منبع: شرکت سخاروش http://www.Srco.ir

NAT چیست؟

اینترنت با سرعتی باورنکردنی همچنان در حال گسترش است . تعداد کامپیوترهای ارائه دهنده اطلاعات (خدمات) و کاربران اینترنت روزانه تغییر و رشد می یابد. با اینکه نمی توان دقیقا" اندازه اینترنت را مشخص کرد ولی تقریبا" یکصد میلیون کامپیوتر میزبان (Host) و ۳۵۰ میلیون کاربر از اینترنت استفاده می نمایند. رشد اینترنت چه نوع ارتباطی با (Network Address Translation NAT) دارد؟ هر کامپیوتر بمنظور ارتباط با سایر کامپیوترها و سرویس دهندگان وب بر روی اینترنت، می بایست دارای یک آدرس IP باشد. IP یک عدد منحصر بفرد ۳۲ بیتی بوده که کامپیوتر موجود در یک شبکه را مشخص می کند.

اولین مرتبه ای که مسئله آدرس دهی توسط IP مطرح گردید، کمتر کسی به این فکر می افتاد که ممکن است خواسته ای مطرح شود که نتوان به آن یک آدرس را نسبت داد. با استفاده از سیستم آدرس دهی IP می توان ٤،٢٩٤،٩٧٦،٢٩٦ (٢٣٢) آدرس را تولید کرد. (بصورت تئوری). تعداد واقعی آدرس های قابل استفاده کمتر از مقدار (بین ۳،۲ میلیارد و ۳،۳ میلیارد) فوق است . علت این امر، تفکیک آدرس ها به کلاس ها و رزو بودن برخی آدرس ها برای multicasting ، تست و موارد خاص دیگر است .

همزمان با انفجار اینترنت (عمومیت یافتن) و افزایش شبکه های کامپیوتری ، تعداد IP موجود، پاسخگوی نیازها نبود. منطقی ترین روش، طراحی مجدد سیستم آدرس دهی IP است تا امکان استفاده از آدرس های IP بیشتری فراهم گردد. موضوع فوق در حال پیاده سازی بوده و نسخه شماره شش IP ، راهکاری در این زمینه است . چندین سال طول خواهد کشید تا سیستم فوق پیاده سازی گردد، چراکه می بایست تمامی زیرساخت های اینترنت تغییر واصلاح گردند. NAT با هدف کمک به مشکل فوق طراحی شده است . NAT به یک دستگاه اجازه می دهد که بصورت یک روتر عمل نماید. در این حالت NAT بعنوان یک آژانس بین اینترنت (شبکه عمومی) و یک شبکه محلی (شبکه خصوصی) رفتار نماید. این بدان معنی است که صرفا" یک IP منحصر بفرد بمنظور نمایش مجموعه ای از کامپیوترها(یک گروه) مورد نیاز خواهد بود.

کم بودن تعداد IP صرفا" یکی از دلایل استفاده از NAT است .در ادامه به بررسی علل استفاده از

NATخواهیم پرداخت .

قابلیت های NAT

عملکرد NAT مشابه یک تلفتچی در یک اداره بزرگ است . فرض کنید شما به تلفنچی اداره خود اعلام نموده اید که تماس های تلفنی مربوط به شما را تا به وی اعلام ننموده اید ، وصل نکند . در ادامه با یکی ازمشتریان تماس گرفته و برای وی پیامی گذاشته اید که سریعا" با شما تماس بگیرد. شما به تلفتچی اداره می گوئید که منتظر تماس تلفن از طرف یکی از مشتریان هستم، در صورت تماس وی ، آن را به دفتر من وصل نمائید. در ادامه مشتری مورد نظر با اداره شما تماس گرفته و به تلفنچی اعلام می نماید که قصد گفتگو با شما را دارد (چراکه شما منتظر تماس وی هستید). تلفنچی جدول مورد نظر خود را بررسی تا نام شما را در آن پیدا نماید. تلفنچی متوجه می شود که شما تلفن فوق را درخواست نموده اید، بنابراین تماس مورد نظر به دفتر شما وصل خواهد شد.

NAT توسط شرکت سیسکو و بمنظور استفاده در یک دستگاه (فایروال ، روتر، کامپیوتر) ارائه شده است .NAT بین یک شبکه داخلی و یک شبکه عمومی مستقر و شامل مدل ها ی متفاوتی است .

