۲- آشنایی با مکانیسم NAT و پروتکل DHCP

۲-۱- هدف آزمایش

هدف از انجام این آزمایش آشنایی با آدرس‌دهی شبکه برای استفاده از سرویس‌های اینترنت است. بدین منظور عملکرد و پیکربندی مکانیسم NAT، PAT و پروتکل DHCP بررسی می‌شود.

۲-۲- مطالب مقدماتی

مکانیسم NAT برای تبدیل یک فضای آدرس IP به یک فضای آدرس دیگر انجام می‌شود. یکی از کاربردهای مهم این مکانیسم در تبدیل آدرس خصوصی و عمومی به یکدیگر است که برای دسترسی سیستم‌های با آدرس IP خصوصی به شبکه اینترنت ضروری است.

در NAT آشنایی با مفاهیم آدرس IP خصوصی[۳۵] یا غیر معتبر[۳۶] و آدرس IP عمومی یا معتبر از اهمیت ویژه‌ای برخوردار است. طبق RFC ۱۹۱۸، آدرس‌های IP خصوصی، آدرس‌هایی هستند که به‌وسیله شبکه‌هایی که مستقیما به اینترنت متصل نیستند، استفاده می‌شوند. در RFC۶۸۹۰ لیستی از آدرس‌های IP خصوصی و نحوه برخورد با آن‌ها ارائه شده است. به منظور اینکه سیستم‌ها با آدرس شبکه‌های خصوصی به اینترنت متصل شوند می‌بایست از NAT استفاده شود. آدرس‌های IP خصوصی در اینترنت قابل مسیریابی نیستند و معمولا توسط ISP[۳۷] ها فیلتر می‌شوند. یک آدرس IP عمومی در اینترنت قابل مسیریابی است. سازمان IANA[۳۸] مسئول اختصاص آدرس IP عمومی در اینترنت است. سازمان IANA نیز این مسئولیت را به سازمان‌های محلی واگذار می‌کند، به عنوان مثال ARIN[۳۹] مسئول تخصیص آدرس‌های IP عمومی در آمریکای شمالی است.

مکانیسم NAT، یک آدرس (معمولا آدرس مبدا) در سرآیند بسته‌ها با یک آدرس دیگر (معمولا آدرس عمومی) جایگزین می‌کند. این مکانیسم معمولا در دیواره آتش شبکه پیاده‌سازی می‌شود. در حالت کلی، سه روش برای پیاده‌سازی NAT وجود دارد.

- Static: در این حالت یک نگاشت یک‌به‌یک و ثابت بین آدرس‌های اصلی و مپ شده وجود دارد. در این حالت اگر ده آدرس خصوصی داشته باشید، نیاز به ده آدرس

[۳۵] private
[۳۶] invalid
[۳۷] Internet Service Provider
[۳۸] Internet Address Numbers Authority
[۳۹] Ameriacan Registry for Internet Numbers

عمومی خواهید داشت.

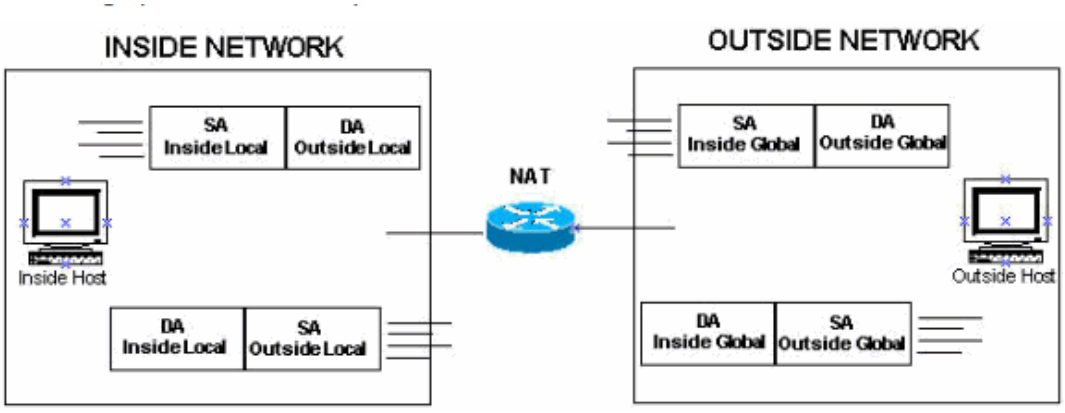
- Dynamic: در این حالت دستگاه‌ها در شبکه داخلی، به‌صورت خودکار از یک pool آدرس عمومی، آدرس دریافت می‌کنند.
- Overload: در این حالت، یک بازه از آدرس‌های خصوصی، به یک آدرس عمومی مپ می‌شوند. در این حالت برای اینکه مسیریاب قادر به تفکیک درخواست‌ها باشد، شماره پورت موجود دربسته‌ها را نیز با یک شماره پورت دیگر عوض کرده و نگاشتی از این تعویض پورت نگهداری می‌کند.

