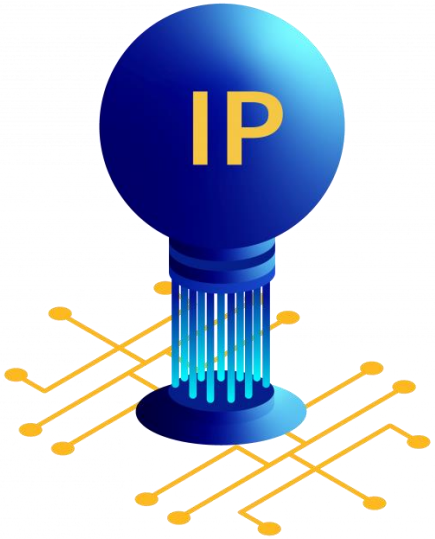
شبکه های کامپیوتری

(آمادگی برای آزمون Network+)

اسلاید چهارم

«معرفی IP، انواع IP، بررسی NATوPAT، انواع کلاس ، Subnet Mask، Supernetting»



درس
شبکه های کامپیوتری
۴

محمد سعید صفایی صادق

۱۴۰۳

www.SaeidSafaei.ir

اهمیت آدرس گذاری در ارتباطات شبکه

آدرس‌گذاری در شبکه‌های کامپیوتری یکی از مهم‌ترین اصول و مبانی است که برای اطمینان از انتقال صحیح داده‌ها بین دستگاه‌ها ضروری است.

آدرس‌دهی در شبکه به دستگاه‌های مختلف این امکان را می‌دهد که یکدیگر را شناسایی کنند و با هم ارتباط برقرار کنند.

آدرس‌گذاری یکی از اصلی‌ترین پایه‌های شبکه‌های کامپیوتری است که بدون آن امکان برقراری ارتباط، مسیریابی، مدیریت و امنیت در شبکه‌ها وجود نخواهد داشت.

هر دستگاه در شبکه برای ارسال و دریافت اطلاعات به آدرس‌های دقیق نیاز دارد تا بتواند با دستگاه‌های دیگر به‌درستی ارتباط برقرار کند.

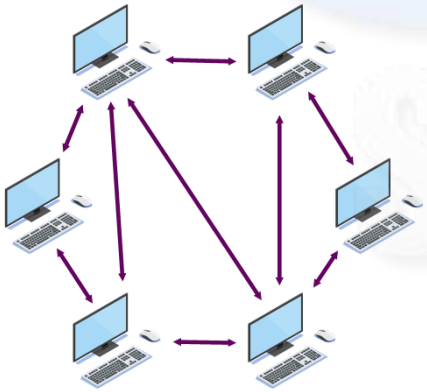
ارتباطات P2P در شبکه:

در شبکه‌های کامپیوتری، Peer-to-Peer و Point-to-Point دو مدل مختلف از ارتباطات شبکه هستند.

۱- Peer-to-Peer همتا به همتا:

در مدل Peer-to-Peer، هر دستگاه در شبکه به‌عنوان همتا عمل می‌کند و می‌تواند به‌طور مستقیم با دستگاه‌های دیگر ارتباط برقرار کند.

در این مدل، هیچ سرور مرکزی وجود ندارد و هر دستگاه به‌عنوان هم سرور و هم کلاینت عمل می‌کند.



مثال: شبکه‌های اشتراک‌گذاری فایل مانند BitTorrent.

ارتباطات P2P در شبکه:

۲-Point-to-Point نقطه به نقطه: یا PPP (Proin to Point Protocol)

تعریف: در مدل Point-to-Point، تنها دو دستگاه مستقیماً به یکدیگر متصل می‌شوند و بین این دو نقطه ارتباط برقرار می‌شود.

این نوع ارتباط معمولاً برای انتقال داده بین دو دستگاه خاص استفاده می‌شود.

مثال: اتصال مستقیم بین دو کامپیوتر با استفاده از کابل شبکه، یا ارتباط بین مودم و روتر.

ارتباطات P2P در شبکه:

تفاوت کلیدی:

Peer-to-Peer ساختار توزیع‌شده و چندین دستگاه با یکدیگر در ارتباط هستند.

Point-to-Point تنها دو دستگاه به‌صورت مستقیم با هم ارتباط دارند.

آدرس گذاری در شبکه
Network Addressing
معرفی IP

آدرس گذاری در شبکه

هر کامپیوتر یا دستگاهی در شبکه دو نوع آدرس دارد: آدرس فیزیکی و آدرس اینترنتی.

همانطور که در فصل قبل توضیح دادیم، آدرس فیزیکی که به آن مک آدرس نیز گفته می‌شود، برای شناسایی دستگاه متصل به شبکه اترنت یا LAN کاربرد دارد.

آدرس اینترنتی یا آدرس IP نیز دستگاه را در سطح جهانی (اینترنت) شناسایی می‌کند.

آدرس IP چیست ؟

نشانی پروتکل اینترنت Internet Protocol Address یا به اختصار نشانی آی‌پی IP Address نشانی عددی است که به هریک از دستگاه‌ها و رایانه‌های متصل به شبکه رایانه‌ای که بر مبنای مجموعه پروتکل اینترنت کار می‌کند، اختصاص داده می‌شوند.

پیام‌هایی که دیگر رایانه‌ها برای این رایانه می‌فرستند با این نشانه عددی همراه است و مسیریاب های شبکه آن را مانند «نشانی گیرنده» در نامه‌های پستی تعبیر می‌کنند، تا در نهایت پیام به رابط شبکه رایانه مورد نظر برسد.

IP یک مفهوم زیربنایی در سطح شبکه است و هر چیزی که بر زیربنای شبکه ساخته می‌شود به نوعی با آدرس آی پی ارتباط پیدا می‌کند.

آدرس IP چیست ؟

اطلاعات در سطح اینترنت به‌صورت بسته یا Packet داده منتقل می‌شوند.

مثلاً زمانی که شما از یک سایت بازدید می‌کنید، بسته‌های داده زیادی بین سایت و سرور آن جابه‌جا می‌شوند و هر کدام از این بسته‌ها حاوی اطلاعاتی هستند؛ مجموع این اطلاعات باعث می‌شود سایت به شما نمایش داده شود.

پروتکل IP اطلاعاتی مثل آدرس مبدا و آدرس مقصد بسته‌های داده و برخی اطلاعات دیگر را برای شناسایی دستگاه و انتقال صحیح داده فراهم می‌کند.

در واقع آدرس آی‌پی کمک می‌کند که در شلوغی و ازدحام رفت‌وآمد بسته‌های داده، هیچ داده‌ای گم نشود و هر بسته به سلامت به آدرس درست ارسال شود.

آدرس IP چیست ؟

با توجه به توضیحات گفته شده نقش پروتکل آی‌پی را می‌توانیم در یک جمله خلاصه کنیم:

پروتکل IP آدرس مبدا و مقصد و برخی اطلاعات کلیدی دیگر را برای انتقال بسته‌های داده فراهم می‌کند.

به این ترتیب بدون نیاز به مانیتورینگ یا یک Node مرکزی انتقال داده انجام می‌شود.

آدرس IP یک شناسه عددی منحصربه‌فرد است (مثلاً ۱۵۲.۴۳.۵۲.۱۰) که هر دستگاهی در اینترنت یا شبکه محلی را قابل شناسایی می‌کند.

آدرس IP چیست ؟

این شناسه‌های عددی، حاوی اطلاعات مکان هستند و وجود آن‌ها برای برقراری ارتباط بین دستگاه‌های مختلف ضروری‌اند؛ چرا که امکان ارسال اطلاعات بین دستگاه‌های موجود در شبکه را با شناسایی تمام دستگاه‌ها، امکان‌پذیر می‌کنند.

هر بسته‌ای که در اینترنت مبادله می‌شود، هم حاوی آدرس IP مبدا و هم آدرس IP مقصد است.

این آدرس‌های IP نشان می‌دهند که بسته از کجا می‌آید و باید به کجا برود.

هر کامپیوتر یا دستگاه دیگری که به اینترنت متصل است، باید یک آدرس IP معتبر و منحصربه‌فرد داشته باشد.

در غیر این‌صورت، عملا نمی‌تواند به اینترنت متصل شود پس: نه می‌تواند داده‌ای بفرستد و نه داده‌ای دریافت کند.

آدرس IP چیست ؟

آدرس‌های IP به هر دستگاه یک شناسه یکتا اختصاص می‌دهند.

این شناسه باعث می‌شود که دستگاه‌ها در یک شبکه محلی یا اینترنت به‌درستی شناسایی شوند.

بدون آدرس‌دهی، تعیین مقصد و مبدأ اطلاعات ممکن نخواهد بود.

انواع نسخه های آدرس IP :

پروتکل اینترنت IP در سیر تکامل خود، در دو نسخه اصلی تثبیت شد:

۱- نسخه چهارم موسوم به IPv4

۲- نسخه ششم که IPv6 نام دارد.

نسخه چهارم یا IPv4 هنوز پرکاربردترین نسخه پروتکل اینترنت است اما با رشد فزاینده شمار کاربران اینترنت و نیز سربرآوردن اینترنت اشیاء، ظرفیت IPv4 دیگر پاسخگوی این حجم از تجهیزات نخواهدبود.

چنین مواردی سبب شد IPv6 جایگزین آتی IPv4شود، گرچه هم‌اکنون نیز استفاده از IPv6 امکان‌پذیر است.

انواع نسخه های آدرس IP :

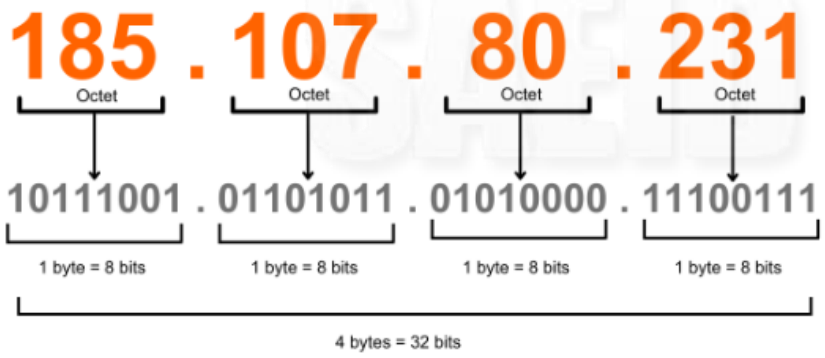
مفهوم آدرس IP ورژن۴ IPv4

در نسخه چهارم پروتکل اینترنت یا IPv4، آدرس‌های آی پی ۳۲ بیتی هستند. (۴ تا OCT)

هر آدرس IP از چهار بخش عددی تشکیل شده است که با نقطه از هم جدا می‌شوند.

هر بخش می‌تواند یکی از اعداد ۰ تا ۲۵۵ باشد، مثل ۱۲۷.۰.۰.۱.

در IPv4 آدرس‌های آی پی از ۰.۰.۰.۰ شروع می‌شوند و با ۲۵۵.۲۵۵.۲۵۵.۲۵۵ پایان می‌یابند.



انواع نسخه های آدرس IP :

مفهوم آدرس IP ورژن۴ IPv4

با فرمت IPv4 می‌توان در کل ۲ به توان ۳۲ یعنی ۴.۲۹۴.۹۶۷۲۹۶ آدرس آی پی ایجاد کرد.

شاید در نگاه نخست این عدد بزرگ به نظر برسد اما باتوجه به افزایش شمار کاربران و دستگاه‌های متصل به اینترنت و نیز سربرآوردن اینترنت اشیاء که میلیون‌ها وسیله جدید را به اینترنت اضافه خواهدکرد، فرمت IPv4 دیگر کافی نیست.

32-bit address space
=
4,294,967,296 (2^32)
unique addresses

به همین جهت نسخه دیگری از پروتکل اینترنت موسوم به IPv6 ارائه شد.

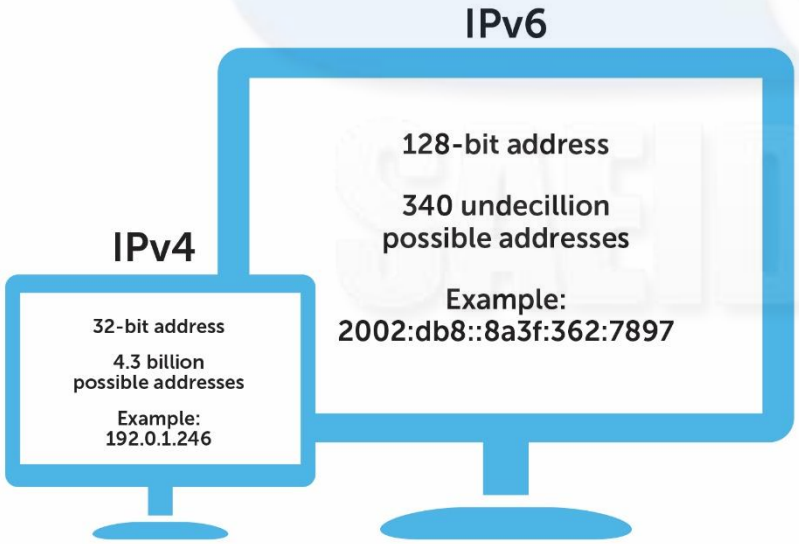
انواع نسخه های آدرس IP :

مفهوم آدرس IP ورژن۶ IPv6

در نسخه ششم پروتکل اینترنت یا IPv6، فرمت آدرس‌های آی پی ۱۲۸ بیتی است. (۸ تا Hex)

در IPv6 هر آدرس آی پی از هشت قسمت تشکیل شده است که هر قسمت دارای چهار رقم اصطلاحا شانزده‌شانزدهی (هگزادسیمال) است.

