



**计算机网络实验报告**

**姓名： 曾小港**

**学号： 2015111123**

**专业： 网络工程**

**Windows下网络命令的理解**

# 一、【实验目的】

## 学会使用netsh命令测试本机的TCP/IP网络配置

## 学会使用netstat命令以及检测网络连接

## 了解ARP原理以及使用ARP探索攻击源头

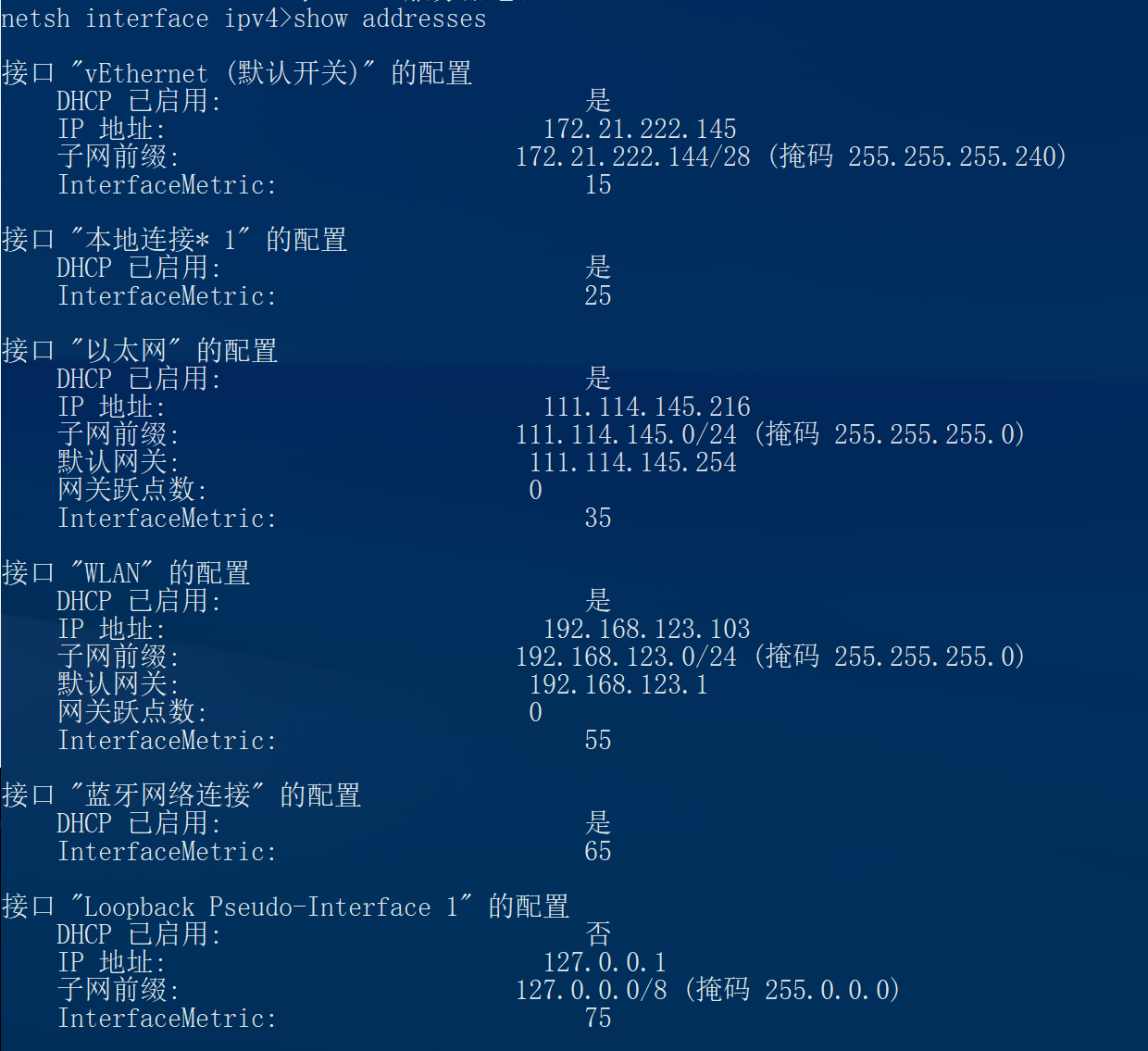
## 了解Nsiookup命令的用法

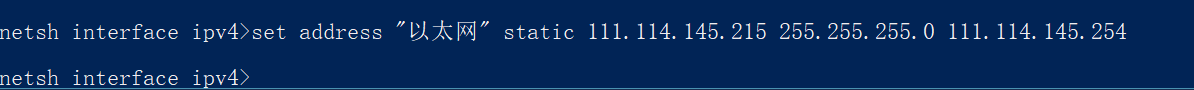
# 二、【实验环境】

Windows dos

# 三、【实验要求】

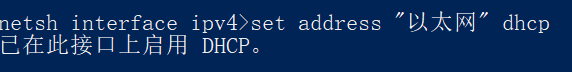
## 使用netsh命令查看本机的IP地址，并修改本机的静态或者动态IP地址并截图显示

.