- NAT ایستا :

عملیات مربوط به ترجمه یک آدرس IP غیر ریجستر شده (ثبت شده) به یک آدرس IP ریجستر شده را انجام می دهد. (تناظر یک به یک) روش فوق زمانیکه قصد استفاده از یک دستگاه را از طریق خارج از شبکه داشته باشیم، مفید و قابل استفاده است . در مدل فوق همواره IP 192.168.32.10 به IP 213.18.123.110 ترجمه خواهد شد.

- NAT پویا :

یک آدرس IP غیر ریجستر شده را به یک IP ریجستر شده ترجمه می نماید. در ترجمه فوق از گروهی آدرس های IP ریجستر شده استفاده خواهد شد.

- OverLoading :

مدل فوق شکل خاصی از NAT پویا است . در این مدل چندین IP غیر ریجستر شده به یک IP ریجستر شده با استفاده از پورت های متعدد، ترجمه خواهند شد. به روش فوق Port Address(PAT Translation)

نیز گفته می شود.

- Overlapping :

در روش فوق شبکه خصوصی از مجموعه ای IP ریجستر شده استفاده می کند که توسط شبکه دیگر استفاده می گردند. NAT می بایست آدرس های فوق را به آدرس های IP ریجستر شده منحصربفرد ترجمه نماید.

NAT همواره آدرس های یک شبکه خصوصی را به آدرس های ریجستر شده منحصر بفرد ترجمه می نماید. NAT همچنین آدرس های ریجستر شده عمومی را به آدرس های منحصر بفرد در یک شبکه خصوصی ترجمه می نماید. (در هر حالت خروجی NAT ، آدرس های IP منحصر بفرد خواهد بود. آدرس های فوق می تواند در شبکه های عمومی ریجستر شده جهانی باشند و در شبکه های خصوصی ریجستر شده محلی باشند)

شبکه اختصاصی (خصوصی) معمولا" بصورت یک شبکه LAN می باشند . به این نوع شبکه ها که از آدرس های IP داخلی استفاده می نمایند حوزه محلی می گویند. اغلب ترافیک شبکه در حوزه محلی بصورت داخلی بوده و بنابراین ضرورتی به ارسال اطلاعات خارج از شبکه را نخواهد داشت . یک حوزه محلی می تواند دارای آدرس های IP ریجستر شده و یا غیرریجستر شده باشد. هر کامپیوتری که از آدرس های IP غیرریجستر شده استفاده می کنند، می بایست از NAT بمنظور ارتباط با دنیای خارج از شبکه محلی استفاده نمایند.

NAT می تواند با استفاده از روش های متفاوت پیکربندی گردد. در مثال زیر NAT بگونه ای پیکربندی شده است که بتواند آدرس های غیر ریجستر شده IP (داخلی و محلی) که بر روی شبکه خصوصی (داخلی) می باشند را به آدرس های IP ریجستر شده ترجمه نماید.

- یک ISP (مرکز ارائه دهنده خدمات اینترنت) یک محدوده از آدرس های IP را برای شرکت شما در نظر می گیرد. آدرس های فوق ریجستر و منحصر بفرد خواهند بود . آدرس های فوق Inside global نامیده می شوند. آدرس های IP خصوصی و غیرریجستر شده به دو گروه عمده تقسیم می گردند : یک گروه کوچک که توسط NAT استفاده شده (Outside local address) و گروه بزرگتری

که توسط حوزه محلی استفاده خواهند شد (Inside local address) . آدرس های Outside local بمنظور ترجمه به آدرس های منحصربفرد IP استفاده می شوند.آدرس های منحصر بفرد فوق، outside global نامیده شده و اختصاص به دستگاههای موجود بر روی شبکه عمومی (اینترنت) دارند.

- اکثر کامپیوترهای موجود در حوزه داخلی با استفاده از آدرس های inside local با یکدیگر ارتباط برقرار می نمایند.

- برخی از کامپیوترهای موجود در حوزه داخلی که نیازمند ارتباط دائم با خارج از شبکه باشند ،از آدرس های inside global استفاده و بدین ترتیب نیازی به ترجمه نخواهند داشت .

- زمانیکه کامپیوتر موجود در حوزه محلی که دارای یک آدرس inside local است، قصد ارتباط با خارج شبکه را داشته باشد بسته های اطلاعاتی وی در اختیار NAT قرار خواهد گرفت .