فرمت IPv6 تعداد آدرس‌های آی پی ممکن را بسیار افزایش می‌دهد.



128-bit address space
=
340,282,366,920,938,463,463,374,
607,431,768,211,456 (2^128)
unique addresses

example:
2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

انواع آدرس IP از لحاظ ثبات (تغییر ناپذیری):

منظور از آدرس IP استاتیک و داینامیک چیست؟

یکی از دسته‌بندی‌های مهم آدرس‌های IP، استاتیک یا داینامیک بودن آن‌هاست.

اما پیش از آن بهتر است در رابطه با DHCP اطلاعاتی را کسب کنیم.

انواع آدرس IP از لحاظ ثبات (تغییر ناپذیری):

سرور DHCP

Dhcp Server یا (Dynamic Host Configuration Protocol)

یک سرور در سمت میزبانی شبکه میباشد که به صورت اتوماتیک آدرس آی پی کلاینت های مختلف را تعیین میکند.

ISP ها معمولا به همین صورت عمل میکنند و زمانی که شما مودم خود را خاموش و روشن میکنید، یک آی پی جدید به شما اختصاص داده میشود.

نحوه کار DHCP سرور به این صورت است که: دستگاه های متصل به این سرور با توجه به تنظیماتی که بر روی آنها انجام شده است، میدانند که باید برای دریافت آی پی آدرس به این سرور درخواست ارسال کنند.

سپس سرور DHCP درخواست ها را دریافت و برای هر کدام از این کلاینت ها یک آی پی مخصوص تعیین و ارسال مینماید.

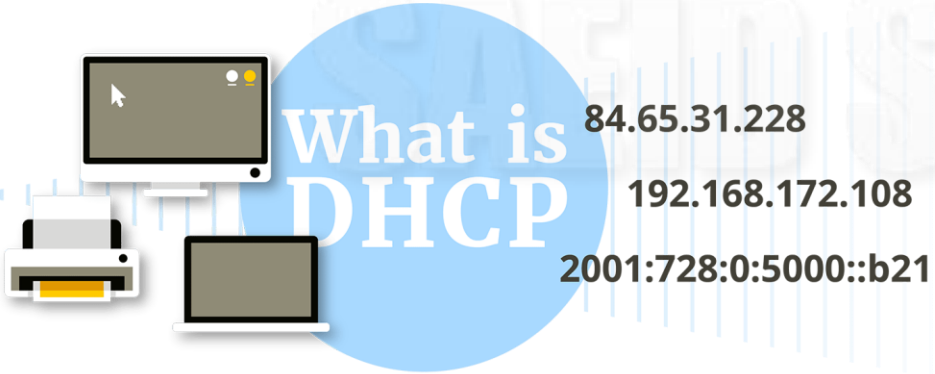
انواع آدرس IP از لحاظ ثبات (تغییر ناپذیری):

Lease Time در سرور DHCP :

در سرورهای DHCP معمولا یک بازه زمانی برای IP های اختصاص داده شده تعیین میگردد که به Lease Time معروف است.

در صورت اتمام این بازه زمانی، آی پی از کلاینت مورد نظر پس گرفته میشود و آی پی جدیدی بر روی آن تنظیم میگردد.

نکته: سرورهای DHCP به غیر از اختصاص آی پی آدرس، میتوانند Default Gateway و DNS را نیز بر روی کلاینت ها تنظیم نمایند.



انواع آدرس IP از لحاظ ثبات (تغییر ناپذیری):

۱- آی پی پویا یا داینامیک Dynamic

آدرس آی پی داینامیک یا پویا به نوعی از آی پی گفته می‌شود که در هر بار اتصال به اینترنت، به دستگاه شما اختصاص داده می‌شود.

بسیاری از دستگاه‌های خانگی از این نوع IP استفاده می‌کنند.

شما زمانی که خدمات اینترنت مانند وای فای را از شرکت‌های مختلف ارائه دهنده این خدمات خریداری می‌کنید، در واقع آدرس آی پی پویا به شما تعلق می‌گیرد.

انواع آدرس IP از لحاظ ثبات (تغییر ناپذیری):

نحوه کار آی پی پویا یا داینامیک Dynamic

این آدرس‌ها به تعداد مشخصی در اختیار شرکت‌های مختلف قرار داده می‌شود.

به طور مثال، شرکت مخابرات ممکن است IP های رنج ۰.۰.۰.۰ تا ۱۲۵.۱۲۵.۱۲۵.۱۲۵ را داشته باشد.

و شرکت‌های دیگر نیز هر کدام تعدادی آی پی در اختیار دارند.

این آی‌پی‌ها در Pool نگهداری می‌شوند و زمانی که یکی از کاربران به اینترنت متصل می‌شود، این آدرس در اختیار دستگاه متصل شده قرار می‌گیرد.

پس از قطعی اینترنت، آی پی مورد نظر دوباره به Pool باز می گردد تا در اختیار دستگاه دیگری قرار بگیرد.

انواع آدرس IP از لحاظ ثبات (تغییر ناپذیری):

۲- آی پی ثابت یا استاتیک Static

IP ثابت توسط شرکت‌های ارائه دهنده خدمات اینترنتی، به یک کاربر و دستگاهش اختصاص داده می‌شود.

در قبال این خدمات هزینه‌ای از کاربر گرفته می‌شود. در این صورت، تا زمانی که کاربر اجاره آی پی خود را پرداخت می‌کند، این آی پی مختص دستگاه مورد نظر خواهد بود و به دستگاه دیگری تعلق نمی‌گیرد.

انواع آدرس IP از لحاظ ثبات (تغییر ناپذیری):

ریموت کار کردن با آی پی ثابت و پویا

این اواخر، به علت گسترش تکنولوژی همه مشاغل به سمت ریموت و دورکاری می‌روند.

از آنجایی که آی پی ثابت به یک دستگاه به طور دائمی اختصاص داده می‌شود و تغییر نمی‌کند، امکان پیدا کردن و وصل شدن سایر دستگاه‌ها به دستگاهی با آی پی ثابت، آسان و ممکن خواهد بود.

اما اگر دستگاه مرکزی، آی پی داینامیک داشته باشد، یافتن آی پی آن دستگاه بسیار سخت خواهد بود.

همچنین، IP داینامیک با هر بار قطعی، یک آی پی جدید دریافت می‌کند و دستگاه‌های دیگر نمی توانند آی پی جدید را پیدا کنند.

بنابراین برای دورکاری، آی پی ثابت بهتر است.

تفاوت IP پویا و ثابت :

آی پی Static	آی پی Dynamic
توسط ISP (ارائه دهنده خدمات اینترنتی) ارائه می شود.	توسط سرور DHCP میزبان ارائه میشود.
آدرس آی پی استاتیک تغییر نمی کند، به این معنی است که اگر یک آدرس آی پی ثابت ارائه شود، نمی توان آن را تغییر داد.	آی پی آدرس های داینامیک همیشه تغییر میکنند.
آی پی های استاتیک امنیت پایین تری دارند.	به دلیل تغییر آی پی آدرس به صورت مکرر، امنیت آن نیز بیشتر است.
تنظیم آی پی آدرس استاتیک در بعضی مواقع سخت میباشد.	تنظیم نمودن آی پی داینامیک خیلی ساده است.
دستگاهی که از آی‌پی استاتیک استفاده میکند، قابل ردیابی است.	آی پی های داینامیک قابل ردیابی نیستند.
آدرس IP استاتیک پایدارتر از آدرس آی پی داینامیک است.	آدرس آی‌پی داینامیک نسبت به آدرس آی پی استاتیک ثبات کمتری دارد.
معمولا هزینه نگهداری آدرس آی پی ثابت بیشتر از آدرس IP داینامیک است.	هزینه نگهداری آدرس IP داینامیک کمتر از آدرس IP ثابت است.
در جایی استفاده می شود که داده های محرمانه کمتری دارند.	معمولا در جایی استفاده میشود که داده ها به امنیت بیشتری نیاز دارند.

انواع آدرس IP از نظر عمومی و خصوصی:

آدرس‌های آی پی توسط IANA که مخفف عبارت Internet Assigned Numbers Authority می‌باشد، تولید می‌شود.

سپس، IANA این آدرس‌ها را در اختیار شرکت‌های ارائه دهنده خدمات اینترنتی قرار می‌دهد و ما به عنوان مصرف کننده اینترنت، با خرید اینترنت می‌توانیم از مزایای اینترنت استفاده کنیم.

پس دستگاهی که توسط آن به اینترنت متصل می‌شویم، دارای آی پی خواهد بود. اما IP بر دو نوع است:

۱- آی پی عمومی Public

۲- آی پی خصوصی Private

انواع آدرس IP از نظر عمومی و خصوصی:

۱- آی پی عمومی Public:

آدرس آی پی عمومی Public IP address، آدرسی است که به هر دستگاه متصل به اینترنت اختصاص می‌یابد و لذا می‌توان از اینترنت به آن دسترسی یافت.

وقتی با کامپیوتر، گوشی یا هر وسیله دیگری به اینترنت متصل می‌شوید، آدرس آی پی منحصربه‌فردی به آن وسیله اختصاص می‌یابد که به آن آدرس آی پی عمومی Public IP address می‌گویند.

در اینترنت، هیچ دو وسیله‌ای را نمی‌توان یافت که آدرس آی پی عمومی آن‌ها یکسان باشد.

در این نوع آدرس IP محلی نیست و در سطح اینترنت آدرس دهی می شود.

انواع آدرس IP از نظر عمومی و خصوصی:

۲- آی پی خصوصی Private:

آدرس‌های آی پی خصوصی Private IP address آدرس‌هایی هستند که برای استفاده در شبکه‌های خصوصی و غیرمرتبط با اینترنت رزرو شده‌اند.

آدرس‌های آی پی خصوصی در اینترنت کاربرد ندارند.

شخصی که یک شبکه خانگی (فرض کنید الف) متشکل از چند کامپیوتر دارد، به هر یک از آن‌ها یک آدرس آی پی خصوصی اختصاص می‌دهد تا با یکدیگر مرتبط شوند.

ممکن است شخص دیگری در همان شهر یا جای دیگری از دنیا شبکه خصوصی دیگری (مثلا ب) ایجاد کرده باشد که آدرس گره‌های آن شبیه آدرس گره‌های شبکه «الف» است.

انواع آدرس IP از نظر عمومی و خصوصی:

۲- آی پی خصوصی Private:

اما چون این دو شبکه با هر ارتباط ندارند و به اینترنت نیز متصل نیستند، تشابه آدرس آن‌ها هیچ ایرادی ندارد.

در واقع هزاران شبکه خصوصی در دنیا می‌توانند از آدرس‌های آی پی خصوصی مشابهی استفاده کنند.

اما این شبکه‌ها اگر بخواهند به اینترنت متصل شوند باید با شیوه‌ای خاص، آدرس خصوصی خود را به آدرس عمومی منحصربه‌فرد تبدیل کنند.

برای این منظور از قابلیتی موسوم به «ترجمه آدرس شبکه» استفاده می‌شود که به آن NAT نیز می‌گویند.

مخفف Network Address Translation

ترجمه آدرس Address Translation

همان‌طور که توضیح داده شده است، برخی از آدرس‌های IP قابل مسیریابی از طریق اینترنت عمومی هستند و برخی دیگر آدرس‌های خصوصی هستند که برای استفاده درون سازمانی طراحی شده‌اند.

ترجمه آدرس شبکه NAT به آدرس‌های IP خصوصی (که در RFC 1918 تعریف شده‌اند) این امکان را می‌دهد که به آدرس‌های IP قابل مسیریابی در اینترنت (آدرس‌های IP عمومی) ترجمه شوند.

این بخش عملکرد NAT پایه و یک نوع متغیر به نام ترجمه آدرس پورت PAT را بررسی می‌کند.

ترجمه آدرس همچنین می‌تواند برای پورت‌های خاصی که به یک آدرس IP مرتبط هستند انجام شود.

زمانی که این کار انجام می‌شود، معمولاً به آن پورت فورواردینگ (Port Forwarding) گفته می‌شود.

NAT چیست؟

NAT (Network Address Translation) به‌معنی «ترجمه آدرس شبکه»، روشی هوشمندانه برای مدیریت آدرس‌های IPاست که به شما امکان می‌دهد چندین دستگاه متصل به اینترنت را در یک شبکه داخلی (مثلاً شبکه خانگی یا شرکتی که در آن کار می‌کنیم) ساماندهی کنید.

در این روش، تمامی دستگاه‌های موجود در شبکه داخلی، از یک آدرس IP مشترک استفاده می‌کنند.

