بررسی کامل IPv4,IPv6,NAT و وضعیت ایران در استفاده از IPv6

IPv4چیست؟

Internet Protocol version 4یا همان IPv4 نسخه چهارم پروتکل اینترنت (IP) است. این یکی از پروتکل های اصلی روش های کار با اینترنت مبتنی بر استانداردها در اینترنت و سایر شبکه های دارای بسته است IPv4 .اولین نسخه برای تولید در ARPANET در سال 1983 بود. امروزه هنوز بیشتر ترافیک اینترنت را IPv4 هدایت می کند. این پروتکل با هدف ایجاد یک سیستم ارتباطی پایدار و مقیاس پذیر برای شبکه‌های کامپیوتری طراحی شد . در اوایل ، IPv4به عنوان یک راه‌حل موقت در نظر گرفته می‌شد، اما به مرور زمان و با گسترش سریع اینترنت ، به پروتکل اصلی تبدیل شد.

مفهوم آدرس Ip ورژن 4(IPv4)

IPv4از ۴ قسمت تشکیل شده است که هر قسمت شامل یک عدد است که می تواند مقدار آن از ۰ تا ۲۵۵ متغیر باشد، به عبارت دیگر هر قسمت آن معرف یک Byte است و هر Byte هم از ۸ bit تشکیل شده است.همانطو که گفتیم هر قسمت IPشامل ۱ بایت می شود و هر بایت هم شامل ۸ بیت می شود. بیت ها تنها می تواند دو حالت صفر و یک داشته باشند. در نتیجه تمامی ۴ بایت IPv4 که شامل ۳۲ بیت است شامل اعداد صفر و یک است.اگر این ۳۲ بیت را در کنار یکدیگر بگذاریم و به هر کدام از آن ها یک وزن بدهیم و کل این بیت ها به اعداد Decimal تبدیل کنیم، هر قسمت می تواند یک عدد تشکیل دهد که از صفر تا ۲۵۵ می تواند متغیر باشد.

طرز کار IPV4 به صورت یک آدرس 32 بیتی است که شناسایی دستگاه‌های موجود در شبکه را ممکن می‌کند IPV4 . حجم بسیاری از ترافیک شبکه را به خود اختصاص می‌دهد (بالای 90 درصد) و با قابلیت ذخیره‌ی بیش از 4 میلیارد آدرس، به عنوان پروتکل اصلی اینترنت در این زمینه پیشتاز است IPV4.به صورت یک رشته عدد و رقم است که با نقطه یا دات (.) از هم جدا می‌شوند. این اعداد در مبنای 10 هستند ولی برای یک کامپیوتر در مبنای 2 قابل فهم هستند.

مثلا اگر یک آدرس IP از نوع IPV4 به شکل زیر داشته باشیم :172.16.17.1برای یک کامپیوتر به شکل زیر دیده می‌شود:

00000001 . 00010001 . 00010000 . 10101100

در مبنای 10 هر قسمت از اعداد بالا بین صفر و 225 قرار می‌گیرد و در مبنای 2 هر بخش متشکل است از 8 بیت بین صفر و یک، و هر کدام از این قسمت‌ها 1 بایت هستند.از آن جایی که هر کدام از قسمت‌ها می‌تواند از عدد صفر تا 255 یعنی 256 عدد را شامل شود به طور دقیق IPV4 می‌تواند 4294967296 سیستم را پوشش دهد. البته به دلایل مختلفی مانند افزایش سرورها به صورت روزانه باعث محدودیت استفاده از این نوع IP شده است به همین دلیل IPV6 به وجود آمده است.

کلاس‌های آدرسIPv4

درIPv4 ، آی پی ها به پنج دستهA ، B، C، Dو E تقسیم می‌شوند و هر کلاس دارای رنج مختص به خود است. توسط کلاس هایIPv4 ، تعداد دستگاه‌های موجود در یک شبکه تعیین می‌گردد. در درجه اول، کلاس‌هایA ، Bو C قرار دارند که توسط اکثر دستگاه‌های موجود در اینترنت استفاده می‌شوند. علاوه بر این، کلاس‌های D و E برای موارد خاص کاربرد دارند.

رنج IP عمومی و خصوصی کلاسA

کلاس A مخصوص شبکه هایی با تعداد هاست بالا است. این کلاس با استفاده از octet اول برای) network ID شناسه شبکه)، می‌تواند 126 شبکه داشته باشد. بیت اول در اینoctet ، همیشه صفر است و 7 بیت باقی مانده در آن، network IDرا کامل می‌کنند. 24 بیت بعدی در سه octet باقی مانده،) hosts IDشناسه میزبان) خواهند بود. به عبارت دیگر، تقریبا 17 میلیون هاست به ازای هر شبکه وجود خواهد داشت.

