تنظیم VLAN و NAT در روتر سیسکو

در دنیای امروز که شبکه‌های کامپیوتری به عنوان قلب تپنده‌ی هر سازمان و کسب‌وکار شناخته می‌شوند، راه‌اندازی و پیکربندی صحیح زیرساخت‌های شبکه از اهمیت بسیار بالایی برخوردار است. یکی از گام‌های کلیدی در این مسیر، بهره‌گیری از تنظیمات پیشرفته‌ای همچون VLAN و NAT در روترهای سیسکو است. این قابلیت‌ها نه‌تنها موجب بهبود امنیت، تفکیک منطقی بخش‌های مختلف شبکه و افزایش بهره‌وری می‌شوند، بلکه زیرساختی منسجم و قابل مدیریت را برای مدیران شبکه فراهم می‌کنند.

در صورتی که در حال طراحی یا بازطراحی ساختار شبکه سازمان خود هستید و یا قصد بهینه‌سازی مسیرهای ارتباطی درون‌سازمانی را دارید، آشنایی و تسلط بر نحوه‌ی پیاده‌سازی VLAN و NAT در روترهای سیسکو برای شما الزامی خواهد بود. به‌علاوه، در فرآیند راه‌اندازی چنین شبکه‌هایی، **فروش تجهیزات پسیو شبکه** نظیر کابل‌های شبکه، پچ پنل، رک، کیستون و دیگر ملزومات نقش حیاتی دارند؛ چراکه بدون انتخاب دقیق و اصولی این تجهیزات، حتی بهترین تنظیمات نرم‌افزاری نیز نمی‌توانند عملکرد مطلوبی را تضمین کنند.

در این مقاله قصد داریم تا با رویکردی گام‌به‌گام و آموزشی، شما را با مفاهیم پایه، روش‌های پیکربندی، و نکات کلیدی مربوط به VLAN و NAT در روترهای سیسکو آشنا سازیم؛ به گونه‌ای که در پایان مطالعه، بتوانید با دانش فنی کامل نسبت به طراحی و پیاده‌سازی شبکه‌ای کارآمد و پایدار اقدام نمایید.

VLANچیست و چرا استفاده می‌شود؟

VLANیا **شبکه محلی مجازی (Virtual LAN)** یکی از مفاهیم بنیادی در طراحی و مدیریت شبکه‌های پیشرفته است. در حالت عادی، تمامی دستگاه‌هایی که به یک سوئیچ متصل هستند در یک Broadcast Domainقرار دارند؛ یعنی هر پیام Broadcast که از سوی یکی از دستگاه‌ها ارسال شود، به تمام دستگاه‌های دیگر در همان دامنه ارسال می‌گردد. این موضوع علاوه بر ایجاد ترافیک اضافی، می‌تواند تهدیدی برای امنیت شبکه نیز به شمار رود.

اینجاست که VLAN وارد عمل می‌شود. با تعریفVLAN ، می‌توان چندین دامنه‌ی مجزای Broadcast بر روی یک سوئیچ فیزیکی ایجاد کرد. در واقع، VLANبه شما این امکان را می‌دهد تا **چند شبکه‌ی منطقی مستقل** را بر بستر یک زیرساخت فیزیکی واحد راه‌اندازی کنید. تنظیم VLAN و NAT در روتر سیسکو به بیان ساده‌تر، با استفاده ازVLAN ، می‌توانید یک سازمان را که شامل بخش‌هایی مثل مالی، منابع انسانی، فروش و پشتیبانی است، به صورت مجازی و بدون نیاز به سخت‌افزار مجزا، از هم تفکیک کنید.شما میتوانید با بهترین **قیمت روتر شبکه** را در اوج گستران خریداری کنید.

برای درک بهتر این موضوع، تصور کنید که درون یک ساختمان، اتاق‌هایی مجزا با درهای بسته ایجاد کرده‌اید، به طوری که تنها افراد خاصی به هر اتاق دسترسی دارند .VLAN نیز دقیقاً چنین کاری را در دنیای شبکه انجام می‌دهد؛ با استفاده از پیکربندی نرم‌افزاری، ارتباط میان بخش‌های مختلف را مدیریت و کنترل می‌کند.