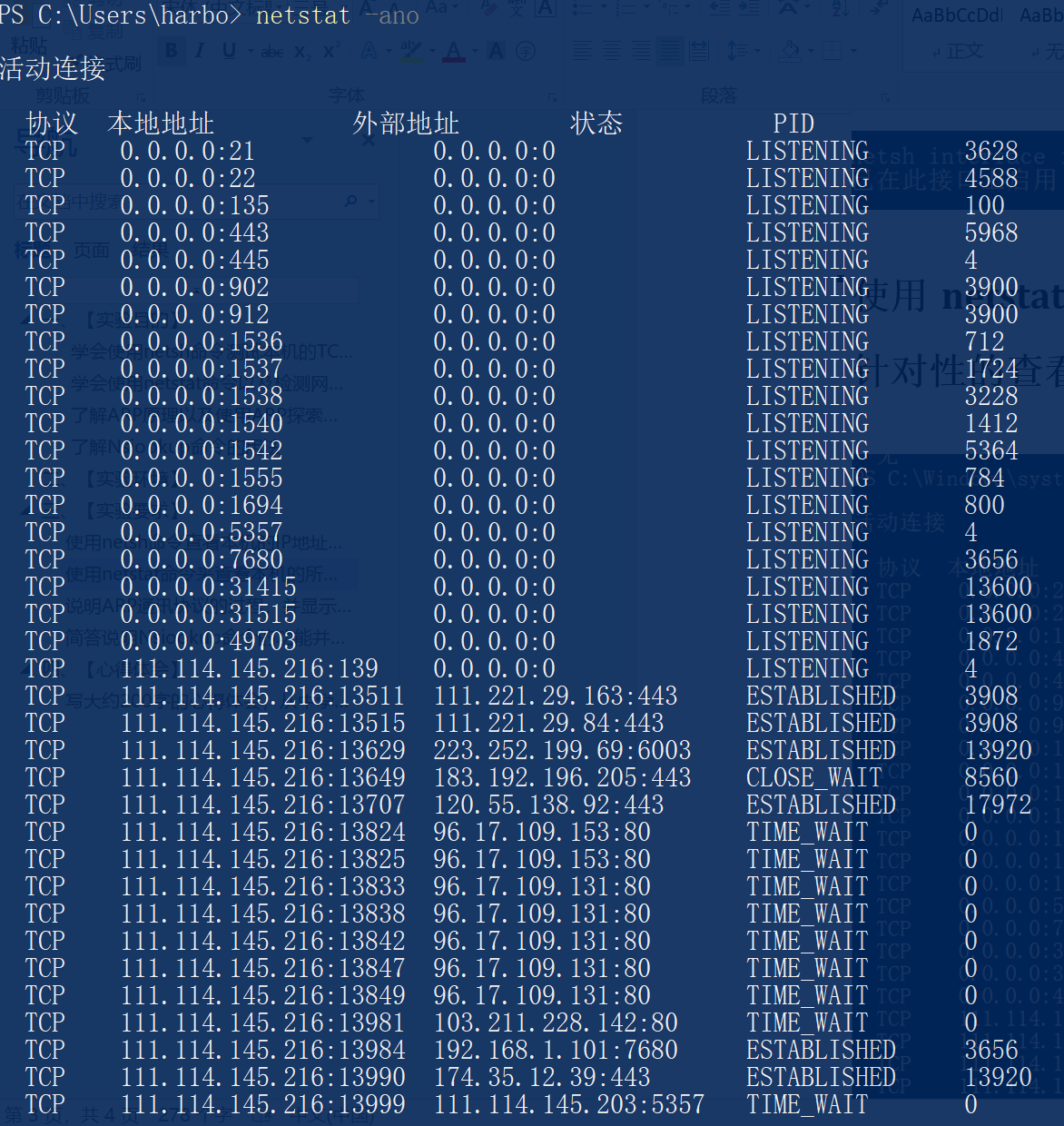


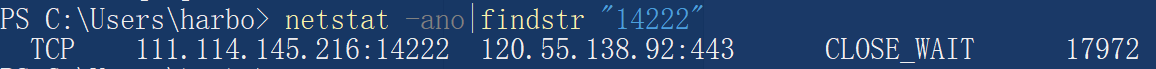
然后就不能上网了





## 使用netstat命令来查看本机的所有的端口和PID，以及有针对性的查看某个端口的PID并截图显示



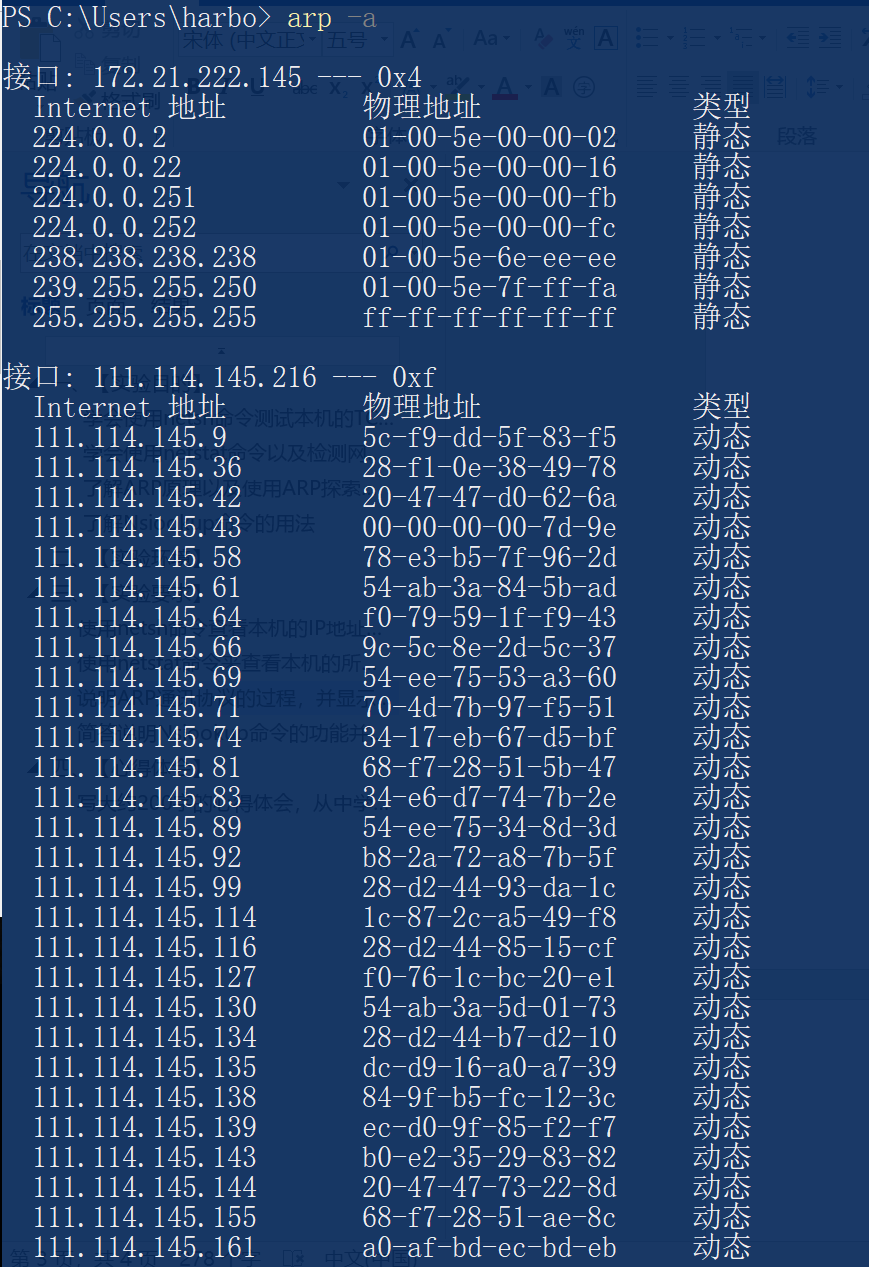


## 说明ARP通讯协议的过程，并显示本机中的ARP的缓存表，说明ARP欺骗的原理以及如何防范这种攻击

