سوال 1: مفهوم NAT چیست و چگونه کار میکند؟

جواب: NAT مخفف Network Address Translation به معنای «ترجمه نشانی‌های شبکه» است . NAT یک فناوری در سطح روتر یا فایروال است که برای ترجمه آدرس‌های IP خصوصی شبکه داخلی به آدرس‌های IP عمومی (و بالعکس) به کار می‌رود. این فرآیند به دستگاه‌های موجود در شبکه داخلی (LAN) اجازه می‌دهد تا بتوانند به اینترنت (WAN) دسترسی داشته باشند، در حالی که تنها از یک یا چند آدرس IP عمومی استفاده می‌شود.

هنگامی که یک دستگاه در شبکه داخلی (مثلاً با آدرس 192.168.1.5) قصد ارسال درخواست به اینترنت را دارد، این درخواست ابتدا به روتر ارسال می‌شود. روتر آدرس IP خصوصی مبدأ را با آدرس IP عمومی خود جایگزین کرده و بسته را به مقصد در اینترنت ارسال می‌کند. همچنین، روتر در یک جدول موسوم به NAT Table نگهداری می‌کند که کدام IP خصوصی، چه پورتی را برای برقراری ارتباط استفاده کرده است. پس از بازگشت پاسخ از مقصد، روتر با مراجعه به این جدول، پاسخ را به IP خصوصی مربوطه هدایت می‌کند.

سوال 2: تفاوت بین آدرس های IPخصوصی و عمومی در رابطه با NAT چیست؟

جواب: آدرس‌های IP به دو دسته کلی **خصوصی (Private)** و **عمومی (Public)** تقسیم می‌شوند. تفاوت این دو نوع آدرس در محدوده استفاده و نقش آن‌ها در ارتباطات شبکه‌ای، به‌ویژه در رابطه با **NAT (Network Address Translation)**، به صورت زیر میتوان گفت:

- NAT به‌عنوان یک واسط عمل که آدرس‌های خصوصی شبکه داخلی را به یک یا چند آدرس عمومی ترجمه می‌کند.
- دستگاه‌های دارای IP خصوصی به‌طور مستقیم به اینترنت دسترسی ندارند و تمام ترافیک خروجی آن‌ها باید از طریق آدرس IP عمومی روتر و با کمک NAT عبور کند.
- NAT باعث می‌شود چندین دستگاه دارای آدرس خصوصی بتوانند به‌صورت هم‌زمان و با استفاده از یک آدرس IP عمومی به اینترنت متصل شوند.

در سیستم‌های مبتنی برNAT ، آدرس‌های خصوصی برای استفاده در شبکه داخلی و آدرس‌های عمومی برای ارتباط با دنیای بیرون (اینترنت) در نظر گرفته می‌شوند NAT .این امکان را فراهم می‌سازد که تعداد زیادی دستگاه داخلی بتوانند از طریق یک یا چند آدرس عمومی به اینترنت متصل شوند، بدون نیاز به تخصیص IP عمومی مجزا به هر دستگاه.

سوال 3: چه تفاوتی بین Static NAT و Dynamic NAT وجود دارد؟

جواب: **Static NAT** و **Dynamic NAT** دو نوع از روش‌های پیاده‌سازی NAT هستند که تفاوت‌هایی در نحوه تخصیص آدرس دارند:

Static NAT یا ترجمه ایستا:

- در این روش، هر آدرس IP خصوصی به‌صورت **ثابت و دائمی** به یک آدرس IP عمومی خاص نگاشت می‌شود.
- این نگاشت از پیش تعریف شده است و تغییر نمی‌کند.
- بیشتر در مواردی استفاده می‌شود که یک دستگاه خاص در داخل شبکه (مانند یک وب‌سرور یا دوربین نظارتی) نیاز به دسترسی دائم و مستقیم از اینترنت داشته باشد.