در کتب درسی، هر سه این مکانیسم‌ها به صورت یکپارچه با نام NAT شناخته می‌شود.

در مکانیسم NAT آدرس‌های مختلفی ممکن است به دستگاه‌ها تعلق بگیرد که عبارت‌اند از:

- Inside Local: آدرس IP خصوصی یک دستگاه در شبکه داخلی.
- Inside Global: آدرس IP عمومی یک دستگاه در شبکه داخلی. این آدرس، می‌تواند آدرسی باشد که آدرس خصوصی به آن مپ شده است.
- Outside Local: آدرس IP یک دستگاه در شبکه خارجی که برای شبکه داخلی قابل رویت است. این آدرس الزاما یک آدرس عمومی نیست ولی لزوما باید قابل مسیریابی در شبکه داخلی باشد. در حالتی که از NAT برای آدرس‌های مقصد استفاده شود این آدرس می‌تواند با آدرس Outside Global متفاوت باشد. در غیر این صورت مقدار آن برابر Outside Global است.
- Outside Global: آدرس IP عمومی یک دستگاه در شبکه خارجی.

روند کلی تغییر آدرس‌ها را در شکل (۴-۸) مشاهده می‌کنید.



شکل (۴-۸) روند کلی تغییر آدرس‌ها

در این حالت مسیریاب هم‌زمان آدرس مبدا و آدرس مقصد بسته را ترجمه می‌کند. در این آزمایش صرفا به تغییر آدرس مبدا بسته خواهیم پرداخت.

مراحل تنظیم NAT به صورت پویا عبارت است از:

۱. ایجاد یک لیست ACL که بیانگر این است چه آدرس‌هایی می‌توانند از این مکانیسم استفاده کنند.
۲. ایجاد یک pool آدرس عمومی که می‌تواند به صورت پویا به آدرس‌های شبکه خصوصی اختصاص یابد.
۳. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
٤. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
٥. تنظیم دسترسی ACL برای استفاده از NAT و pool ایجاد شده.

در این حالت به راحتی می‌توان مشاهده کرد که آدرس‌های Inside local به چه آدرس Inside global مپ شده و به چه آدرس outside global متصل شده است.

برای تنظیم مپ کردن به صورت ایستا نیازی به تعریف ACL ندارید. مراحل تنظیم NAT ایستا عبارت است از:

۱. به‌صورت ایستا، برای هر آدرس داخلی یک آدرس خارجی تعریف کنید.
۲. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
۳. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.

در این حالت ازآنجایی‌که نشست‌ها به صورت پویا برقرار نمی‌شوند، اطلاعات نشست شامل اینکه آدرس داخلی به چه آدرس outside global متصل شده است وجود نخواهد داشت.

همان‌گونه که توضیح داده شد، مکانیسم‌های NAT توضیح داده شده نیاز به تعداد زیادی آدرس عمومی دارند تا بتواند تبدیل آدرس را انجام دهد. با توجه به محدودیت آدرس‌های IPv٤، نیاز به مکانیسم دیگری احتیاج می‌شود که آدرس‌های خصوصی را به تعداد محدودی آدرس عمومی نگاشت کند. این مکانیسم که بخش دیگری از مکانیسم NAT است از تبدیل پورت مبدا در سرآیند بسته استفاده می‌کند و با نام PAT نیز شناخته می‌شود. همان‌طور که میدانید، در سرآیند TCP و UDP آدرس پورت مبدا و مقصد نیز وجود دارد. در این مکانیسم علاوه بر تبدیل آدرس در سرآیند IP،

آدرس پورت مبدا نیز در سرآیند TCP و UDP نیز با یک مقدار یکتای دیگر جـایگزین می‌شـود. ایـن مقدار، به یک پورت بر روی دستگاهی که مکانیسم PAT را پیاده‌سازی کرده اشاره می‌کنـد؛ بنـابراین همه دستگاه‌های شبکه داخلی می‌توانند صرفا یک آدرس global local داشته باشند و بـا اسـتفاده از پورت از یکدیگر تشخیص داده شوند.

