تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

آموزش رایگان دوره نتورک‌پلاس (Network+) آشنایی با آدرس‌های IPv4، NAT،SNAT، DNAT (بخش 18)

در شماره‌های گذشته آموزش نتورک‌پلاس با آدرس‌های آی‌پی، آدرس‌های مک و نقش آن‌ها در شناسایی و ارتباط دستگاه‌ها با یکدیگر آشنا شدیم. در این شماره قصد داریم به آدرس‌های آی‌پی نسل چهارم و جزییات مربوط به تبدیل آدرس‌های عمومی به خصوصی و بالعکس نگاهی داشته باشیم.

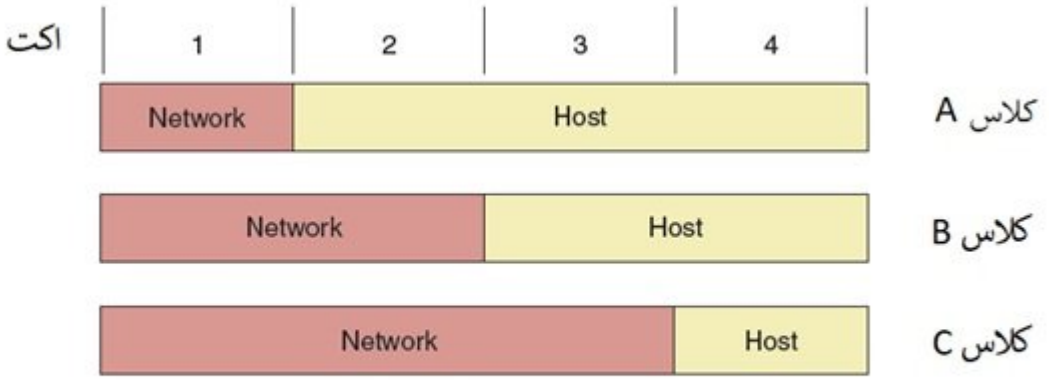
برای مطالعه بخش هفدهم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

قالب آدرس‌های IPv4

بخش اول یک آدرس آی‌پی برای شناسایی یک شبکه و بخش دوم برای شناسایی میزبان استفاده می‌شود. زمانی که تصمیم می‌گیرید از آدرس‌های طبقه‌بندی شده استفاده کنید که در اصل روش سنتی مدیریت محدوده آدرس‌های آی‌پی هستند، خط تقسیم بخش شبکه و بخش میزبان با محدوده اعدادی که اشاره به آدرس‌های آی‌پی دارند ممکن است کمی مشکل است. آدرس‌های IPv4 به پنج کلاس A، B، C، D و E تقسیم می‌شوند. جدول زیر محدوده آدرس‌های آی‌پی عمومی نسل چهارم هر یک از این کلاس‌ها را نشان می‌دهد.

کلاس‌های آدرس آی‌پی			
کلاس	اکت شبکه	تعداد تقریبی شبکه‌های ممکن	تعداد تقریبی آدرس‌های آی‌پی در دسترس در هر شبکه
A	x.y.z to 126.x.y.z.1	126	16 میلیون
B	x.y to 191.255.x.y.128.0	16,000	65,000
C	x to.192.0.0 223.255.255.x	2 میلیارد	254

x، y و z در یک آدرس آی‌پی بیان‌گر اکتی است که برای شناسایی میزبان‌ها روی یک شبکه از آن استفاده می‌شود. شکل زیر نشان می‌دهد که چگونه کلاس‌های A، B و C در بخش شبکه و میزبان تقسیم می‌شوند.



بخش شبکه و بخش میزبان برای هر کلاس آدرس IP

نکته: آزمون **نتورک‌پلاس** از شما انتظار دارد که بتوانید کلاس هر آدرس آی‌پی را تشخیص دهید. به همین دلیل لازم است که جدول بالا را حفظ کنید. شما با نگاه کردن به یک آدرس آی‌پی باید بتوانید بگویید که یک آدرس به چه کلاسی تعلق دارد.

کلاس A، B و C آدرس‌های آی‌پی مجاز در دسترسی هستند که روی بستر اینترنت استفاده شده و به همین دلیل به آن‌ها آدرس‌های آی‌پی عمومی گفته می‌شود. برای حفظ آدرس‌های آی‌پی عمومی به شکلی که هم اکنون از آن‌ها استفاده می‌شود، یک شرکت می‌تواند از آدرس‌های آی‌پی خصوصی روی شبکه خصوصی خودش استفاده کند. شبکه‌ای که قرار نیست به شکل مستقیم به اینترنت متصل شود. آیانا پیشنهاد می‌کند که سازمان‌ها از آدرس‌های آی‌پی زیر در شبکه‌های خصوصی خود استفاده کنند.

