Lab3

171830635 俞星凯

|  |  |
| --- | --- |
| 实验目的 | 1. 配置一个静态的包含多个子网的网络环   境   1. 学会NAT的组网方式 2. 进一步了加深对于“跳”的理解 |
| 网络拓扑配置 | 见附表及附图 |
| 路由规则配置 | Router0:  sudo ip route add 192.168.2.0/25 via 192.168.2.1  sudo ip route add 192.168.2.128/25 via 192.168.2.129  sudo ip route add 192.168.3.0/24 via 192.168.1.2  Router1:  sudo ip route add 192.168.2.0/24 via 192.168.1.1  sudo ip route add 210.18.130.0/24 via 192.168.1.1 |
| NAT设置命令 | sudo iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.0/24 -j SNAT --to 210.28.130.166 |
| 数据包截图及协议报文分析 | 1.  SNAT之前：  PC0，PC2，PC3两两ping通  0to2  2to3  3to0  2.  SNAT之后：  PC0，PC2，PC3仍然可以两两ping通  0to2()  2to3()  3to0()  3.  但是用内网去ping外网时，用外网观测，可以看出SNAT发挥作用，内网的全部私有IP变成了公有IP。例如用内网中的PC0或者PC3去ping外网中的PC2时，在PC2上可以观察到私有IP均被公有IP 210.28.130.166代替。  0to2()3to2()  4.  进一步实验，当用PC0和PC3同时ping PC2时，在PC0上观察：  wtf  可以看出PC2与PC0，PC3之间均有数据包收发。如果在PC3上观察则情况也类似。  再在PC2上观察：  wtf  只出现了公有IP 210.28.130.166和PC2的IP，这是因为内网中的私有IP全部被公有IP替代，以至于在这张图中甚至无法分辨哪些数据包是PC0和PC2传输的，哪些又是PC3和PC2传输的。  5.  综上，使用NAT技术可以在多重 Internet子网中使用相同的IP,从而解决了IP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。而NAT的运作机制则是自动修改IP报文的源IP地址和目的IP地址。 |

附表

|  |  |  |  |
| --- | --- | --- | --- |
| 节点名 | 虚拟设备名 | ip | netmask |
| Router0 | UT-574 | eth0:192.168.1.1 | 255.255.255.0 |
| eth1:192.168.2.1 | 255.255.255.0 |
| eth2:192.168.2.129 | 255.255.255.0 |
| Router1 | UT-575 | eth0:192.168.1.2 | 255.255.255.0 |
| eth1:192.168.3.1 | 255.255.255.0 |
| PC0 | U-571 | eth0:192.168.2.2 | 255.255.255.128 |
| PC1 | UT-576 | eth0:192.168.2.3 | 255.255.255.128 |
| PC2 | U-572 | eth0:192.168.2.130 | 255.255.255.0 |
| PC3 | U-573 | eth0:192.168.3.2 | 255.255.255.128 |

附图