- NAT جدول روتینگ خود را بررسی تا به این اطمینان برسد که برای آدرس مقصد یک entry در اختیار دارد. در صورتیکه پاسخ مثبت باشد، NAT بسته اطلاعاتی مربوطه را ترجمه و یک entry برای آن ایجاد و آن را در جدول ترجمه آدرس (ATT) ثبت خواهد کرد. در صورتیکه پاسخ منفی باشد بسته اطلاعاتی دور انداخته خواهد شد.

- با استفاده از یک آدرس global inside ، روتر بسته اطلاعاتی را به مقصد مورد نظر ارسال خواهد کرد.

- کامپیوتر موجود در شبکه عمومی (اینترنت)، یک بسته اطلاعاتی را برای شبکه خصوصی ارسال می دارد. آدرس مبداء بسته اطلاعاتی از نوع outside global است . آدرس مقصد یک آدرس inside global است .

- NAT در جدول مربوطه به خود جستجو و آدرس مقصد را تشخیص و در ادامه آن را به کامپیوتر موجود در حوزه داخلی نسبت خواهد کرد.

- NAT آدرس های inside global بسته اطلاعاتی را به آدرس های inside local ترجمه و آنها را برای کامپیوتر مقصد ارسال خواهد کرد.

روش Overloading از یک ویژگی خاص پروتکل TCP/IP استفاده می نماید. ویژگی فوق این امکان

را فراهم می آورد که یک کامپیوتر قادر به پشتیبانی از چندین اتصال همزمان با یک و یا چندین کامپیوتر با استفاده از پورت های متفاوت TCP و یا UDP باشد.. یک بسته اطلاعاتی IP دارای یک هدر(Header) با اطلاعات زیر است :

آدرس مبداء . آدرس کامپیوتر ارسال کننده اطلاعات است .

پورت مبداء. شماره پورت TCP و یا UDP بوده که توسط کامپیوتر مبداء به بسته اطلاعاتی نسبت داده شده است .

آدرس مقصد : آدرس کامپیوتر دریافت کننده اطلاعات است .

پورت مقصد. شماره پورتTCP و یا UDP بوده که کامپیوتر ارسال کننده برای باز نمودن بسته اطلاعاتی برای گیرنده مشخص کرده است .

آدرس ها ، کامپیوترهای مبداء و مقصد را مشخص کرده ، در حالیکه شماره پورت این اطمینان را بوجود خواهد آورد که ارتباط بین دو کامپیوتر دارای یک مشخصه منحصر بفرد است . هر شماره پورت از شانزده بیت استفاده می نماید.(تعداد پورت های ممکن ٦٥٥٣٦ (١٦ ٢) خواهد بود) . عملا" از تمام محدوده پورت های فوق استفاده نشده و ٤٠٠٠ پورت بصورت واقعی استفاده خواهند شد.

NAT پویا و Overloading

نحوه کار NAT پویا بصورت زیر است :

- یک شبکه داخلی (حوزه محلی) با استفاده از مجموعه ای از آدرس های IP که توسط Internet Assigned Numbers(Authority IANA) به شرکت و یا موسسه ای اختصاص داده نمی شوند پیکربندی می گردد. (سازمان فوق مسئول اختصاص آدرس های IP در سطح جهان می باشد) آدرس های فوق بدلیل اینکه منحصربفرد می باشند، غیر قابل روتینگ نامیده می شوند.

- موسسه مربوطه یک روتر با استفاده از قابلیت های NAT را پیکربندی می نماید. روتر دارای یک محدوده از آدرس های IP منحصر بفرد بوده که توسط IANA د ر اختیار موسسه و یا شرکت مربوطه گذاشته شده است .

- یک کامپیوتر موجود بر روی حوزه محلی سعی درایجاد ارتباط با کامپیوتری خارج از شبکه (مثلا" یک سرویس دهنده وب) را دارد.

- روتر بسته اطلاعاتی را از کامپیوتر موجود در حوزه محلی دریافت می نماید.

- روتر آدرس IP غیرقابل روت را در جدول ترجمه آدرس ها ذخیره می نماید. روتر آدرس IP غیر قابل روت را با یک آدرس از مجموعه آدرس های منحصر بفرد جایگزین می نماید. بدین ترتیب جدول ترجمه، دارای یک رابطه (معادله) بین آدرس IP غیرقابل روت با یک آدرس IP منحصر بفرد خواهد بود.

