**云南大学软件学院**

**实 验 报 告**

课程： 计算机网络实践 任课教师： 李海

姓名： 陈俊宏 学号： 20211060245 专业：人工智能 成绩：

实验一 熟悉常用的Windows网络命令实验报告



1. 实验目的
2. 学会使用常用ipconfig, ping, nslookup, netstat，tracert和arp 等常用网络命令。检测网络连通、了解网络的配置状态，跟踪路由等相关网络问题。
3. 了解各层地址信息，进一步深入理解TCP/IP网络体系结构
4. 实验环境
5. 运行windows 7或windows7以上的PC一台。
6. 每台PC机具有一块网卡，通过双绞线与局域网相连。
7. 局域网能连接Internet。
8. 实验步骤
9. 在命令提示符窗口输入ipconfig/all命令查看网络接口的相关配置。
10. 在命令提示符窗口输入ping命令，查看网络连接情况。
11. 输入nslookup命令，查看DNS解析。
12. 输入netstat命令，查看TCP连接情况。
13. 输入tracert命令，查看路由跟踪情况。
14. 输入arp命令，查看局域网路地址映射情况。
15. 实验分析
16. 在Windows命令行下运行ipconfig/all 命令查看本机所有接口的TCP/IP协议配置，并将**以太网适配器的本地连接（局域网）**的相关信息填写在下表

|  |  |
| --- | --- |
| IPv4地址 | 10.100.146.64 |
| 子网掩码 | 255.255.0.0 |
| 默认网关 | fe80::9e52:f8ff:feec:1148%17 |
| IPv6 地址 | 240c:cf81:0:e3df:2ffb:5bda:1778:23b0 |
| 物理地址 | 74-4C-A1-44-2B-9F |
| 首选DNS服务器地址 | 2001:250:2800::13:51 |
| DHCP是否已经启用 | 是 |

根据所填内容回答问题

1. 什么是DHCP？你的计算机以太网接口的IPv4地址是手动获取还是自动获取？为什么？如果要想手动配置IPV4地址，该如何操作？

答：DHCP（Dynamic Host Configuration Protocol）是一种网络协议，它允许计算机自动获取IP地址和其他网络配置信息，而无需手动配置。DHCP服务器是网络上的设备，它负责为连接到网络的设备分配IP地址、网关、子网掩码和DNS服务器等信息，从而使设备能够与其他设备进行通信。通过使用DHCP，网络管理员可以更轻松地管理网络上的设备，并减少手动配置的工作量。我计算机以太网接口的IPv4地址是自动获取的，因为在网卡属性中的Internet协议版本(TCP/IPv4)属性中设置为自动获得IP地址，如果要想手动配置IPV4地址，可以在网卡属性中的Internet协议版本(TCP/IPv4)属性中设置为手动配置。

1. 什么是DNS？为什么需要在主机配置DNS服务器地址？

答：DNS代表域名系统（Domain Name System），是一种用于将域名转换为IP地址的分布式命名系统。简单来说，DNS是一种将易于记忆的域名转换为计算机能够理解的IP地址的系统。在主机上配置DNS服务器地址是因为当输入一个域名时，计算机需要通过DNS服务器来查找域名对应的IP地址。如果没有配置DNS服务器地址，计算机将不知道如何将域名转换为IP地址，从而无法连接到相应的网站或服务器。因此，需要在主机上配置DNS服务器地址，以便计算机可以正确地查找域名对应的IP地址并连接到相应的网站或服务器。

1. 比较IPV4、IPv6和物理地址的格式有什么不同（从长度，进制，分隔符和作用来区分）？

答：IPv4、IPv6和物理地址的格式有以下不同：

长度：IPv4地址为32位，IPv6地址为128位，而物理地址为48位。

进制：IPv4和IPv6地址都采用十六进制表示法，而物理地址采用十六进制和二进制混合表示法。

分隔符：IPv4地址由4个8位的十进制数组成，用点号"."分隔，例如：192.168.0.1；IPv6地址由8组16位的十六进制数组成，每组用冒号":"分隔，例如：2001:0db8:85a3:0000:0000:8a2e:0370:7334。物理地址则由6个8位的十六进制数组成，用冒号":"分隔，例如：00:1a:2b:3c:4d:5e。

