

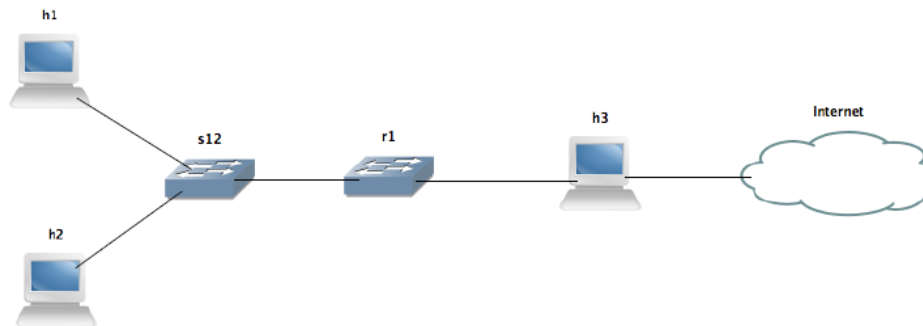
آزمایشگاه شبکه

آزمایش ۴: اتصال محیط مجازی به دنیای واقعی با استفاده از NAT

هدف این آزمایش، برقراری ارتباط شبکه مجازی ایزوله‌ای است که در آزمایش ۳ راه‌اندازی کردیم با شبکه اینترنت واقعی.

الف) مقدمه

با شبکه‌ای که در شکل ۱ نشان داده شده است، کار می‌کنیم. ماشین‌های h1 و h2 نقش دو workstation را بازی می‌کنند، r1 روتر ما خواهد بود و h3 نیز روتر مرزی است که قرار است اتصال ما را به دنیای خارج برقرار نماید.



شکل ۱- پیکربندی شبکه دارای ارتباط با دنیای واقعی

سوال ۱- فرض کنید تنها یک ارتباط واقعی با دنیای بیرون داریم (یعنی: تنها یک آدرس IP معتبر در اختیار داریم). می‌خواهیم برای دو کلاینت h1 و h2 دسترسی اینترنت فراهم کنیم. از چه راهکاری برای حل این مسأله باید بهره‌برداری کرد؟ توضیح دهید که این راهکار چگونه مشکل را برطرف خواهد نمود.

- دو گام اساسی برای اتصال محیط مجازی به محیط واقعی اینترنت وجود دارد:

۱) نیازمند یک آدرس IP واقعی روی اینترفیس h3-eth1 از ماشین h3 هستیم.

۲) باید ترافیک وارده از سوی h1 و h2 را جعل هویت یا اصطلاحاً masquerade نماییم.

ب) قرض گرفتن اتصال مبتنی بر آدرس IP واقعی

همانطور که قبلاً گفتیم، برای اتصال به اینترنت، نیازمند یک آدرس IP معتبر هستیم. در این بخش، فرض می‌کنیم کامپیوتری که در حال حاضر روی آن کار می‌کنید (یعنی: ماشین میزبان VM)، دارای اتصال به اینترنت می‌باشد. برای اینکه بتوانیم اتصال IP کامپیوتر خود را برای h3 قرض بگیریم، دو گام زیر باید طی شوند:

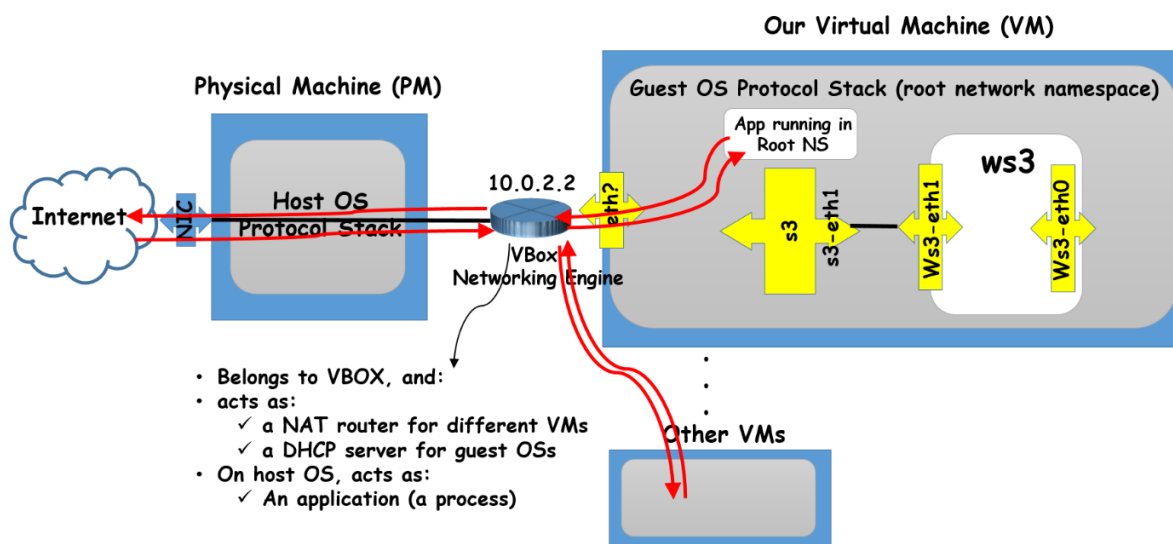
۱) ایجاد یک پل (bridge) مابین ارتباطی که با ماشین میزبان داریم و اینترفیس eth1 از h3.

