

بسم الله الرحمن الرحيم



دانشکده مهندسی کامپیوتر  
آزمایشگاه شبکه‌های کامپیوتری  
استاد : خانم دکتر زهرا رشیدی  
گزارش کار آزمایش چهارم

سید محمد مهدی رضوی - محمدرضا بابایی

اردیبهشت ۱۴۰۲

## فهرست مطالب

۳	۱ سوال اول
۴	۲ سوال دوم
۵	۳ سوال سوم
۶	۴ سوال چهارم
۷	۵ سوال پنجم
۸	۶ سوال ششم

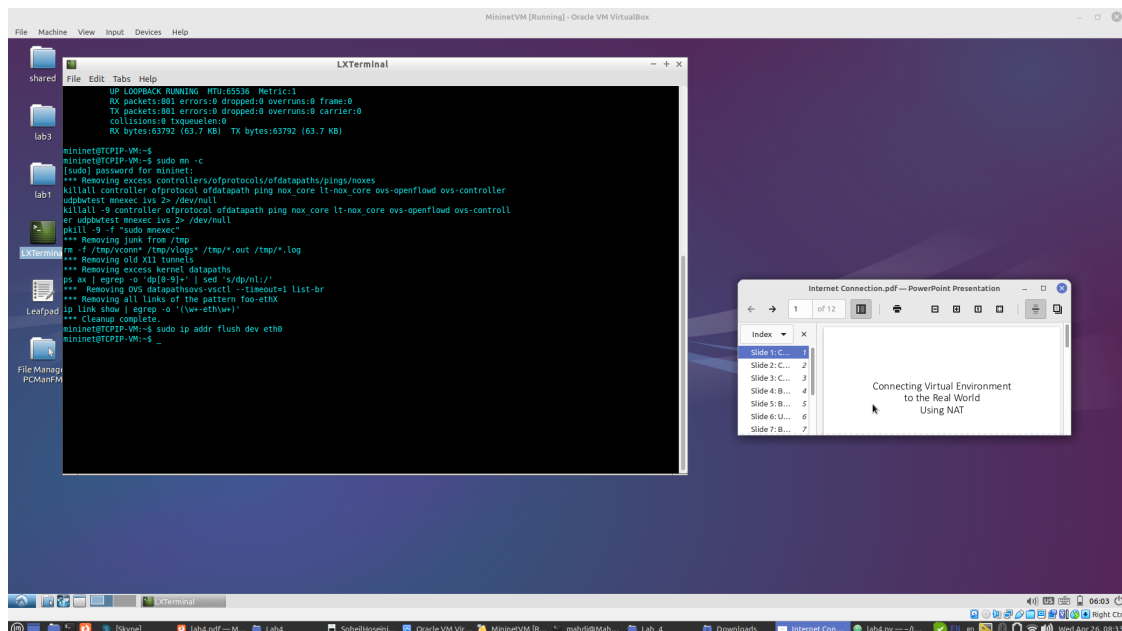
## فهرست تصاویر

۳	۱ سوال اول
۴	۲ سوال دوم
۵	۳ ping google.com

## ۱ سوال اول

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 مساله باید بهره برداری کرد ؟ توضیح دهید که این راهکار چگونه مشکل را برطرف خواهد نمود.