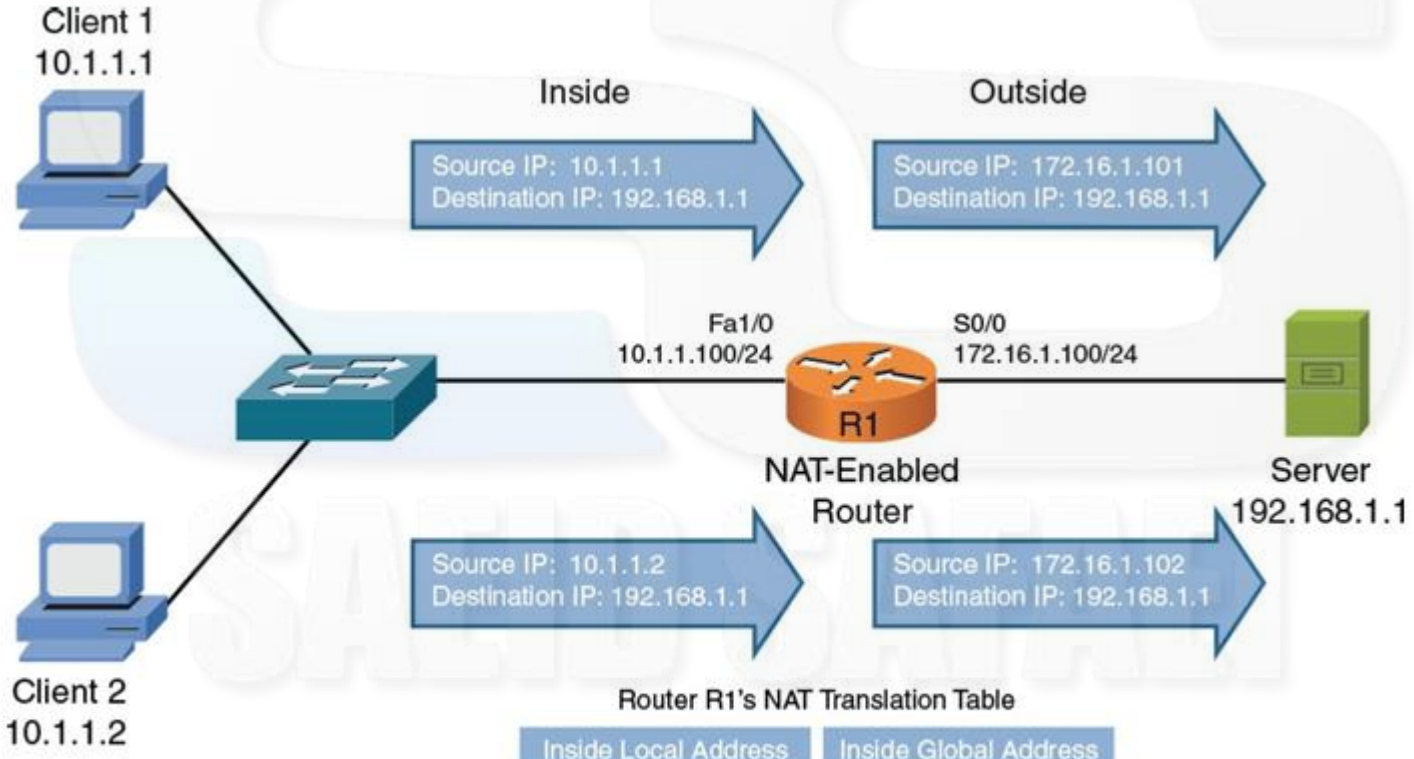
بنابراین، به جای اینکه هر دستگاه نیاز به آدرس IPمجزا داشته باشد، بسیاری از آن‌ها می‌توانند از یک IPمشترک استفاده کرده و مشکل کمبود آدرس‌های IPرا حل کنند.

اگر کسی همین الان از من بپرسد که مهم‌ترین مزایا تکنولوژی NATچیست، حتماً به او می‌گویم همین که غائله‌ی تمام شدن آدرس‌های IPحل شد، خودش مهم‌ترین مزیت NAT است.

نکته: با توجه به بالابودن تعداد زیاد IPv6 در این نوع نیازی به NAT نیست.

NAT

در این توپولوژی Basic NAT Topology، دو کلاینت با آدرس‌های IP خصوصی ۱۰.۱.۱.۱ و ۱۰.۱.۱.۲ می‌خواهند با یک سرور وب در اینترنت عمومی ارتباط برقرار کنند. آدرس IP سرور ۱۹۲.۱۶۸.۱.۱ است. روتر R1 برای NAT پیکربندی شده است.



Router R1's NAT Translation Table

Inside Local Address	Inside Global Address
10.1.1.1	172.16.1.101
10.1.1.2	172.16.1.102

NAT

به‌عنوان مثال، روتر R1 بسته‌هایی که از ۱۰.۱.۱.۱ به مقصد ۱۹۲.۱۶۸.۱.۱ می‌آیند را دریافت کرده و آدرس IP مبدا در هدر بسته‌ها را به ۱۷۲.۱۶.۱.۱۰۱ تغییر می‌دهد (که برای مقاصد این بحث، فرض می‌کنیم این آدرس یک آدرس IP عمومی قابل مسیریابی است).

زمانی که سرور با آدرس IP 192.168.1.1 ترافیک را از کلاینت دریافت می‌کند، ترافیک برگشتی سرور به آدرس مقصد ۱۷۲.۱۶.۱.۱۰۱ ارسال می‌شود.

هنگامی که روتر R1 ترافیک دریافتی از شبکه بیرونی که به مقصد ۱۷۲.۱۶.۱.۱۰۱ است را دریافت می‌کند، روتر آدرس IP مقصد را به ۱۰.۱.۱.۱ ترجمه کرده و ترافیک را به شبکه داخلی ارسال می‌کند، جایی که کلاینت ۱ این ترافیک را دریافت می‌کند.

به همین ترتیب، آدرس IP کلاینت ۲ که ۱۰.۱.۱.۲ است به آدرس IP 172.16.1.102 ترجمه می‌شود.

NAT

درNAT، اصطلاحات مختلفی برای اشاره به آدرس‌های IP داخلی و خارجی وجود دارد که به شرح زیر است:

۱- Inside Local :

یک آدرس IP خصوصی است که به یک دستگاه درون شبکه داخلی اشاره می‌کند. این آدرس معمولاً برای دستگاه‌های داخلی مانند کامپیوترها یا سرورها استفاده می‌شود که به طور مستقیم از طریق اینترنت دسترسی ندارند.

۲- Inside Global :

یک آدرس IP عمومی است که به یک دستگاه داخلی اشاره می‌کند. این آدرس به دستگاه‌های داخلی اجازه می‌دهد تا از طریق اینترنت قابل شناسایی باشند. این آدرس معمولاً توسط NAT برای ترجمه آدرس‌های IP خصوصی به آدرس‌های عمومی استفاده می‌شود.

NAT

۳- Outside Local :

یک آدرس IP خصوصی است که به یک دستگاه خارجی (در اینترنت) اشاره می‌کند. به عبارت دیگر، این آدرس به دستگاهی خارج از شبکه داخلی مربوط می‌شود، اما در اینترنت از یک آدرس خصوصی استفاده می‌کند.

۴- Outside Global :

یک آدرس IP عمومی است که به یک دستگاه خارجی اشاره می‌کند. این آدرس به دستگاه‌های بیرونی (در اینترنت) مربوط است و معمولاً برای شناسایی و مسیریابی آن‌ها در اینترنت استفاده می‌شود.

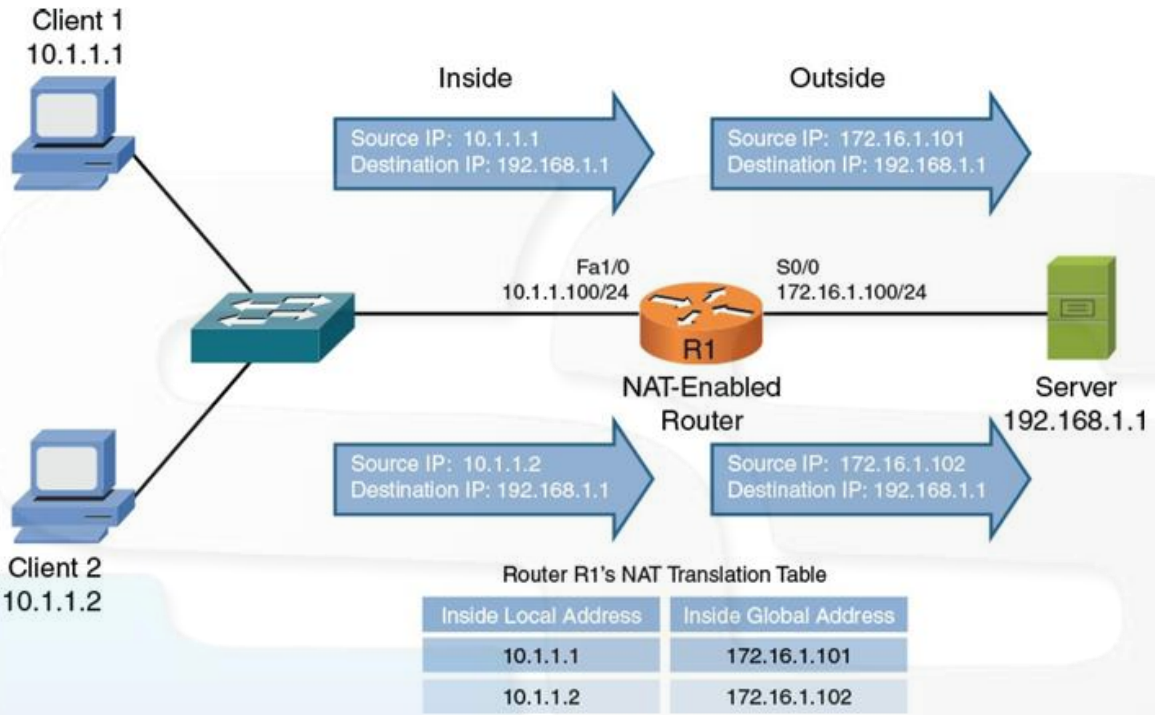
Inside Local: آدرس خصوصی دستگاه داخلی.

Inside Global: آدرس عمومی دستگاه داخلی.

Outside Local: آدرس خصوصی دستگاه خارجی.

Outside Global: آدرس عمومی دستگاه خارجی.

NAT



Router R1's NAT Translation Table

Inside Local Address	Inside Global Address
10.1.1.1	172.16.1.101
10.1.1.2	172.16.1.102

NAT IP Address	NAT IP Address Type
Inside local	10.1.1.1
Inside local	10.1.1.2
Inside global	172.16.1.101
Inside global	172.16.1.102
Outside local	None
Outside global	192.168.1.1

NAT

NAT همیشه مجبور نیست بین آدرس‌های خصوصی و عمومی انجام شود.

به‌عنوان مثال، NAT می‌تواند بین دو بازه آدرس خصوصی یا دو بازه آدرس عمومی نیز پیاده‌سازی شود.

مثال‌ها:

۱- NAT **بین دو آدرس خصوصی**: فرض کن دو شبکه خصوصی با آدرس‌های IP متفاوت وجود دارند که می‌خواهند با یکدیگر ارتباط برقرار کنند.

در این حالت، می‌توان از NAT برای ترجمه آدرس‌های IP خصوصی استفاده کرد تا این شبکه‌ها بتوانند به یکدیگر متصل شوند، حتی اگر به طور مستقیم در یک شبکه خصوصی قرار نداشته باشند.

۲- NAT **بین دو آدرس عمومی**: در برخی موارد، ممکن است NAT بین دو بازه آدرس IP عمومی انجام شود. این معمولاً زمانی اتفاق می‌افتد که سازمان‌ها بخواهند بین دو شبکه عمومی ارتباط برقرار کنند یا وقتی که یک سرویس‌دهنده اینترنت ISP برای مدیریت آدرس‌های IP عمومی خود از NAT استفاده می‌کند.

اینکه یک آدرس Inside Local به طور تصادفی از یک مجموعه آدرس‌های Inside Global تخصیص داده شود یا اینکه یک آدرس از پیکربندی استاتیک انتخاب شود، نوع NAT مورد استفاده را مشخص می‌کند. این دو روش مختلف برای NAT به نام‌های DNAT و SNAT شناخته می‌شوند:

DNAT (Dynamic NAT) :

در این روش، آدرس‌های Inside Local به طور خودکار از یک مجموعه آدرس‌های عمومی موجود به آدرس‌های Inside Global ترجمه می‌شوند.

این روش به عنوان NAT دینامیک شناخته می‌شود. در این حالت، بسیاری از کاربران داخلی (یک شبکه) به یک مجموعه از آدرس‌های Inside Global نگاشته می‌شوند.

این روش معمولاً به عنوان "چند به چند" many-to-many شناخته می‌شود، زیرا چندین آدرس داخلی به مجموعه‌ای از آدرس‌های عمومی نگاشته می‌شوند.

SNAT (Static NAT) :

گاهی اوقات، شما می‌خواهید آدرس Inside Global که به یک دستگاه خاص داخل شبکه‌تان اختصاص داده شده است را به صورت استاتیک پیکربندی کنید.

برای مثال، ممکن است یک سرور ایمیل در شبکه داخلی خود داشته باشید و بخواهید سرورهای ایمیل اینترنتی پیام‌ها را به این سرور ارسال کنند.

سرورهای ایمیل اینترنتی باید به یک آدرس IP خاص اشاره کنند، نه آدرسی که به طور تصادفی از یک مجموعه آدرس‌های IP انتخاب شده است.

در این شرایط، می‌توانید نگاشت یک آدرس Inside Local آدرس IPسرور ایمیل داخلی شما به یک آدرس Inside Global آدرسی که سرورهای ایمیل اینترنتی برای ارسال ایمیل‌ها به آن نیاز دارند را به صورت استاتیک پیکربندی کنید.

این روش به عنوان NAT استاتیک شناخته می‌شود و معمولاً به عنوان "چند به یک many-to-one نگاشته می‌شود.