از جمله مزایای کلیدی استفاده از VLAN می‌توان به موارد زیر اشاره کرد:

- **افزایش امنیت :**با جداسازی منطقی کاربران، می‌توان دسترسی کاربران یک بخش را به اطلاعات بخش دیگر محدود کرد.
- **کاهش ترافیک غیرضروری :**پیام‌های Broadcast فقط در محدوده‌ی همان VLAN منتقل می‌شوند، در نتیجه پهنای باند بهینه‌تر مصرف می‌شود.
- **مدیریت ساده‌تر شبکه :**در صورت نیاز به جابجایی کاربران یا دستگاه‌ها، تنها کافی‌ست پورت آن‌ها را به VLAN مناسب اختصاص دهید، بدون نیاز به تغییر فیزیکی کابل‌کشی.
- **کاهش هزینه‌ها :**با بهره‌گیری ازVLAN ، دیگر نیازی به خرید چندین سوئیچ برای جداسازی منطقی شبکه نخواهد بود.

به همین دلیل است که در شبکه‌های حرفه‌ای و سازمانی، استفاده از VLAN نه‌تنها رایج بلکه به‌نوعی الزامی به حساب می‌آید. چه در هنگام راه‌اندازی یک ساختار جدید و چه در زمان بررسی **قیمت سوئیچ شبکه** برای تهیه تجهیزات مورد نیاز، در نظر گرفتن امکان پیاده‌سازی VLAN باید بخشی جدایی‌ناپذیر از استراتژی طراحی شبکه باشد.

NATچیست و چه کاربردی دارد؟

NATیا **Network Address Translation**یکی از مهم‌ترین فناوری‌های مورد استفاده در شبکه‌های مدرن است که نقشی کلیدی در اتصال شبکه‌های داخلی به اینترنت ایفا می‌کند. به زبان ساده، NAT روشی برای ترجمه‌ی آدرس‌های IP خصوصی به آدرس‌های IP عمومی است؛ بدین معنا که به کمک NAT، دستگاه‌های داخل شبکه می‌توانند بدون نیاز به داشتن آدرس IP عمومی منحصربه‌فرد، با دنیای بیرون (یعنی اینترنت) ارتباط برقرار کنند.

در شبکه‌های سازمانی و حتی خانگی، معمولاً از آدرس‌های IP خصوصی) مانند ۱۹۲٫۱۶۸ x.x یا ۱۰ (x.x.x. استفاده می‌شود. این آدرس‌ها در اینترنت قابل مسیریابی نیستند و تنها در محدوده‌ی داخلی شبکه معنا دارند. اما وقتی دستگاهی از داخل شبکه بخواهد به اینترنت دسترسی پیدا کند، روتر با استفاده از مکانیزمNAT ، آدرس خصوصی آن را به یک آدرس عمومی ترجمه می‌کند. سپس، زمانی که پاسخ از اینترنت بازمی‌گردد، روتر مجدداً آدرس عمومی را به آدرس خصوصی اولیه برمی‌گرداند تا بسته‌ی اطلاعاتی به دستگاه مربوطه برسد.

به این ترتیب، NATمانند **دروازه‌ای هوشمند بین شبکه داخلی و اینترنت** عمل می‌کند. این فناوری نه‌تنها امکان اتصال چندین دستگاه داخلی به اینترنت را از طریق یک آدرس IP عمومی فراهم می‌سازد، بلکه در بسیاری از موارد به افزایش امنیت نیز کمک می‌کند؛ چرا که دستگاه‌های داخل شبکه از دید مستقیم اینترنت پنهان می‌مانند.

برخی از مهم‌ترین کاربردهای NAT عبارت‌اند از:

- **صرفه‌جویی در مصرف آدرس‌های IP عمومی :**با توجه به محدود بودن تعداد آدرس‌هایIPv4 ، استفاده از NAT به سازمان‌ها اجازه می‌دهد تا با یک یا چند IP عمومی، صدها یا هزاران کاربر داخلی را به اینترنت متصل کنند.
- **ایجاد ساختار شبکه‌ای ساده‌تر :**بدون نیاز به اختصاص IP عمومی به هر دستگاه، مدیریت شبکه داخلی آسان‌تر و مقرون‌به‌صرفه‌تر می‌شود.
- **افزایش سطح امنیت :**به دلیل پنهان ماندن آدرس‌های داخلی، مهاجمان از بیرون شبکه نمی‌توانند به‌راحتی به دستگاه‌ها دسترسی پیدا کنند.
- **پشتیبانی از سرویس‌هایی مانند VPN یا :VoIP** بسیاری از این سرویس‌ها نیاز به ترجمه‌ی آدرس دارند تا بتوانند در یک بستر ناهمگون عمل کنند.