### ARP协议工作过程

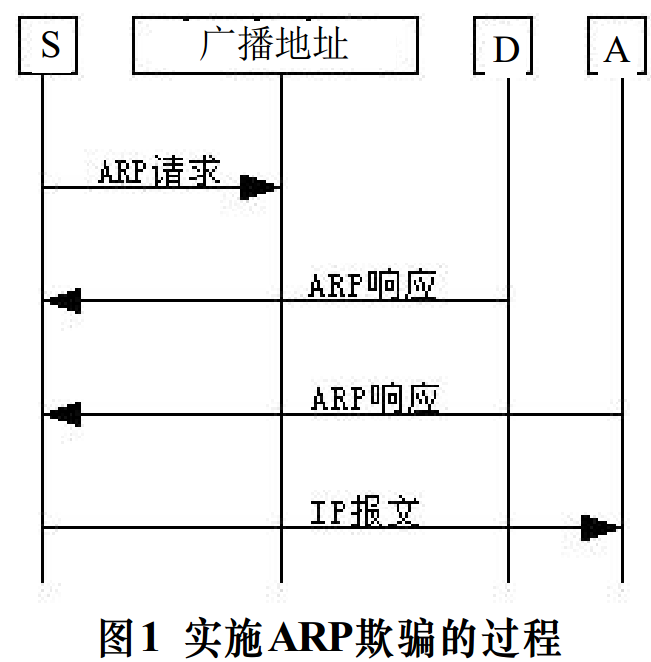
1. A先在其ARP高速缓存中查看有无B的IP地址。如有，就在ARP高速缓存中查出其对应的硬件地址，再把这个硬件地址写入MAC帧，然后通过局域网把该MAC帧发往此硬件地址。如果查不到B的IP的项目，则进入第（2）步。
2. A的ARP进程在本局域网上广播发送一个ARP请求分组，主要内容是A自己的IP地址、MAC地址，询问的IP地址（也就是B的IP地址）。
3. 在本局域网上的所有主机运行的ARP进程都收到此ARP请求分组。
4. 主机B的IP地址与ARP请求分组中要查询的IP地址一致，就收下这个ARP请求分组，并向A单播发送ARP响应分组（其中写入了B自己的硬件地址），同时将A的地址映射写入自己的ARP高速缓存中。由于其余的所有主机IP地址都与ARP请求分组要查询的IP地址不一致，因此都不理睬这个ARP请求分组。
5. A收到B的ARP响应分组后，就在其ARP高速缓存中写入B的IP地址到硬件地址的映射。

