实验指导书

专业班级_____ 学号 _____ 姓名_____日期_____
课程名称_计算机网络基础_____实验（3）_____常用的 TCP/IP 网络命令_____

一、 实验目的：

1、 查看 windows 环境下 IP 地址的配置方式
2、 熟悉 windows 环境下的常用网络命令；
3、 掌握常用命令及其用法；
4、掌握 IP 网络连通性测试方法。
5、利用网络命令进行一般故障的分析。

二、 实验环境和准备：

1、 实验环境：联网的计算机网络实验室；
2、 实验时数：2 学时；
3、 实验准备：
   1） 阅读教材关于常用网络命令方面的相关内容；
   2） 预习实验指导书，了解网络命令的基础知识。

三、 实验内容：

（一）、以图形化的方式查看当前网络的配置：

在控制面板上，选中“网络和 Internet”，选择“以太网”，之后选择“更改适配器选项”，右键“以太网”，选择“属性”，如下图：

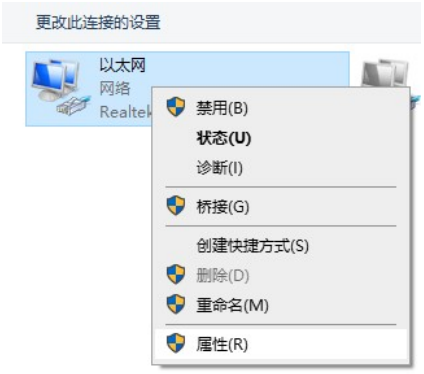


图 1

a) 请同学们自己截图你当前的网络连接对话框的内容：

b) 设想一下，你如果通过无线网络上网，在该对话框内会有“无线网络连接”图标

c) 如果你通过电信的宽带连接，在该对话框内会有“宽带连接”图标

选中“本地连接”，右键“属性”，弹出“本地连接”属性对话框

d) 请同学们自己截图你当前的本地连接属性对话框的内容，该本地连接已经安装的组件是，用自己的话回答：

e)在上图中选中“Internet 协议（TCP/IP）”，单击属性，弹出 TCP/IP 的配置，如下图

请同学们自己截图你当前 TCP/IP 的配置内容：用自己的话概括 TCP/IP 的配置有几种方式，分别是，在配置 TCP/IP 时需要指定哪些参数？

f)你设想一下，若网络中采用自动获取 IP 地址，DHCP 服务器需要配置哪些内容，各客户端的 PC 机才能获取上述内容？

g)在右键“我的电脑”点击“属性”，---网络标识，查看自己的

工作组=
计算机名是=

(二)、常用网络命令简介

下面这些命令的使用要在“命名提示符”窗口下进行，进入“命名提示符”窗口的方法，“开始”--→“运行”--→输入 cmd

1. ipconfig

ipconfig 命令以窗口的形式显示本机 IP 协议的具体配置信息。命令可以显示网络适配器的物理地址、主机的 IP 地址、子网掩码以及默认网关等，还可以查看主机名、DNS 服务器、节点类型等相关信息。其中网络适配器的物理地址在检测网络错误时非常有用。

1) 命令格式：

ipconfig [/? | /all | /release [adapter] | /renew [adapter]
| /flushdns | /registerdns
| /showclassid adapter
| /setclassid adapter [classidtoset]]

2) 主要参数含义：

- /all 显示所有的有关 IP 地址的配置信息；
- /renew 对于使用动态获取 ip 的主机重新获取一次 ip 地址

3) **练习示例**：ipconfig 可以只显示 IP 地址、子网掩码和每个网卡的默认网关值。如：

C:\>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

Connection-specific DNS Suffix . :
IP Address. . . . . : 172.17.9.178 //IP 地址
Subnet Mask . . . . . : 255.255.255.0 //子网掩码
Default Gateway . . . . . : 172.17.9.254 //缺省网关

C:\>ipconfig /displaydns //显示本机上的 DNS 域名解析列表

C:\>ipconfig /flushdns //删除本机上的 DNS 域名解析列表

4) 输入 ipconfig/all，其结果，截图，简要说出截图显示的内容

2. PING

PING 是测试网络联接状况以及信息包发送和接收状况非常有用的工具，是网络测试最常用的命令。PING 向目标主机（地址）发送一个回送请求数据包，要求目标主机收到请求后给予答复，从而判断网络的响应时间和本机是否与目标主机联通。

1) 基本命令格式：

PING IP 地址或主机名 [-t] [-n count] [-l size]

2) 基本参数含义：

- -t 不停地向目标主机发送数据；
- -n count 指定要 PING 多少次，具体次数由 count 来指定 ；
- -l size 指定发送到目标主机的数据包的大小。