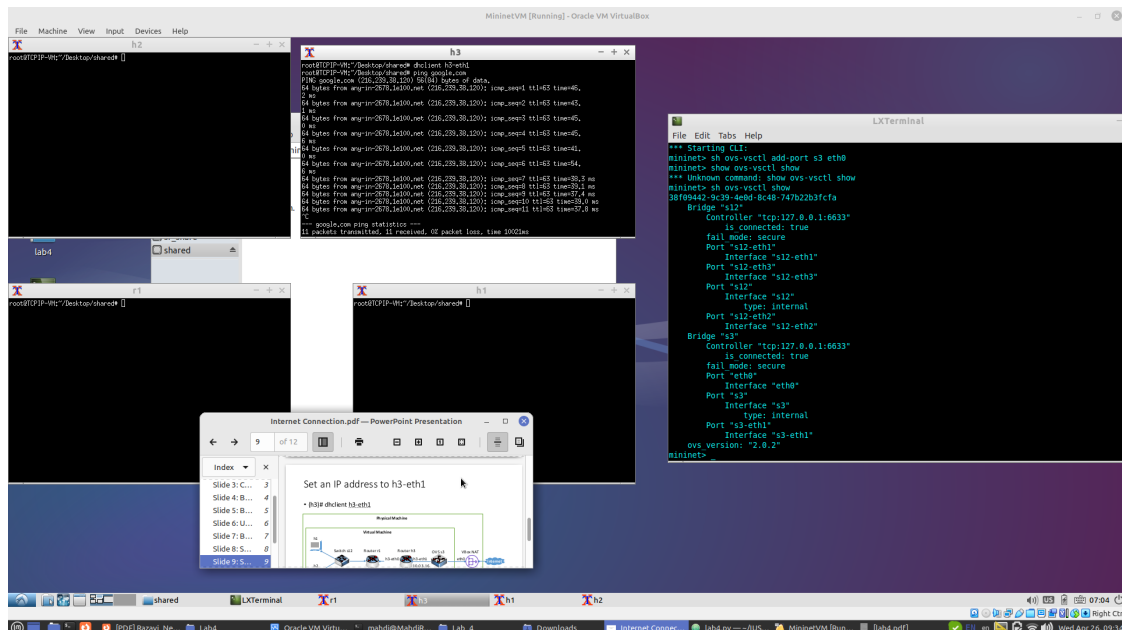
با فرض برقرار بودن اتصال VM به اینترنت ، از VM یک آدرس VM حقیقی روی پورت VM نیاز داریم و سپس ترافیک وارد شده از VM و VM را می‌کنیم چرا که اگر آدرس مبدا packet های دریافتی به صورت local باشند ، در h3 این بسته‌ها drop میشوند و اتصال به اینترنت برای h1 و h2 برقرار نخواهد شد.  
با تغییر IP می‌توان این دو host را به اینترنت متصل نمود.



شکل ۱: سوال اول

آدرس IP مورد استفاده برای دسترسی به اینترنت چیست ؟

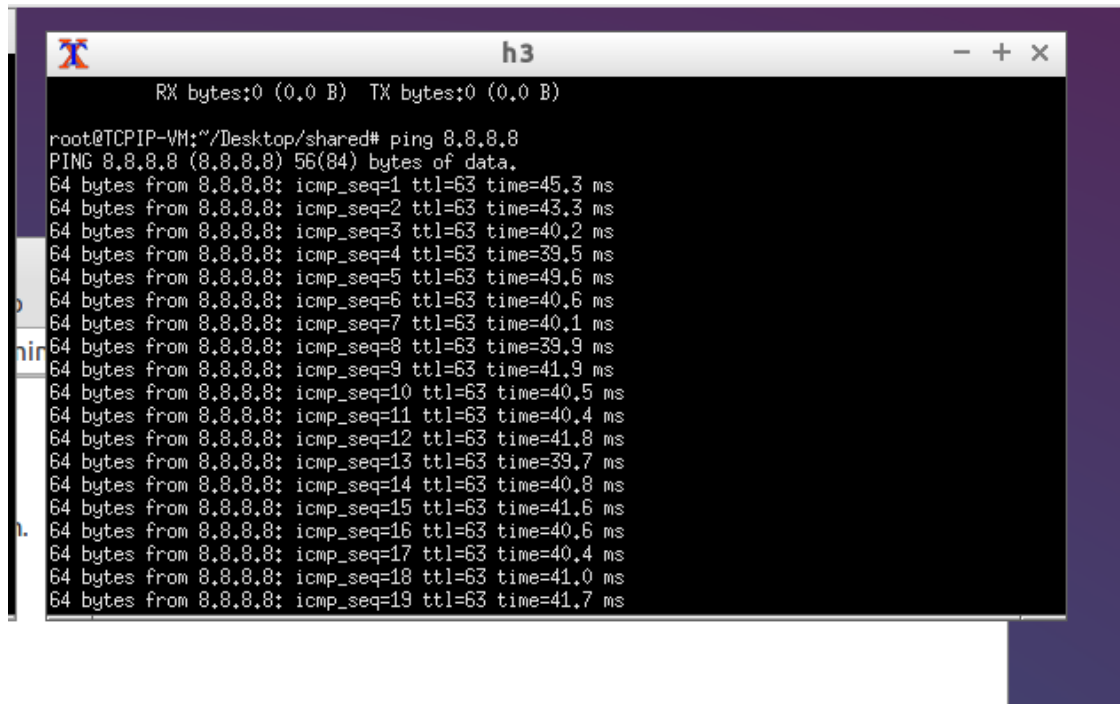
سپس اسکریپت پایتونی را اجرا خواهیم کرد. سپس با دستور `show` اینترفیس ایجاد شده را چک خواهیم کرد. همانطور که در شکل ۲ مشاهده خواهید کرد یک IP قابل استفاده برای اینترفیس `eth1` از `h3` ایجاد کرده و اجازه دسترسی به اینترنت از طریق پل ایجاد شده را به `h3` می‌دهیم. همانطور که مشاهده می‌شود ، پینگ گرفته و اتصال با گوگل قابل مشاهده است. `google.com` آدرسی که پورت `h3-eth1` خواهد داشت ، برابر با `10.0.2.16` خواهد بود. ممکن است با خطای `Temporary failure in name resolution` روبرو شویم که به علت عدم توانایی سیستم در ترجمه اسم دامنه سایت به IP آن خواهد بود.



