1 接入网关的配置

1.1 配置静态IP地址

(1) 首先使用 vim 编辑器打开/etc/network/interfaces，命令如下:

sudo vim /etc/network/interfaces

(2) 然后往里面输入如下代码：

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens33
iface ens33 inet static
address 192.168.11.1
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255

auto ens38
iface ens38 inet dhcp
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/network/interfaces" 19L, 431C                                   1,1           All
```

注意：网关服务器有两个网卡，一个是ens33，作为接入网关；另一个是ens38，作为NAT网关。

(3) 配置后，重启网卡使其生效，命令如下：

sudo /etc/init.d/networking restart

(4) 查看静态IP地址是否配置成功，命令为：ifconfig。

(5) 配置成功后，可以看到如下情况：

```
li@ubuntu:~$ sudo /etc/init.d/networking restart
[ ok ] Restarting networking (via systemctl): networking.service.
li@ubuntu:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:f1:ab:0b
          inet addr:192.168.11.1  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef1:ab0b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:486 (486.0 B)  TX bytes:1226 (1.2 KB)

ens38     Link encap:Ethernet  HWaddr 00:0c:29:f1:ab:15
          inet addr:192.168.230.143  Bcast:192.168.230.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef1:ab15/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4649 (4.6 KB)  TX bytes:5476 (5.4 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:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:49 (49.0 B)  TX bytes:49 (49.0 B)

li@ubuntu:~$
```

1.2 配置DHCP服务器

(1) 安装DHCP服务，命令如下：

sudo apt-get install isc-dhcp-server

(2) 配置DHCP服务。

I. 首先用vim编辑器打开/etc/default/isc-dhcp-server文件，命令如下：

sudo vim /etc/default/isc-dhcp-server

II. 然后，对里面的内容修改如下：

```
# Defaults for isc-dhcp-server initscript
# sourced by /etc/init.d/isc-dhcp-server
# installed at /etc/default/isc-dhcp-server by the maintainer scripts

#
# This is a POSIX shell fragment
#

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPD_CONF=/etc/dhcp/dhcpd.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPD_PID=/var/run/dhcpd.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="ens33"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/default/isc-dhcp-server" 21L, 658C                                1,1           All
```

III. 然后用vim编辑器打开 /etc/dhcp/dhcpd.conf 文件，命令如下：

sudo vim /etc/dhcp/dhcpd.conf

IV. 最后，往该文件添加如下内容：

```
# 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;
#}
subnet 192.168.11.0 netmask 255.255.255.0 {
   range 192.168.11.20 192.168.11.40;
   option routers 192.168.11.1;
   option subnet-mask 255.255.255.0;
   option broadcast-address 192.168.11.255;
   option domain-name-servers 192.168.11.1;
   option ntp-servers 192.168.11.1;
   option netbios-name-servers 192.168.11.1;
   option netbios-node-type 8;
}

