی توان در زمان برگشت ترافیک، تشخیص داد که ترافیک به کدام کاربر متعلق است، لذا علاوه بر آدرس مبدا، پورت مبدا نیز تغییر داده می شود به طوری که پورت مبدا در سطح کل شبکه به ازاء هر session منحصربفر باشد. در این مثال پورت مبدا به ۱۰۲۴، ۱۰۲۵ و ۱۰۲۶ تغییر داده شده است. بنابراین در زمان برگشت ترافیک، از روی پورت مقصد می توان تشخیص داد که ترافیک به کدام کاربر و session تعلق دارد و آدرس IP و شماره پورت مجددا به حالت اولیه برگردانده می شود و سپس ترافیک تحویل کاربر مورد نظر می گردد. البته در این مثال لازم نبود تا شماره پورت هر سه session تغییر نماید. در صورتی که فقط شماره پورت session مربوط به کاربر اول و یا دوم نیز تغییر داده می شد، باز هم شماره پورت ها منحصربفرد و قابل تشخیص بوده اند.



Inside Local	Inside Global
10.1.1.1: **1024**	200.1.1.2: **1024**
10.1.1.2: **1024**	200.1.1.2: **1025**
10.1.1.3: **1033**	200.1.1.2: **1026**

مکانیزم PAT Source