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255

- 192.168.0.0 through 192.168.255.255

آدرس‌های آی‌پی کلاس‌های E و D برای استفاده عمومی در دسترس نیستند. آدرس‌های کلاس D از اکت 224 آغاز شده و به اکت 239 ختم می‌شوند و برای انتقال چندبخشی (multicast) که در آن یک میزبان پیامی را برای چند میزبان دیگر ارسال می‌کند استفاده می‌شوند. یک مثال در این زمینه موقعی است که میزبانی یک کنفرانس ویدویی را از طریق اینترنت با چند شرکت دیگر برگزار می‌کند. آدرس‌های کلاس E که از اکت 240 آغاز شده و تا اکت 254 ادامه پیدا می‌کنند برای جست‌وجو اختصاص یافته‌اند. علاوه بر این، آدرس‌های آی‌پی که در جدول زیر مشاهده می‌کنید برای استفاده‌های خاص پروتکل TCP/IP در نظر گرفته شده‌اند و نباید به دستگاهی روی شبکه تخصیص داده شوند.

آدرس‌های آی‌پی	عملکرد
255.255.255.255	از سوی پردازه‌های پس‌زمینه TCP/IP برای ارسال پیام‌ها به شکل همه پخشی (broadcast) استفاده می‌شود. همه‌پخشی به معنای آن است که در یک شبکه یک دستگاه برای همه کامپیوترهای عضو شبکه اطلاعات را ارسال کرده که در اصلاح تخصصی به آن همه‌پخشی می‌گویند.
255.255.255.255	در حال حاضر تخصیص پیدا نکرده است.
127.0.0.1 through 127.255.255.254	برای جست‌وجو یا نشان دادن کامپیوتر شما استفاده شده که در این حالت به آدرس loopback معروف است.
169.254.0.1 through 169.254.255.254	برای ساخت یک آدرس آی‌پی خصوصی خودکار (APIPA) زمانی استفاده می‌شود که یک کامپیوتر برای DHCP پیکربندی شده و برای اتصال به شبکه قادر نیست از آدرس IPv4 که سرور DHCP ارائه می‌کند استفاده کند.

نکته: اگر به خاطر داشته باشید، به شما گفتیم که یک شبکه محلی به گروهی از کامپیوترها و دستگاه‌های مختلف اشاره دارد که می‌توانند بدون نیاز به یک روتر و از طریق یک آدرس به شکل مستقیم با یکدیگر در ارتباط باشند. به لحاظ فنی، به یک شبکه محلی که شامل گره‌هایی است که اطلاعات را به شکل همه‌پخشی ارسال می‌کنند دامنه همه‌پخشی (broadcast domain) می‌گویند. در یک چنین شبکه‌هایی روترها پیام‌های همه‌پخشی را فوروارد نکرده و بنابراین مرز مشخصی برای یک شبکه محلی ایجاد می‌شود.

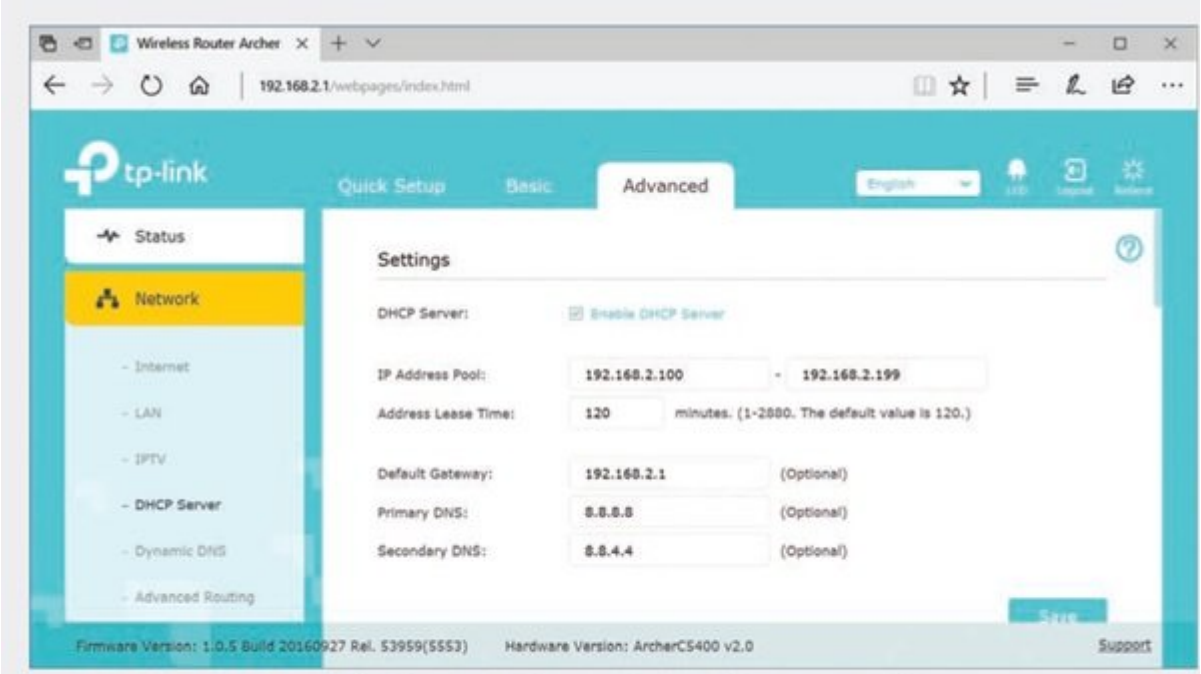
نکته: در حالت کلی در آزمون‌های **نتورک‌پلاس** به APIPA اشاره می‌شود.