مراحل تنظیم PAT عبارت است از:

۱. ایجاد یک لیست ACL که بیانگر این است چه آدرس‌هایی می‌توانند از ایـن مکانیسـم استفاده کنند.
۲. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
۳. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبـدیل آدرس را انجام دهد.
٤. تنظیم دسترسی ACL برای استفاده از PAT: به این صورت که یک اینترفیس باید بـه صورت overload مشخص شود.

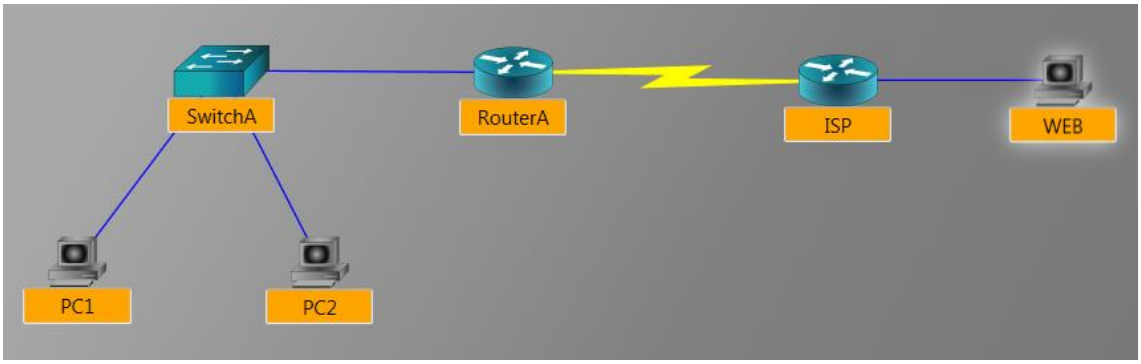
به عنوان یک مثال کلی، هنگامی‌که بسته SYN بـه سـمت دروازه شـبکه فرسـتاده می‌شـود، دستگاه NAT آدرس IP و شماره پورت در سرآیند TCP را با آدرس IP عمومی و یـک شـماره پـورت یکتا عوض می‌کند و بسته را به سمت شبکه عمومی ارسال می‌کند. در جواب اگر آدرس پورت مقصـد بسته در جدول دستگاه NAT وجود داشته باشد، تبدیل آدرس دوباره انجام می‌شود و بسته به شـبکه داخلی ارسال می‌شود.

۳-۲- شرح آزمایش

در ابتدا به بررسی مکانیسم NAT می‌پردازیم و با تنظیمات NAT پویا، NAT ایسـتا و PAT آشنا خواهیم شد. سپس پروتکل DHCP را موردبررسی قرار خواهیم داد

۱-۳-۲- مکانیسم NAT

توپولوژی که در این آزمایش بررسی می‌شود در شکل (۴-۹) نشان داده است. آدرس‌هـای IP واسطها در این آزمایش در جدول (۴-۳) آمده است.



شکل (۹-۴) توپولوژی آزمایش NAT

جدول (۳-۴) آدرس‌های موردنیاز آزمایش NAT

Subnet Mask	IP Address	Interface	Device
۲۵۵.۲۵۵.۲۵۵.۰ ۲۵۵.۲۵۵.۲۵۵.۲۵۲	۱۹۲.۱۶۸.۱۰۰.۱ ۲۰۰.۱۵۲.۲۰۰.۲	FastEthernet ۰/۰ Serial ۰/۰	RouterA
۲۵۵.۲۵۵.۲۵۵.۲۵۲ ۲۵۵.۲۵۵.۲۵۵.۲۵۲	۲۵.۱۶.۵۹.۱ ۲۰۰.۱۵۲.۲۰۰.۱	FastEthernet ۰/۰ Serial ۰/۰	ISP
Default Gateway	Subnet Mask	IP Address	Device
۱۹۲.۱۶۸.۱۰۰.۱	۲۵۵.۲۵۵.۲۵۵.۰	۱۹۲.۱۶۸.۱۰۰.۲	PC۱
۱۹۲.۱۶۸.۱۰۰.۱	۲۵۵.۲۵۵.۲۵۵.۰	۱۹۲.۱۶۸.۱۰۰.۱۲۹	PC۲
۲۵.۱۶.۵۹.۱	۲۵۵.۲۵۵.۲۵۵.۲۵۲	۲۵.۱۶.۵۹.۲	Web

۱-۱-۳-۲- مکانیسم NAT ایستا

۱. واسط‌های دستگاه‌ها مطابق آدرس‌های داده شده در جدول (۴-۳) تنظیم شده است. آیا PC۱ و PC۲ قادر به Ping کردن یکدیگر هستند؟ چرا؟ آیا از PC۱ می‌توانید ISP را Ping کنید؟ چرا؟

۲. بر روی مسیریاب RouterA باید مکانیسم NAT تنظیم شود. برای این کار، ابتدا از محیط تنظیم عمومی وارد تنظیمات اینترفیس fastethernet ۰/۰ شده سپس با استفاده از دستور

ip nat inside

آن را به عنوان اینترفیس داخلی انتخاب کنید. سپس وارد تنظیم اینترفیس serial ۰/۰ شوید و با دستور

ip nat outside

آن را به عنوان اینترفیس خارجی انتخاب کنید.

