实验三 子网划分和NET配置

邱梓豪

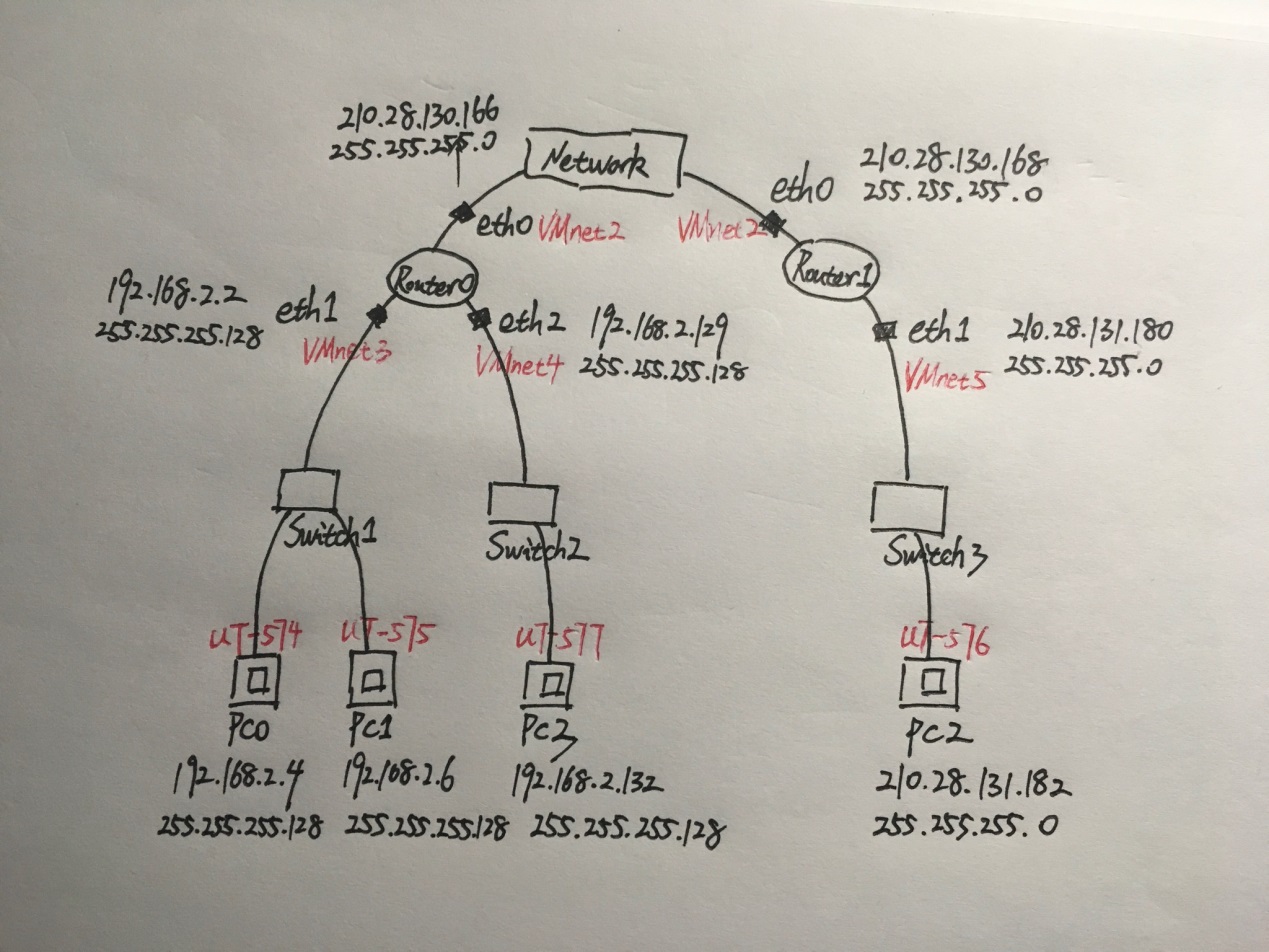
141130077

一、实验目的

本实验的主要目的是学习按照需求配置一个静态的包含多个子网的网络环境，学习利用子网掩码进行子网的划分。了解NAT技术，学会使用NAT组网技术，学习相关的linux指令，为以后的实验过程中搭建组网打下基础。

二、网络拓扑配置

网络拓扑结构如下：



相关结点的虚拟设备名、IP及Netmask如下

|  |  |  |  |
| --- | --- | --- | --- |
| 节点名 | 虚拟设备名 | IP | Netmask |
| Router0 | U-571 | Eth0 210.28.130.166 | 225.255.255.0 |
| Eth1 192.168.2.2 | 225.255.255.128 |
| Eth2 192.168.2.129 | 225.255.255.128 |
| Router1 | U-572 | Eth0 210.28.130.168 | 225.255.255.0 |
| Eth1 210.28.131.180 | 225.255.255.0 |
| PC0 | UT-574 | 192.168.2.4 | 225.255.255.128 |
| PC1 | UT-575 | 192.168.2.6 | 225.255.255.128 |
| PC2 | UT-576 | 210.28.131.182 | 225.255.255.0 |
| PC3 | UT-577 | 192.168.2.132 | 225.255.255.128 |