خلاصه:

DNAT (Dynamic NAT) : آدرس‌های داخلی به طور خودکار به آدرس‌های عمومی اختصاص می‌یابند (چند به چند).

SNAT (Static NAT) :آدرس‌های داخلی به یک آدرس عمومی خاص به صورت ثابت نگاشته می‌شوند (چند به یک).

معنی دیگر SNAT و DNAT:

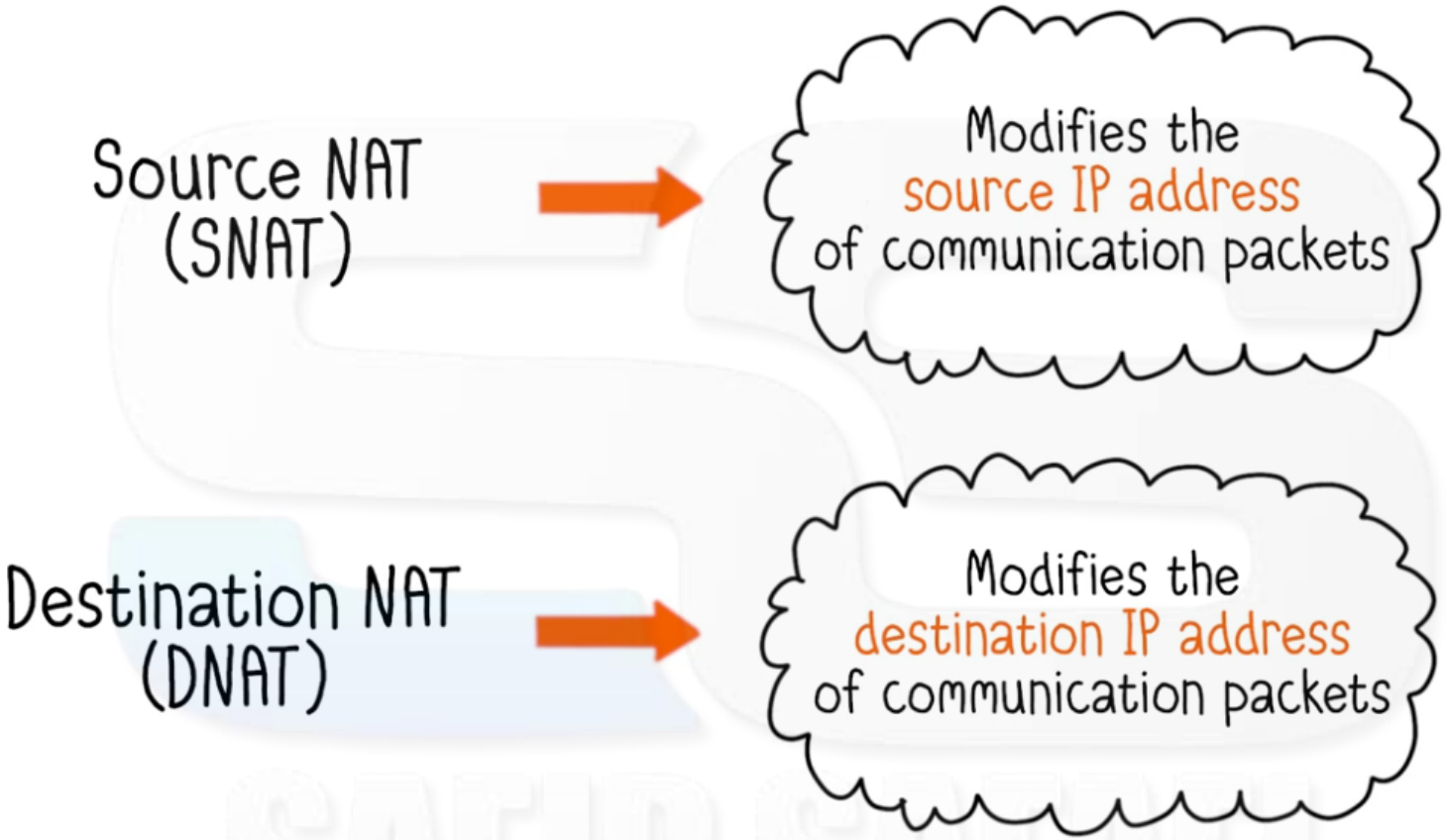
SNAT به معنای Source Network Address Translation است که برای تغییر آدرس IP مبدا بسته‌ها به کار می‌رود.

در این فرآیند، آدرس IP مبدا بسته‌های خروجی تغییر می‌کند تا به یک آدرس IP عمومی و پورت اختصاصی دستگاه اعمال شده توسط SNAT تطابق داشته باشد.

در حالی که **DNAT** (Destination Network Address Translation) مربوط به تغییر آدرس IP مقصد است، که در آن آدرس مقصد بسته‌های ورودی به آدرس‌های خصوصی شبکه ترجمه می‌شود.

SNAT : تغییر آدرس IPمبدا بسته‌ها برای تطابق با آدرس IPعمومی و پورت.

DNAT : تغییر آدرس IPمقصد بسته‌ها برای ارسال به آدرس‌های خصوصی شبکه.



با SNAT ، یک بالانسر بار Load Balancer، گیت‌وی ترجمه آدرس شبکه NAT Gateway، روتر یا هر دستگاه دیگری که SNAT انجام می‌دهد، آدرس IP مبدا و پورت بسته‌های خروجی را تغییر می‌دهد تا با آدرس IP عمومی و پورت خود مطابقت داشته باشد.

SNAT با پنهان کردن آدرس‌های IP خصوصی دستگاه‌ها، امنیت را افزایش می‌دهد و به حفظ آدرس‌های IP عمومی کمک می‌کند.

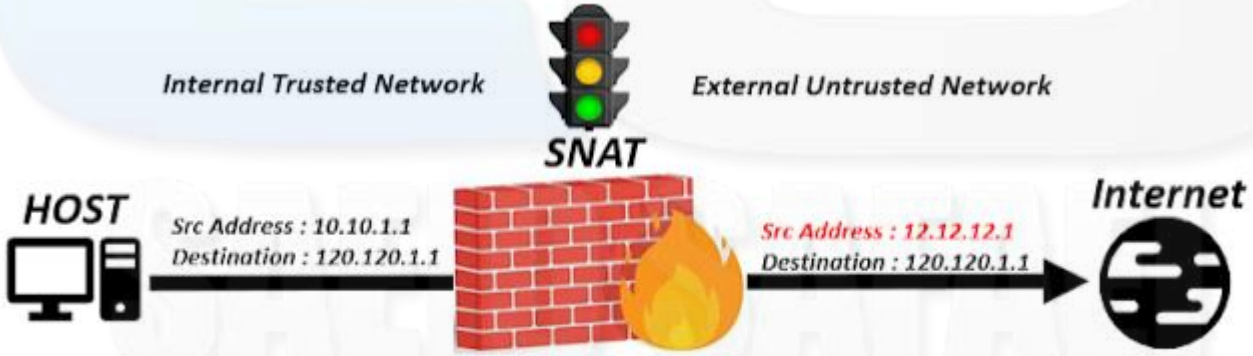


Fig 1.2- SNAT

DNAT یک فناوری است که به دستگاه‌ها در شبکه عمومی این امکان را می‌دهد که به دستگاه‌ها یا خدمات در شبکه خصوصی دسترسی پیدا کنند، با استفاده از یک آدرس IP عمومی و پورت.

DNAT آدرس IP مقصد و پورت بسته‌های ورودی را تغییر می‌دهد تا با آدرس IP خصوصی و پورت دستگاه یا سرویس DNAT که ممکن است یک فایروال، گیت‌وی ترجمه آدرس شبکه NAT Gateway یا روتر باشد مطابقت پیدا کند.

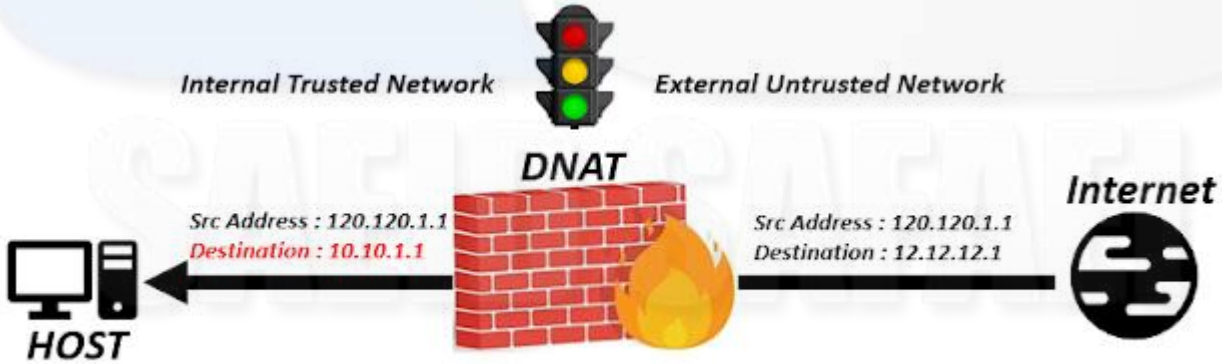
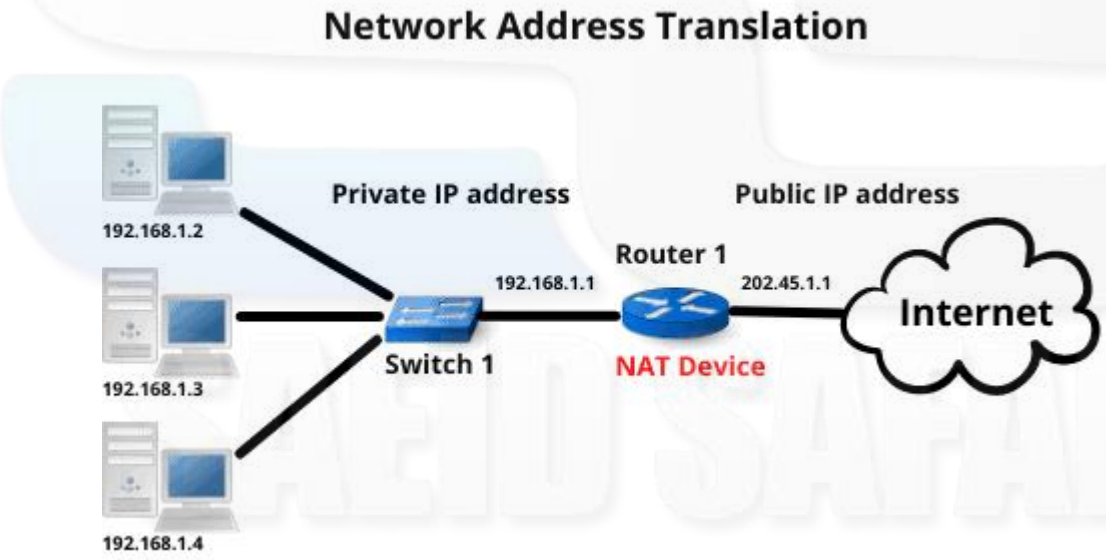


Fig 1.3- DNAT

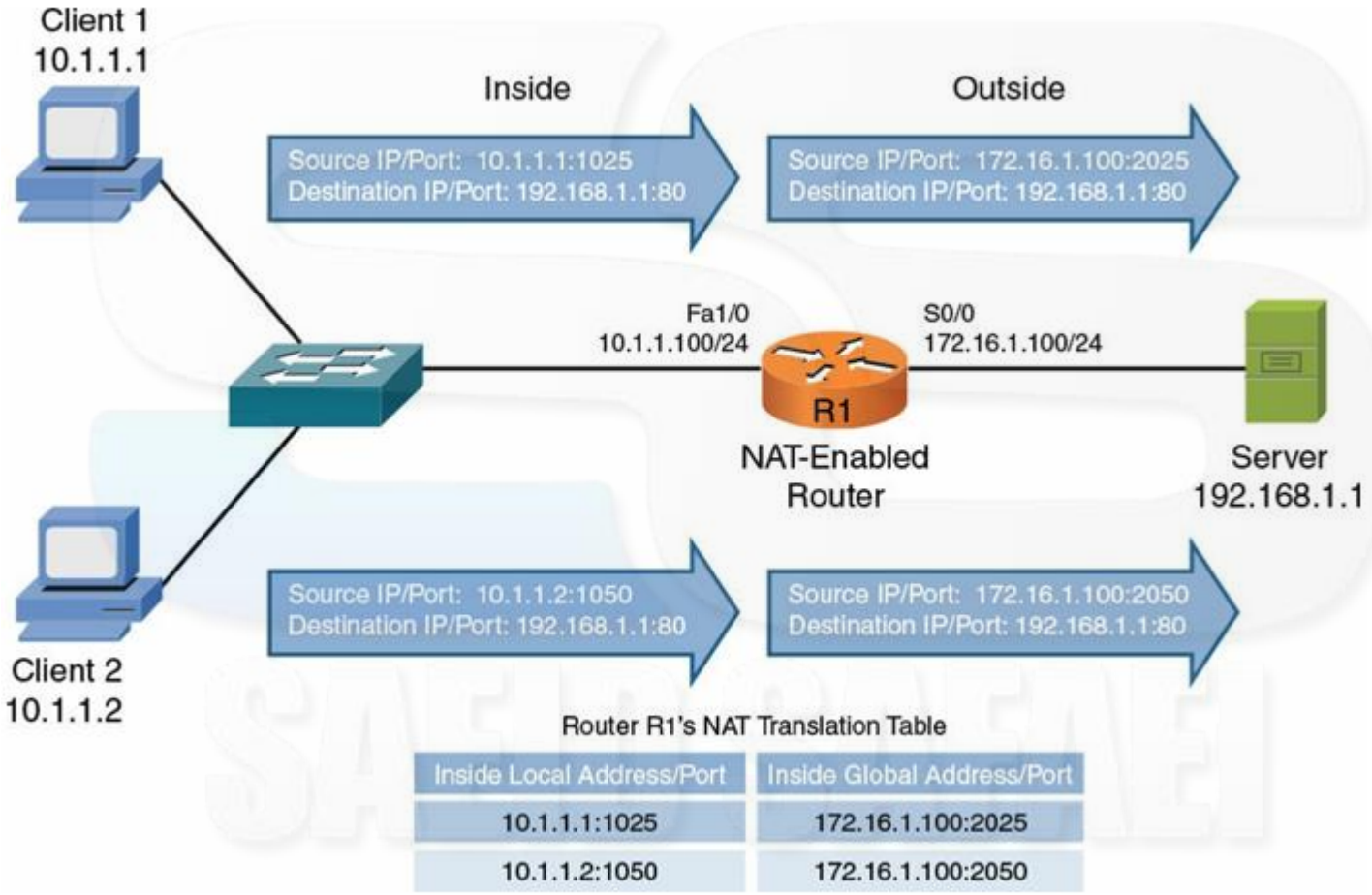
PAT (Port Address Translation) چیست؟

PAT (ترجمه آدرس پورت) یک نوع NAT داینامیک است که چندین دستگاه شبکه داخلی را با استفاده از پورت‌های متفاوت به یک آدرس IP عمومی متصل می‌کند.