至此，A得到了从B的IP地址到其MAC地址的映射。当这个映射项目在高速缓存中保存超过生存时间，将被从高速缓存中删除。



### ARP欺骗的原理与现象

ARP欺骗的核心思想就是向目标主机发送伪造的ARP应答，并使目标主机接收应答中伪造的IP地址与MAC地址之间的映射对，以此更新目标主机ARP缓存。下面就在理论上说明实施ARP欺骗的过程(见图 ： 1) S代表源主机，也就是将要被欺骗的目标主机； D代表目的主机，源主机本来是向它发送数据； A代表攻击者，进行ARP欺骗。



从影响网络连接通畅的方式来看，ARP欺骗分为二种，一种是对路由器ARP表的欺骗；另一种是对内网PC的网关欺骗。

一般来说，ARP欺骗攻击的后果非常严重，大多数情况下会造成大面积掉线；如果是被中间人攻击，截取Internet与这个目标主机的之间的全部通信，则会导致信息泄露，在主机看来访问外部服务的响应变慢；或者对于服务器而言，上层应用忙于处理这种异常而无法响应外来请求。

### ARP欺骗的防范

1.主机级被动检测

当系统接收到来自局域网上的ARP请求时，系统检查该请求发送端的IP地址是否与自己的IP地址相同。如果相同，则说明该网络上另有一台机器与自己具有相同的IP地址。

2.主机级主动检测

主机定期向所在局域网发送查询自己IP地址的ARP请求报文。如果能够收到另一ARP响应报文，则说明该网络上另

有一台机器与自己具有相同的IP地址。

3.服务器级检测

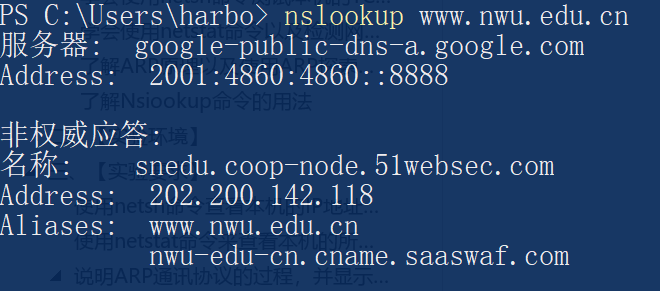
当服务器收到ARP响应时，为了证实它的真实性，根据反向地址解析协议(RARP)就用从响应报文中给出的 地 MAC

址再生成一个RARP请求，它询问这样一个问题：“如果你是这个MAC地址的拥有者，请回答你的IP地址”。这样就会查询到这个MAC地址对应的IP地址，比较这两个IP地址，如果不同，则说明对方伪造了ARP响应报文。

4.网络级检测

配置主机定期向中心管理主机报告其ARP缓存的内容。这样中心管理主机上的程序就会查找出两台主机报告信息的不一致，以及同一台主机前后报告内容的变化。这些情况反映了潜在的安全问题。或者利用网络嗅探工具连续监测网络内主机硬件地址与IP地址对应关系的变化。

## 简答说明Nsiookup命令的功能并查看西北大学此域名所对应的IP地址并截图显示



# 四、【心得体会】

本次上机主要学到了一些网络管理上常用的命令，包括netsh的对网络ip，子网掩码，网关的设置，以及ARP其基本作用，明白了欺骗的原理，其次对欺骗的防范有了一定的理解，不足之处在于对基础知识的理解不到位，不知道如何攻击室友的英雄联盟，让他玩不成从而声音小一点，被嗞哇嗞哇的吵人，但是随后通过查资料以及上网查询得到了较为详细的解释。所以今后应加强预习，同时课后要及时复习，使得知识掌握的更加牢固。