پروتکل پیکربندی پویای میزبان (DHCP)

آدرس‌های آی‌پی ایستا به شکل دستی از سوی مدیر یک شبکه تنظیم می‌شوند، در حالی که سرور پروتکل پیکربندی پویای میزبان هر زمان دستگاهی به شبکه متصل شود، مسئولیت تخصیص آدرس‌های آی‌پی پویا را عهده‌دار است. از آن‌جایی که فرآیند تخصیص آدرس‌های آی‌پی پویا به شکل ایستا فرآیند پیچیده و مشکلی است و مدیریت آن‌ها نیز به سختی انجام می‌شود، بیشتر مدیران شبکه تصمیم می‌گیرند از تکنیک تخصیص پویای خودکار استفاده کنند.

پیکربندی یک سرور پروتکل پیکربندی پویای میزبان

هر نرم‌افزار سرور DHCP به شکل متفاوتی پیکربندی می‌شود. به‌طور کلی، شما طیفی از آدرس‌های آی‌پی که به نام دامنه پروتکل پیکربندی پویای میزبان (DHCP scope) شهرت دارند را تعریف می‌کنید تا دستگاه‌های کلاینت هر زمان درخواست آدرس آی‌پی را دادند، این آدرس‌ها به آن‌ها تخصیص داده شود. به‌طور مثال، در شکل زیر تصویری از میان‌افزار یک روتر خانگی را همراه با سرور DHCP آن مشاهده می‌کنید. با استفاده از صفحه مدیریت و پیکربندی DHCP شما می‌توانید آدرس‌هایی آی‌پی که در بازه 192.168.2.100 تا 192.68.2.199 قرار داشته و در دامنه DHCP قرار دارند را تنظیم کنید.



تنظیم محدوده ای از آدرس های آی پی روی یک سرور پروتکل پیکربندی پویای میزبان

Source: TP-Link Technologies Co., Ltd.

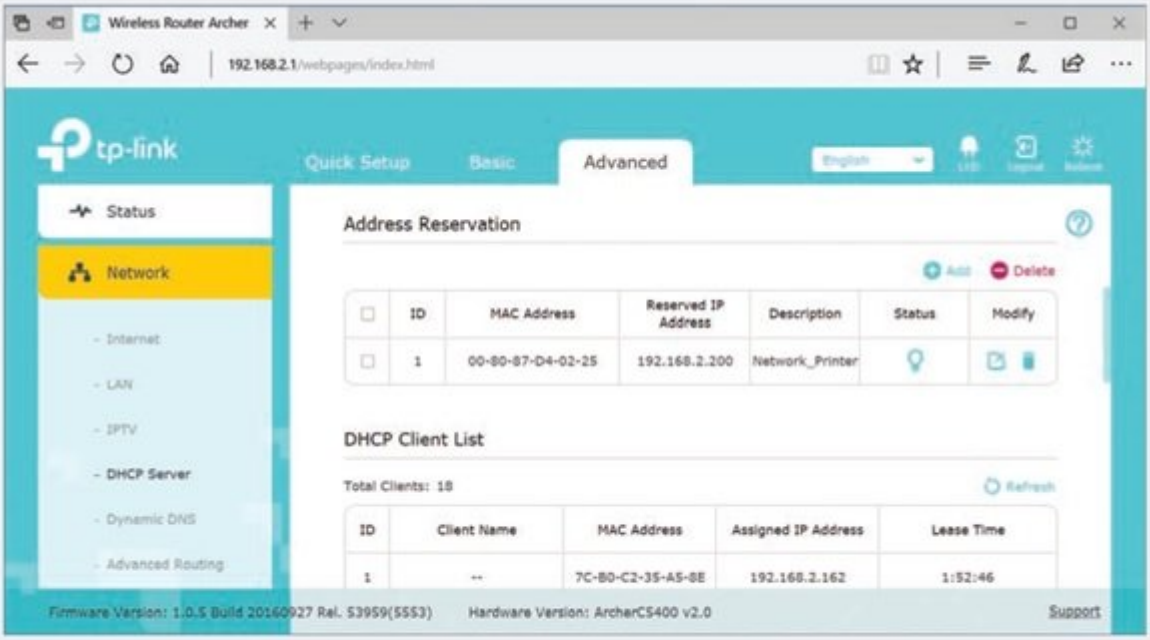
این محدوده شامل اطلاعات اضافی دیگری نیز هستند که به نام گزینه‌های دامنه شهرت دارند و به شرح زیر هستند:

یک محدودیت زمانی که به زمان اجاره نام دارد.

آدرس آی‌پی گیت‌وی پیش‌فرض

آدرس‌های سرور اولیه و ثانویه سامانه نام دامنه

در شبکه‌هایی که گره‌ها اغلب مجبور هستند به‌طور متناوب آدرس آی‌پی کلاینت خاصی را به دست آورند، بهتر است از DHCP استفاده کنید تا در هر بار اتصال یک کلاینت به شبکه آدرس یکتایی در اختیار داشته باشد. سرور DHCP با استفاده از مک‌آدرس می‌تواند یک کلاینت را شناسایی کند، آدرس آی‌پی که DHCP برای یک کلاینت و بر مبنای مک‌آدرس رزرو می‌کند به نام‌های مختلفی همچون MAC، رزرو، آی‌پی رزرو شده یا پروتکل پیکربندی پویای میزبان رزرو شده صدا زده می‌شود. به‌طور مثال، یک چاپگر شبکه در زمان اتصال به شبکه باید دارای آدرس یکسانی باشد تا کامپیوترهای روی شبکه همواره بتوانند آن‌را پیدا کنند. شکل زیر رابط مدیریتی برای روتر TP-Lick SOHO و یک چاپگر تحت شبکه که دارای آدرس رزرو شده 192.168.2.200 است را نشان می‌دهد.

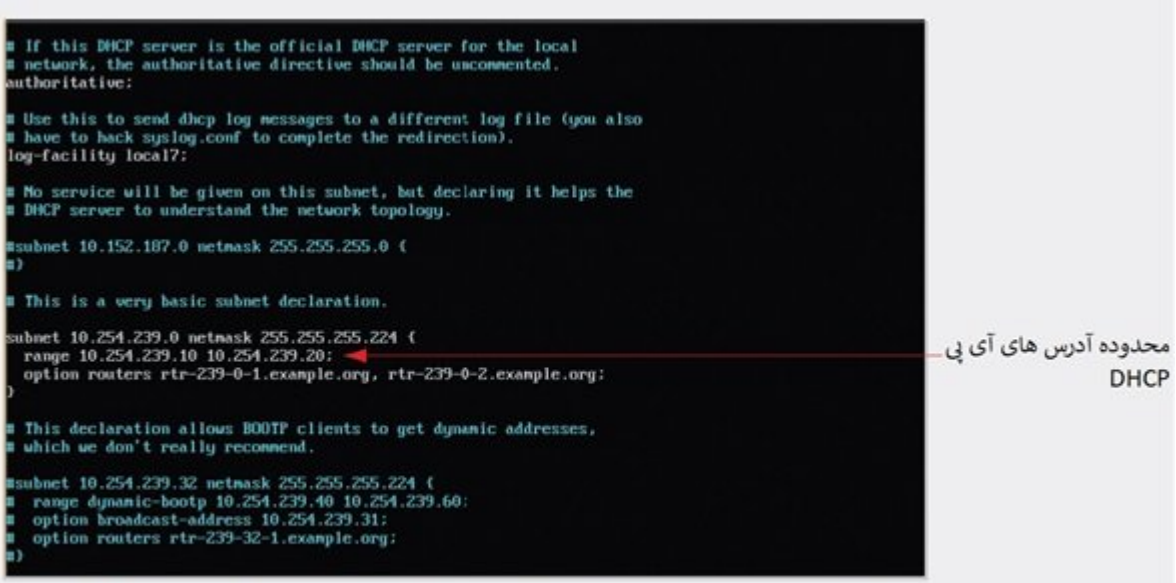


یک آدرس آی پی رزرو شده برای یک یا چند کلاینت شبکه، همچون یک چاپگر شبکه

Source: TP-Link Technologies Co., Ltd.