تنظیم VLAN و NAT در روتر سیسکو ، نقش NAT در روترهای سیسکو بسیار حیاتی است، به‌ویژه زمانی که شما در حال طراحی یک شبکه گسترده هستید یا به دنبال راهکارهایی برای اتصال امن و پایدار به اینترنت می‌باشید. در چنین شرایطی، هم انتخاب درست تجهیزات و هم آشنایی دقیق با نحوه پیکربندی NAT از اهمیت بالایی برخوردار است. به همین دلیل، هنگام **خرید تجهیزات پسیو شبکه** و همچنین تجهیزات اکتیو مانند روتر و فایروال، باید به قابلیت پشتیبانی آن‌ها از NAT توجه ویژه‌ای داشت.

آشنایی با انواع VLAN در سیسکو

در معماری شبکه‌های مبتنی بر تجهیزات سیسکو، VLANنقش مهمی در تفکیک منطقی ترافیک و مدیریت ساختار داخلی شبکه ایفا می‌کند. این فناوری به مدیران شبکه اجازه می‌دهد تا گروه‌های مختلفی از کاربران یا دستگاه‌ها را، بدون در نظر گرفتن موقعیت فیزیکی آن‌ها، در یک دامنه‌ی مشترک قرار دهند. در تجهیزات سیسکو، VLANدر قالب‌های مختلفی قابل پیاده‌سازی است که در ادامه به معرفی و بررسی سه نوع رایج آن می‌پردازیم:

Static VLAN VLANایستا

در حالت **VLANایستا**، تخصیص پورت‌ها به‌VLAN ها به‌صورت دستی توسط مدیر شبکه انجام می‌شود. به این معنا که هر پورت از سوئیچ یا روتر به‌طور مشخص به یک VLAN خاص تعلق می‌گیرد و این تنظیمات به‌صورت دائمی در حافظه دستگاه ذخیره می‌شوند.

این نوع VLAN ساده‌ترین و رایج‌ترین روش پیاده‌سازی در شبکه‌های سازمانی است، زیرا کنترل کاملی بر روی توپولوژی منطقی شبکه فراهم می‌سازد. برای مثال، اگر پورت شماره ۱۰ به VLAN 20 اختصاص داده شده باشد، هر دستگاهی که به آن پورت متصل شود، به‌صورت خودکار عضوی از VLAN 20 خواهد بود.

مزایا:

- امنیت بالا از طریق کنترل دقیق دسترسی
- پیاده‌سازی آسان در شبکه‌های کوچک و متوسط
- سازگاری بالا با تجهیزات پسیو و اکتیو

محدودیت‌ها:

- عدم انعطاف‌پذیری در جابه‌جایی کاربران
- نیاز به پیکربندی مجدد در صورت تغییر مکان فیزیکی دستگاه‌ها

Dynamic VLAN VLANپویا

در مدل **VLANپویا**، اختصاص کاربران یا دستگاه‌ها به‌VLAN ها به‌صورت خودکار و براساس اطلاعاتی مانند **MAC Address**، **نام کاربری (Username)** یا **پروفایل لاگین** انجام می‌شود.تنظیم VLAN و NAT در روتر سیسکو این فرآیند معمولاً از طریق یک سرور مرکزی مانند **VMPS (VLAN Management Policy Server)**مدیریت می‌گردد.

با استفاده از این نوع‌VLAN ، هنگامی که یک کاربر وارد شبکه می‌شود، سوئیچ با مراجعه به پایگاه‌داده‌ی مرکزی، VLANمناسب را برای آن کاربر مشخص و اعمال می‌کند. این ویژگی به‌ویژه در شبکه‌هایی با کاربران سیار یا لپ‌تاپ‌های قابل حمل بسیار مفید است.