این روش به ویژه برای شبکه‌های خانگی و کسب‌وکارهای کوچک مناسب است؛ زیرا با استفاده از یک آدرس IP عمومی، امکان دسترسی همزمان تعداد زیادی دستگاه به اینترنت را فراهم می‌کند.



PAT (Port Address Translation) چیست؟



Router R1's NAT Translation Table

Inside Local Address/Port	Inside Global Address/Port
10.1.1.1:1025	172.16.1.100:2025
10.1.1.2:1050	172.16.1.100:2050

PAT (Port Address Translation) چیست؟

مثال:

فرض کنید مودم شما دارای یک آدرس IP عمومی است و دو دستگاه داخلی (مثل لپ‌تاپ و موبایل) قصد اتصال به یک وب‌سایت دارند:

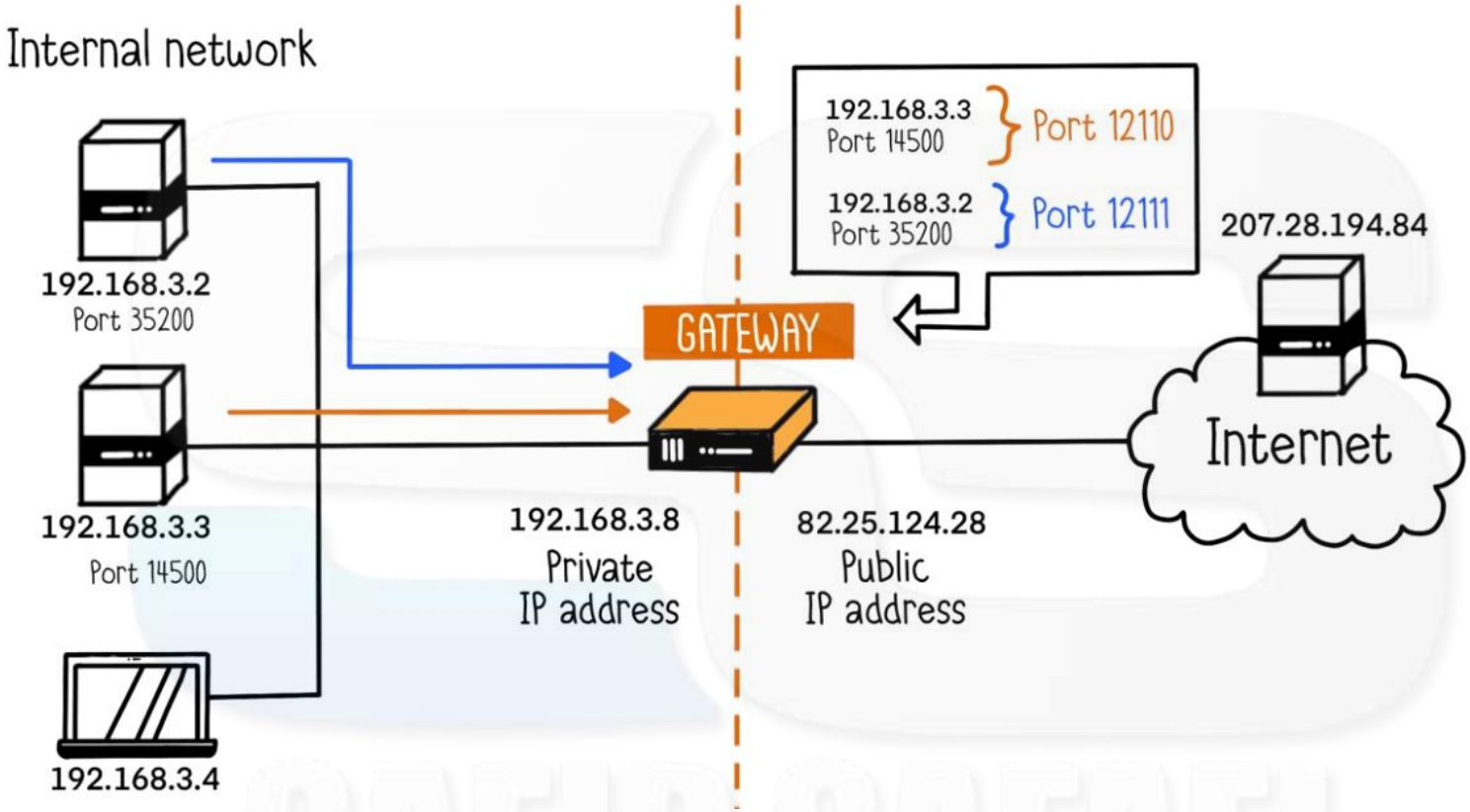
لپ‌تاپ با آدرس داخلی ۱۹۲.۱۶۸.۱.۲ و موبایل با آدرس داخلی ۱۹۲.۱۶۸.۱.۳ است.

مودم برای لپ‌تاپ پورت ۵۰۰۱ و برای موبایل پورت ۵۰۰۲ را اختصاص می‌دهد.

هنگام ارسال داده به اینترنت، مودم این ترافیک‌ها را با استفاده از آدرس IP عمومی خود (مثلاً ۲۰۳.۰.۱۱۳.۱) و شماره پورت‌های مربوطه به وب‌سایت ارسال می‌کند.

وقتی پاسخ از وب‌سایت به مودم می‌رسد، مودم با توجه به شماره پورت، تشخیص می‌دهد که ترافیک مربوط به لپ‌تاپ یا موبایل است و آن را به دستگاه مناسب ارسال می‌کند.

آدرس گذاری



Port Forwarding چیست؟

Port Forwarding یک روش است که به دستگاه‌های خارجی (مثلاً در اینترنت) اجازه می‌دهد تا به دستگاهی خاص در شبکه داخلی از طریق یک پورت مشخص دسترسی پیدا کنند.

در این روش، شما یک پورت مشخص در روتر (پورت خارجی) را به یک دستگاه داخلی و یک پورت خاص (پورت داخلی) در شبکه خصوصی اختصاص می‌دهید.

عملکرد: وقتی یک درخواست از اینترنت به پورت خاصی از روتر شما ارسال می‌شود، روتر آن درخواست را به دستگاه داخلی خاصی هدایت می‌کند.

این روش به شما امکان می‌دهد که دستگاه‌های خارجی به دستگاه‌های شبکه داخلی مانند سرورها، دوربین‌های امنیتی یا گیمینگ‌ها دسترسی داشته باشند.

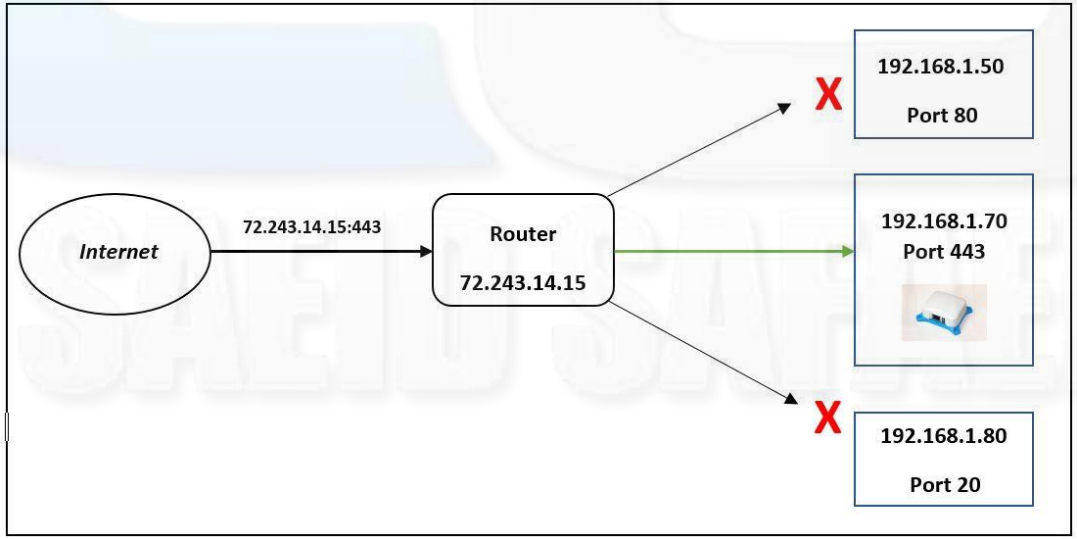
Port Forwarding چیست؟

مثال:

شما می‌خواهید از طریق اینترنت به دوربین امنیتی خود در خانه دسترسی پیدا کنید.

شما پورت ۸۰۸۰ در روتر را به پورت ۸۰ در دستگاه دوربین امنیتی با آدرس داخلی ۱۹۲.۱۶۸.۱.۴ هدایت می‌کنید.

هرگاه کسی به آدرس IP عمومی روتر شما (مثلاً ۲۰۳.۰.۱۱۳.۱) با پورت ۸۰۸۰ متصل شود، روتر آن درخواست را به دوربین داخلی در آدرس ۱۹۲.۱۶۸.۱.۴ هدایت می‌کند.



تفاوت NAT، PAT، Port Forwarding :

ویژگی	NAT (Network Address Translation)	PAT (Port Address Translation)	Port Forwarding
تعریف	ترجمه آدرس‌های IP خصوصی به IPعمومی برای ارتباط با اینترنت	نوعی NAT که از پورت‌ها برای شناسایی چندین دستگاه با یک IPعمومی استفاده می‌کند	هدایت ترافیک ورودی به یک دستگاه خاص در شبکه داخلی با استفاده از پورت
کاربرد	تبدیل آدرس IP خصوصی به عمومی و بالعکس	مدیریت چندین ارتباط خروجی از طریق یک آدرس IPعمومی	فراهم کردن دسترسی از بیرون به دستگاه‌های خاص در شبکه داخلی
پورت‌های استفاده‌شده	نیازی به تغییر پورت‌ها ندارد	از پورت‌های مختلف برای شناسایی هر دستگاه داخلی استفاده می‌کند	پورت‌های خاص به‌صورت دستی برای هر دستگاه تنظیم می‌شود

تفاوت NAT، PAT، Port Forwarding :

ویژگی	NAT (Network Address Translation)	PAT (Port Address Translation)	Port Forwarding
مبدأ و مقصد ترافیک	ترافیک خروجی از شبکه داخلی به اینترنت	ترافیک خروجی از شبکه داخلی به اینترنت با ترجمه پورت‌ها	ترافیک ورودی از اینترنت به شبکه داخلی
تعداد IP عمومی مورد نیاز	امکان استفاده از چندین IP عمومی یا تنها یک IP عمومی	فقط یک آدرس IP عمومی برای چندین دستگاه داخلی استفاده می‌شود	معمولاً از یک آدرس IP عمومی برای هدایت به دستگاه خاص استفاده می‌شود
مثال	ترجمه IPخصوصی ۱۹۲.۱۶۸.۱.۲ به IP عمومی ۲۰۳.۰.۱۱۳.۱	ترجمه IPداخلی ۱۹۲.۱۶۸.۱.۲ به IP عمومی با پورت ۵۰۰۱	هدایت ترافیک از پورت ۸۰۸۰ به پورت ۸۰ روی آدرس ۱۹۲.۱۶۸.۱.۴

IP های رزرو شده

آدرس IP رزرو شده:

کارگروه مهندسی اینترنت IETF و نهاد متصدی انتساب اعداد در اینترنت IANA شماری از آدرس‌های آی پی را رزرو کرده‌اند.

این آدرس‌ها برای کاربردهای خاصی رزرو شده‌اند.

در ادامه برخی از آدرس‌های آی پی رزرو شده به‌اختصار توضیح داده می‌شوند.

آدرس آی پی 0.0.0.0 چیست؟

آدرس آی پی ۰.۰.۰.۰ یک آدرس غیرقابل مسیریابی است که معمولا نامعتبر یا ناشناخته بودن مقصد را نشان می‌دهد.

البته این آدرس روی دستگاه‌های کلاینت و سرور کاربردها و معانی متفاوتی دارد.