مشخصات کلاس A به صورت زیر است:

رنج آی پی عمومی: 1.0.0.0 تا 127.0.0.0

محدوده مقدار octet اول: از 1 تا 127

رنج آی پی خصوصی: 10.0.0.0 تا 10.255.255.255

) Subnet Maskمشخص می‌کند میزبان در حال حاضر در کدام شبکه قرار دارد): 255.0.0.0 (8 بیت)

تعداد شبکه ها: 126

تعداد هاست در هر شبکه: 16,777,214

رنج IP عمومی و خصوصی کلاسB

کلاس B برای شبکه‌هایی با ابعاد متوسط رو به بالا، کاربردی‌تر است. این مورد از کلاس های IPv4 با استفاده از دو octetاول (16 بیت)، می‌تواند تعداد 16384 شبکه برای network ID فراهم کند. در octet اول، دو بیت ابتدایی، همیشه 0 1 در نظر گرفته می‌شوند. 6 بیت باقی مانده، همراه با 8 بیت دوم، network IDرا کامل می‌کنند. 16 بیت مربوط به octet سوم و چهارم، نشان‌دهنده hosts ID هستند که تقریبا امکان ارائه 65000 میزبان به ازای هر شبکه را ممکن می‌سازند.

در لیست زیر می‌توانید مشخصات کلاس B را مشاهده نمایید:

رنج آی پی عمومی: 128.0.0.0 تا 191.255.0.0

محدوده مقدار octet اول: از 128 تا 191

رنج آی پی خصوصی: 172.16.0.0 تا 172.31.255.255

Subnet Mask:مقدار 255.255.0.0 (16 بیت)

تعداد شبکه ها: 16,382

تعداد هاست در هر شبکه: 65,534

رنج IP عمومی و خصوصی کلاسC

کلاس C در شبکه‌های محلی کوچک (LAN) استفاده می‌شود. این کلاس با استفاده از سه octet اول (24 بیت) برای network ID، تقریبا می‌تواند 2 میلیون شبکه داشته باشد.

در یک آدرس IP کلاسC ، سه بیت اول از نخستین octet به صورت ثابت 0 1 1 است. 21 بیت باقی مانده از سه octetاول، network IDرا کامل می‌کنند. 8 بیت آخر نشان دهنده Host ID است که می‌تواند در هر شبکه، 254 عدد HOSTارائه نماید.

در زیر مشخصات کلاس C را می‌توانید مشاهده نمایید:

رنج آی پی عمومی: 192.0.0.0 تا 223.255.255.0

محدوده مقدار octet اول: از 192 تا 223

رنج آی پی خصوصی: 192.168.0.0 تا 192.168.255.255

رنج آی پی ویژه: 127.0.0.1 تا 127.255.255.255

Subnet Mask:مقدار 255.255.255.0 (24 بیت)

تعداد شبکه ها: 2,097,150

تعداد هاست در هر شبکه: 254

رنج آدرس IP کلاسD

آدرس‌های IP کلاسD ، به هاست‌ها تعلق نمی‌گیرند و برای multicasting کاربرد دارند Multicasting .به هاست این امکان را می‌دهد تا به صورت همزمان مجموعه‌ای از داده‌ها را به هزاران هاست در سراسر اینترنت، ارسال کند. در اکثر مواقع برای پخش صدا و تصویر، مانند شبکه‌های تلویزیونی کابلی مبتنی بر IP استفاده می‌شود.

رنج: 224.0.0.0 تا 239.255.255.255

محدوده مقدار octet اول: از 224 تا 239

تعداد شبکه ها: نامشخص

تعداد هاست در هر شبکهMulticasting :

رنج آدرس IP کلاسE

آدرس‌های IP کلاس E نیز به هاست تعلق نمی‌گیرند و کاربرد عمومی ندارند. آنها صرفا برای اهداف تحقیقاتی رزرو شده اند.

رنج: 240.0.0.0 تا 255.255.255.255

محدوده مقدار octet اول: از 240 تا 255

تعداد شبکه ها: نامشخص

تعداد هاست در هر شبکه: برای اهداف تحقیقاتی و پژوهشی رزرو شده اند.

روش های پیدا کردن IPv4 در سیستم

می‌توانید آدرس IPv4 خود را با تایپ "What's my IP" در Google.com پیدا کرده و بدون نیاز به باز کردن هیچ صفحه‌ای، آن را مشاهده کنید.

اگر از ویندوز استفاده می‌کنید، می‌توانید Cmd را باز کرده و "Ipconfig" را تایپ نمایید. سپس پیکربندی کامل IP را مشاهده خواهید کرد.

در لینوکس، پس از باز کردن ترمینال، عبارت Ip addr را تایپ کنید. سپس با جستجوی عبارتinet ، آدرس IP خود را مشاهده خواهید نمود. علاوه بر این، در لینوکس وmacOS ، می‌توانید IPv4 خود را با دستور Dig نیز به دست آورید.اپلیکیشن Terminal را باز کرده و دستور زیر را تایپ کنید dig example.com:به جای example.com نام دامنه موردنظرتان را جایگزین نموده و سپس آدرس IPv4 مربوط به آن را مشاهده نمایید.

یکی دیگر از روش هایی که می توانید برای فهمیدن آی پی آدرس کامپیوتر مورد استفاده قرار دهید استفاده از بخش کنترل پنل و بخش Network connection می باشد. با استفاده از این بخش می توانید به تمام ویژگی های شبکه های متصل شده مانند نام شبکه، نوع اتصال، نوع DNS و ... دسترسی داشته باشید. با توجه به کارکرد صحیح این روش، می توانید آن را در نسخه های مختلف ویندوز مورد استفاده قرار دهید و بدون هیچ مشکلی به IP خود دسترسی داشته باشید.