- زمانیکه یک بسته اطلاعاتی از کامپیوتر مقصد مراجعت می نماید، روتر آدرس مقصد بسته اطلاعاتی را بررسی خواهد کرد.بدین منظور روتر در جدول آدرسهای ترجمه شده جستجو تا از کامپیوتر موجود در حوزه محلی که بسته اطلاعاتی به آن تعلق دارد، آگاهی پیدا نماید.روتر آدرس مقصد بسته اطلاعاتی را تغییر (از مقادیر ذخیره شده قبلی استفاده می کند) و آن را برای کامپیوتر مورد نظر ارسال خواهد کرد. در صورتیکه نتیجه جستجو در جدول، موفقیت آمیز نباشد، بسته اطلاعاتی دور انداخته خواهد شد.
- کامپیوتر موجود در حوزه ، بسته اطلاعاتی را دریافت می کند. فرآیند فوق مادامیکه کامپیوتر با سیستم خارج از شبکه ارتباط دارد، تکرار خواهد شد.

نحوه کار Overloading پویا بصورت زیر است :

- یک شبکه داخلی (حوزه محلی) با استفاده از مجموعه ای از آدرس های IP که توسط Internet Assigned(Numbers Authority IANA) به شرکت و یا موسسه ای اختصاص داده نمی شوند پیکربندی می گردد. آدرس های فوق بدلیل اینکه منحصربفرد می باشند غیر قابل روتینگ نامیده می شوند.

- موسسه مربوطه یک روتر را با استفاده از قابلیت های NAT ، پیکربندی می نماید. روتر دارای یک

محدوده از آدرس های IP منحصر بفرد بوده که توسط IANA د ر اختیار موسسه و یا شرکت مربوطه گذاشته شده است .

- یک کامپیوتر موجود بر روی حوزه داخلی ، سعی درایجاد ارتباط با کامپیوتری خارج از شبکه(مثلا" یک سرویس دهنده وب) را دارد.

- روتر بسته اطلاعاتی را از کامپیوتر موجود در حوزه داخلی دریافت می نماید.

- روتر آدرس IP غیرقابل روت و شماره پورت را در جدول ترجمه آدرس ها ذخیره می نماید. روتر آدرس IP غیر قابل روت را با یک آدرس منحصر بفرد جایگزین می نماید. روتر شماره پورت کامپیوتر ارسال کننده را با شماره پورت اختصاصی خود جایگزین و آن را در محلی ذخیره تا با آدرس کامپیوتر ارسال کننده اطلاعات ، مطابقت نماید.

- زمانیکه یک بسته اطلاعاتی از کامپیوتر مقصد مراجعت می نماید ، روتر پورت مقصد بسته اطلاعاتی را بررسی خواهد کرد.بدین منظور روتر در جدول آدرس های ترجمه شده جستجو تا از کامپیوتر موجود در حوزه داخلی که بسته اطلاعاتی به آن تعلق دارد آگاهی پیدا نماید.روتر آدرس مقصد بسته اطلاعاتی و شماره پورت را تغییر (از مقادیر ذخیره شده قبلی استفاده می کند) و آن را برای کامپیوتر مورد نظر ارسال خواهد کرد. در صورتیکه نتیجه جستجو در جدول ، موفقیت آمیز نباشد بسته اطلاعاتی دور انداخته خواهد شد.

- کامپیوتر موجود در حوزه داخلی ، بسته اطلاعاتی را دریافت می کند. فرآیند فوق مادامیکه کامپیوتر با سیستم خارج از شبکه ارتباط دارد، تکرار خواهد شد.

- با توجه به اینکه NAT آدرس کامپیوتر مبداء و پورت مربوطه آن را در جدول ترجمه آدرس ها ذخیره شده دارد، مادامیکه ارتباط فوق برقرار باشد از شماره پورت ذخیره شده (اختصاص داده شده به بسته اطلاعاتی ارسالی) استفاده خواهد کرد. روتر دارای یک Timer بوده وهر بار که یک آدرس از طریق آن استفاده می گردد reset می گردد.در صورتیکه در مدت زمان مربوطه (Timer صفر گردد) به اطلاعات ذخیره شده در NAT مراجعه ای نشود، اطلاعات فوق (یک سطر از اطلاعات) از داخل جدول حذف خواهند شد.