3) 完整命令格式：

PING [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list

4) 完整命令参数：

- -t PING 指定的计算机直到中断。
- -a 将地址解析为计算机名。
- -n count 发送 count 指定的 ECHO 数据包数。默认值为 4。
- -l length 发送包含由 length 指定的数据量的 ECHO 数据包。默认为 32 字节；最大值是 65,527。
- -f 在数据包中发送“不要分段”标志。数据包就不会被路由上的网关分段。
- -i ttl 将“生存时间”字段设置为 ttl 指定的值。
- -v tos 将“服务类型”字段设置为 tos 指定的值。
- -r count 在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少 1 台，最多 9 台计算机。
- -s count 指定 count 指定的跃点数的时间戳。
- -j computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。
- -k computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。
- -w timeout 指定超时间隔，单位为毫秒。
- destination-list 指定要 PING 的远程计算机。

5) 较一般的用法是通过下面的操作来验证本地网络的连通性

a) ping 127.0.0.1 验证本机 TCP/IP 协议是否安装好，其结果截图：

b) ping 本机 IP 验证用户本机 IP 地址是否配置完成或者网卡物理属性是否完好，其结果截图：

c) Ping 网关 IP 验证从用户主机到网关的物理线路是否连通，其结果截图：

d) **你也可以 ping 域名，自己练习，**其结果也截图：

PING www.zju.edu.cn

例如：

C:\>ping www.zju.edu.cn

Pinging www.zju.edu.cn [218.75.70.222] with 32 bytes of data:

Reply from 218.75.70.222: bytes=32 time=4ms TTL=55

Reply from 218.75.70.222: bytes=32 time=4ms TTL=55

Reply from 218.75.70.222: bytes=32 time=4ms TTL=55

Reply from 218.75.70.222: bytes=32 time=4ms TTL=55

Ping statistics for 218.75.70.222:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

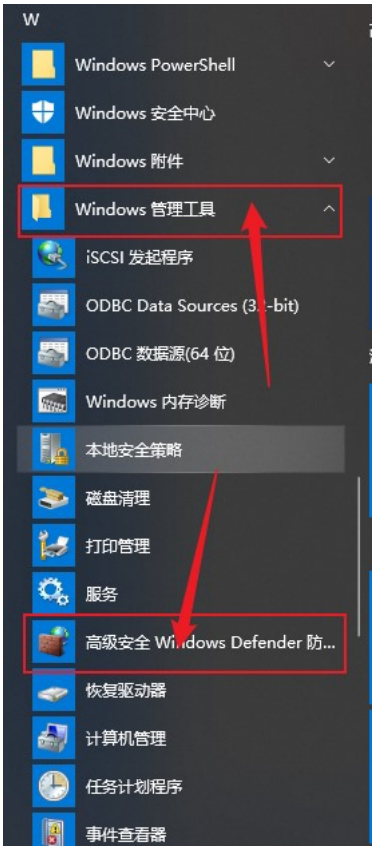
Approximate round trip times in milli-seconds:

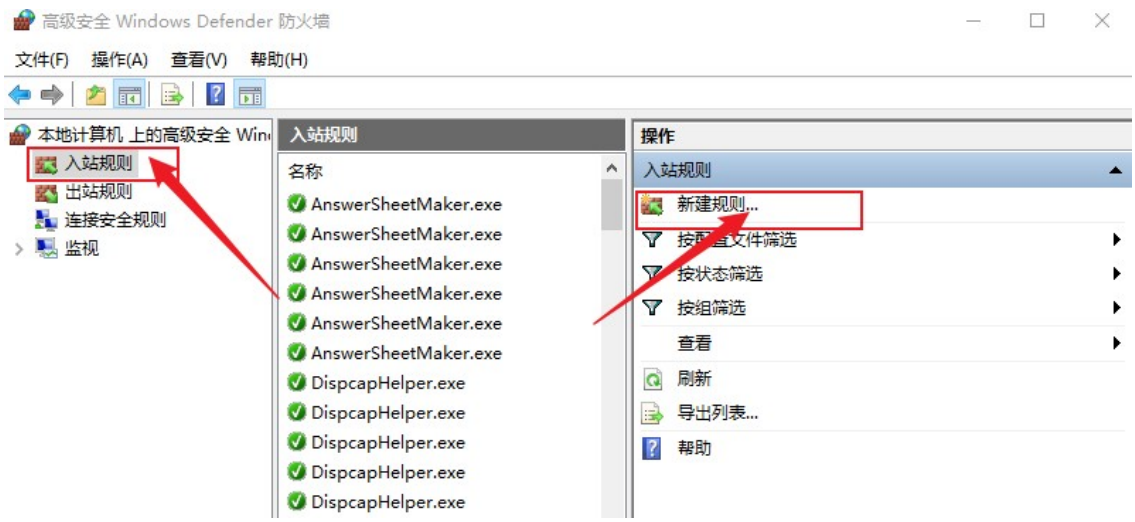
Minimum = 4ms, Maximum = 4ms, Average = 4ms

2.1 win10 开启 ICMP 防火墙规则

Windows10 由于使用了安全等级更高的防火墙，默认禁止 icmp 数据包通过，需要通过如下步骤开启：

在“开始菜单”下找到“windows 管理工具”选择“高级安全 windows defender 防火墙”