انواع مختلف آدرس‌هایIP

ما در این مقاله به بررسی Ipv4 چیست پرداخته ایم در اینجا لازم است درمورد انواع مختلف آدرس های IP بیشتر بدانیم.آدرس‌های IP در انواع مختلفی وجود دارند که هر کدام کاربردهای خاصی دارند:

IPخصوصی

IPخصوصی امروزه نقش بسزایی در حفظ حریم خصوصی آنلاین افراد ایفا می‌کند. این نوع آدرس اینترنتی، جلوگیری از ردیابی و نظارت ناخواسته توسط شرکت‌ها یا هکرها را فراهم می‌کند. با استفاده از IP خصوصی، افراد می‌توانند به طور امن‌تر و حفظ حریم خصوصی، اطلاعات خود را در فضای مجازی به اشتراک بگذارند. این امکان باعث افزایش اعتماد و امنیت در تبادل اطلاعات شخصی می‌شود و نقش مهمی در حفظ امنیت آنلاین افراد ایفا می‌کند.

IPخصوصی برای شبکه‌های داخلی مانند شبکه‌های خانگی یا دفتری استفاده می‌شود. این آدرس‌ها در فضای بیرونی شبکه قابل دسترس نیستند و برای ایجاد یک شبکه امن و بسته کاربرد دارند.

IPعمومی

آدرس IP عمومی، شناسه‌ای یکتاست که به هر دستگاه در اینترنت اختصاص می‌یابد. این آدرس اجازه اتصال دستگاه به شبکه را می‌دهد و به عنوان شناسه خاصی در ارتباط با دیگر دستگاه‌ها عمل می‌کند. با این حال، مصرف آدرس IP عمومی ممکن است به دلیل کمبود منابع، مسائل امنیتی یا حفظ حریم خصوصی، به چالش کشیده شود و راه‌حل‌های متنوعی برای مدیریت بهتر استفاده از آن وجود دارد.

آدرس‌های IP عمومی برای دستگاه‌هایی که به شبکه بین‌المللی اینترنت متصل هستند، استفاده می‌شود. این آدرس‌ها در سراسر جهان یکتا هستند و امکان ارتباط بین شبکه‌های مختلف را فراهم می‌کنند.

IPپویا

آدرس IP پویا یک راه حل مدرن برای مدیریت نیازهای شبکه است. در این سیستم، دستگاه‌ها به طور خودکار آدرس IP دریافت می‌کنند، که به بهره‌وری و امنیت شبکه کمک می‌کند. این رویکرد از اختصاص آدرس‌های ثابت جلوگیری می‌کند و امکان اختصاص آدرس‌های متغیر به دستگاه‌ها را فراهم می‌سازد، که در بهینه‌سازی مدیریت شبکه و جلوگیری از تداخل‌های IP موثر است.

IPاستاتیک

آدرس IP استاتیک یک شناسه ثابت است که به دستگاه‌ها در شبکه اختصاص می‌یابد و تغییر نمی‌کند. این نوع آدرس به ابزارهایی نظیر سرورها یا دستگاه‌هایی که به دسترسی ثابت نیاز دارند، اختصاص می‌یابد. استفاده از آدرس IP استاتیک مزایایی از قبیل مدیریت آسان شبکه و دسترسی ثابت را فراهم می‌کند. با این حال، ممکن است مشکلات امنیتی را به دنبال داشته باشد و نیاز به پیکربندی دقیق توسط مدیران داشته باشد.

آی پی اشتراکی

آی‌پی اشتراکی یک مدل است که چندین دستگاه به یک آدرس آی‌پی مشترک متصل می‌شوند. این رویکرد معمولاً در شبکه‌های کوچک یا مناطق عمومی به‌کار می‌رود. با اشتراک آدرسIP ، مدیران می‌توانند منابع شبکه را بهینه کنند و هزینه مدیریت زیرساخت را کاهش دهند. اما باید به دقت به مسائل امنیتی و مدیریت تداخل دقت شود.

تهدیدهای امنیتی آدرس IP

در دنیای دیجیتال امروز، موضوع "تهدیدهای امنیتی آدرس IP" اهمیت ویژه‌ای دارد. آدرسIP ، که به عنوان شناسه هر دستگاه در شبکه عمل می‌کند، می‌تواند در معرض انواع حملات در شبکه های کامپیوتری قرار گیرد. از جمله این تهدیدها می‌توان به حملات سایبری مانند دسترسی غیرمجاز، جاسوسی دیجیتال، و حملات DDoS اشاره کرد. این حملات می‌توانند به سرقت اطلاعات، اختلال در دسترسی به سرویس‌ها، و حتی خسارات مالی منجر شوند.

محافظت از آدرس IP با استفاده از تدابیر امنیتی مانند فایروال‌ها، سیستم‌های تشخیص نفوذ، و رمزگذاری اطلاعات، برای جلوگیری از این تهدیدها ضروری است. همچنین، استفاده از VPN برای مخفی کردن آدرس IP واقعی و افزایش حریم خصوصی توصیه می‌شود.

ویژگی های کلیدیIPv4

IPv4یک پروتکل بدون اتصال است.

اجازه ایجاد یک لایه ارتباط مجازی ساده بر روی دستگاه های متنوع را میدهد.

IPv4به حافظه کمتری نیاز دارد و به راحتی آدرس ها را به خاطر می سپارد.

پروتکل های این IP قبلاً توسط میلیون ها دستگاه پشتیبانی شده است.

IPv4کتابخانه های ویدیویی و کنفرانس ها را به راحتی ارائه می دهد.