نکته: دقت کنید یک آدرس آی‌پی رزرو شده یکسان با یک آدرس آی‌پی ایستا/ثابت نیست. یک آدرس آی‌پی رزرو شده زمانی که یک کلاینت درخواست یک آدرس آی‌پی می‌کند از سوی DHCP به کلاینت واگذار می‌شود، در حالی که یک آدرس آی‌پی ثابت روی خود یک کلاینت پیکربندی شده و در نتیجه یک کلاینت در وهله اول هیچ‌گاه از DHCP درخواست آدرس آی‌پی نخواهد کرد. اگر یک یا چند کلاینت روی شبکه دارید که آدرس‌های آی‌پی ثابتی دارند، شما باید روی سرور DHCP یک محدودیت آی‌پی یا به عبارت دقیق‌تر یک حالت استثنا مشخص کنید تا سرور نتواند این آدرس‌ها را در زمان تخصیص آدرس‌های آی‌پی به سایر دستگاه‌های شبکه تخصیص دهد.

در سیستم‌های لینوکسی، شما با ویرایش یک فایل متنی، نرم‌افزار DHCP را پیکربندی می‌کنید. به‌طور مثال، یک سرور DHCP در یک توزیع لینوکسی در فایل dhcpd.conf و در پوشه / etc / dhcp ذخیره می‌شود. شکل زیر این فایل متنی را درون ویرایشگر متنی vim در محیط لینوکس نشان می‌دهد.




```
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.

subnet 10.254.239.0 netmask 255.255.255.224 {
  range 10.254.239.10 10.254.239.20;
  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}
```

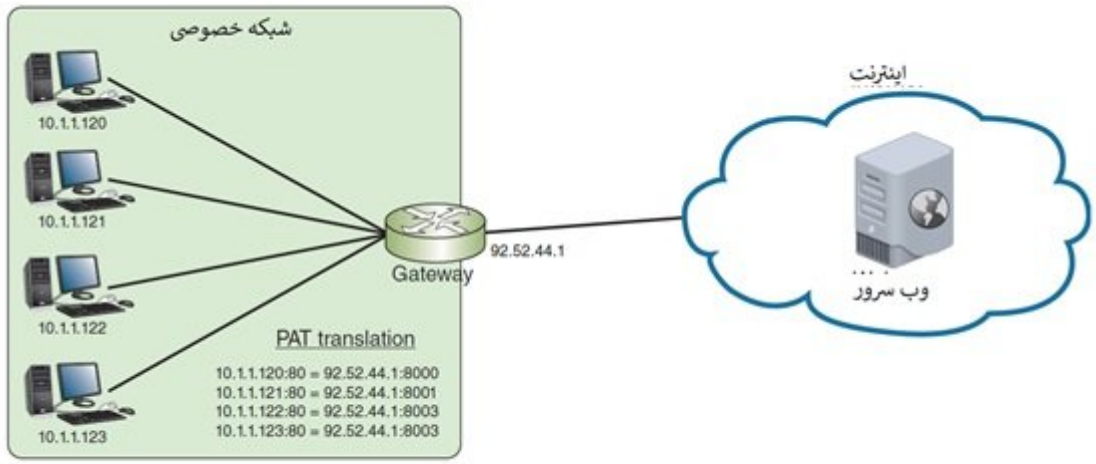
با ویرایش یک فایل متنی در لینوکس شما قادر به تنظیم محدوده آدرس های آی پی برای سرور DHCP هستید

کاراکتر # در ابتدای برخی از خطوط برای بیان توضیحات استفاده شده و اجرا نمی‌شود. در این تصویر محدوده

آدرس‌های آی‌پی که به کلاینت‌ها تخصیص داده شده در بازه 10.254.239.10 تا 10.254.239.20 قرار دارند که در مجموع 11 آدرس آی‌پی را شامل می‌شود.. DHCP برای سرورهای IPv4 در پورت 67 آماده است درخواست‌ها را دریافت کرده و کلاینت‌های DHCPv4 نیز روی پورت 68 آماده دریافت پاسخ‌ها هستند. هنگام استفاده از DHCP روی IPv6 که DHCPv6 نامیده می‌شود، سرورهای DHCP از پورت 546 برای دریافت درخواست‌ها و کلاینت‌ها از پورت 547 برای دریافت واکنش‌ها استفاده می‌کنند.