۲) یافتن و تنظیم یک آدرس IP مناسب برای h3-eth1.

ب-۱) ایجاد پل بین اینترفیس مجازی eth1 و اتصال به بیرون

شکل ۲ به صورت شماتیک، وضعیت ارتباط مابین دو دنیای واقعی و مجازی را قبل از فرآیند پل‌سازی (bridging) نشان می‌دهد.

Vbox NAT Mode



شکل ۲- اتصال بین دنیای مجازی و اینترنت

- به منظور پل‌سازی، ابتدا باید تعیین کنیم که VM ما از کدام اینترفیس برای دسترسی به اینترنت استفاده می‌کند.
- برنامه WireShark را روی VM اجرا کنید. روی تک‌تک اینترفیس‌ها capture کنید و با پینگ کردن google.com، تشخیص دهید که کدام اینترفیس برای دسترسی به اینترنت استفاده می‌شود. از این پس، این اینترفیس را با eth? نشان می‌دهیم.

سوال ۲- آدرس IP مورد استفاده برای دسترسی به اینترنت چیست؟

- حال که می‌دانیم کدام اینترفیس توسط VM استفاده می‌شود، گام بعدی، ایجاد یک پل بین eth? و h3-eth1 است.
- در Mininet، ما با استفاده از برنامه OVS (OpenVSwitch) می‌توانیم پل تولید کنیم.
- اسکریپت lab4.py را اجرا نمایید. این اسکریپت همان توپولوژی شکل ۱ را ایجاد می‌کند (همراه با بیشتر پیکربندی‌های لازم و ضمناً یک OVS اضافی به نام s3 هم برای انجام عملیات پل تولید می‌نماید).
- از خط دستور Mininet، با استفاده از دستور ovs-vsctl و add-port، اینترفیس eth? را به پل s3 اضافه کنید. این کار باعث می‌شود تا eth? به جای اتصال سابقش به پشته IP سیستم (IP stack)، به پل متصل شود.

- با اجرای دستور `ovs-vsctl show` در فضای نام ریشه، می‌توان چک کرد که آیا `eth?` به عنوان یک پورت به `s3` اضافه شده است یا خیر.
- `eth?` دیگر از جنس اینترفیس یک `host` نیست؛ بلکه عملاً پورتی از سویچ `s3` است و ما به طور مستقیم از طریق `eth?` به اینترنت متصل نمی‌شویم. ضمناً، ما به پورت یک سویچ `IP` نمی‌دهیم. بنابراین، با استفاده از دستور `ip addr flush dev eth?` آدرس `IP` این اینترفیس (پورت) را حذف کنید.
- به پنجره ترمینال `h3` رفته و دستور مقابل را اجرا نمایید: `dhclient h3-eth1`. این دستور یک آدرس `IP` قابل استفاده برای اینترفیس `eth1` از `h3` ایجاد می‌کند و اجازه می‌دهد که از طریق پل که ایجاد کردیم، به اینترنت دسترسی داشته باشد.
- پیکربندی ایجاد شده را با پینگ کردن گوگل از داخل `h3` تست نمایید.

ب-۲) پیکربندی NAT

- در این بخش، قصد داریم ارتباط `h1` و `h2` با اینترنت را فراهم نماییم.
- ابتدا بررسی کنید که وقتی از `h1` (بر اساس همان آدرس‌های `IP` اولیه خودش) به سوی گوگل پینگ می‌کنید، چه اتفاقی می‌افتد؟ برای این منظور، با استفاده از `Wireshark` روی اینترفیس `eth0` از `h1` و همچنین، روی اینترفیس `eth1` از `h3` گوش دهید و از `h1` نام دامنه گوگل را (یک مرتبه) پینگ نمایید.
- سوال ۳-** با تحلیل بسته‌های صادره از سوی `h1` توضیح دهید که چرا نتوانستید با سرور گوگل ارتباط برقرار نمایید.
- حال، از `h1` آدرس `IP` گوگل را (یک مرتبه) پینگ نمایید.
- سوال ۴-** در `h3-eth1` چه مشاهده می‌شود؟ علت عدم موفقیت چیست؟
- سوال ۵-** دستور `iptables -t nat` مناسب برای ایجاد یک پیکربندی NAT مناسب در `h3` را بیان کنید.
- پس از اجرای دستور مورد نظر در سوال ۵، مجدداً از `h1` ارتباط اینترنتی خود را با پینگ کردن `Google` (بر اساس نام دامنه) آزمایش کنید. با مشاهده پیام‌های `DNS` و `ICMP`، مطمئن شوید که به طور موفقیت‌آمیزی توانسته‌اید روتر `h3` را به عنوان یک NAT router پیکربندی نمایید.
- ** سوال ۶-** هنگام پینگ کردن از طرف `h1`، پیکربندی NAT در `h3` بر چه اساسی پاسخ‌های `ICMP` دریافتی را برای `h1` می‌فرستد؟ (راهنمایی: فکر می‌کنید چه فیلدی در بسته‌های درخواست/پاسخ `ICMP` برای شناسایی سوره حقیقی بسته‌ها مورد استفاده قرار می‌گیرد؟)