۳. در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید. با استفاده از این دستور صرفا آدرس IP مبدا در بسته خروجی از شبکه تغییر می‌کند.

ip nat inside source static ۱۹۲,۱۶۸,۱۰۰,۲ ۲۰۰,۱۵۲,۲۰۰,۱

سوال ۱: از PC۱ و PC۲ مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

سوال ۲: با استفاده از دستور

show ip nat translations

جدول NAT در RouterA را مشاهده کنید و آن را شرح دهید.

۲-۱-۳-۲- مکانیسم NAT پویا

۱. بر روی مسیریاب RouterA باید مکانیسم NAT تنظیم شود. برای این کار ابتدا وارد محیط تنظیمات عمومی شوید. سپس با استفاده از دستور

access-list ۱ permit ۱۹۲,۱۶۸,۱۰۰,۰ ۰,۰,۰,۲۵۵

۲. یک لیست دسترسی ایجاد کنید.

سوال ۳: این لیست چه کاری انجام می‌دهد.

۳. در ادامه یک pool آدرس تعریف کنید. دستور زیر را وارد کنید.

ip nat pool pool۱ ۲۰۰,۱۵۲,۱۰۰,۶۵ ۲۰۰.۱۵۲.۱۰۰.۷۰ netmask ۲۵۵.۲۵۵.۲۵۵.۲۴۸

سوال ۴: این دستور چه کاری انجام می‌دهد؟

٤. از محیط تنظیم عمومی وارد تنظیمات اینترفیس ۰/۰ fastethernet شده سپس با استفاده از دستور

ip nat inside

آن را به عنوان اینترفیس داخلی انتخاب کنید. سپس وارد تنظیم اینترفیس ۰/۰ serial شوید و با دستور

ip nat outside

آن را به عنوان اینترفیس خارجی انتخاب کنید.

۵. در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید.

ip nat inside source list ۱ pool pool۱

سوال ۵: از PC۱ , PC۲ مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

٦. با استفاده از دستور

show ip nat translations

سوال ۶: جدول NAT را مشاهده کنید و با آزمایش قبلی مقایسه کنید.

۳-۱-۳-۲- مکانیسم PAT

۷. بر روی مسیریاب RouterA باید مکانیسم NAT تنظیم شود. برای این کار ابتدا وارد محیط تنظیمات عمومی شوید. سپس با استفاده از دستور

access-list ۲ permit ۱۹۲,۱۶۸,۱۰۰,۰ ۰,۰,۰,۲۵۵

یک لیست دسترسی ایجاد کنید.

سوال ۷: این لیست چه کاری انجام می‌دهد؟

۸. از محیط تنظیم عمومی وارد تنظیمات اینترفیس fastethernet ۰/۰ شده سپس با استفاده از دستور

ip nat inside

آن را به عنوان اینترفیس داخلی انتخاب کنید. سپس وارد تنظیم اینترفیس serial ۰/۰ شوید و با دستور

ip nat outside

آن را به عنوان اینترفیس خارجی انتخاب کنید.

۹. در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید.

ip nat inside source list ۲ interface serial ۰/۰ overload

سوال ۸: از PC۱ و PC۲ مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

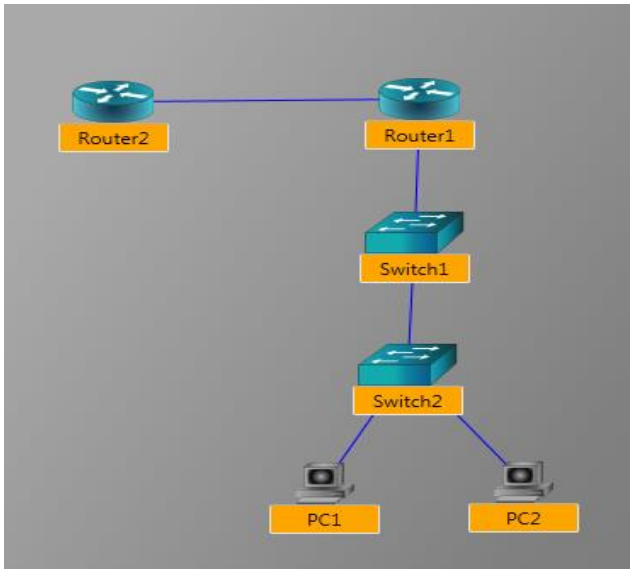
سوال ۹: با استفاده از دستور

show ip nat translations

جدول NAT را مشاهده کنید و با آزمایش قبلی مقایسه کنید.

