
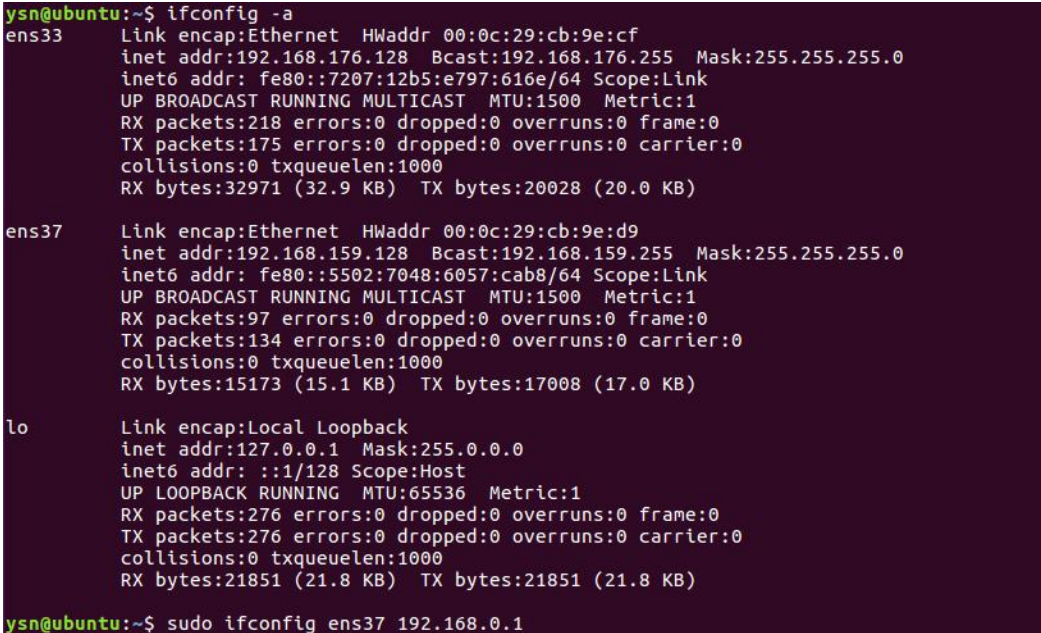


实验名称	NAT 实验		
姓名		学号	
实验步骤	所有实验均在 VMware 17.6.1 虚拟机环境下的 Ubuntu 16.04.7 系统中完成。		
	一、NAT 服务器设置		
	1、网卡编辑		
			
2、设置 IP 地址			
			
PS: 对 ens33 即 NAT 网卡, VMware 默认就是 DHCP 分配地址			
3、打开转发功能			

```
ysn@ubuntu:~$ sudo gedit /etc/sysctl.conf

(gedit:2613): IBUS-WARNING **: The owner of /home/ysn/.config/ibus/bus is not root!

(gedit:2613): IBUS-WARNING **: Unable to connect to ibus: Unexpected lack of content trying to read a line

(gedit:2613): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files

** (gedit:2613): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported

** (gedit:2613): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

** (gedit:2613): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
```

4、添加 NAT 功能

```
ysn@ubuntu:~$ sudo iptables -t nat -A POSTROUTING -s "192.168.0.1/24" -o ens33 -j MASQUERADE
ysn@ubuntu:~$ sudo /sbin/sysctl -p
net.ipv4.ip_forward = 1
```

二、HOST 设置

1、网卡设置



2、设置 ip 地址

```
ysn@ubuntu:~$ ifconfig -a
ens33: Link encap:Ethernet HWaddr 00:0c:29:1d:d9:08
       inet addr:192.168.159.129 Bcast:192.168.159.255 Mask:255.255.255
       inet6 addr: fe80::5df6:c1f9:2f1b:c6f5/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:6 errors:0 dropped:0 overruns:0 frame:0
       TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:760 (760.0 B) TX bytes:10360 (10.3 KB)

lo:    Link encap:Local Loopback
       inet addr:127.0.0.1 Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING MTU:65536 Metric:1
       RX packets:204 errors:0 dropped:0 overruns:0 frame:0
       TX packets:204 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:14654 (14.6 KB) TX bytes:14654 (14.6 KB)

ysn@ubuntu:~$ sudo ifconfig ens33 192.168.0.2
[sudo] password for ysn:
```

3、修改 DNS

```

ysn@ubuntu:~$ sudo gedit /etc/resolv.conf

(gedit:2726): IBUS-WARNING **: The owner of /home/ysn/.config/ibus/bus is not root!

(gedit:2726): IBUS-WARNING **: Unable to connect to ibus: Unexpected lack of content trying to read a line

(gedit:2726): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files

** (gedit:2726): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported

** (gedit:2726): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

** (gedit:2726): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported

```

PS: PPT 上要求修改默认 DNS 为 1.2.4.8, 但是 ping 不通; 请教助教后改成了 8.8.8.8。

4、设置局域网内默认网关

```

ysn@ubuntu:~$ sudo route add default gw 192.168.0.1

```

三、使用 host 机 ping 通外网

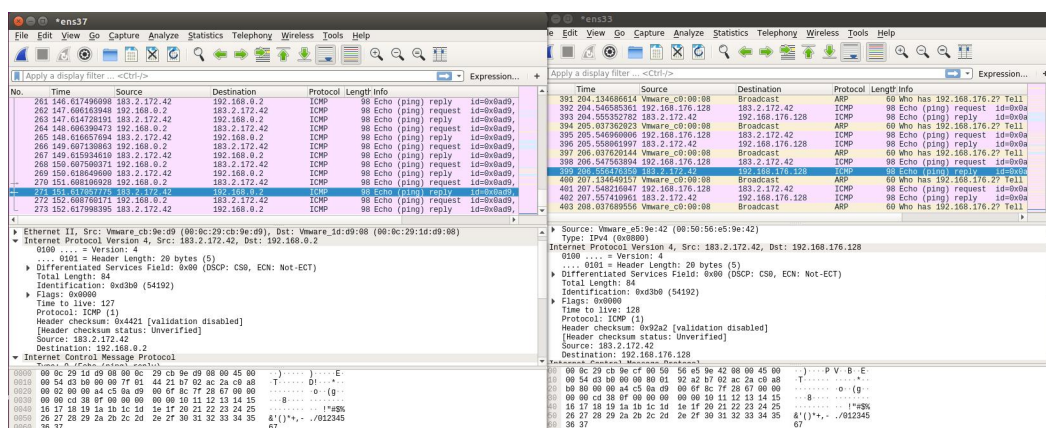
```

ysn@ubuntu:~$ ping www.baidu.com
PING www.a.shifen.com (183.2.172.42) 56(84) bytes of data:
64 bytes from 183.2.172.42: icmp_seq=1 ttl=127 time=11.0 ms
64 bytes from 183.2.172.42: icmp_seq=2 ttl=127 time=16.5 ms
64 bytes from 183.2.172.42: icmp_seq=3 ttl=127 time=12.6 ms
64 bytes from 183.2.172.42: icmp_seq=4 ttl=127 time=13.6 ms
64 bytes from 183.2.172.42: icmp_seq=5 ttl=127 time=8.18 ms
64 bytes from 183.2.172.42: icmp_seq=6 ttl=127 time=7.78 ms
64 bytes from 183.2.172.42: icmp_seq=7 ttl=127 time=7.35 ms

64 bytes from 183.2.172.42: icmp_seq=37 ttl=127 time=23.4 ms
64 bytes from 183.2.172.42: icmp_seq=38 ttl=127 time=31.9 ms
64 bytes from 183.2.172.42: icmp_seq=39 ttl=127 time=13.6 ms
64 bytes from 183.2.172.42: icmp_seq=40 ttl=127 time=9.56 ms
64 bytes from 183.2.172.42: icmp_seq=41 ttl=127 time=13.8 ms
^C
--- www.a.shifen.com ping statistics ---
41 packets transmitted, 41 received, 0% packet loss, time 40061ms
rtt min/avg/max/mdev = 7.355/15.066/36.907/6.428 ms

```


使用命令 ping www.baidu.com 后在 NAT 服务器打开 wireshark 软件抓包，结果如下：



1、观察 NAT 服务器对分组进行地址和端口翻译的过程

由图可知,在NAT网卡期间,从baidu.com返回的包的目的地址会从192.168.176.128转换为192.168.0.2,实现了NAT的地址翻译。不过软件并没有提供端口信息。

2、观察 NAT 对分组校验和的修改

由图可知,在NAT网卡期间,由于目的地址的变化,包的Header checksum由0x4421转变为0x92a2,体现了NAT对分组校验和的修改。

1、NAT 协议中，需要对 UDP 会话中的 UDP 校验和进行修改，选哪个修改。为什么 UDP 校验和为 0 时不需要修改？请结合 UDP 原理回答。

在 NAT 协议中，当 UDP 会话经过 NAT 设备时，通常需要对 UDP 校验和进行重新计算并更新。这是因为 NAT 设备在转换 IP 地址（如目的 IP 地址和端口）时，修改了 UDP 数据包的内容，而 UDP 校验和用于确保数据包在传输过程中没有被篡改或损坏，因此需要重新计算。

具体而言，UDP 校验和的计算包括 UDP 头部和数据部分的内容，以及伪头部，伪头部包含源 IP、目标 IP、协议号和 UDP 长度等信息。NAT 修改 IP 地址后，伪头部中的 IP 地址信息改变，因此 NAT 设备必须重新计算校验和，以确保接收端能正确验证数据包的完整性。

然而，当 UDP 校验和的值为 0 时，情况有所不同。根据 UDP 协议，校验和值为 0 表示不使用校验和，接收方会忽略校验和的验证。这在一些对延迟敏感的应用中很有用，因为可以省去校验和的计算过程。在这种情况下，即使 NAT 修改了数据包的 IP 地址或端口，由于校验和的值为 0，NAT 设备不需要对其重新计算或更新，因为接收方不会进行校验和检查。