مزایا:

- افزایش انعطاف‌پذیری و پویایی شبکه

- مناسب برای سازمان‌هایی با ساختار غیرثابت و متحرک
- عدم نیاز به تغییر پیکربندی دستی سوئیچ‌ها

محدودیت‌ها:

- نیازمند زیرساخت پیچیده‌تر و استفاده از سرورVMPS
- نیاز به مدیریت و نگهداری دقیق پایگاه دادهMAC Address ها

Voice VLAN VLANصوتی

Voice VLANیک نوع ویژه از VLAN است که به‌صورت اختصاصی برای ترافیک صوتی در شبکه‌های مبتنی بر **VoIP (Voice over IP)**طراحی شده است. در این ساختار، پورت‌های سوئیچ به گونه‌ای پیکربندی می‌شوند که به‌طور هم‌زمان بتوانند هم ترافیک داده (Data) و هم ترافیک صوتی (Voice) را پشتیبانی کنند، ولی این دو نوع ترافیک را درVLAN های مجزا نگه می‌دارند.

Voice VLANبه کیفیت تماس‌های صوتی کمک می‌کند زیرا:

- **اولویت‌بندی ترافیک صوتی** در شبکه فعال می‌شود) با استفاده از(QoS
- تأخیر (Delay) و لرزش (Jitter) در ارتباط صوتی به حداقل می‌رسد
- ترافیک صوتی از ازدحام ترافیک‌های دیگر در امان می‌ماند

مزایا:

- تضمین کیفیت خدمات صوتی(QoS)
- جداسازی منطقی و امن ترافیک صوتی
- مدیریت ساده‌تر تلفن‌هایIP

محدودیت‌ها:

- نیاز به پیکربندی دقیق و سازگاری تجهیزات
- الزامات خاص در طراحی تجهیزات پسیو شبکه برای) VoIP مانند کابل‌کشی مناسب برای دستگاه‌های تلفن(IP

در فرآیند طراحی و پیاده‌سازی هر کدام از این انواعVLAN ، استفاده از تجهیزات مناسب اهمیت بالایی دارد. بنابراین در زمان **خرید تجهیزات پسیو شبکه** مانند کابل‌هایCAT6/7 ، کیستون‌های مخصوص VoIP، پچ‌پنل و رک، باید به پشتیبانی آن‌ها از ساختار منطقی شبکه شامل Voice VLAN یا Dynamic

VLANتوجه شود. تنظیم VLAN و NAT در روتر سیسکو ، طراحی اصولی به همراه انتخاب تجهیزات باکیفیت، تضمین‌کننده عملکرد پایدار و قابل اتکای شبکه شما خواهد بود.

مزایای پیاده‌سازی VLAN در شبکه

استفاده از VLAN در طراحی و مدیریت شبکه‌های مدرن نه‌تنها یک انتخاب هوشمندانه، بلکه یک الزام فنی در بسیاری از سازمان‌ها و شرکت‌هاست. پیاده‌سازی VLAN مزایای متعددی به همراه دارد که به بهبود امنیت، کارایی و مدیریت منابع شبکه منجر می‌شود. در ادامه به بررسی مهم‌ترین این مزایا می‌پردازیم:

تفکیک منطقی شبکه

یکی از مهم‌ترین مزایایVLAN ، امکان **تفکیک منطقی کاربران و بخش‌های مختلف سازمان** است، بدون اینکه نیاز به ایجاد زیرساخت فیزیکی مجزا مانند کابل‌کشی جداگانه یا استفاده از سوئیچ‌های متعدد باشد.

برای مثال، می‌توان کاربران بخش مالی را از کاربران بخش فروش، منابع انسانی یا IT جدا کرد و به هرکدام VLAN مخصوص اختصاص داد. این تفکیک باعث می‌شود که هر گروه تنها به منابع مورد نیاز خود دسترسی داشته باشد و ترافیک داخلی آن‌ها نیز از دیگر بخش‌ها جدا باقی بماند.

این موضوع نه‌تنها در ساختارهای بزرگ و پیچیده سازمانی، بلکه حتی در شبکه‌های کوچک‌تر نیز موجب نظم، کنترل و سهولت در مدیریت شبکه می‌شود.

افزایش امنیت شبکه

وقتی بخش‌های مختلف شبکه درVLAN های جداگانه قرار می‌گیرند، عملاً هر VLAN به یک **Broadcast Domainمستقل** تبدیل می‌شود. این جداسازی باعث می‌شود که ترافیک ناخواسته یا مخرب از یک بخش نتواند به راحتی به سایر بخش‌ها دسترسی یابد.