ویژگی‌ها و مزایایIPv4

IPv4به دلیل طراحی ساده و قدمت طولانی ، به خوبی توسط اکثر دستگاه‌ها و شبکه ها پشتیبانی می‌شود . این سازگاری باعث شده تا پیاده سازی و استفاده از آن در شبکه‌های مختلف آسان باشد.

استفاده از NAT یکی از مزایای ای پی وی فور ، امکان استفاده از ترجمه آدرس شبکه (NAT) است که به شبکه های محلی اجازه می‌دهد با استفاده از یک آدرس IP عمومی ، تعداد زیادی دستگاه را به اینترنت متصل کنند . این ویژگی به بهینه‌سازی مصرف آدرس های IPv4 کمک می‌کند.

IPv4با مجموعه‌ای از پروتکل‌ها و فناوری‌های مرتبط مانند DHCP (Dynamic Host Configuration Protocol) که برای تخصیص خودکار آدرس‌های IP استفاده می‌شود ، کار می‌کند. این پروتکل‌ها به مدیریت آسان تر شبکه ها کمک می‌کنند.

یکی از مزایای IPv4 ایمن بودن و حفظ حریم خصوصی آن است IPv4 .را می توان رمزگذاری کرد و به آن اجازه می دهد تا با پیشرفت های امنیت IP و حفظ حریم خصوصی مطابقت داشته باشد.

تخصیص شبکه ها در IPV4 قدرتمند است و حدود 85000 روتر کاربردی دارد.

IPv4خدمات ارتباطی با کیفیت و انتقال دانش اقتصادی را ارائه می دهد.

آدرس های IPV4 امکان رمزگذاری مجدد را فراهم می کنند.

IPv4امکان آدرس دهی جمعی را فراهم می کند زیرا مسیریابی مقیاس پذیر و مقرون به صرفه است.

IPv4ارتباط داده های شبکه را در سازمان های چند پخشی امکان پذیر می کند.

محدودیت‌ها و مشکلاتIPV4

یکی از بزرگترین محدودیت‌ها ، تعداد محدود آدرس‌های IP است. با افزایش تعداد دستگاه‌های متصل به اینترنت، این محدودیت به یک چالش جدی تبدیل شده است. این مشکل منجر به پیدایش و توسعه IPv6 شده است.

IPv4به طور پیش‌فرض ویژگی‌های امنیتی قوی ندارد. امنیت شبکه‌های IPV4 نیازمند پیاده‌سازی و پیکربندی جداگانه است که می‌تواند پیچیدگی‌های اضافی ایجاد کند.

با افزایش تعداد دستگاه‌ها و پیچیدگی شبکه‌ها، مدیریت آدرس‌های IPv4می‌تواند دشوار و زمان‌بر باشد. این مشکل به خصوص در شبکه‌های بزرگتر و پیچیده‌تر محسوس است.

مسیریابی اینترنت در IPv4 بی اثر است.

IPv4کمی گران است زیرا هزینه مدیریت سیستم بالایی دارد.

IPv4پیچیده، کند و در برابر خطاها آسیب پذیر است.

IPv4کار فشرده است و ویژگی های امنیتی آن غیر اجباری است.

وقتی صحبت از رشد خالص می شود، IPv4مانع استفاده از سود خالص برای کاربران جدید می شود و رشد خالص آن را برای کاربران فعلی محدود می کند.

کاربردهایIPv4

IPv4در طیف گسترده‌ای از کاربردهای شبکه ای مورد استفاده قرار می‌گیرد:

–شبکه‌های خانگی و اداری : اکثر شبکه‌های خانگی و اداری از IPv4 برای اتصال دستگاه‌های خود به اینترنت استفاده می‌کنند.

–سرورها و خدمات وب: بسیاری از سرورها و خدمات اینترنتی همچنان از آدرس‌های IPv4 استفاده می‌کنند.

–شبکه‌های اختصاصی و محلی: بسیاری از شبکه‌های محلی و خصوصی به دلیل سازگاری بالا و سادگی IPv4 از این پروتکل بهره می‌برند.

نتیجه‌گیری

IPv4به عنوان یکی از اساسی‌ترین پروتکل‌های اینترنت ، نقش مهمی در توسعه و گسترش شبکه‌های کامپیوتری ایفا کرده است. با وجود محدودیت‌ها و چالش‌های آن، IPv4همچنان به عنوان یک پروتکل قابل اعتماد و پرکاربرد باقی مانده است. اما با افزایش تقاضا برای آدرس‌های IP و نیاز به امنیت بیشتر، مهاجرت به IPv6 به عنوان یک راه‌حل پایدارتر و بلندمدت ضروری به نظر می‌رسد.

Ipv6چیست؟

IPv6 (Internet Protocol version 6)جدیدترین و بهبودیافته‌ترین نسخه IP است که توسط گروه ویژه مهندسی اینترنت ((IETFدر سال 1998 ایجاد شده است (Internet Protocol) IP .شناسه منحصربه‌فردی است که هویت هر یک از کامپیوترها یا دیگر تجهیزات متصل به شبکه را مشخص می‌کند. در شبکه‌های مبتنی بر پروتکل اینترنت (آی‌پی)، هر کامپیوتر یا دستگاه متصل به شبکه، یک آدرس آی‌پی (IP address) دارد که آن را از دیگر کامپیوترهای تحت شبکه متمایز می‌کند. پروتکل اینترنت یا آی‌پی، آدرس مقصد بسته‌های داده را تعیین و بسته‌ها را از مبدأ تا مقصد مسیریابی می‌کند. پروتکل اینترنت نسخه 6 پروتکلی است که ظرفیت انتقال اطلاعات در شبکه اینترنت یا همان ترافیک را افزایش دهد.