作用：IPv4和IPv6地址用于标识互联网上的计算机或设备，物理地址用于标识局域网上的计算机或设备。IPv4和IPv6地址是逻辑地址，而物理地址是硬件地址。

1. 填写和你在同一个网络中邻居的IPv4地址，子网掩码，默认网关和DNS服务器的信息。你能发现什么？

答：IPv4地址：10.100.56.24；

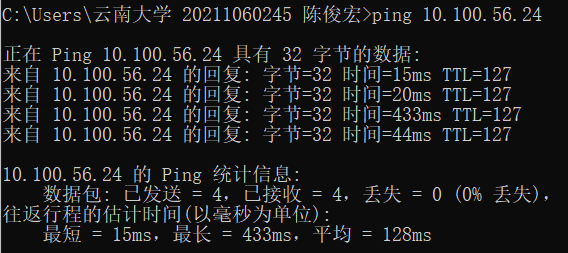
子网掩码：255.255.0.0；

默认网关：fe80::9e52:f8ff:feec:1148%5；

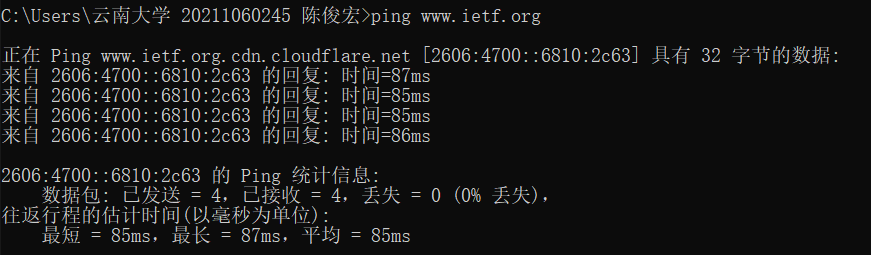
DNS服务器：2001:250:2800::13:51；

我发现和我的同一个网络中邻居的IPv4地址前五位是一致的，默认网关的%之前的位数是一致的，子网掩码和DNS服务器的信息是完全一致的。

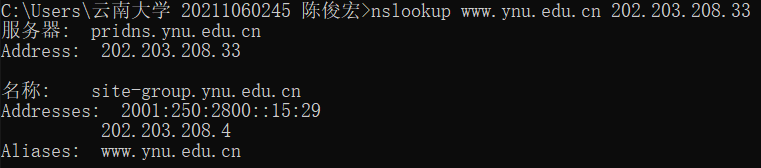
1. 在获取本机和邻居的IP地址之后，运行Ping命令，填写实验运行结果。
2. ping 邻居的IP地址并截图



1. ping [www.ietf.org](http://www.ietf.org) 并截图

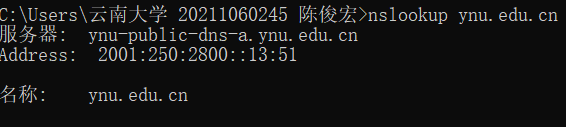


1. 用nslookup命令进行域名解析。
2. 执行nslookup [www.y](http://www.y)nu.edu.cn 8.8.8.8和执行nslookup [www.ynu.edu.cn](http://www.ynu.edu.cn) 202.203.208.33,附截图，并解释实验运行结果。