ترجمه/برگردان آدرس

برگردان نشانی شبکه (NAT) سرنام Network Address Translation تکنیکی است که برای ارسال و دریافت ترافیک شبکه از رویکرد مسیریابی که بر پایه بازنویسی آی‌پی یا شماره درگاه‌ها یا شماره درگاه‌های TCP/UDP که بسته‌های آی‌پی از آن‌ها عبور می‌کند دلالت دارد. به عبارت دیگر، برگردان نشانی شبکه تکنیکی است که به منظور حفظ تعداد آدرس‌های آی‌پی که یک شبکه به آن‌ها نیاز دارد استفاده می‌شود. گیت‌وی که میان یک شبکه خصوصی و سایر شبکه‌ها قرار می‌گیرد، زمانی که کامپیوترها روی یک شبکه خصوصی قصد دارند به شبکه‌ای دیگر یا اینترنت متصل شوند، آدرس‌های آی‌پی خصوصی که کامپیوترهای عضو یک شبکه خصوصی از آن‌ها استفاده می‌کنند را به آدرس‌های عمومی آی‌پی تبدیل می‌کند. به این فرآیند تبدیل برگردان آدرس می‌گویند. تکنیک NAT ضمن آن‌که یک آدرس آی‌پی عمومی در اختیار یک شبکه خصوصی قرار می‌دهد، در ارتباط با مباحث امنیتی نیز تاثیر مثبتی دارد. گیت‌وی می‌تواند یک شبکه خصوصی را پشت یک آدرس پنهان کند. گیت‌وی چگونه اطلاع پیدا می‌کند چه میزبان محلی باید پاسخ ارسالی از میزبانی که روی اینترنت قرار دارد را دریافت کند؟ این مشکل را تکنیکی موسوم به برگرداندن نشانی درگاه (PAT) سرنام Port Address Translation حل می‌کند که یک درگاه TCP جداگانه را به هر نشستی که میان یک میزبان محلی و یک میزبان روی اینترنت قرار دارد اختصاص می‌دهد. شکل زیر نشان می‌دهد که چگونه زمانی که یک میزبان روی اینترنت به یک میزبان محلی پاسخ می‌دهد. گیت‌وی از PAT برای تعیین این‌که چه میزبان محلی باید پاسخ را دریافت کند استفاده می‌کند.



برگردان نشانی درگاه (PAT) Port Address Translation

دو نوع برگردان نشانی شبکه وجود دارد که باید از وجود آن‌ها مطلع باشید. این دو نوع به شرح زیر هستند:

برگردان نشانی شبکه ایستا/ثابت یا بازنشانی آدرس شبکه مبدا (SNAT) سرنام Static Network Address Translation or Source Network

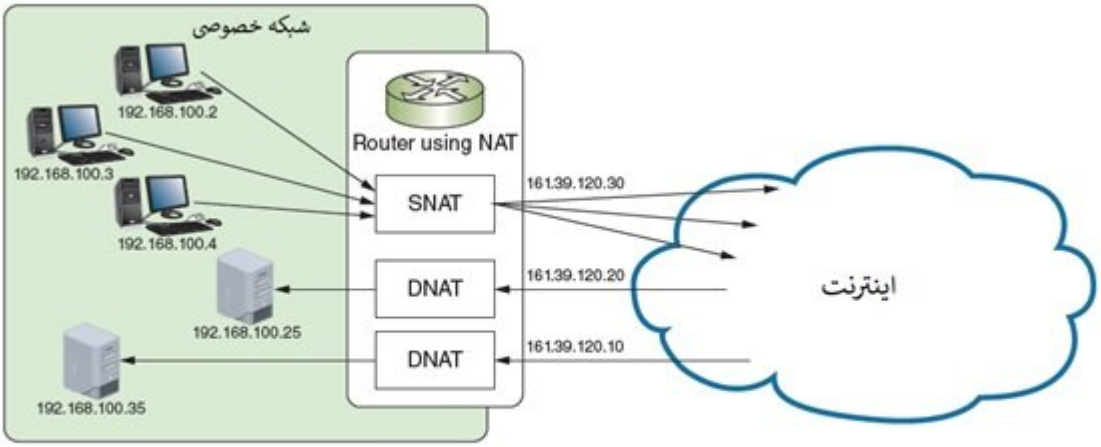
در این مدل گیت‌وی هر زمان که یک میزبان درخواست دسترسی به اینترنت را ارائه می‌کند یک آدرس آی‌پی عمومی به میزبان تخصیص می‌دهد. شبکه‌های خانگی کوچک از یک آدرس آی‌پی عمومی منفرد که ISP از طریق SNAT به آن‌ها تخصیص می‌دهد استفاده می‌کنند.