هر رایانه، تلفن همراه، اتوماسیون خانگی، حسگر اینترنت اشیا و سایر دستگاه‌های متصل به اینترنت برای برقراری ارتباط بین سایر دستگاه‌ها به یک آدرس IP احتیاج دارند. طرح اصلی آدرس IP که IPv4 نامیده می‌شود، به دلیل استفاده گسترده و زیاد شدن دستگاه‌های متصل به اینترنت، در حال اتمام است.

همان‌طور که گفتیم IP یا Internet Protocol Address شناسه‌ای است که به دستگاه‌های متصل یا شبکه‌های در حال استفاده از اینترنت از طریق سرویس‌دهنده اینترنت یا ISP اختصاص داده می‌شود. هر آدرس IP از 4 بخش یا Octet تشکیل شده و این آی‌پی مجموعاً از 32 بیت تشکیل می‌شود و IPv4 نام دارد.

در نسخه 6 از IP ها، یک آدرس آی‌پی 128 بیتی شامل 8 اکت 16 بیتی خواهیم داشت. از آنجایی که هر دستگاهی در اینترنت آی‌پی منحصربه‌فردی دارد. آدرس‌های IPv6 از رقم هگزا دسیمال 128 بیتی تشکیل شده است که امکان افزایش چشمگیر تعداد ماشین‌هایی را فراهم می‌کند که اینترنت از عهده آن‌ها بر می‌آید و در 64 بیت اول آدرس، آدرس شبکه Network Prefixو 64 بیت دوم آدرس منحصربه‌فرد کارت‌های شبکه هستند.

IPها یک جز ضروری برای دستگاه‌های مجهز به اینترنت است که نحوه ارتباط این دستگاه‌ها با یکدیگر را مشخص می‌کند. آن‌ها به‌عنوان شناسه برای بخش‌های خاص در یک شبکه عمل می‌کنند و امکان ایجاد ارتباط بین یک مقصد ارتباطی و منبع را فراهم می‌کنند. در حال حاضر، ارائه‌دهندگان خدمات اینترنتی دو نسخه از آدرس IPv4 – IP و IPv6 را ارائه می‌دهند. در مقاله قبلی تفاوت بین این دو نوع آدرس IP را بیان کردیم و در ادامه قصد داریم در مورد مزایای IPv6)پروتکل اینترنت نسخه 6) صحبت کنیم.

مزایای IPv6 چیست؟

IPv6مزایای زیادی نسبت به IPv4 دارد و تنها مزیت آن تعداد بالای رنج آی‌پی و یا آدرس‌های شبکه نیست. در اینجا برخی دیگر از مزایا و پیشرفت‌هایی که با استفاده از این IP به دست می‌آید را مطرح می‌کنیم.

مسیریابی کارآمد

همان‌طور که محاسبات شبکه بیان می‌کند، IPv6اندازه جداول مسیریابی را کاهش می‌دهد. این امر باعث مسیریابی کوتاه‌تر شود، بنابراین نیازی نیست که کنترل مجدد در هر پرش روتر انجام شود، یعنی آی‌پی نسخه 6 به ISP ها اجازه می‌دهد پیشوندهای شبکه‌های مشتریان خود را در یک پیشوند واحد جمع کرده و این پیشوند را به اینترنت IPv6 اعلام کنند.

پردازش بهتر پکت‌ها

IPv6دارای پردازش ساده‌تری نسبت به IPv4 است، بنابراین داده‌ها می‌توانند از طریق یک شبکه ارتباطی به‌سرعت حرکت کنند. پردازش بهتر پکت‌ها، مسیر رسیدن به مقصد را بهبود می‌بخشد و اگر در این مسیر خطایی به وجود آید امکان تشخیص خطا برای رفع مشکل را امکان‌پذیر می‌کند.

پیکربندی ساده‌تر شبکه

این آی‌پی به‌صورت خودکار پیکربندی آدرس را انجام می‌دهد، این بدان معنی است که میزبان می‌تواند آدرس IP خود را ایجاد کند، راه‌اندازی شبکه شما را ساده کرده و هزینه استقرار IPv6 را کاهش دهد. به‌طور مثال برای پیکربندی IPv4 در MAC، سیستم‌عامل نیاز به DHCP دارد، اما این فرآیند اضافی در IPv6 لازم نیست.

حرکت در مسیرهای مختلف بدون تغییرIP

برای استفاده از این نوع ا آی‌پی‌ها دیگر نیاز نیست برای رسیدن به مقصد میزبان آی‌پی تغییر نماید و دستگاه می‌تواند بدون از دست دادن اتصال به آدرس IP خود، بین پیوندهای مختلف حرکت کند.

آدرس‌های IP بیشتر

این‌یکی از اساسی‌ترین مزایای استفاده از IPv6 نسبت به IPv4 است IPv4 .از 4.3 میلیارد آدرس پشتیبانی می‌کند و IPv6 از 340 تریلیون آدرس پشتیبانی می‌کند.