در نتیجه، احتمال نفوذ، استراق سمع، شنود داده‌ها یا حملات سایبری از طریق نقاط آسیب‌پذیر شبکه کاهش می‌یابد. این ویژگی به‌خصوص در سازمان‌هایی که اطلاعات حساس مالی یا شخصی نگهداری می‌شود، بسیار حیاتی است.

همچنین با استفاده از قابلیت‌های امنیتی پیشرفته روترهای حرفه‌ای، مانند روترهای برند سیسکو، می‌توان سیاست‌های فایروال، ACL (Access Control List)و بررسی‌های ترافیک بینVLAN ها را

پیاده‌سازی کرد. به همین دلیل، **خرید روتر سیسکو** برای سازمان‌هایی که نیازمند امنیت بالا هستند، یک انتخاب حرفه‌ای و قابل اعتماد خواهد بود.

بهینه‌سازی عملکرد شبکه

یکی از مشکلات رایج در شبکه‌های بزرگ، حجم بالای ترافیک غیرضروری (Broadcast و Multicast) است که می‌تواند پهنای باند شبکه را اشغال کرده و باعث افت عملکرد شود. با پیاده‌سازیVLAN ، می‌توان این ترافیک را به بخش‌های مربوطه محدود کرد و مانع از انتشار بی‌رویه آن در کل شبکه شد.

این موضوع باعث می‌شود:

- **سرعت انتقال داده‌ها افزایش یابد**
- **بار پردازشی سوئیچ‌ها و روترها کاهش پیدا کند**
- **کیفیت ارتباط در سرویس‌هایی مانندVoIP ، کنفرانس‌های ویدیویی یا انتقال فایل‌های حجیم بهبود یابد**

همچنین، VLANاین امکان را فراهم می‌کند که مدیریت منابع و ترافیک شبکه به‌صورت دقیق‌تر و هوشمندانه‌تری انجام شود. برای مثال، می‌توان اولویت‌بندی ترافیک را برایVLAN های خاص فعال کرد، مانند اختصاص پهنای باند بیشتر به VLAN مربوط به تیم پشتیبانی یا مرکز تماس.

در نهایت باید توجه داشت که بهره‌گیری از مزایایVLAN ، زمانی به حداکثر می‌رسد که زیرساخت سخت‌افزاری شبکه نیز توانایی پشتیبانی از این قابلیت را داشته باشد. تنظیم VLAN و NAT در روتر سیسکو ، در این میان، **خرید روتر سیسکو** به دلیل پشتیبانی کامل از پروتکل‌هایVLAN ، امکانات امنیتی گسترده، و قابلیت‌های مدیریتی پیشرفته، راهکاری مطمئن برای شرکت‌ها و سازمان‌هایی است که به دنبال شبکه‌ای پایدار، ایمن و انعطاف‌پذیر هستند.

مراحل اولیه تنظیم VLAN در روتر سیسکو

اتصال به روتر از طریق کنسول

ابتدا با کابل کنسول به روتر متصل شوید و از نرم‌افزارهایی مانند PuTTY استفاده کنید.

ورود به محیط پیکربندی(Configuration Mode)

```
Router> enable
Router# configure terminal
```

تعریف VLAN جدید

```
Router(config)# vlan 10
Router(config-vlan)# name Marketing
```

اختصاص پورت بهVLAN

```
Router(config)# interface FastEthernet0/1
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 10
```

آموزش تصویری تنظیم VLAN در روتر سیسکو

یکی از گام‌های کلیدی در طراحی و پیاده‌سازی شبکه‌های ساختارمند و حرفه‌ای، راه‌اندازی VLAN بر روی تجهیزات سیسکو است. برای این منظور، استفاده از ابزارهای شبیه‌سازی نظیر **Cisco Packet Tracer**به‌شدت توصیه می‌شود؛ چرا که به شما این امکان را می‌دهد بدون نیاز به تجهیزات فیزیکی، مراحل پیکربندی را به‌صورت عملی تمرین کنید.