注意在虚拟机配置中确认每个router和pc的网络适配器！！

三、路由规则设置

（1）先不设置NAT，观察此时的网络连接状态

Ip设置命令：

Router0 U-571：sudo ifconfig eth0 210.28.130.166 netmask 255.255.255.0

sudo ifconfig eth1 192.168.2.2 netmask 255.255.255.128

sudo ifconfig eth2 192.168.2.129 netmask 255.255.255.128

Router1 U-572：sudo ifconfig eth0 210.28.130.168 netmask 255.255.255.0

sudo ifconfig eth1 210.28.131.180 netmask 255.255.255.0

PC0 UT-574: sudo ifconfig eth0 192.168.2.4 netmask 255.255.255.128

PC1 UT-575: sudo ifconfig eth0 192.168.2.6 netmask 255.255.255.128

PC2 UT-576: sudo ifconfig eth0 210.28.131.182 netmask 255.255.255.0

PC3 UT-577: sudo ifconfig eth0 192.168.2.132 netmask 255.255.255.128

网关设置命令：

PC0 UT-574: sudo route add default gw 192.168.2.2

PC1 UT-575: sudo route add default gw 192.168.2.2

PC2 UT-576: sudo route add default gw 210.28.131.180

PC3 UT-577: sudo route add default gw 192.168.2.129

注意：这里仅设置主机的默认网关，不设置路由器的默认网关

添加路由规则命令：

Router0 U-571：sudo ip route add 192.168.2.0/25 via 192.168.2.2

sudo ip route add 192.168.2.128/25 via 192.168.2.129

sudo ip route add 210.28.131.0/24 via 210.28.130.168

Router1 U-572：sudo ip route add 210.28.131.0/24 via 210.28.131.180

注意：这里不设置Router1向内网的转发规则

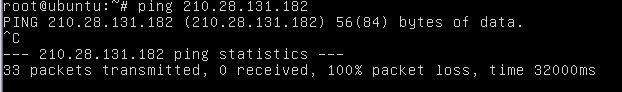
允许转发命令（在router1和router2中设置）

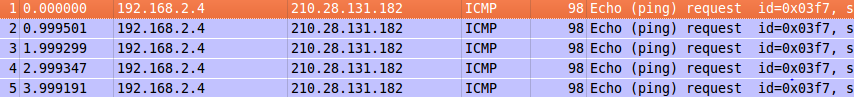
echo 1 > /proc/sys/net/ipv4/ip\_forward

四、网络连接状态测试（设置NAT前）

PC0、PC2、PC3之间互ping（未设置iptables规则时）

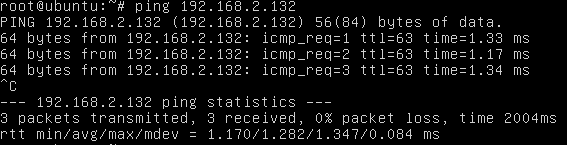
1. PC0 ping PC2

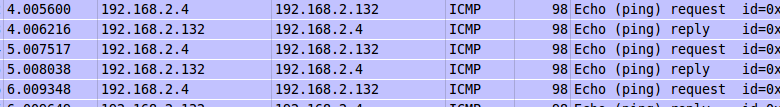




无法ping通。未设置NAT时，内网和公网是隔离的，所以内网的主机无法ping外网的主机。

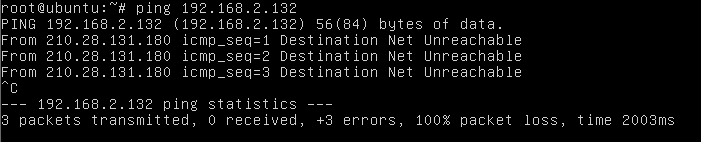
1. PC0 ping PC3

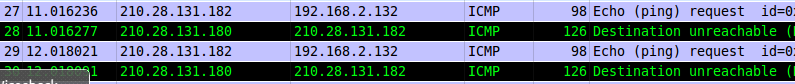




可以ping通。两台主机属于同一个子网，所以可以相互通信。

（3）PC2 ping PC3





无法ping通。内网和公网此时不相连，所以公网的主机无法ping内网的主机。

五、设置iptables规则

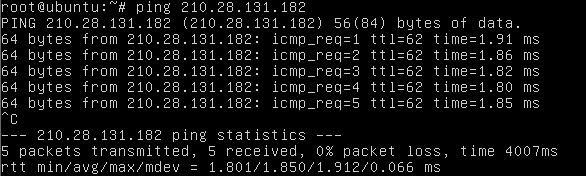
在Router0设iptables规则，使得内网的主机可以使用Router0的外部ip与公网上的主机通信，linux命令如下：