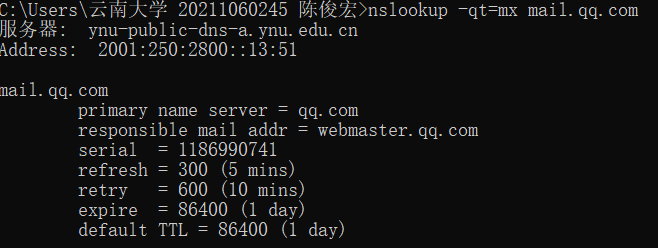


答：[www.ynu.edu.cn的IP](http://www.ynu.edu.cn的IP)地址为202.203.208.33，所以在执行nslookup www.ynu.edu.cn 8.8.8.8时，域名解析结果与该网址IP地址不一致，就出现了请求超时的错误。

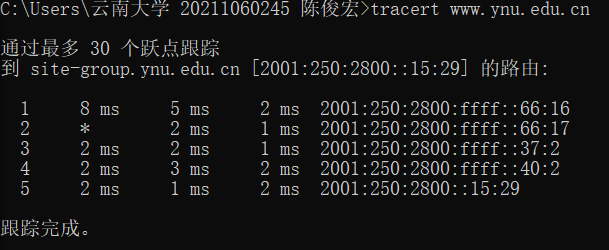
1. 查找[ynu.edu.cn](http://www.ynu.edu.cn)的授权域名服务器（提示利用ns类型字段）



1. nslookup查询解析qq邮件服务器的域名和对应的IP地址，附截图，并解释实验运行结果（提示利用mx类型字段）



1. 利用路由跟踪命令tracert，跟踪路由
2. 跟踪到达www.ynu.edu.cn的路由信息。附截图



1. 为什么能利用tracert跟踪路由信息，试查找资料说明原理。

答：Tracert跟踪路由，是路由跟踪实用程序，主要用于查看源端到目的端的路径信息，从而检测网络是否可达。tracert是基于ICMP协议来实现的，当网络出现故障时，可以使用tracert确定故障点

Tracert交互过程：

1.源端电脑向目的3.3.3.3发送一个UDP报文，TTL值为1，目的UDP端口号大于30000的随机端口

2.对端第一跳收到源端发送的UDP报文后，判断报文目的IP地址不是本机地址，将TTL值减1，TTL值等于0后，则丢弃报文，并向源端发送一个ICMP超时的报文，这样源端便得到了第一跳网络设备的地址

3.该报文会发送3次，每次的交互流程一致，源端以发出与接收的时间间隔来判断对应的延时情况，并回显tracert界面中

4.源端收到第一跳节点发送的ICMP超时报文后，再次项目目的端发送一个TTL值是2的UDP报文

5.第二跳节点收到源端发送的UDP报文后，回应一个ICMP超时报文/端口不可达报文，这样源端就得到了该节点的地址，交互流程与第一跳一致（同样发送3次报文），只有当目的端收到源端发送的UDP报文之后，判断出目的IP地址与本机IP地址一致，则处理该报文，根据目的UDP端口号寻找对应的上层协议，一般目的端没有该应用程序使用该端口号，所以会向源端返回一个目的端口不可达报文