۲-۳-۲- پروتکل DHCP

توپولوژی که در این آزمایش بررسی می‌شود در شکل (۴-۱۰) نشان داده است.



شکل (۴-۱۰) توپولوژی آزمایش DHCP

آدرس‌های IP واسطهای مسیریاب Router۱ در این آزمایش در جدول (۴-۴) آمده است

جدول (۴-۴) آدرس‌های موردنیاز آزمایش DHCP

Device	Interface	IP Address	Subnet Mask
Router۱	Fastethernet ۰/۱	۱۸۰.۱۰.۱.۲	۲۵۵.۲۵۵.۲۵۵.۰
	Fastethernet ۰/۰	۱۹۲.۱۶۸.۱.۱	۲۵۵.۲۵۵.۲۵۵.۰

۱. واسط‌های مسیریاب Router۱ را مطابق اطلاعات آدرس‌های داده شده تنظیم کنید.

۲. در محیط تنظیم عمومی مسیریاب Router۱ با استفاده از دستور

service dhcp

سرویس DHCP را فعال کنید. سپس با استفاده از دستورهای

ip dhcp excluded-address ۱۸۰,۱۰,۱,۲
ip dhcp excluded-address ۱۹۲,۱۶۸,۱,۱

آدرس‌های مربوط به اینترفیس‌های فعلی مسیریاب را از لیست اختصاص آدرس‌های DHCP خارج کنید.

۳. در محیط تنظیم عمومی، با استفاده از دستور

ip dhcp pool pool۱

وارد تنظیم DHCP شوید. سپس با استفاده از دستور

network ۱۹۲,۱۶۸,۱,۰ ۲۵۵,۲۵۵,۲۵۵,۰
lease ۲

آدرس شبکه و زمان رهاسازی آدرس اختصاص‌یافته را مشخص کنید. در مقابل دستور lease ابتدا روز، سپس ساعت و دقیقه می‌تواند قرار بگیرد؛ بنابراین lease ۲ ٤ به معنی دو روز و چهار ساعت است.

در ادامه با استفاده از دستور

default-router ۱۹۲,۱۶۸,۱,۱

آدرس دروازه پیش‌فرض برای کسانی که از این سرور DHCP استفاده می‌کنند را مشخص کنید.

٤. بر روی سیستم PC۱ دستور

ipconfig /ip dhcp

را وارد کنید. خروجی دستور

ipconfig /all

را مشاهده کنید.

٥. بر روی مسیریاب Router۱ دستور

show ip dhcp binding

را اجرا کنید و خروجی را مشاهده کنید.

٦. بر روی مسیریاب Router۱ دستور

show ip dhcp server statistics

را اجرا کنید و خروجی را مشاهده کنید.

۷. بر روی مسیریاب Router۱ دومین Pool را نیز تنظیم کنید. در محیط تنظیم عمومی، با استفاده از دستور

ip dhcp pool pool۲

وارد تنظیم DHCP شوید. سپس با استفاده از دستور

network ۱۸۰,۱۰,۱,۲ ۲۵۵,۲۵۵,۲۵۵,۰
lease ۲

۸. دومین pool را نیز تنظیم کنید.

۹. در مسیریاب Router۲، وارد محیط تنظیم واسط fastethernet۰/۰ شوید. ابتدا با دستور

no shut

واسط را فعال کنید. سپس با دستور

ip dhcp client lease ۱

تنظیم کنید که مسیریاب، آدرس DHCP را با مقدار lease ۱ درخواست کند. سپس با دستور

ip address dhcp

تنظیم آدرس واسط مسیریاب را در حالت DHCP قرار دهید.

سوال ۱۰: در مسیریاب Router۲ از محیط تنظیمات خارج شوید. با استفاده از دستور

Show dhcp lease

مشخص کنید زمان‌های lease، Renewal و Rebind چقدر هستند و چه ارتباطی با یکدیگر دارند.