2、跨越 NAT 网关还能使用 ping 和 traceroute 么？

(1) 跨越 NAT 网关使用 Ping

Ping 使用 ICMP 协议发送 echo request 消息，并等待 echo reply 消息来测试网络连通性。对于 Ping 来说，跨越 NAT 网关的情况如下：

- 出站 Ping（从内网设备发往外网）：大多数 NAT 设备会支持 Ping 请求的转发，因此内网设备发起的 Ping 可以正常跨过 NAT 网关。NAT 设备会将出站 ICMP 请求重新映射到外部 IP，并在收到应答后，将应答映射回内网设备。

- 入站 Ping（从外网发往内网）：一般情况下，NAT 不会自动将外部 Ping 请求路由到内网设备，除非 NAT 设备进行了专门的配置，将 Ping 请求引导到特定内网主机。因此，通常外网设备无法直接 Ping 到内网设备的私有 IP 地址。

(2) 跨越 NAT 网关使用 Traceroute

Traceroute 用于追踪数据包到目标主机的路径，通常会利用 ICMP 或 UDP 协议的超时特性。Traceroute 逐跳发送数据包，查看每跳路由器返回的超时信息，以显示路径中的路由器列表。在跨越 NAT 时，Traceroute 的行为如下：

- 出站 Traceroute（从内网设备发往外网）：Traceroute 可以跨越 NAT 网关并显示路径上的各个路由器，但 Traceroute 可能只显示到达 NAT 网关后的跳数。NAT 设备会掩盖内部网络的拓扑结构，因此可能只显示 NAT 设备的公共 IP，而不会显示内网的各个设备和路由器。

- 入站 Traceroute（从外网发往内网）：通常无法直接追踪到内网设备，因为 NAT 隐藏了内部 IP 地址，外部只能看到 NAT 设备的外部 IP。除非对 NAT 网关进行了特殊配置，使得 Traceroute 的 ICMP 或 UDP 包可以路由到内网特定设备，否则无法直接在外网进行内网的路径追踪。

3、分析 NAT 技术的优缺点。

优点：

(1) **节省 IP 地址：**NAT 通过将多个内网设备的私有 IP 映射到单个或少量公共 IP 上，使得多个设备可以共享一个公网 IP 地址。这在 IPv4 地址资源紧张的情况下尤为重要，有效地延长了 IPv4 的寿命。

	<p>(2) 增强网络安全性: NAT 隐藏了内网的真实 IP 地址, 使得外部用户无法直接访问内网设备, 从而为内网增加了一层安全防护。攻击者只能看到 NAT 设备的公网 IP, 这使得内网免受直接扫描和攻击。</p> <p>(3) 简化网络重组: 使用 NAT 后, 内部网络的 IP 地址不需要与外部网络相匹配。内网地址可以根据组织需求任意分配, 简化了内部网络结构调整和重新规划的复杂性。即使外部网络更改, 内部网络也可以保持不变。</p> <p>(4) 提高路由效率: NAT 在一定程度上可以减少路由表的规模, 因为外网路由器只需处理少量公共 IP, 而不需处理每个内网设备的私有 IP, 这有助于提高网络的整体路由效率。</p> <p>缺点:</p> <p>(1) 影响某些协议的功能: 一些协议 (如 IPSec、SIP、FTP 等) 在数据包中嵌入了源 IP 地址, NAT 修改 IP 地址后会导致协议无法正常工作, 必须借助特殊方法 (如 ALG 或穿透技术) 来支持此类协议。这增加了复杂性和潜在的性能开销。</p> <p>(2) 增加网络延迟和处理负荷: NAT 设备需要实时修改每个数据包中的 IP 地址和端口信息, 这会增加处理负担, 尤其是在大规模网络中, NAT 设备可能成为瓶颈, 从而增加延迟, 影响网络性能。</p> <p>(3) 破坏端到端通信: NAT 打破了 IP 协议的端到端原则, 使得内外网设备间的直接通信更加复杂。由于 NAT 隐藏了内网的 IP 地址, 外部设备很难直接访问内网设备, 从而阻碍了某些应用的正常运行。</p>
经验总结	<p>(实验过程中遇到的困难, 试验中需要额外注意的事项, 实验中激发的灵感等)</p> <p>1、一开始遇到的最大困难就是不知道网卡在 Ubuntu 中的名字具体是什么, 想了很久才想起来问 GPT, 马上就知道了可以用 ifconfig 命令得知。</p> <p>2、完成 NAT 服务器和 HOST 机的配置后, ping baidu.com 后得到 unknown host, 查了半天资料也不知道原委, 请教助教后才得知需要把 host 机上的 DNS 改为 8.8.8.8。(菜就多问, GPT 或助教都行)</p> <p>3、我用的是虚拟机是 VMware, 和实验指导书中的 Virtualbox 不同, 使得我在配置网卡时也遇到了一点困扰, 因为 VMware 管网卡叫网络适配器, 管 internal network 叫仅主机模式。</p>