برای شروع، کافی‌ست یک سناریوی ساده طراحی کنید؛ به‌عنوان مثال، دو سوئیچ و یک روتر را به هم متصل کرده و چند دستگاه (PC) به پورت‌های مختلف متصل کنید. سپس می‌توانید مراحل زیر را به ترتیب اجرا کنید:

۱. **تعریف VLAN در سوئیچ‌ها**
با دستور [vlanشماره]و سپس اختصاص نام، VLANهای موردنظر را تعریف کنید.

۲. **اختصاص VLAN به پورت‌ها**
وارد تنظیمات هر پورت شوید و با دستور [switchport access vlanشماره]VLAN ، پورت را به VLANمشخص اختصاص دهید.

۳. **فعال‌سازی Trunk بین سوئیچ و روتر**
پورت بین سوئیچ و روتر را به حالت trunk تنظیم کنید تا امکان عبور چندین VLAN از آن فراهم شود.

۴. **پیکربندی Subinterface در روتر سیسکو**
در روتر باید برای هر VLAN یک Subinterface تعریف کنید (مثلاً FastEthernet0/0.10 :برای VLAN 10).سپس با دستور encapsulation dot1Q 10 شناسه VLAN را تعیین کرده و با دستور ip addressآدرس IP به آن اختصاص دهید.

۵. **تست اتصال بین دستگاه‌ها**
حالا می‌توانید با دستور ping یا سایر ابزارها، ارتباط بین کلاینت‌هایی که در VLAN های مختلف قرار دارند را بررسی کنید.

این مراحل به شما کمک می‌کند تا درک عملی عمیقی از عملکرد VLAN در محیط سیسکو داشته باشید و در پروژه‌های واقعی، با اطمینان پیکربندی‌های مشابه را اجرا کنید.

آشنایی با NAT و انواع آن

در شبکه‌های امروزی، به‌ویژه هنگام اتصال شبکه داخلی به اینترنت، وجود مکانیزمی برای ترجمه آدرس‌های IP خصوصی به آدرس‌های عمومی ضروری است. تنظیم VLAN و NAT در روتر سیسکو ، این وظیفه را **NAT (Network Address Translation)** برعهده دارد .یکی از اجزای کلیدی روترهای سیسکو است که به‌درستی پیکربندی شود، نقش دروازه‌ی ارتباطی بین شبکه داخلی و دنیای خارج را ایفا می‌کند.

انواع NAT شامل موارد زیر است:

Static NAT

در این روش، برای هر دستگاه داخلی یک آدرس IP عمومی خاص و ثابت در نظر گرفته می‌شود. این نوع NAT معمولاً برای سرورهایی استفاده می‌شود که نیاز به دسترسی مداوم از خارج دارند؛ مانند وب‌سرور، سرور ایمیل یا دوربین‌های نظارتی.

مثال:

ip nat inside source static 192.168.1.10 80.80.80.10

این خط کد مشخص می‌کند که آدرس داخلی ۱۹۲/۱۶۸/۱/۱۰ همیشه به آدرس عمومی ۸۰/۸۰/۸۰/۱۰ ترجمه شود.

Dynamic NAT

درDynamic NAT ، مجموعه‌ای از آدرس‌های عمومی (Pool) در اختیار روتر قرار می‌گیرد و به‌صورت پویا به کاربران داخلی اختصاص داده می‌شود. این روش زمانی کاربرد دارد که تعداد IP عمومی محدود باشد ولی کاربران زیادی به اینترنت متصل می‌شوند.

مثال:

ip nat pool MyPool 80.80.80.1 80.80.80.10 netmask 255.255.255.0
ip nat inside source list 1 pool MyPool

در این مثال، هر کاربر داخلی که در Access List شماره ۱ باشد، از این Pool برای اتصال به اینترنت استفاده می‌کند.

NAT OverloadیاPAT (Port Address Translation)

این روش محبوب‌ترین و رایج‌ترین نوع NAT در شبکه‌های خانگی و اداری است. درPAT ، تنها یک آدرس عمومی برای تمام کاربران داخلی استفاده می‌شود، اما به کمک پورت‌های مجزا، روتر می‌تواند ترافیک را به‌درستی بین کاربران مختلف هدایت کند.