برگردان آدرس شبکه مقصد (DNAT) سرنام Destination Network Address Translation

میزبان خارج از محدوده آدرس یک شبکه، کامپیوتری است که درون شبکه‌ای قرار دارد و یک آدرس آی‌پی عمومی از

پیش تعریف شده به آن تخصیص داده شده است. هنگامی که یک پیام فرستاده شده برای یک آدرس آی‌پی عمومی به روتری می‌رسد که DNAT را مدیریت می‌کند، آدرس آی‌پی مقصد به آدرس آی‌پی خصوصی میزبانی که درون شبکه قرار دارد تغییر پیدا می‌کند. در این‌جا، روتر باید جدولی که در آن آدرس‌های آی‌پی عمومی نگاشت شده به میزبان‌های مختلف درون شبکه در آن قرار دارند را نگه‌داری و مدیریت کند.

شکل زیر تفاوت عملکردی دو مدل SNAT و DNAT را نشان می‌دهد.



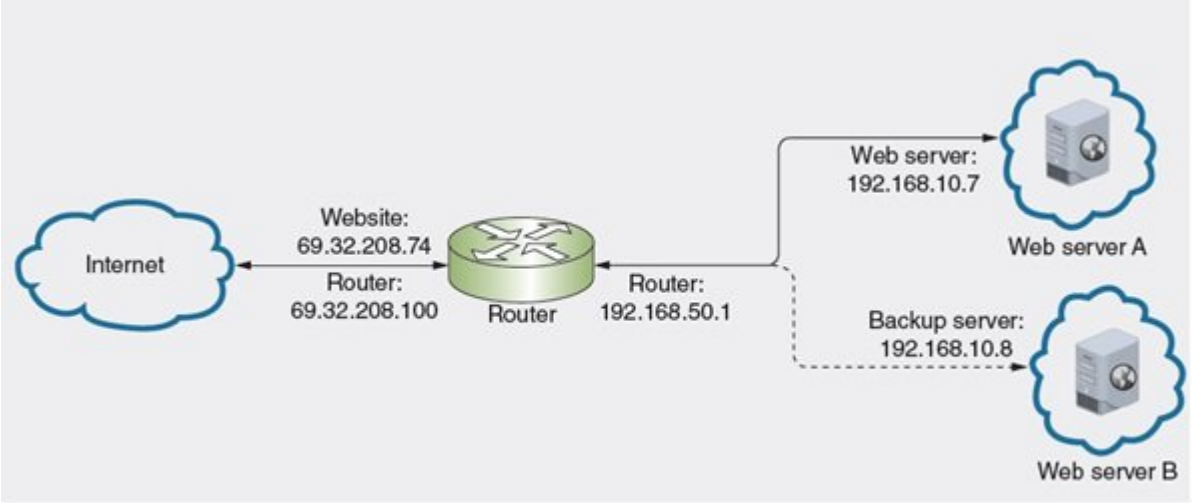
SNAT برای پیام های خروجی و DNAT برای پیام های وارد شونده

SNAT آدرس‌های آی‌پی بسته‌هایی که قرار است ارسال شوند (پیام‌های خروجی) را در سرآیند آی‌پی تغییر داده و برای کم کردن تعداد آدرس‌های آی‌پی عمومی که یک شبکه به آن‌ها نیاز دارد استفاده می‌شود.

DNAT آدرس آی‌پی پیام‌های واردشونده را تغییر می‌دهد. DNAT اغلب در سازمان‌های بزرگی که سرویس‌هایی را روی بستر اینترنت ارائه می‌کنند استفاده می‌شود. سرورهای مختلف می‌توانند از آدرس‌های آی‌پی خصوص برای حفظ امنیت استفاده کرده و همچنین به مدیران شبکه اختیار عمل بیشتری بدهند تا سرورها را به شکل بهتری مدیریت کنند. به‌طور مثال، مدیران شبکه می‌توانند با اعمال یک تغییر ساده در تنظیمات DNAT روتر، به یک وب‌سرور برای پشتیبان‌گیری از کامپیوتر در مدت زمان تعمیر و نگه‌داری سرور اصلی سوییچ کنند و به این شکل یک آدرس آی‌پی عمومی برای پشتیبان‌گیری از کامپیوتر به دست آورند.