NATوIPv6

یکی دیگر از مزایای استفاده از آدرس IPv6 این است که نیاز به NAT را به شدت کاهش می‌دهد Network Address. Translation (NAT)آدرس IP کامپیوترهای موجود در شبکه محلی را به یک آدرس IP واحد ترجمه می‌کند و معمولاً برای محدود کردن آدرس‌های IP مورد استفاده سازمان برای اهداف امنیتی استفاده می‌شود. به دلیل کمبود آدرس اینترنتی، NATیکی از اجزای ضروری IPv4 است، اما از آنجا که IPv6 از مقدار تقریباً نامحدودی آدرس IP پشتیبانی می‌کند، دیگر نیازی به NAT نیست NAT .اجازه استفاده از محدوده‌های IP خصوصی بر روی شبکه‌های محلی و اشتراک‌گذاری یک آدرس اینترنتی خارجی را می‌دهد که این شیوه در شبکه IPv4 مرسوم است.

VoIPدرIPv6

با رشد چشمگیر VoIP در کسب‌وکارها، کمبود فضای آدرس به یک نگرانی قطعی تبدیل می‌شود.نهاد طرح آدرس‌دهی IPv6، همراه با بهبود موارد مختلف دیگر از جمله کیفیت خدمات، به VoIP کمک می‌کند تا به اصلی‌ترین ارتباطات جهانی تبدیل شود.در حال حاضر، کاربران شبکه‌های IP مبتنی بر IPv4 به دلیل از دست رفتن بسته یا تأخیر در شبکه، گاهی اوقات با تأخیر و اکو صدا مواجه می‌شوند IPv6 .آماده است تا با رعایت مجموعه‌ای از خدمات، با ارائه عملکرد مطلوب هنگام انتقال ترافیک (از جمله صدا) از طریق شبکه، این موارد را اصلاح کند.

NATچیست؟

NATکه مخفف عبارت Network Address Translation به معنای «ترجمه آدرس شبکه» است، یکی از فناوری های بنیادی در زیرساخت های ارتباطی شبکه به شمار می رود. این تکنولوژی به مدیران شبکه این امکان را می دهد که چندین دستگاه موجود در یک شبکه محلی (Local Area Network LAN) یا بتوانند با استفاده از یک آدرس IP عمومی (Public IP Address)، به اینترنت متصل شوند. در واقع، NATبا تبدیل آدرس های خصوصی (Private IP Addresses)به آدرس عمومی و بالعکس، فرآیند ارتباط بین شبکه داخلی و اینترنت را تسهیل می کند.

این مکانیزم نه تنها به صرفه جویی در مصرف آدرس های IPv4 کمک می کند، بلکه با پنهان سازی ساختار داخلی شبکه، لایه ای از امنیت نیز به ارتباطات اضافه می نماید. به همین دلیل، NATبه عنوان یکی از راهکارهای کلیدی برای مقابله با محدودیت آدرس های IP و ارتقاء امنیت در شبکه های خانگی و سازمانی شناخته می شود.

انواع NAT در شبکه

آشنایی با انواع NAT و کاربرد آن ها، به مدیران شبکه و متخصصان فناوری اطلاعات کمک می کند تا مناسب ترین ساختار را برای بهینه سازی مصرف IP و افزایش امنیت انتخاب کنند. در ادامه به بررسی مهم ترین انواع NAT می پردازیم:

انواع NAT در شبکه

Static NAT

در NAT استاتیک، یک آدرس IP خصوصی به صورت دائمی به یک آدرس IP عمومی مشخص نگاشت می شود. این نوع NAT مناسب برای دستگاه هایی مانند وب سرورها، سرورهای ایمیل و دوربین مداربسته است که نیاز به دسترسی مداوم از خارج شبکه دارند Static NAT .شفافیت و ثبات بالا را فراهم می سازد اما به ازای هر دستگاه، نیاز به یک آدرس IP عمومی وجود دارد.

Dynamic NAT

NATداینامیک از یک استخر (Pool) از آدرس های IP عمومی استفاده می کند و به صورت موقتی به دستگاه های داخلی که به اینترنت نیاز دارند، آدرس عمومی اختصاص می دهد. برخلاف NAT ایستا ، این نگاشت دائمی نیست و تنها در زمان نیاز ایجاد می شود. این روش برای سازمان هایی با تعداد زیادی کلاینت و محدودیت در تعداد IP عمومی، گزینه ای کارآمد به شمار می رود.

NAT Overloaad یاPAT

PAT: Port Address Translationنوعی پیشرفته از NAT پویا است که در آن چندین دستگاه داخلی از طریق یک آدرس IP عمومی و با پورت شبکه متفاوت به اینترنت متصل می شوند. این روش که با نام NAT Overload نیز شناخته می شود، در شبکه های خانگی و کسب وکارهای کوچک بسیار رایج است PAT .با صرفه جویی حداکثری در منابع IP و امکان اتصال همزمان تعداد زیادی کاربر به اینترنت، یک راه حل بسیار محبوب و مقرون به صرفه است.

Full-Cone NAT

درFullcone NAT ، زمانی که یک اتصال از داخل شبکه به خارج برقرار شود، هر ترافیکی که از همان آدرس IP و پورت بازگشت کند، بدون محدودیت پذیرفته می شود. این نوع NAT برای بازی های آنلاین، تلفن VoIP و اپلیکیشن هایی که به ارتباطات آزاد و سریع نیاز دارند بسیار مناسب است.