مثال:

ip nat inside source list 1 interface FastEthernet0/0 overload

در این خط فرمان، کاربران داخلی از آدرس IP موجود روی اینترفیس FastEthernet0/0 برای اتصال به اینترنت استفاده می‌کنند، و روتر با ترکیب آدرس IP و شماره پورت، هر اتصال را ردیابی و مدیریت می‌کند.

مزیت اصلی PAT این است که امکان استفاده چندین کاربر از یک IP عمومی را فراهم می‌کند، که در شرایطی که آدرس‌های عمومی محدود هستند، بسیار کارآمد است.

در مجموع، آشنایی با انواع NAT و نحوه پیاده‌سازی آن بر روی روتر سیسکو، یکی از مهم‌ترین مهارت‌های لازم برای مدیران شبکه و متخصصان IT است. این دانش به شما کمک می‌کند تا کنترل دقیقی بر جریان داده‌ها داشته باشید و با بهره‌گیری بهینه از منابع شبکه، عملکرد و امنیت سیستم‌های خود را بهبود ببخشید.

مراحل پیاده‌سازی NAT در روتر سیسکو

تعریف آدرس‌های داخلی و خارجی

Router(config)# interface FastEthernet0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

```
Router(config-if)# ip nat inside
```

تنظیمAccess List

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

اعمال ترجمه آدرس‌ها روی اینترفیس

```
Router(config)# ip nat inside source list 1 interface FastEthernet0/1 overload

Router(config)# interface FastEthernet0/1

Router(config-if)# ip address 100.100.100.1 255.255.255.0

Router(config-if)# ip nat outside
```

ترکیب VLAN و NAT در یک سناریوی عملی

برای درک عمیق‌تر مفهوم VLAN و NAT در روترهای سیسکو، بررسی یک **سناریوی عملی و واقعی** می‌تواند بسیار مفید و آموزنده باشد. ترکیب این دو قابلیت نه‌تنها به تفکیک منطقی شبکه داخلی کمک می‌کند، بلکه ارتباط ایمن و کنترل‌شده‌ای با شبکه خارجی (اینترنت) برقرار می‌سازد. این نوع پیکربندی در سازمان‌هایی که به دنبال مدیریت هوشمندانه منابع شبکه و بهینه‌سازی امنیت هستند، اهمیت دوچندانی دارد.

طراحی سناریو: سازمان با دو بخش مجزا و دسترسی به اینترنت

فرض کنید یک سازمان متوسط دارید که شامل دو بخش کلیدی است:

- **واحد فروش (Sales)** در VLAN 10
- **واحد حسابداری (Finance)** در VLAN 20

هر دو بخش باید به اینترنت دسترسی داشته باشند، اما به‌صورت جداگانه و بدون تداخل اطلاعات. در این سناریو، VLANبرای جداسازی داخلی و NAT برای ترجمه آدرس‌های داخلی به آدرس‌های عمومی استفاده خواهد شد.

پیکربندی مرحله به مرحله ترکیب VLAN وNAT

۱ .تعریفVLAN ها در سوئیچ

در گام اول، بایدVLAN ها را در سوئیچ تعریف کنید:

```
Switch(config)# vlan 10
Switch(config-vlan)# name Sales
Switch(config)# vlan 20
Switch(config-vlan)# name Finance
```

۲ .اختصاص پورت‌ها به VLAN مناسب

هر پورت سوئیچ که به دستگاه خاصی متصل است باید به VLAN مربوطه اختصاص یابد:


```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
```

۳ .تنظیم Trunk بین سوئیچ و روتر سیسکو

برای عبور ترافیکVLAN ها از سوئیچ به روتر:

```
Switch(config)# interface FastEthernet0/24
Switch(config-if)# switchport mode trunk
```

۴ .ایجاد Subinterface در روتر برایVLAN هر

روتر باید برای هر VLAN یک Subinterface داشته باشد:

```
Router(config)# interface FastEthernet0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0Router(config)# interface
FastEthernet0/0.20
```

Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0

۵ .تعریف Access List برایNAT

Access Listبرای تعیینIP هایی که باید NAT شوند:

Router(config)# access-list 1 permit 192.168.10.0 0.0.0.255
Router(config)# access-list 1 permit 192.168.20.0 0.0.0.255