پیکربندی برگردان آدرس با استفاده از NAT

برای گیت‌وی‌های پیش‌فرض ساده همچون روترهای خانگی، پیکربندی برگردان آدرس به معنای آن است که مطمئن شوید NAT روشن باشد. این تمام آن کاری است که باید انجام دهید. برای گیت‌وی‌های پیشرفته همچون روترهای سیسکو با درجه صنعتی یا سرور لینوکس، شما نرم‌افزار NAT را از طریق ویرایش جدول برگردان NAT که روی دستگاه ذخیره شده است پیکربندی می‌کنید. به‌طور مثال، فرض کنید شبکه شما از وب‌سروری پشتیبانی می‌کند که می‌توان از طریق اینترنت به آن دسترسی داشت. در بستر اینترنت سایت‌های دارای یک آدرس آی‌پی عمومی شبیه به 69.32.208.74 هستند و با این آدرس شناخته می‌شوند. شکل زیر یک فایل متنی ساده در محیط لینوکس را نشان می‌دهد که برای تنظیم/ویرایش جدول برگردان DNAT به آن نیاز دارید. فایلی که قرار است DNAT را به شکلی پیکربندی کند تا بر مبنای یک آدرس آی‌پی خصوصی شبیه به 192.168.10.7 ترافیک را به سمت وب‌سرور هدایت کند. دقت کنید هر خط که با علامت تعجب آغاز می‌شود یک توضیح متنی است.




```
interface serial 0/0
  ip address 69.32.208.100 255.255.255.0
  ip nat outside

!--- Defines the serial 0/0 interface as the router's NAT outside interface
!--- with an IP address of 69.32.208.100

interface ethernet 1/1
  ip address 192.168.50.1 255.255.255.0
  ip nat inside

!--- Defines the Ethernet 1/1 interface as the router's NAT inside interface
!--- with an IP address of 192.168.50.1


ip nat inside source static 192.168.10.7 69.32.208.74

!--- States that source information about the inside host will be translated
!--- so the host's private IP address (192.168.10.7) will appear as the
!--- public IP address (69.32.208.74). Both ingoing and outgoing traffic
!--- exchanged with the public IP address will be routed to the host at the
!--- private IP address.
```

اولین گروه از خطوط تصویر بالا رابط خارجی روتر را تعریف می‌کنند که برای اتصال به یک شبکه خارجی از آن استفاده شده و رابط سریالی نام دارد. گروه دوم رابط اترنت داخلی روتر را تعریف می‌کنند. خط آخر اعلام می‌دارد زمانی‌که کلاینت‌ها از اینترنت درخواستی را برای آدرس آی‌پی 69.32.208.7 ارسال می‌کنند، درخواست باید به آدرس آی‌پی 192.168.10.7 ترجمه شود.

برای آن‌که بهتر درک کنید که آدرس‌های آی‌پی در یک جدول ترجمه شده/برگردان از کجا می‌آیند، به پرسش‌های زیر که در ارتباط با سه شکل قبلی است پاسخ دهید:

آدرس آی‌پی رابط خارجی روتر چیست؟

آدرس آی‌پی رابط داخلی روتر چیست؟

آدرس آی‌پی عمومی یک وب‌سایت چیست؟

آدرس آی‌پی خصوصی یک وب‌سرور فعال چیست؟

در شماره آینده آموزش **نتورک‌پلاس** به سراغ آدرس‌های نسخه ششم اینترنت IPv6 خواهیم رفت.

لطفا نظرات خود در مورد این آموزش و ادامه آن را در بخش دیدگاه در انتهای صفحه اعلام نمایید و نظارت سایر کاربران را نیز ببینید.

تمام قسمت‌های دوره نتورک پلاس (Network+)

معرفی آموزشگاه‌های معتبر دوره نتورک پلاس در سراسر کشور

استان تهران (تهران): آموزشگاه عصر شبکه
برگزار کننده دوره‌ها بصورت حضوری و مجازی هم‌زمان
تلفن: 02188735845 کانال: @Asrehshabakeh

استان گیلان (رشت): آموزشگاه هیوا شبکه
تلفن: 01333241269 کانال: @HivaShabake

تاریخ انتشار:
24 بهمن 1397

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/14622/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D8%A2%D8%AF%D8%B1%D8%B3%E2%80%8C%D9%87%D8%A7%DB%8C-ipv4%D8%8C-nat%D8%8Csnat%D8%8C