آدرس آی پی ۰.۰.۰.۰ در کامپیوتر شخصی و کلاینت نشان می‌دهد که دستگاه به شبکه TCP/IP متصل نیست و احتمالا آفلاین است.

گاهی نیز اگر تخصیص آدرس آی پی دچار نقص شود، DHCP به‌طور خودکار این آدرس آی پی را به دستگاه اختصاص می‌دهد.

وقتی آدرس آی پی کامپیوتر ۰.۰.۰.۰ باشد، نمی‌تواند با هیچ‌یک از تجهیزات متصل به شبکه مرتبط شود.

آدرس آی پی 0.0.0.0 چیست؟

اما کاربرد آدرس آی پی ۰.۰.۰.۰ در سرورهای شبکه متفاوت است. برخی تجهیزات به‌ویژه سرورهای شبکه بیش از یک کارت شبکه دارند و به هر کارت شبکه نیز آی پی متفاوتی اختصاص می‌یابد.

اپلیکیشن‌های TCP/IP با استفاده از آدرس ۰.۰.۰.۰ ترافیک شبکه را روی همه آدرس‌های آی پی اختصاص یافته به کارت‌های شبکه آن سرور که به چند شبکه متصل است، مانیتور می‌کنند.

آدرس آی پی 127.0.0.1 چیست؟

آدرس آی پی ۱۲۷.۰.۰.۱ را هاست محلی (لوکال‌هاست) نیز می‌نامند.

هر کامپیوتری برای اشاره به خود از آدرس آی پی ۱۲۷.۰.۰.۱ استفاده می‌کند.

اما با این آدرس آی پی نمی‌توان به شبکه یا به اینترنت متصل شد.

می‌توانید به کامپیوترتان یک آدرس آی پی خصوصی مثل ۱۹۲.۱۶۸.۱.۱۱۵ اختصاص دهید تا با روتر و دیگر گره‌های شبکه مرتبط شود. اما حتی در این‌صورت نیز هویت فردی کامپیوترتان با آدرس آی پی ۱۲۷.۰.۰.۱ تعریف می‌شود.

به عبارت دیگر، آدرس آی پی ۱۲۷.۰.۰.۱ فقط توسط خود کامپیوتر و روی همان کامپیوتر کاربرد دارد.

آدرس آی پی 8.8.8.8 و آدرس آی پی 8.8.4.4 چیست؟

آدرس آی پی ۸.۸.۸.۸ و نیز ۸.۸.۴.۴ متعلق به سرورهای DNS عمومی گوگل است.

گوگل این سرویس را برای افزایش سرعت وب‌گردی راه‌اندازی کرده است.

این دو آدرس ضریب اطمینان‌پذیری زیادی دارند و می‌توان گفت همیشه آنلاین هستند.

لذا کاربران برای اطمینان از این‌که آیا کامپیوترشان آنلاین است یا نه می‌توانند آن را با آدرس آی پی ۸.۸.۸.۸ یا ۸.۸.۴.۴ پینگ کنند.

اگر پس از پینگ با پیغام خطا مواجه شدند، به احتمال زیاد ایراد از سمت کاربر است و او باید تنظیمات کامپیوتر یا شبکه را بازنگری کند.

کلاس بندی IP

رنج IP چیست؟

دامنه آدرس آی پی، محدوده آدرس‌های آی پی مجاز و معتبر را تعیین می‌کند.

در فرمت IPv4 دامنه آدرس‌های آی پی از ۰.۰.۰.۰ شروع می‌شود و با ۲۵۵.۲۵۵.۲۵۵.۲۵۵ خاتمه می‌یابد.

پس برای مثال، آدرس آی پی ۱۰.۰.۰.۰ معتبر اما آدرس آی پی ۳۰۰.۰.۰.۰ نامعتبر است، چون خارج از دامنه مجاز آدرس‌های آی پی است.

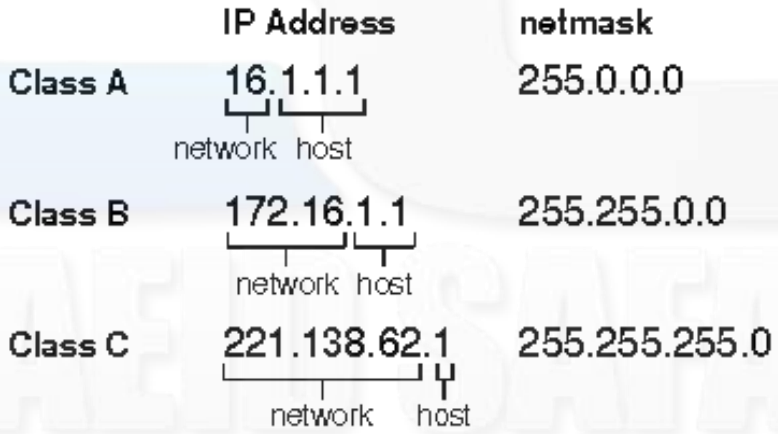
علاوه بر این، بسته به کاربردهای مختلف می‌توان دامنه‌های دیگری نیز تعریف کرد. مثلا پیش‌تر، در توضیح آدرس‌های آی پی عمومی و خصوصی گفته شد که هر یک از آن‌ها دامنه یا محدوده مشخصی دارند.

کلاس‌های آدرس آی پی از دیگر مواردی هستند که هر یک دامنه مختص خود را دارند.

کلاس بندی IP:

همان طور که در قسمت پیشین ساختار ای پی ها متوجه شدید یک ای پی از ۴ قسمت مختلف به نام Octet تشکیل گشته است.

حال بسته به یک شکل بودن اکتت های ای پی ها دو پارامتر دیگر به نام Network ID و Host ID تعریف میگردد.



کلاس بندی IP:

آدرس آی پی ورژن چهار ۳۲ بیت است و این ۳۲ بیت برای اینکه ما انسانها و خود سیستم ها راحت تر با این آدرس کار کنند در قالب ۴ بایت استفاده میشه و به هر بایت که هشت بیت هست یک Octet گفته میشود و بین این octet ها یا بایت ها توسط یک نقطه از یکدیگر جدا میشوند .

۱۱۰۰۰۰۰۰.۱۰۱۰۱۰۰۰.۰۰۰۰۰۰۰۰.۰۰۰۰۱۰۱۰

این عدد باینری معادل آی پی ۱۹۲.۱۶۸.۰.۱۰

خود آی پی هم از دو بخش تشکیل میشود یک بخش که شماره شبکه هست باعنوان NetID و بخش دیگر که شماره کامپیوتر هست را HostID می نامند.

کلاس بندی IP:

Network ID (رنج آی پی)

به Station های ثابت در یک شبکه Network ID گفته میشود.

برای مثال دو ای پی ۸۷.۱۰۷.۲۵.۶۷ و ۸۷.۱۰۷.۵۹.۴۷ را در نظر بگیرید همان طور که میبینید دو octet اول این ای پی ها برابر و یکسان هستند بنابراین دو Octet ابتدایی که ۸۷.۱۰۷ میباشد Network ID نام میگیرد زیرا این دو قسمت در تمامی ادرس ها یکسان است و تغییر نمیکند.

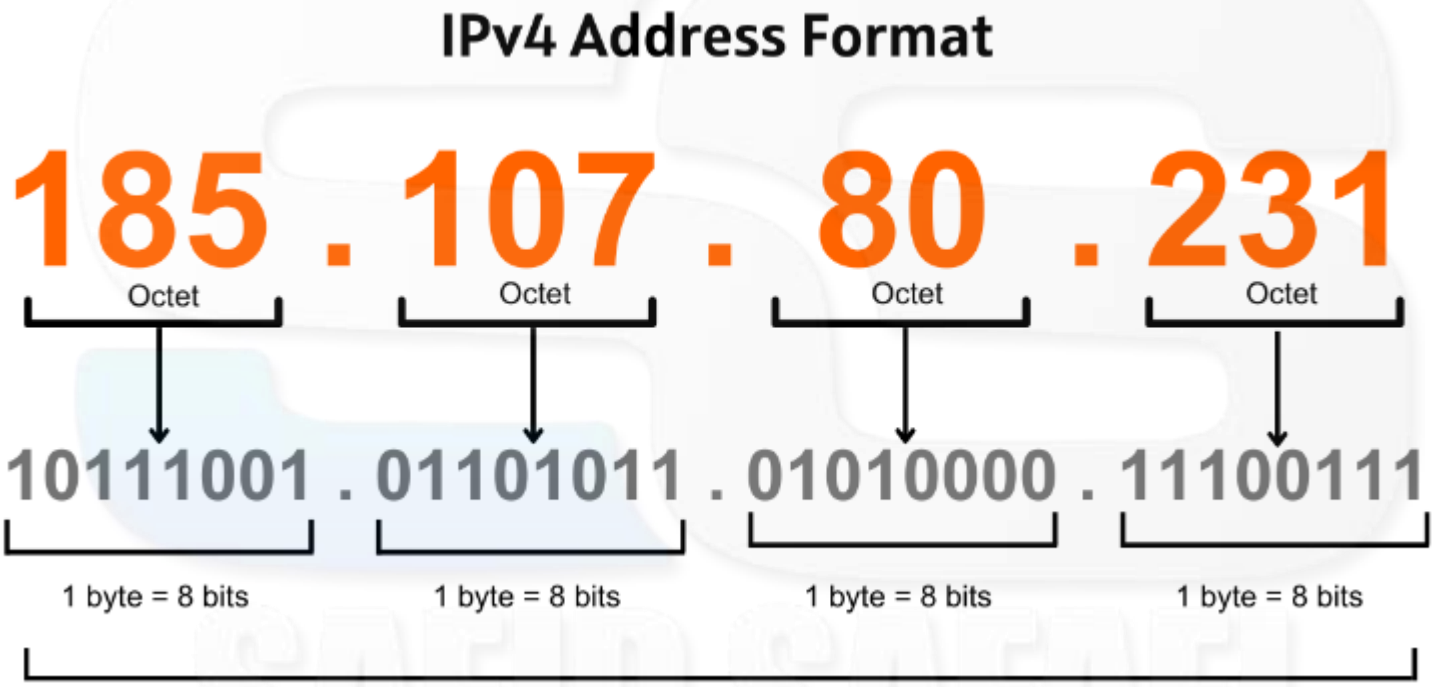
کلاس بندی IP:

Host ID

این بخش از ای پی ادرس ها نقش مهمتری را بازی میکند و در واقع وجه تمایز اکتت ها با یکدیگر است بنابراین تفاوت ای پی ها با یکدیگر از بخش دوم یا هاست ای دی مشخص میگردد.

در مثال قبل بالا ۲۵.۶۷ و ۵۹.۴۷ هاست ای دی ادرس ها هستند.

کلاس بندی IP:



کلاس بندی IP:

128	64	32	16	8	4	2	1
0	1	1	1	1	1	1	1

← ۱۲۷

در تصویر فوق جدولی را مشاهده میکنید که به ازاء هر بیت یک عدد در بالای آن قرار گرفته است اگر بیتی یک باشد عدد بالای آن را حساب میکنیم و اگر بیتی صفر بود عدد بالای آن محاسبه نمیشود.

پس برای محاسبه اینگونه عمل میکنیم :

0+64+32+16+8+4+2+1=127

Network	Host		
1 to 126	x	x	x

کلاس بندی IP:

ولی شاید با خود بگویید چرا در تصویر فوق کلاس A از ۱ تا ۱۲۶ است در صورتی که می بایست تا ۱۲۷ باشد؟

در پاسخ به این سوال باید بگویم ۱۲۷ آدرسی است که به عنوان IP نمیتوان در سیستم ها استفاده نمود ۱۲۷ آدرسی است که به آن Loopback Address گفته میشود و برای تست و سلامتی کارت شبکه مورد استفاده است . (صفحه ۳۰ همین اسلاید)

Class A

Network	Host		
1 to 126	x	x	x

کلاس بندی IP:

	128 2^7	64 2^6	32 2^5	16 2^4	8 2^3	4 2^2	2 2^1	1 2^0
کلاس A	0	1	1	1	1	1	1	1
	0+64+32+16+8+4+2+1 = 127							
کلاس B	1	0	1	1	1	1	1	1
	128+0+32+16+8+4+2+1= 191							
کلاس C	1	1	0	1	1	1	1	1
	128+64+0+16+8+4+2+1=223							
کلاس D	1	1	1	0	1	1	1	1
	128+64+32+0+8+4+2+1=239							

کلاس بندی IP:

کلاس B :

در این کلاس دو تا octet اول NetId هست و دوتا octet باقی مانده HostId هستند.

همانند کلاس A این کلاس نیز دارای نشانه ای هست، دو بیت اول Octet اول با ۱۰ شروع می شود و نمیتوان این دو بیت را تغییر داد ، بنا بر این Octet اول فقط ۶ بیت داریم و در مجموع برای Netid ما از ۱۴ بیت میتوانیم استفاده کنیم و برای Hostid این تعداد به ۱۶ میرسد.

بنابر این دو به توان ۱۶ البته منهای دو میشود ۶۵۵۳۴ عدد آی پی مورد استفاده برای سیستم های داخل شبکه پس میبینیم که در کلاس B تعداد آی پی های مورد استفاده به مراتب کمتر از کلاس A می باشد.