6.源端收到ICMP端口不可达报文后，判断出UDP报文已经到达目的端，则停止tracert程序，从而得到了数据报文从源端到目的端的路径信息

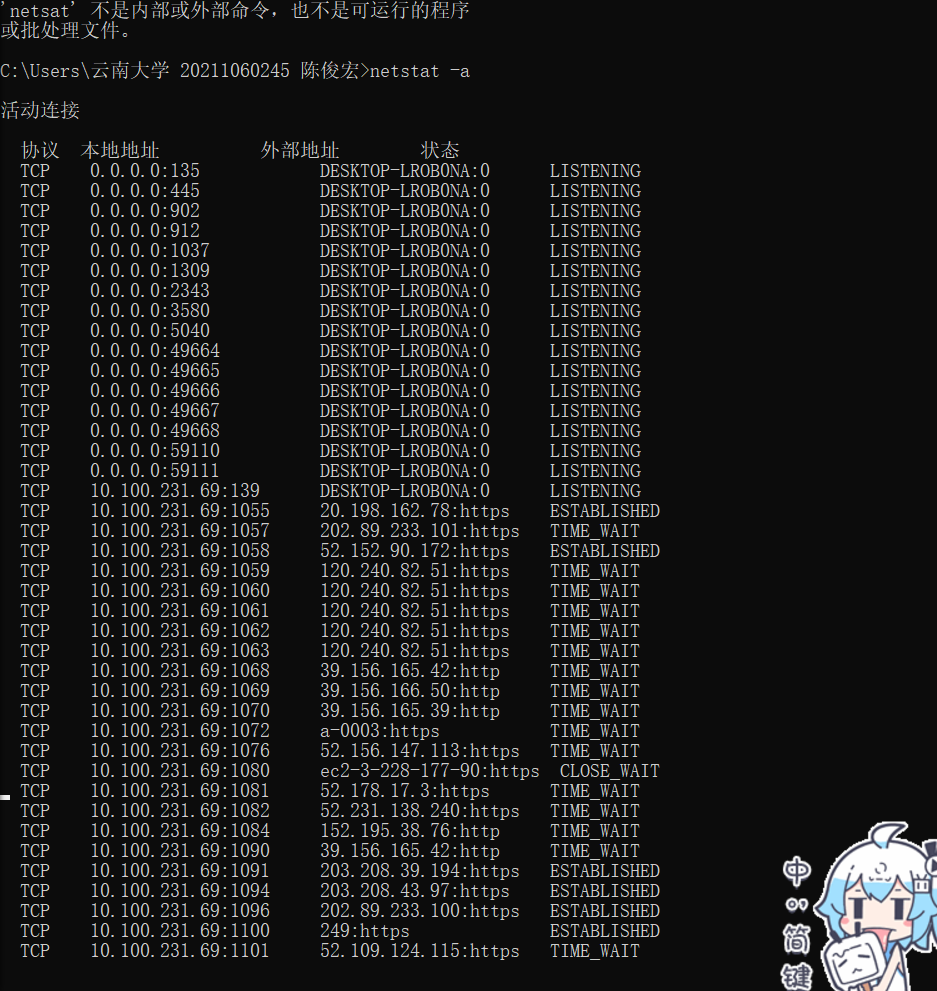
1. 解释截图每一列所代表的含义

答：1、最左侧的1,2,3,4,5，标明在我使用的宽带上，经过5个路由节点，可以到达[www.ynu.edu.cn](http://www.ynu.edu.cn)的服务；