Dynamic NAT یا ترجمه پویا:

- در این روش، آدرس IP خصوصی هنگام نیاز به اینترنت، به‌صورت **پویا** و **غیردائمی** از بین یک مجموعه ازIP های عمومی موجود ترجمه می‌شود.
- نگاشت در زمان استفاده ایجاد شده و پس از پایان ارتباط حذف می‌شود.
- بیشتر برای سازمان‌هایی با تعداد زیادی کاربر و محدودیت در تعدادIP های عمومی مفید است.

ویژگی	STATIC NAT	DYNAMIC NAT
نوع نگاشت	ثابت (ایستا)	پویا (موقت)
تعداد IP عمومی لازم	به ازای هر IP خصوصی، یک IP عمومی	مجموعه‌ای ازIP های عمومی به اشتراک گذاشته‌شده
استفاده رایج	سرورها، دستگاه‌هایی با دسترسی دائمی	کاربران داخلی با نیاز به اتصال موقت
پیکربندی	ساده و مشخص	نیاز به پیکربندی دقیق‌تر
امنیت	پایین‌تر	نسبتاً بالاتر

سوال 4: چه روشهایی برای بررسی عملکرد و خطایابی در شبکه های دارای NAT وجود دارد؟

جواب: ابزار های این کار عبارتند از:

۱ .بررسی جدول NAT (NAT Table Inspection)

- روترها و فایروال‌هایی که NAT را پیاده‌سازی می‌کنند، معمولاً دارای **جدول NAT** هستند که نگاشت بینIP های خصوصی و عمومی و همچنین شماره پورت‌ها را نشان می‌دهد.
- بررسی این جدول برای تحلیل مسیر ترافیک و شناسایی مشکل در ترجمه IP بسیار مؤثر است.
- این کار معمولاً از طریق دستورات مدیریتی در روتر یا فایروال انجام می‌شود.

مثال در روترCisco :

- show ip nat translations

۲ .استفاده از ابزار Ping و Traceroute

- ابزار **Ping** برای بررسی دسترسی‌پذیری یک مقصد استفاده می‌شود. اگر پینگ از داخل شبکه موفق نباشد، می‌تواند نشان‌دهنده مشکل در ترجمه NAT یا مسیریابی باشد.
- ابزار **Traceroute** (در ویندوز tracert): برای ردیابی مسیر بسته‌ها تا مقصد استفاده می‌شود و می‌تواند نقاطی که بسته‌ها متوقف می‌شوند یا ترجمه نشده‌اند را مشخص کند.

۳ .بررسی Log ها و Event ها در دستگاه NAT

- بسیاری از فایروال‌ها و روترها دارای سیستم ثبت گزارش (Logging) هستند.
- خطاهای مربوط بهNAT ، مانند نبود IP عمومی آزاد در Dynamic NAT یا تنظیمات اشتباه درStatic NAT ، در این گزارش‌ها ثبت می‌شود.

۴ .استفاده از Packet Snifferهامانند Wireshark

- ابزارهایی مانند **Wireshark** امکان بررسی بسته‌های شبکه را فراهم می‌کنند.
- با تحلیل بسته‌ها قبل و بعد از NAT می‌توان صحت عملکرد ترجمه آدرس و پورت را بررسی کرد.
- این ابزارها به‌ویژه در محیط‌های تست و اشکال‌زدایی حرفه‌ای بسیار کاربردی هستند.

۵ .بررسی تنظیمات NAT در روتر یا فایروال

- اطمینان از پیکربندی صحیح دستورات NAT مانند تعریف درست آدرس‌ها، پورت‌ها، ACL ها و ... ضروری است.
- در برخی موارد ممکن است خطا ناشی از اشتباه در اولویت‌بندی قوانین NAT باشد.

۶ .تست عملکرد با ابزارهای شبکه

- ابزارهایی مانند **iperf**, **NetFlow**, یا **SNMP مانیتورینگ** برای اندازه‌گیری نرخ انتقال، تأخیر و از دست رفتن بسته‌ها استفاده می‌شوند.
- این ابزارها می‌توانند نشان دهند که NAT موجب کندی یا اشکال در ارتباط شده است یا خیر.