Symmetric NAT

Symmetric NATبرای هر اتصال خروجی، یک نگاشت یکتا بین آدرس IP داخلی و خارجی ایجاد می کند. در نتیجه، فقط سرورهایی که دستگاه داخلی ابتدا به آنها متصل شده، قادر به پاسخ دهی هستند. این ویژگی باعث افزایش امنیت شبکه می شود، اما ممکن است با برخی نرم افزارها و پروتکل های شبکه مانند P2P و فایل شیرینگ سازگاری کامل نداشته باشد.

نحوه کار NAT در شبکه

نحوه کار NAT مبتنی بر تبدیل و مدیریت آدرس های IP میان شبکه داخلی و اینترنت است. در یک سناریوی رایج مانند شبکه خانگی، همه دستگاه ها (نظیر لپ تاپ، تلفن همراه یا تلویزیون هوشمند) از طریق یک روتر به اینترنت متصل هستند. این روتر، که معمولاً توسط ارائه دهنده خدمات اینترنت (ISP) پیکربندی شده است، دارای یک آدرس IP عمومی (Public IP)است.

وقتی یکی از این دستگاه ها قصد دسترسی به اینترنت را دارد، تکنولوژی NAT وارد عمل شده و آدرس IP خصوصی (Private IP)آن دستگاه را به IP عمومی ترجمه می کند. پس از ارسال درخواست به سرور مقصد، پاسخ دریافتی نیز توسط NAT مجدداً به آدرس IP داخلی دستگاه مبدا بازگردانده می شود. این فرآیند ترجمه دوسویه، نه تنها موجب صرفه جویی در مصرف آدرس های IPv4 می شود، بلکه سطحی از امنیت و کنترل را نیز برای شبکه داخلی فراهم می سازد.

کاربردهای NAT در شبکه های کامپیوتری

NATدر شبکه های کامپیوتری به عنوان یکی از اجزای حیاتی برای مدیریت آدرس های IP و برقراری ارتباط امن و پایدار با اینترنت شناخته می شود. استفاده از NAT این امکان را فراهم میسازد که دستگاه های متعدد داخل یک شبکه ی محلی (LAN) بدون نیاز به داشتن آدرس IP عمومی اختصاصی، به صورت همزمان به اینترنت متصل شوند. این ویژگی به ویژه در زمان بحران کمبود آدرس هایIPv4 ، تحولی بزرگ در دنیای شبکه ایجاد کرد.

از مهم ترین کاربردهای NAT در شبکه می توان به تبدیل آدرس های IP خصوصی (Private IP) به IP عمومی (Public IP)و بالعکس اشاره کرد. این تبدیل به روتر یا فایروال اجازه می دهد تا نقش واسطه بین شبکه داخلی و اینترنت را ایفا کند؛ به گونه ای که ترافیک ورودی و خروجی به صورت هدفمند و کنترل شده هدایت شود. همچنین، استفاده از NAT سطحی از امنیت را فراهم می کند، چرا که آدرس های داخلی از دید مستقیم کاربران خارجی پنهان می مانند.

NATعلاوه بر صرفه جویی در منابعIP ، در پیاده سازی سرویس های خاصی مانندVPN ، بازی های آنلاین، دسترسی به سرورهای داخلی از خارج شبکه) با استفاده از(Port Forwarding ، و مدیریت پهنای باند نیز نقش کلیدی ایفا می کند. به همین دلیل است که تقریباً در تمام روترها، فایروال ها و زیرساخت های شبکه ای امروزی، استفاده از NAT به یک استاندارد تبدیل شده است.

مزایای استفاده از NAT در شبکه

استفاده از NAT به یک راهکار کاربردی، مؤثر و مقرون به صرفه تبدیل شده است. در ادامه به مهم ترین مزایای این تکنولوژی می پردازیم:

صرفه جویی در مصرف آدرس های IP: NAT با تبدیل آدرس های خصوصی به یک آدرس عمومی، مشکل کمبود IP را برطرف می کند.

افزایش امنیت: با پنهان کردن IP داخلی، نفوذ به شبکه سخت تر می شود.

مدیریت آسان تر شبکه: تغییرات داخلی شبکه بدون نیاز به تنظیمات مجدد در بیرون انجام می شود.

افزایش توسعه پذیری شبکه: افزودن دستگاه جدید به شبکه بدون نیاز به IP جدید ممکن است.

مزایای NAT در شبکه

معایب استفاده ازNAT

با وجود مزایای زیاد، استفاده از NAT بدون محدودیت نیست. این تکنولوژی در کنار کاربردهای فراوانش، چالش هایی هم دارد که باید به آنها توجه کرد.

1

اختلال در ارتباط :End-to-End یکی از مهم ترین مشکلات NAT در شبکه، ایجاد مانع در ارتباط مستقیم بین دستگاه هاست. چون IP داخلی پنهان می ماند، دستگاه ها نمی توانند به راحتی از بیرون شبکه شناسایی شوند.

مشکل در اجرای برخی پروتکل ها: برخی اپلیکیشن ها و پروتکل هایی که بر پایه شناسایی مستقیم IP کار می کنند، در شبکه های NAT دچار اختلال می شوند. این تبدیل IP باعث قطع یا کندی ارتباط می گردد.