2、中间的三列，单位是ms，表示我们连接到每个路由节点的速度，返回速度和多次链接反馈的平均值；

3、后面的IP，就是每个路由节点对应的IP。

1. netstat命令操作
2. 运行netstat命令查看本地活动连接情况,netstat -a，截图



1. TCP是一个面向连接的协议，要保存相应的连接状态，根据实验结果写出至少两种TCP连接状态，查找相应资料，解释是对应的何种状态。

答：LISTENING状态：侦听来自远方TCP端口的连接请求；

ESTABLISHED状态：代表一个打开的连接，数据可以传送给客户；

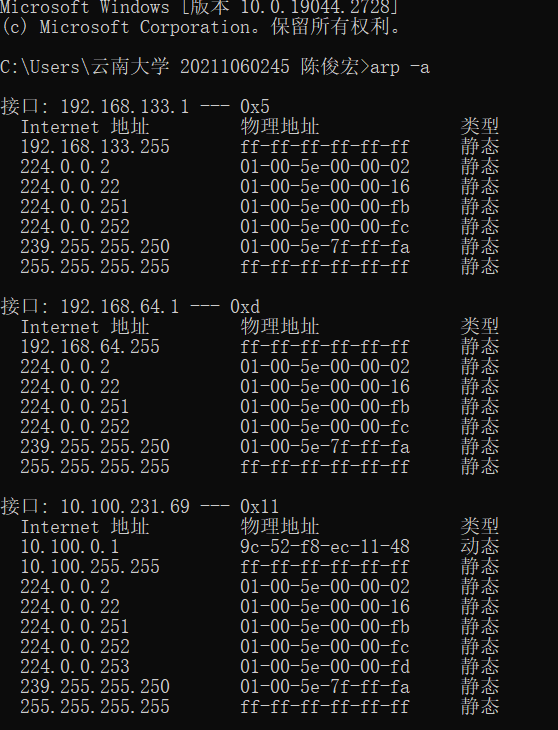
CLOSE\_WAIT状态：等待从本地用户发来的连接中断请求；

TIME\_WAIT状态：等待足够的时间确保远程TCP接受到连接中断请求的确认。

1. 在TCP连接中，我们可以看到IP地址后面用：分隔的一串数字，请问这串数字是什么？有什么作用？

答：IP地址后面用：分隔的一串数字指的是端口号。要想使网络中的计算机能够进行通信，必须为每台计算机指定一个标识号，通过这个标识号来指定接受数据的计算机或者发送数据的计算机。在TCP/IP协议中，这个标识号就是IP地址，它可以唯一标识一台计算机。通过IP地址可以连接到指定计算机，但如果想访问目标计算机中的某个应用程序，还需要指定端口号。在计算机中，不同的应用程序是通过端口号区分的。端口号是用两个字节（16位的二进制数）表示的，它的取值范围是0~65535，其中，0~1023之间的端口号用于一些知名的网络服务和应用，用户的普通应用程序需要使用1024以上的端口号，从而避免端口号被另外一个应用或服务所占用。

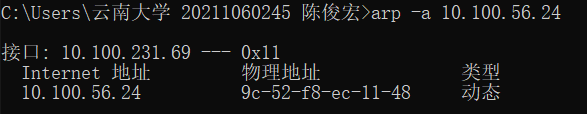
1. arp命令
2. 运行arp -a命令，查找本机ARP缓存的动态映射记录，附上**动态映射**的记录。



1. ping 本局域网上的一台主机A的IP，如能ping通，则找出此**动态映射**记录。

A主机的IP地址 10.100.56.24

含有此映射的截图



1. 实验总结
2. 在TCP/IP体系结构分为几层，每层有什么作用？为什么要分层？

答：TCP/IP体系结构分为四层，从上到下依次是应用层、传输层、网络层、数据链路层。

应用层：决定了向用户提供应用服务时通信的活动，将要进行的操作或者数据进行一个打包；

传输层：提供数据传输的方法，TCP（Transmission Control Protocol， 传输控制协议） 和 UDP（User Data Protocol，用户数据报协议）；

网络层：处理网络上流动的数据包，该层规定了以什么杨的路径进行数据的传送；

物理层：控制连接网络的一些硬件。操作系统、设备驱动、网卡、适配器、网线等。

因为计算机网络是一个非常复杂的系统。两台计算机之间的通信协调相当复杂。为了设计这样复杂的计算机网络，所以最早ARPANET设计计算机网络时，提出了分层的想法。

分层就是把庞大复杂的问题转化为若干个较小的局部问题，较小的局部问题旧比较容易研究和处理。当对网络进行分层之后，会产生诸多的好处：1、灵活性好。当任何一层发生变化时(例如由于技术的变化),只要层间接口关系保持不变，则在这层以上或以下各层均不受影响；2、结构上可分割开。各层都可以采用最合适的技术来实现。3、易于实现和维护。这种结构使得实现和调试一个庞大而又复杂的系统变得易于处理，因为整个的系统已被分解为若干个相对独立的子系统。

1. 通过实验我们可以发现在进行网络通信中会牵扯到很多地址，实验中都用到了哪些地址，思考这些地址分别对应TCP/IP协议栈哪一个层次。

答：实验中用到了IPv4地址、IPv6地址、物理地址和DNS服务器地址等，IP协议些地址对应TCP/IP协议栈中的网络层，物理地址对应了TCP/IP协议栈中的数据链路层，DNS服务器地址对应了TCP/IP协议栈中的应用层。