Source

Computer Source	Computer's IP Address	Source Computer's Port	Router's NAT IP Address	NAT Router's Assigned Port Number
A	١٩٢,١٦٨,٣٢,١٠	٤٠٠	٢١٥,٣٧,٣٢,٢٠٣	١
B	١٩٢,١٦٨,٣٢,١٣	٥٠	٢١٥,٣٧,٣٢,٢٠٣	٢
C	١٩٢,١٦٨,٣٢,١٥	٣٧٥٠	٢١٥,٣٧,٣٢,٢٠٣	٣
D	١٩٢,١٦٨,٣٢,١٨	٢٠٦	٢١٥,٣٧,٣٢,٢٠٣	٤

در صورتیکه برخی ازکامپیوترهای موجود در شبکه خصوصی از آدرس های IP اختصاصی خود استفاده می نمایند ، می توان یک لیست دستیابی از آدرس های IP را ایجاد تا به روتر اعلام نماید که کدامیک از کامپیوترهای موجود در شبکه به NAT نیاز دارند.

تعداد ترجمه های همزمانی که یک روتر می تواند انجام دهد، ارتباط مستقیم با حافظه اصلی سیستم دارد. با توجه به اینکه در جدول ترجمه آدرس هر entry صرفا" ١٦٠ بایت را اشغال خواهد کرد، یک روتر با ٤ مگابایت حافظه قادر به پردازش ٢٦،٢١٤ ترجمه همزمان است. مقدار فوق برای اغلب موارد کافی بنظر می آید.

IANA محدوده ای از آدرس های IP را که غیرقابل روت بوده و شامل آدرس های داخلی شبکه هستند مشخص نموده است .آدرس های فوق غیرریجستر شده می باشند.. هیچ شرکت و یا آژانسی نمی تواند ادعای مالکیت آدرس های فوق را داشته باشد و یا آنها را در شبکه های عمومی (اینترنت) استفاده نماید. روترها بگونه ای طراحی شده اند که آدرس های فوق را عبور (Forward) نخواهند کرد.

through 10.255.255.255 Range 1: Class A - 10.0.0.0
Range 2: Class B - 172.16.0.0 through 172.31.255.255
Range 3: Class C - 192.168.0.0 through 192.168.255.255

امنیت

همزمان با پیاده سازی یک NAT پویا، یک فایروال بصورت خودکار بین شبکه داخلی و شبکه های خارجی ایجاد می گردد. NAT صرفا" امکان ارتباط به کامپیوترهائی را که در حوزه داخلی می باشند را خواهد داد. این بدان معنی است که یک کامپیوتر موجود در خارج از شبکه داخلی ، قادر به ارتباط مستقیم با یک کامپیوتر موجود در حوزه داخلی نبوده ، مگر اینکه ارتباط فوق توسط کامپیوتر شما مقدار

دهی اولیه (هماهنگی های اولیه از بعد مقداردهی آدرس های مربوطه) گردد. شما براحتی قادر به استفاده از اینترنت دریافت فایل و ... خواهید بود ولی افراد خارج از شبکه نمی توانند با استفاده از آدرس IP شما، به کامپیوتر شما متصل گردند. NAT ایستا ، امکان برقراری ارتباط با یکی از کامپیوترهای موجود در حوزه داخلی توسط دستگاههای موجود در خارج از شبکه را ، فراهم می نمایند.

برخی از روترهای مبتنی بر NAT امکان فیلترینگ و ثبت ترافیک را ارائه می دهند. با استفاده از فیلترینگ می توان سایت هائی را که پرسنل یک سازمان از آنها استفاده می نمایند را کنترل کرد.با ثبت ترافیک یک سایت می توان از سایت های ملاقات شده توسط کاربران آگاهی و گزارشات متعددی را بر اساس اطلاعات ثبت شده ایجاد کرد.

NAT دربرخی موارد با سرویس دهندگان Proxy ، اشتباه در نظر گرفته می شود. NAT و Proxy دارای تفاوت های زیادی می باشند. NAT بی واسطه بین کامپیوترهای مبداء و مقصد قرار می گیرد. Proxy بصورت بی واسطه نبوده و پس از استقرار بین کامپیوترهای مبداء و مقصد تصور هر یک از کامپیوترهای فوق را تغییر خواهد داد. کامپیوتر مبداء می داند که درخواستی را از Proxy داشته و می بایست بمنظور انجام عملیات فوق (درخواست) پیکربندی گردد. کامپیوتر مقصد فکر می کند که سرویس دهنده Proxy بعنوان کامپیوتر مبداء می باشد. Proxy در لایه چهارم (Transport) و یا بالاتر مدل OSI ایفای وظیفه می نماید در صورتیکه NAT در لایه سوم (Network) فعالیت می نماید. Proxy ، بدلیل فعالیت در لایه بالاتر در اغلب موارد از NAT کندتر است .