# 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;
                                                              57,1          24%
```

1.3 配置NAT服务

sudo iptables -t nat -A POSTROUTING -s 192.168.11.0/24 -o ens38 -j MASQUERADE

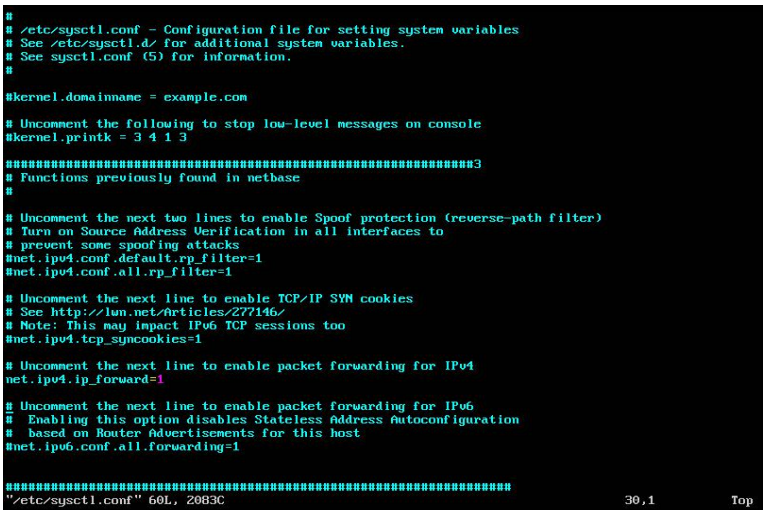
1.4 配置接入网关服务器的转发功能

因为接入网关服务器有两个网卡，要让连接到服务器ens33网卡的接入主机发送的数据包能够通过服务器的ens38网卡传递到外界，必须要打开服务器的路由转发功能。配置过程如下所示。

(1) 使用vim编辑器打开/etc/sysctl.conf文件，命令如下：

sudo vim /etc/sysctl.conf

(2) 将“net.ipv4.ip_forward=1”所在的那一行“#”去掉，如下所示：



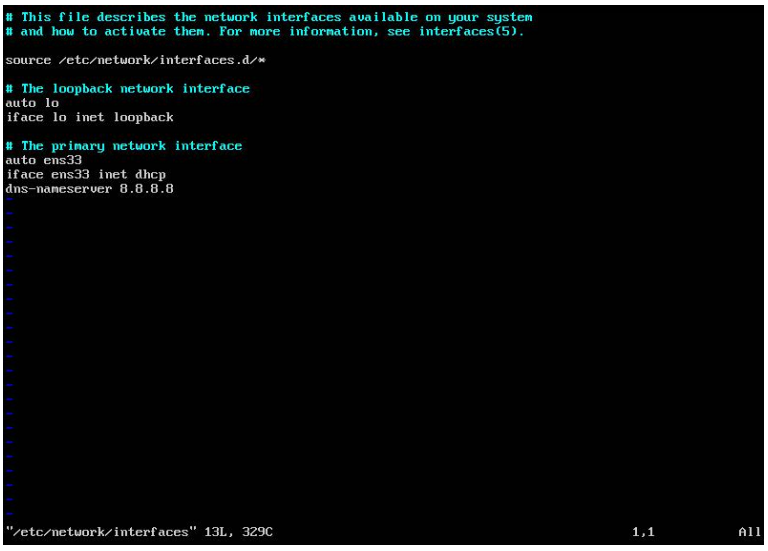
1.5 配置接入主机的DNS地址

为了能够让接入主机上网还需要最后一步：配置接入主机的DNS地址。以其中一个接入主机为例（其他两个接入主机的配置过程完全一致），配置过程如下所示：

(1) 使用vim编辑器打开/etc/network/interfaces，命令如下：

sudo vim /etc/network/interfaces

(2) 往该文件中添加DNS地址，如下所示：



2 绑定与过滤功能配置

2.1 ACL、MAC地址绑定配置

ACL（Access Control List，访问控制列表），能够用来控制某些数据包进出端口。ACL 通过帮助用户定义一组权限规则，说明什么样的数据包才能够对其访问，用 IPTABLES 命令对其进行配置。

MAC 地址绑定，我的理解是它属于 ACL 当中的一个具体的实现策略。通过 IP 与 MAC 地址绑定，使得数据包只有同时匹配到 ACL 规则设定的 IP 和 MAC 地址才能转发，能有效地减少 ARP 攻击，从而提高整个网络的安全性。

在接入网关服务器上配置 IP 与 MAC 地址绑定的 ACL 策略过程如下：

1. 打开接入主机 1，查看其 IP 和 MAC 地址，命令为：ifconfig。

我们可以清楚地看到接入主机 1 的 IP 地址为 192.168.11.20，MAC 地址为 00:0c:29:6b:cb:c5。

```
li@ubuntu:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:6b:cb:c5
          inet addr:192.168.11.20  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6b:cbc5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:147 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22028 (22.0 KB)  TX bytes:14716 (14.7 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:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)
```

2. 设置接入网关服务器的 FORWARD 链默认策略为 DROP，命令如下：

sudo iptables -P FORWARD DROP

3. 设置仅允许接入主机 1 的数据包通过，也就是仅匹配接入主机 1 的 IP 与 MAC 地址，实现 MAC 地址绑定功能。在接入网关服务器输入如下命令：

sudo iptables -A FORWARD -s 192.168.11.20 -m mac --mac-source 00:0c:29:6b:cb:c5 -j ACCEPT

因为 PING 过程中，接入主机除了需要发送数据包外，也要接收对应的数据包，因此我们也要设置目的 IP 为接入主机 1 的数据包都进行接收。在接入网关服务器输入如下命令：

sudo iptables -A FORWARD -d 192.168.11.20 -j ACCEPT

2.2 “非法”IP过滤配置

“非法”IP 过滤是指如果某个数据包的源 IP 为规则中设定的“非法”地址，则将该数据包进行丢弃。（假设接入主机 1 的 IP 为“非法”IP）配置过程如下所示：

1. 在接入网关服务器中删除已有规则，命令为：sudo iptables -F

2. 设置接入网关服务器的 FORWARD 链默认策略为 ACCEPT，命令如下：

sudo iptables -P FORWARD ACCEPT

3. 配置“非法”IP 过滤功能，在接入网关服务器中输入如下命令：

sudo iptables -A FORWARD -s 192.168.11.20 -j DROP

2.3 “非法”PORT过滤配置

“非法”PORT 过滤是指如果某个数据包的 PORT 为规则中设定的“非法”PORT，则将该数据包进行丢弃。（假设“非法”PORT 号为 2500）配置过程如下所示：

1. 在接入网关服务器中删除已有规则，命令为：sudo iptables -F
2. 配置“非法”PORT 过滤功能，在接入网关服务器中输入如下命令：

sudo iptables -A INPUT -p tcp --dport 2500 -j DROP