شکل ۲: سوال دوم

با تحلیل بسته‌های صادره از سوی h1 توضیح دهید که چرا نتوانستید با سرور گوگل ارتباط برقرار نمایید.

دلیل عدم اتصال به سرور گوگل ، محلی بودن آدرس packet های ارسالی است که ماشین مجازی به محض دریافت چنین بسته‌هایی آن‌ها را drop می‌کند. نتیجه پینگ آدرس IP گوگل از h1 در زیر قابل مشاهده است :



```
h3
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
root@TCPIP-VM:~/Desktop/shared# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=63 time=45.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=63 time=43.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=63 time=40.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=63 time=39.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=63 time=49.6 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=63 time=40.6 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=63 time=40.1 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=63 time=39.9 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=63 time=41.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=63 time=40.5 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=63 time=40.4 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=63 time=41.8 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=63 time=39.7 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=63 time=40.8 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=63 time=41.6 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=63 time=40.6 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=63 time=40.4 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=63 time=41.0 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=63 time=41.7 ms
```

شکل ۳: ping google.com

## ۴ سوال چهارم

در `h3-eth1` چه مشاهده می‌شود؟  
علت عدم موفقیت چیست؟

در صورتی که پیکربندی `DNS server` در فایل `resolve.conf` به درستی انجام شده باشد، اتصال بین `h3` و اینترنت هم با آدرس `IP` و هم با دامنه گوگل برقرار است ولی در غیراین صورت، باید پیکربندی `DNS server` با دستور `sudo echo nameserver 8.8.8.8 > /etc/resolv.conf` انجام شود که بتوان با دامنه هم پینگ موفق را ایجاد نمود.

## ۵ سوال پنجم

دستور `iptables -t nat` مناسب برای ایجاد یک پیکربندی NAT مناسب در `h3` را بیان کنید.

با استفاده از دستور

```
iptables -t nat -A POSTROUTING -o h3-eth1 -j MASQUERADE
```

عملیات `MASQUERADE`

را انجام می‌دهیم.

## ۶ سوال ششم

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 سورس حقیقی بسته‌ها مورد استفاده قرار می‌گیرد؟ )

بسته‌های موجود در پروتکل ICMP یا Internet Control Message Protocol که برای تشخیص مشکل یا خطا در شبکه مورد استفاده قرار می‌گیرند ، حاوی پارامترهایی در هدر خود می‌باشند Type ( که ۱ بایت بوده و مشخص می‌کند این بسته برای چه چیزی است ) ، Code ( که ۱ بایت بوده و در مورد نوع ارور اطلاعات بیشتری به دست می‌دهد ) ، و در نهایت Checksum ( که ۲ بایت بوده و برای چک کردن consistency و integrity پیام ارسالی مورد استفاده قرار می‌گیرد )

برای تشخیص مبدا بسته‌ها با توجه به IP مبدا ، فرستنده تعیین می‌شود.

بدین ترتیب با توجه به اطلاعات مذکور موجود در بسته‌ها، پیکربندی NAT در h3 ، پاسخ‌های دریافتی را برای h1 می‌فرستد.