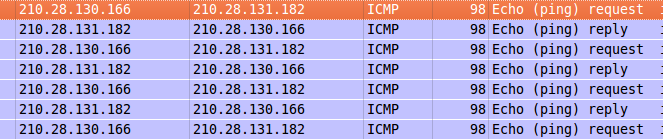
sudo iptables –t nat –A POSTROUTING –o eth0 –s 192.168.2.0/24 –j SNAT –to 210.28.130.166

六、网络连接状态测试（设置NAT后）

PC0、PC2、PC3之间互ping（设置iptables规则后）

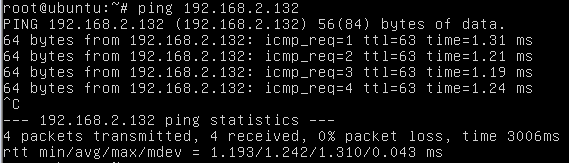
（1）PC0 ping PC2

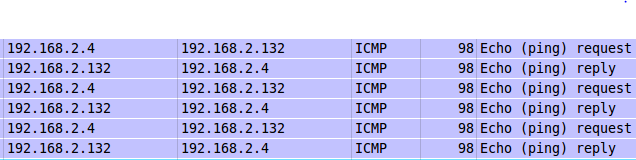




可以ping通。由wireshark抓包结果可知，PC0在ping PC2时用的实际上是Router0的公网ip（210.28.130.166），这样PC0的内网ip经过NAT转换成公网ip后，就可以和公网上其他主机通信了。

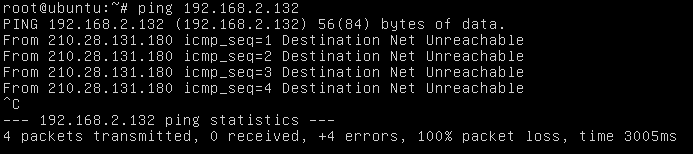
（2）PC0 ping PC3

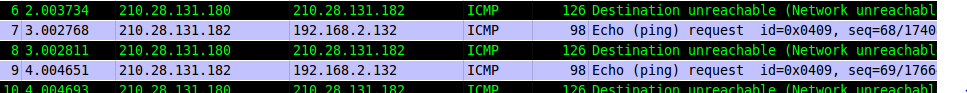




可以ping通。两台主机处于同一内网中，可以ping通。

（3）PC2 ping PC3



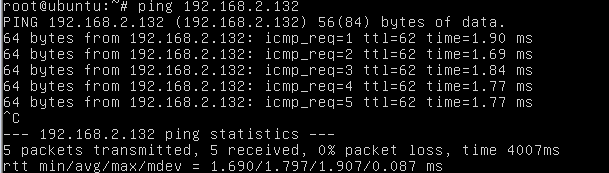


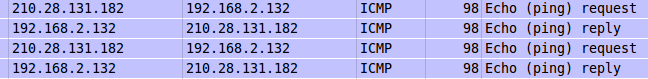
若不设置Router1的路由转发功能，不设置其默认网关，则PC2不能ping通PC3。因为Router1不知道目标ip为210.28.131.180的数据包该发往何处。

若设置Router1的路由转发如下：

sudo ip route add 192.168.2.0/24 via 210.28.130.166

则可以ping通，效果如下：



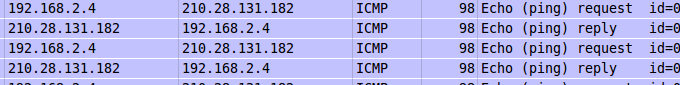


此时数据包将被Router1发送到210.28.130.16处，也就是Router0。然后Router0将这个数据包转给对应的主机。

七、内网公网通信的抓包分析（设置NAT后）

设置iptables之后PC0 ping PC2抓包分析：

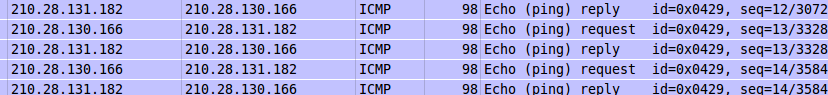
（1）对eth1网卡进行监听：





由此可见。PC0最初发送icmp数据包时，其源地址为192.168.2.4，也就是PC0的内网地址，目标地址是210.28.131.182，是PC2的公网地址。

（2）对eth0网卡进行监听：





当该icmp数据包经过Router0之后，由eth0网卡向外发出时，可以发现该包的源地址已经变成了210.28.130.166，说明NAT会将PDU内原来不合法的内部源ip替换掉，即修改源ip，这样便实现了从内网和公网之间的通信。