افزایش تاخیر :(Latency) ترجمه مداوم آدرس ها در NAT می تواند موجب تاخیر در شبکه و انتقال داده ها شود. این تاخیر برای فعالیت های حساس مثل تماس های VoIP یا بازی های آنلاین محسوس است.

ناسازگاری با برخی پروتکل های امنیتی: پروتکل هایی مثل IPsec ممکن است به خاطر نیاز به ساختار خاص، با NAT هماهنگ نباشند. این ناسازگاری باعث دردسر در پیاده سازی برخی ارتباطات امن می شود.

نتیجه گیری

در پایان، می توان گفت که فناوری NAT با تمام ابعاد فنی اش، به یکی از موثرترین راهکارهای زیرساختی در معماری شبکه های امروزی تبدیل شده است. با تکیه بر استفاده ازNAT ، امکان طراحی ساختارهای منعطف، مقیاس پذیر و قابل اطمینان فراهم می شود؛ ساختارهایی که پاسخگوی نیازهای متنوع کاربران در محیط های پیچیده و پویا هستند. درک صحیح از نحوه عملکرد و چالش های مرتبط با NAT در شبکه، به تصمیم گیری های دقیق تر و راه اندازی بهینه سامانه های ارتباطی کمک می کند. بنابراین، بهره گیری هدفمند از این فناوری، مستلزم نگاهی متعادل و آینده نگرانه به مزایا و محدودیت های آن است.

وضعیت ایران در استفاده از IPv6 چگونه است؟

IPv6چیست و چرا اهمیت دارد؟

پروتکل IPv6 نسخه جدیدتر پروتکل اینترنت (Internet Protocol) است که برای جایگزینی نسخه قبلی یعنی IPv4 طراحی شده است. مهم‌ترین مزیتIPv6 ، فضای آدرس‌دهی بسیار وسیع‌تر آن است که برای اتصال میلیاردها دستگاه در دنیای دیجیتال امروزی ضروری است. همچنین این پروتکل از نظر امنیت، سرعت و کارایی، به‌طور محسوسی بهبود یافته است و زیرساخت بسیاری از فناوری‌های نوین مانند اینترنت اشیاء (IoT) و خدمات ابری بر آن بنا شده‌اند.

اختلال گسترده و رفع تدریجی محدودیت‌ها

حدود یک ماه پیش، دسترسی به IPv6 به طور ناگهانی برای بسیاری از کاربران ایرانی قطع شد. این محدودیت باعث شد که سرویس‌ها و برنامه‌هایی که به این نسخه از پروتکل متکی بودند، دچار اختلال یا قطع کامل ارتباط شوند. حتی بسیاری از کاربران گزارش داده بودند که وی‌پی‌ان‌های مبتنی بر IPv6 نیز به‌طور کامل غیرفعال شده‌اند.

اما به‌تازگی و بر اساس داده‌های منتشرشده توسط «رادار کلادفلر»(Cloudflare Radar) ، وضعیت دسترسی به IPv6 به حالت عادی برگشته است. این نشان‌دهنده آن است که دسترسی به این پروتکل به‌صورت تدریجی در حال باز شدن برای کاربران مختلف در اپراتورهای اینترنتی ایران است.

کدام اپراتورها IPv6 را فعال کرده‌اند؟

طبق بررسی‌های انجام‌شده، در زمان نگارش این خبر، اپراتورهایی مانند شاتل، همراه اول و آسیاتک به طور رسمی دسترسی به IPv6 را فعال کرده‌اند. با این حال، هنوز این پروتکل روی شبکه ایرانسل فعال نشده و کاربران این اپراتور دسترسی مستقیمی به IPv6 ندارند. البته انتظار می‌رود که ایرانسل نیز در روزهای آینده این قابلیت را فعال کند و به صف دیگر اپراتورها بپیوندد.

چرا IPv6 مسدود شد و چرا بازگشایی آن مهم است؟

به گفته کارشناسان، یکی از دلایل اصلی مسدودسازی مکرر IPv6 در ایران، سختی اعمال فیلترینگ بر این نسخه از پروتکل اینترنت است. برخلاف IPv4 که زیرساخت‌های فیلترینگ برای آن به‌خوبی توسعه یافته‌اند، IPv6به دلیل ساختار پیشرفته‌ترش امکان اعمال محدودیت به‌صورت گسترده را دشوارتر می‌سازد. از همین رو، در مواقعی که نیاز به محدودسازی اینترنت احساس می‌شود، این نسخه از پروتکل به‌صورت کامل غیرفعال می‌شود.

اما بازگشت آن، به معنای گشایش و کاهش سطح محدودیت‌های اینترنتی تلقی می‌شود که می‌تواند گامی مثبت برای بهبود تجربه آنلاین کاربران باشد.

آیا تمام پروتکل‌های اینترنتی اکنون در دسترس هستند؟

بررسی‌ها حاکی از آن است که در حال حاضر، بیشتر پروتکل‌های پرکاربرد اینترنتی به جز HTTP/3 برای کاربران قابل استفاده‌اندHTTP/3 .، که بر پایه QUIC توسعه یافته و سرعت و امنیت بالاتری دارد، همچنان در برخی موارد مسدود یا با اختلال همراه است. با این حال، فعال‌سازی مجدد IPv6 می‌تواند نشانه‌ای از بازگشت تدریجی سایر پروتکل‌ها نیز باشد