کلاس بندی IP:

کلاس B :

Class B

Network		Host	
128 to 191	x	x	x

اگر دو بیت octet اول را که به صورت ثابت ۱۰راقرار دهیم آخرین عدیدی که میتوان قرار داد برابر است با

128+0+32+16+8+4+2+1= 191

کلاس بندی IP:

کلاس C :

حتماً حدس زده اید که این بار سه تا Octet اول مربوط به NetId یا شماره شبکه هست و فقط Octet آخری مربوط به HostId هست و این بار سه بیت اول Octet اول ۱۱۰ هست و این نشانه ای است که فقط مربوط به کلاس C است و در octet اول فقط ۵ بیت میتواند متغیر باشد در این کلاس تعداد بیت های قسمت Netid به ۲۱ میرسد و تعداد Hostid به دو به توان ۸ منهای دو ۲۵۴ آدرس است.

Class C

	Network		Host
192 to 223	x	x	x

کلاس بندی IP:

کلاس D :

آدرس کلاس D برای Multicasting استفاده میشود و در کلاس D چهارمین بیت از Octet اول صفر میباشد البته ۴ بیت اول این Octet به ترتیب ۱۱۱۰ است و این چهار بیت را نمیتوان تغییر داد و این مشخصه مربوط به این کلاس می باشد ، ضمناً محدوده آدرس دهی این کلاس نیز در تصویر زیر مشاهده میشود.

Class D

Network	Host		
224 to 239	x	x	x

Multicast چون یک گروه از کامپیوتر ها را شامل میشود بنابر این اگر بخواهیم بگوییم Netid یا Hostid این کلمه برای این کلاس بی معنی است

کلاس بندی IP:

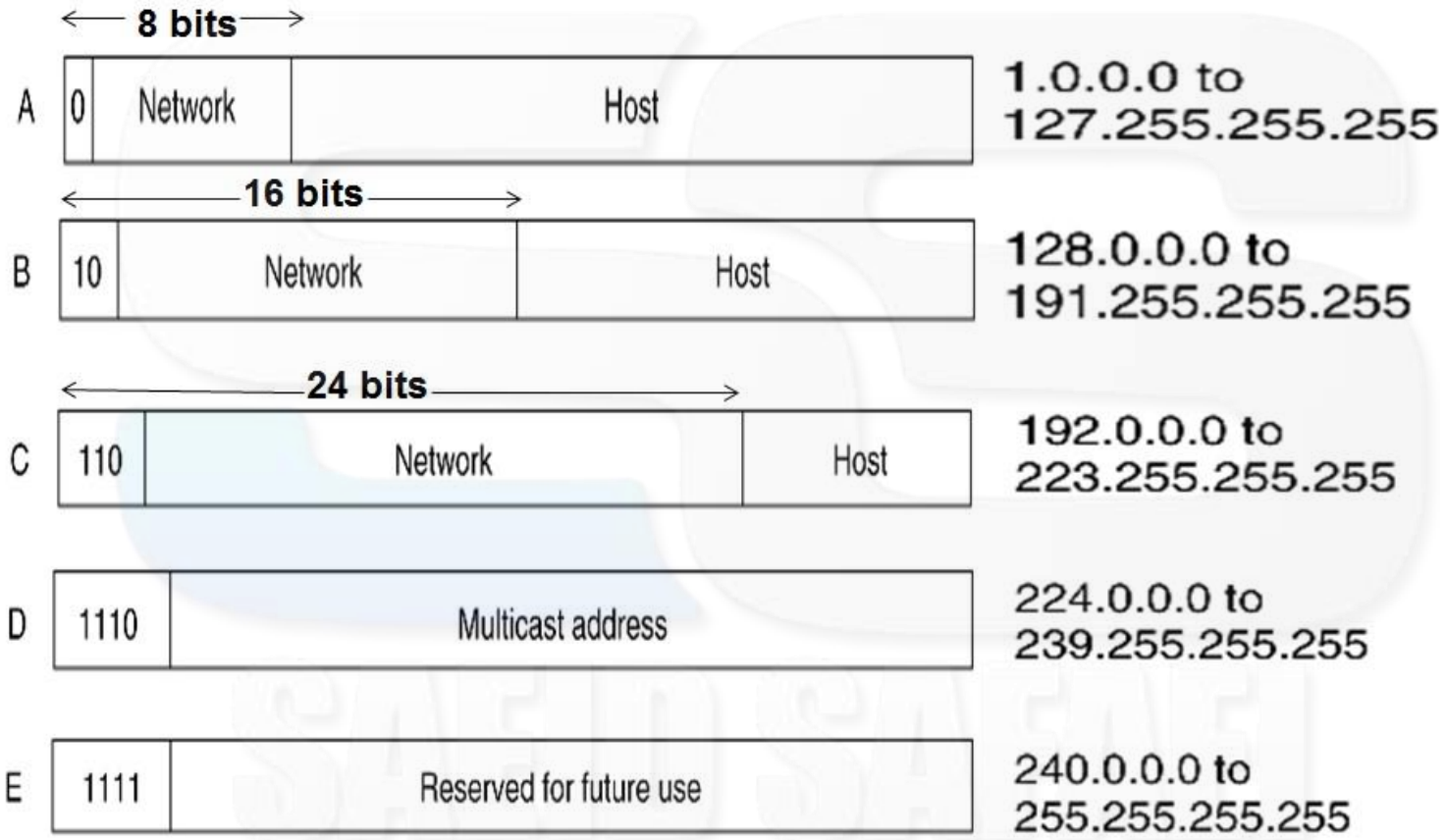
کلاس E :

در این کلاس وضعیت چهار بیت اول ۱۱۱۱ است این کلاس برای کار های تحقیقاتی و تجربی محیا شده است و ما نمیتوانیم از این آدرس استفاده کنیم و برای اینکه یادمان باشد میتوان گفت این کلاس Exprimental است.

Class E

Network	Host		
240 to 254	x	x	x

کلاس بندی IP:



Subnet Mask

SubnetMask چیست؟

سیستم ها برای تشخیص تعلق یا عدم تعلق به یک شبکه از مفهومی به نام Subnet Mask استفاده می کند.

به این صورت که تمام بیت های NetID را ۱ و تمام بیت های HostID را ۰ در نظر می گیرد تا Subnet mask را بسازد.

در نظر داشته باشید که هر کلاسی که ما میتوانیم ازشون به عنوان یک آدرس استفاده کنیم یک SubnetMask استاندارد دارد به عبارت دیگر هر IP دارای یک SubnetMask است و برای کلاس هایی که در بالا گفته شد این SubnetMask ها به صورت استاندارد زیر هستند:

Class A : 255.0.0.0

Class B : 255.255.0.0

Class C: 255.255.255.0

SubnetMask چیست؟

Subnet Mask یک قسمت مهم از تنظیمات کارت شبکه است.

آدرس IPاز دو بخش net-id و host-idتشکیل میشود.

آدرس IP کامپیوترهایی که قرار است در یک شبکه باشند باید طوری تنظیم شود که همه کامپیوترها قسمت net-id یکسان و هر کامپیوتر قسمت host-id مختص به خودش را داشته باشد.

Subnet Mask قسمت Net-ID و Host-ID از آدرس IPرا به پروتکل TCP/IPمعرفی میکند.

علاوه بر این پروتکل آی پی به کمک Subnet Mask میتواند متوجه شود که آدرس ip کامپیوتر مقصد در داخل شبکه است یا بیرون آن.

فواید استفاده از SubnetMask

۱. **تقسیم‌بندی شبکه**: Subnet Mask امکان تقسیم یک شبکه بزرگ به چندین زیرشبکه را فراهم می‌کند.

این امر باعث می‌شود که مدیریت شبکه ساده‌تر شود و ترافیک شبکه بهینه‌تر تقسیم شود.

۲. **افزایش امنیت**: با استفاده از Subnet Mask، می‌توان بخش‌های مختلف شبکه را از هم جدا کرد.

این جداسازی باعث افزایش امنیت می‌شود، زیرا هر بخش به طور مستقل عمل می‌کند و در صورت بروز مشکل یا حمله در یک بخش، بخش‌های دیگر تأثیر نخواهند گرفت.

فواید استفاده از SubnetMask

۳. کاهش ترافیک: Subnet Mask کمک می‌کند تا ترافیک درون شبکه محدود شود.

با تقسیم شبکه به زیرشبکه‌های کوچکتر، ترافیک Broadcastتنها به همان زیرشبکه ارسال می‌شود و به کل شبکه گسترده نمی‌شود. این امر باعث کاهش بار روی شبکه و افزایش کارایی آن می‌شود.

۴. مدیریت بهتر آدرس‌های IP: Subnet Mask به مدیران شبکه اجازه می‌دهد که فضای آدرس‌های IP خود را بهینه‌تر مدیریت کنند.

با تقسیم‌بندی شبکه‌ها، می‌توان از آدرس‌های IP به‌صورت بهینه‌تری استفاده کرد و از هدررفت منابع جلوگیری کرد.

فواید استفاده از SubnetMask

۵. قابلیت گسترش شبکه: با استفاده از Subnet Mask می‌توان به راحتی شبکه را گسترش داد و زیرشبکه‌های جدیدی به آن اضافه کرد بدون این که نیاز به تغییرات اساسی در ساختار اصلی شبکه باشد.

۶. پشتیبانی از توپولوژی‌های پیچیده‌تر: Subnet Mask امکان پیکربندی توپولوژی‌های پیچیده‌تر را می‌دهد، به ویژه در شبکه‌هایی که نیاز به چندین زیرشبکه برای عملکرد بهتر دارند.

مثال ۱ ؟

فرض کنید آدرس IP و Subnet Mask یکی از کامپیوترهای شبکه به ترتیب برابر با ۱۷۲.۱۸.۰.۱ و ۲۵۵.۲۵۵.۰.۰ باشد.

در اینصورت پروتکل IP میتواند از روی Subnet Mask بفهمد:

شناسه شبکه NetID برابر است با ۱۷۲.۱۸

شناسه کامپیوتر HostID برابر است با ۰.۱

Network (Address) ip برابر است با ۱۷۲.۱۸.۰.۰

Broadcast (Address) ip برابر است با ۱۷۲.۱۸.۲۵۵.۲۵۵

Usable ip ها (رنج) یا همان ip کامپیوترهای شبکه از ۱۷۲.۱۸.۰.۱ تا ۱۷۲.۱۸.۲۵۵.۲۵۴ است

مثال ۲ ؟

فرض کنید آدرس IP و Subnet Mask یکی از کامپیوترهای شبکه به ترتیب برابر با ۱۹۲.۱۶۸.۰.۱ و ۲۵۵.۲۵۵.۲۵۵.۰ باشد.

در اینصورت پروتکل IP میتواند از روی Subnet Mask بفهمد:

شناسه شبکه برابر است با ۱۹۲.۱۶۸.۰

شناسه کامپیوتر برابر است با ۱

Network ip برابر است با ۱۹۲.۱۶۸.۰.۰

Broadcast ip برابر است با ۱۹۲.۱۶۸.۰.۲۵۵

Usable ip ها یا همان ip کامپیوترهای شبکه از ۱۹۲.۱۶۸.۰.۱ تا ۱۹۲.۱۶۸.۰.۲۵۴ است

فرمت های نمایش IP:

IP هادر دو صورت قابل نمایش هستند

۱- Subnet Mask Format

۲- Prefix Format

در Subnet Mask Format، آی پی مربوطه را به صورت یک IP به همراه Subnet Mask آن به صورت جداگانه نمایش می دهیم.

مثال:

IP: 192.168.1.2

Subnet mask: 255.255.255.0

فرمت های نمایش IP:

در Prefix Format آی پی و Subnet Mask آن را با هم در یک IP نشان میدهید ، یعنی بعد از IP، یک / (که جداکننده IP از عدد مربوط به Subnet Mask هست) قرار میدهیم و سپس یک عدد نوشته میشود که این عدد تعداد ۱ (تعداد بیتNetID) هایی که در Subnet Mask همان IP داریم می باشد به طور مثال:

192.168.1.2/24

Class	First Octet	Default Subnet Mask	
		Slash	Dotted Decimal
A	1 - 126	/8	255.0.0.0
B	128 - 191	/16	255.255.0.0
C	192 - 223	/24	255.255.255.0
D	224 - 239		
E	240 - 255		

Supernetting

معرفی Supernetting :

Supernetting برعکس عملیات subnetting است ،یعنی شما میتوانید توسط این عملیات تعدادی شبکه کوچک را با هم یکی و ادغام کنید و از تجمیع این شبکه ها یک شبکه بزرگ را تشکیل دهید.

شاید بپرسید این کار به چه دردی میخورد باید بگویم از این عملیات برای کاهش ترافیک شبکه هایی که قرار است Router بسته ای را به چند شبکه ارسال کند استفاده می شود.

به عبارتی ساده تر هدف این کار کاهش پیچیدگی جداول router ها است .

معرفی Supernetting :

مثلا سازمانی میخواهد از ۲۰۰۰ آدرس آی پی استفاده کند برای این منظور مجبور است از کلاس B استفاده کند ولی کلاس B به ما ۶۵.۵۳۴ هزار آی پی میدهد.

طبیعتاً از ۲۰۰۰ آی پی بیشتر است ما میتوانیم به جای استفاده از یک کلاس B از ۸ کلاس متوالی C استفاده کنیم یعنی ۸ تا ۲۵۴ آدرس که جمعاً میشود ۲۰۲۳ که کمی بیشتر از ۲۰۰۰ آدرس آی پی هست.