۶ .تعریف NAT و تنظیم اینترفیس داخلی و خارجی

Router(config)# ip nat inside source list 1 interface FastEthernet0/1 overload
Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside Router(config)# interface FastEthernet0/1
Router(config-if)# ip address [Public IP] 255.255.255.0
Router(config-if)# ip nat outside

تست نهایی اتصال

برای اطمینان از صحت عملکرد، از دستورات زیر استفاده کنید:

- **ping**از یک کلاینت در VLAN 10 یا ۲۰ به آدرس اینترنتی (مثلاً ۸٫۸٫۸٫۸)
- **traceroute**برای بررسی مسیر عبور بسته‌ها
- **show ip nat translations**برای مشاهده ترجمه آدرس‌ها
- **show running-config**جهت بررسی تنظیمات فعلی

نکات مهم در پیکربندی VLAN وNAT

بررسی جدول مسیریابی(Routing Table)

همیشه با دستور show ip routeاز صحت مسیرها مطمئن شوید. اطمینان از وجود مسیر پیش‌فرض (Default Route)برای اینترنت حیاتی است:

Router(config)# ip route 0.0.0.0 0.0.0.0 [Public Gateway IP]

توجه به تداخل IP و استفاده صحیح ازSubnet ها

استفاده ازSubnet های مناسب مثل ۲۴/۱۹۲/۱۶۸/۱۰/۰ و ۲۴/۱۹۲/۱۶۸/۲۰/۰ کمک می‌کند تا بدون تداخل، هر VLAN فضای آدرس‌دهی اختصاصی خود را داشته باشد.

اهمیت تست و مانیتورینگ مداوم

پس از پایان پیکربندی، فراموش نکنید که مرتباً شبکه را بررسی و پایش کنید. دستوراتی مانند:

- show ip nat statisticsبرای مشاهده میزان ترجمه آدرس‌ها
- show interfacesبرای بررسی وضعیت فیزیکی اینترفیس‌ها
- debug ip natبرای عیب‌یابی در لحظه

همه‌ی این موارد به شما کمک می‌کنند تا شبکه‌ای پایدار، امن و عملکردی داشته باشید.

در نهایت، پیاده‌سازی دقیق VLAN و NAT در روترهای سیسکو به شما این امکان را می‌دهد تا یک شبکه کاملاً تفکیک‌شده، ایمن و در عین حال متصل به اینترنت داشته باشید. اگر در حال راه‌اندازی شبکه‌ای حرفه‌ای هستید یا قصد خرید تجهیزات پسیو شبکه یا **خرید روتر سیسکو** دارید، در نظر داشته باشید که زیرساخت مناسب گام اول موفقیت در مدیریت شبکه‌های مدرن است.

نتیجه‌گیری

تنظیم VLAN و NAT در روتر سیسکو نه تنها باعث امنیت و کارایی بیشتر شبکه می‌شود، بلکه انعطاف‌پذیری فوق‌العاده‌ای در مدیریت کاربران و منابع فراهم می‌آورد. با یادگیری و پیاده‌سازی صحیح این دو مفهوم، می‌توانید شبکه‌ای پایدار، امن و قابل توسعه ایجاد کنید.

سوالات متداول

1.آیا VLAN فقط مخصوص سوئیچ است یا در روتر هم کاربرد دارد؟
خیر، VLANدر روترهای لایه ۳ نیز کاربرد دارد و برای مسیریابی بینVLAN ها مورد استفاده قرار می‌گیرد.

2.آیا می‌توان از NAT برای هر VLAN به‌صورت جداگانه استفاده کرد؟
بله، با استفاده از Access List و NAT Overload می‌توان برای هر VLAN به‌صورت جدا NAT تعریف کرد.

3.بهترین روش تست NAT در روتر چیست؟

استفاده از دستور show ip nat translations و انجام ping از دستگاه داخلی به آدرس بیرونی بهترین راه تست است.

4.تفاوت Static NAT و PAT چیست؟

در Static NAT هر IP داخلی به یک IP خارجی خاص متصل می‌شود، اما در PAT چند IP داخلی با یک IP خارجی و پورت‌های مختلف ترجمه می‌شوند.

5.در صورت بروز مشکل درVLAN ، از کجا شروع به عیب‌یابی کنیم؟

از بررسی پورت‌های VLAN و چک کردن تنظیمات با دستور show vlan brief و بررسی interface status شروع کنید.