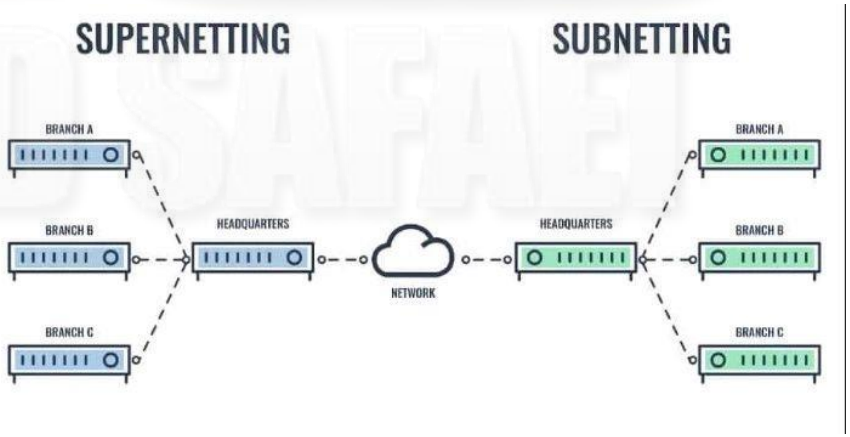
یادتان باشد که ما باید یک عدد از توان ۲ را استفاده کنیم اگر از ۷ کلاس C استفاده کنیم میشود ۱۷۷۸ که به عدد ۲۰۰۰ ای که ما میخواهیم نمیرسد خب این مشکل تعداد آی پی بیهوده ما را حل میکند.

معرفی Supernetting :

ولی اشکال مهم این کار این است که در router های میانی موجود در Internet جهت مسیریابی داده ها و همچنین آدرس‌دهی به همچنین شبکه‌ای باید ۸ ورودی مختلف برای یک شبکه وجود داشته باشد.

که در این صورت ترافیک کار و جدول مسیر یابی بسته ها افزایش میابد و کارsupernetting دقیقاً از همینجا شروع میشود در این حالت از Classless InterDomain Routing یا CIDR استفاده می‌شود.

که این موضوع را با مثالی که در ادامه آمده است توضیح خواهیم داد.



مفهوم CIDR:

CIDR (**Classless** Inter-Domain Routing) یک روش برای تخصیص و مدیریت آدرس‌های IP است که به جای استفاده از سیستم کلاس‌های سنتی A، B، C، به ما امکان می‌دهد تا آدرس‌ها را به صورت انعطاف‌پذیرتر و کارآمدتر مدیریت کنیم.

بیشتر از کلاس‌های سنتی:

در کلاس‌های سنتی، آدرس‌های IP به سه کلاس A، B و Cتقسیم می‌شوند که هر کدام دارای محدوده‌های مشخصی هستند.

CIDR این محدودیت‌ها را حذف کرده و به ما اجازه می‌دهد که هر آدرس IP را با استفاده از یک Prefix تعیین کنیم.

مفهوم CIDR:

Prefix: به جای استفاده از یک Subnet Mask ثابت، CIDR از یک نوتیشن به شکل /N استفاده می‌کند که در آن N تعداد بیت‌های استفاده‌شده برای بخش شبکه را نشان می‌دهد.

به عنوان مثال، در آدرس ۱۹۲.۱۶۸.۱.۰/۲۴، **۲۴ بیت اول** برای بخش شبکه استفاده شده است.

مزایای CIDR:

۱-کاهش هدررفت آدرس: CIDR به ما امکان می‌دهد که آدرس‌های IP را به شکلی تخصیص دهیم که هدررفت آدرس را کاهش دهد. این به معنای استفاده مؤثرتر از فضای آدرس IP است.

۲-خلاصه‌سازی مسیر: با استفاده از CIDR، می‌توان چندین آدرس IP را به یک آدرس شبکه جمع کرد. این کار باعث کاهش تعداد ورودی‌های جدول مسیریابی Routing Table در روترها می‌شود و کارایی شبکه را بهبود می‌بخشد.

۳-انعطاف‌پذیری: CIDR به ما اجازه می‌دهد که به راحتی زیرشبکه‌های بزرگ‌تری ایجاد کنیم یا آن‌ها را به زیرشبکه‌های کوچکتر تقسیم کنیم. این باعث می‌شود که تخصیص آدرس‌های IPبر اساس نیازهای خاص شبکه آسان‌تر باشد.

مثال Supernetting :

در مثال زیر میخواهیم ۴ شبکه با آدرس آی پی های زیر را تبدیل به یک شبکه بزرگتر کنیم که یک آی پی به ما بدهد:

10.128.0.0 /11

10.160.0.0 /11

10.192.0.0 /11

10.224.0.0 /11

درمطالب گذشته توضیح دادیم که آی پی ها را چطور به عدد باینری تبدیل کنیم.

مثال Supernetting :

تمام کارهایی که میخواهیم انجام دهیم مستلزم این است که ابتدا به ساکن آی پی هایمان را به عدد باینری تبدیل کنیم تا بتوانیم روی آن کار انجام دهیم ، پس تمام آدرس های فوق را به باینری تبدیل میکنیم:

Network	Host
00001010 . 100	00000 . 00000000 . 00000000
00001010 . 101	00000 . 00000000 . 00000000
00001010 . 110	00000 . 00000000 . 00000000
00001010 . 111	00000 . 00000000 . 00000000

10.128.0.0 /11
10.160.0.0 /11
10.192.0.0 /11
10.224.0.0 /11

مثال Supernetting :

همانگونه که در تصویر قبل گویا هست تمام ۴ آدرس را به عدد باینری ۰ و ۱ تبدیل کردیم و چون این مثال دارای ۱۱/ بودند پس قسمت Network این آی پی ها را ۱۱ رقم تفکیک میکنیم و مابقی را به قسمت Host میدهیم.

اگر به تصویر قبل نگاهی دقیق بیندازیم متوجه میشویم که این اعداد در ۹ بیت ابتدایی یکی هستند پس میتوان شبکه را در ۹بیت اول یکی کرد.

و هر ۴ شبکه را به یک شبکه تبدیل کنیم پس باید ۹ بیت ابتدایی را نگه داریم و مابقی بیت ها(۲ بیت) را به سمت Host ببریم و از Network کم کنیم در این حالت یک Net ID جدید به وجود می آید که در تمام ۴ شبکه دیده میشود .

مثال Supernetting :

Network ←	Host
00001010 . 100	00000 . 00000000 . 00000000
00001010 . 101	00000 . 00000000 . 00000000
00001010 . 110	00000 . 00000000 . 00000000
00001010 . 111	00000 . 00000000 . 00000000

بدیدن ترتیب Network ما کوچکتر میشود و تعداد بیت های Host Id ما بیشتر میشود و این دقیقاً عکس عملیات subnetting است.

مثال Supernetting :

در تصویر زیر هم همانطور که ملاحضه میشود قسمت network از IP تشکیل شده که کاملاً در هر ۴ شبکه یکسان است.

پس میتوان گفت دو یا چند سگمنت را ترکیب میکنیم و یک سگمنت جدید به دست میاوریم .

Network	Host
00001010 . 1	0000000 . 00000000 . 00000000
00001010 . 1	0100000 . 00000000 . 00000000
00001010 . 1	1000000 . 00000000 . 00000000
00001010 . 1	1100000 . 00000000 . 00000000

مثال Supernetting :

این مثال ما مثلاً کلاس A هست و همانطور که میدانید کلاس A دارای subnetmask 255.0.0.0 هست ولی در این مثال این مورد صدق نمیکند زیرا ما دقیقاً با بازی کردن روی بیت ها این عدد را به هم میریزیم تا شبکه ها ی خود را کوچک و بزرگ کنیم.

Subnetmask یکی از مهمترین تغییراتی است که پس از supernetting به وجود میآید پس subnetmask جدید برای این شبکه به صورت زیر می باشد

255.128.0.0

یا

/9

مثال Supernetting :

Network	Host
11111111 . 1	0000000 . 00000000 . 00000000

/9 OR 255.128.0.0

همینطور Net Id جدید این شبکه به صورت زیر است.

Network	Host
00001010 . 1	0000000 . 00000000 . 00000000

10.128.0.0

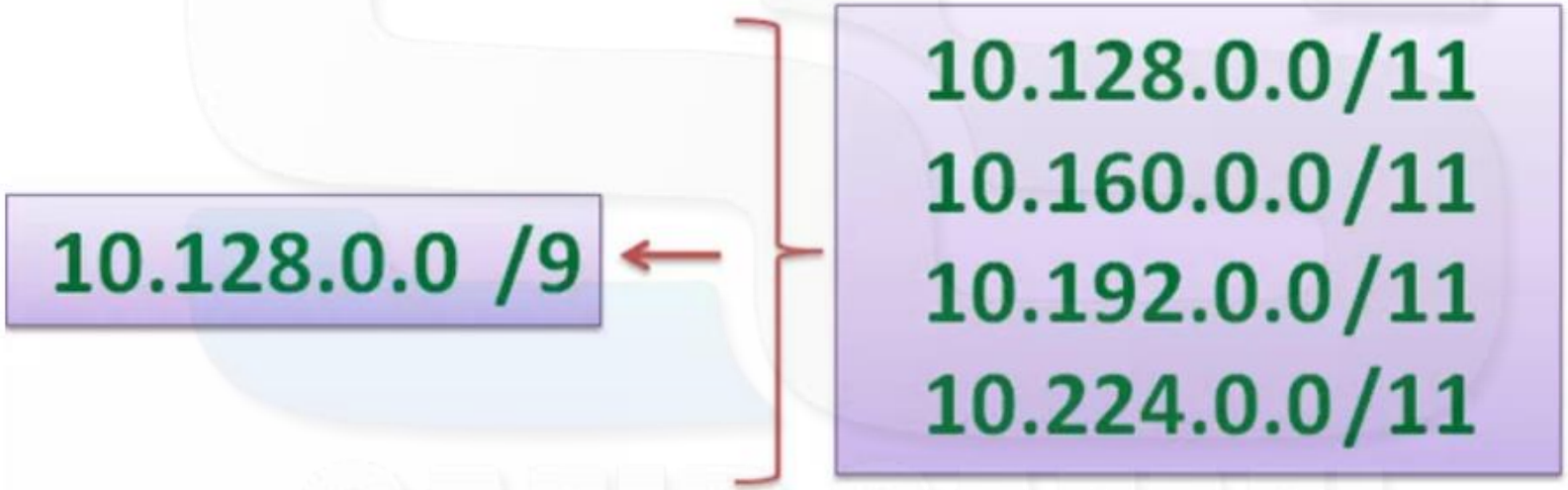
مثال Supernetting :

اگر شما مثلاً به ۵۰۰ تا آی پی نیاز دارید چون کلاس C فقط تا ۲۵۴ تا آی پی را به شما میدهد مجبوراً به سمت کلاس B میروید ولی صحیح نیست که از کلاس B استفاده کرد چون شبکه ما انقدر هم بزرگ نیست که کلاس B را نیاز داشته باشد.

بنابر این اینجا Supernetting به کار می اید ،و وظیفه اش اینست که مثلاً دو تا کلاس C را با هم ادغام کند در این حالت ما به ۵۱۲ آدرس IP میرسیم و این عملیات کلاس بندی IPها رو که همان **Class ful** هست را از بین میبرد.

و به همین دلیل **Class less** نامگذاری شدند یعنی بدون کلاس ، پس ما میتوانیم با ادغام دو کلاس C کوچک به یک کلاس بزرگتری دست پیدا کنیم که ۵۰۰ آی پی به ما میدهد و از کلاس Bخیلی خیلی کوچکتر است.

مثال Supernetting :



تفاوت Classful و Classless:

IP های Classful آی پی هایی هستند که از subnet mask استاندارد استفاده میکنند. یعنی:

Subnet mask class A: 255.0.0.0

Subnet mask class B: 255.255.0.0

Subnet mask class C: 255.255.255.0

و IP های classless آی پی هایی هستند که در اثر subnetting و supernetting ای که بر روی آنها انجام شده از subnet mask استاندارد استفاده نمیکنند. به طور مثال:

255.255.255.128

255.192.0.0

255.255.248.0

نکات:

۱- هر چه مقدار Prefix کمتر شود یعنی مقدار NetID کم شده است پس با افزایش HostID شبکه گسترده تر شده و مقیاس آن بالاتر می رود.

۲- در این حالت اگر Prefix فعلی نسبت به Prefix قبلی کاهش یابد در اصل عمل Supernetting صورت میگیرد.

۳- از سوی دیگر هر چه مقدار Prefix بیشتر شود یعنی مقدار NetID زیاد شده است پس با کاهش HostID شبکه کوچکتر تر شده و مقیاس آن پایینتر می رود، جهت بهبود میزان جدول مسیر یابی یا ...

۴- در این حالت اگر Prefix فعلی نسبت به Prefix قبلی افزایش می یابد در اصل عمل زیر شبکه سازی صورت میگیرد.

۵- هر دو مکانیزم بخشی از CIDR می باشند.

تمرین:

چهار آدرس IP زیر را به صورت Classless تقسیم بندی کرده و در یک رنج CIDR قرار دهید، سپس:

IP Address	Binary Value
192.168.254.4	11000000.10101000.11111110.00000100
192.168.252.16	11000000.10101000.11111100.00010000
192.168.250.128	11000000.10101000.11111010.10000000
192.168.242.30	11000000.10101000.11110010.00011110

الف - مقدار Prefix و NetID آنرا به دست آورید

ب- رنج IP آن را به دست آورید.

ج- آدرس های Network Address و Broadcast Address آن را بنویسید.

با تشکر از همراهی شما

محمد سعید صفایی صادق