高级安全 Windows Defender 防火墙
文件(F) 操作(A) 查看(V) 帮助(H)
本地计算机 上的高级安全 Win
入站规则
出站规则
连接安全规则
监视
入站规则
名称
AnswerSheetMaker.exe
DispcapHelper.exe
操作
入站规则
新建规则...
按配置文件筛选
按状态筛选
按组筛选
查看
刷新
导出列表...
帮助


规则类型
选择要创建的防火墙规则类型
步骤:
规则类型
程序
协议和端口
作用域
操作
配置文件
名称
要创建的规则类型
程序(P)
控制程序连接的规则。
端口(O)
控制 TCP 或 UDP 端口连接的规则。
预定义(E):
@FirewallAPI.dll,-80200
控制 Windows 体验功能连接的规则。
自定义(C)
自定义规则。


新建入站规则向导
协议和端口
指定应用此规则的协议和端口。
选择icmpV4
步骤:
规则类型
程序
协议和端口
作用域
操作
配置文件
名称
此规则应用于哪些端口和协议?
协议类型(P):
ICMPv4
协议号(U):
本地端口(L):
所有端口
示例: 80, 443, 5000-5010
远程端口(R):
所有端口
示例: 80, 443, 5000-5010
Internet 控制消息协议(ICMP)设置:
自定义

3. ARP

ARP 是一个重要的 TCP/IP 协议，用于确定对应 IP 地址的网卡物理地址。利用 ARP 命令，我们能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容；也可以用人工方式静态绑定某个主机的 IP 地址和 MAC 地址，避免 ARP 病毒攻击，减少网络通信量。

1) **命令格式：** ARP [-a] [-s] [-d]

2) **参数含义：**

- -a 用于查看 ARP 高速缓存中的所有项目
- -s 向 ARP 高速缓存中人工输入一个静态项目，也就是通常我们所说的绑定
- -d 使用本命令能够人工删除静态条目。

3）练习例子：下面的操作截图，截你自己本机显示的结果

a)C:\>arp –a （显示当前所有的表项），

Interface: 172.17.9.178 --- 0x2

Internet Address	Physical Address	Type	
172.17.9.251	00-b0-d0-d1-8c-12	dynamic	//物理地址为 6 个字节
172.17.9.253	00-11-25-3f-97-97	dynamic	
172.17.9.254	00-0a-8b-99-c8-0a	dynamic	

b)添加 ARP 动态表项，执行 ping 命令向一个站点发送消息，可以将这个站点的 IP 地址与 MAC 地址的映射关系加入到 ARP 表中，再次执行 arp –a 命令，观察 ARP 表有无变化，这个操作过程截图。

c) 对你当前网络中默认网关实现静态绑定，命令类似如下

C:\>arp -s 172.17.9.254 00-0a-8b-99-c8-0a 静态绑定

(可以再打入 arp –a 验证是否已经加入)

3.1 win10 更新部分

由于 win10 更新了网络安全策略导致类似

arp -s 172.17.61.254 28-6e-d4-8d-59-50（这种方式失败）

win 使用方法如下：

netsh i i show in （查看当前网络的 IDX）

netsh -c "i i" add neighbors 6 "172.17.61.254" "28-6e-d4-8d-59-56"

命令中 6 为上方查询出的 id，每台主机可能不同，要根据自己实际查询结果操作。

4. netstat

Netstat 命令可以帮助网络管理员了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息，例如：显示网络连接、路由表和网络接口信息，可以统计目前总共有哪些网络连接正在运行。

利用命令参数，命令可以显示所有协议的使用状态，这些协议包括 TCP 协议、UDP 协议以及 IP 协议等，另外还可以选择特定的协议并查看其具体信息，还能显示所有主机的端口号以及当前主机的详细路由信息。

1） 命令格式：

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]

2） 参数含义：

- -a 显示所有连接和侦听端口。服务器连接通常不显示。
- -e 显示以太网统计。该参数可以与 -s 选项结合使用。
- -n 以数字格式显示地址和端口号（而不是尝试查找名称）。
- -s 显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。
- -p protocol 显示由 protocol 指定的协议的连接；protocol 可以是 tcp 或 udp。如果与 -s 选项一同使用显示每个协议的统计，protocol 可以是 tcp、udp、icmp 或 ip。
- -r 显示路由表的内容。
- Interval 重新显示所选的统计，在每次显示之间暂停 interval 秒。按 CTRL+B 停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

3）练习示例：，自己截图

C:\>netstat -as

IP Statistics

Packets Received = 256325

…

ICMP Statistics

	Received	Sent
Messages	16	68

…

TCP Statistics

…

Segments Received = 41828

UDP Statistics

Datagrams Received = 82401

…

5. Tracert

Tracert 命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间。命令功能同 PING 类似，但它所获得的信息要比 PING 命令详细得多，它把数据包所走的全部路径、节点的 IP 以及花费的时间都显示出来。该诊断实用程序将包含不同生存时间（TTL）值的 Internet 控制消息协议（ICMP)数据包发送到目标，以决定到达目标采用的路由。要在转发数据包上的 TTL 之前至少递减 1，必需路径上的每个路由器，所以 TTL 是有效的跃点计数。数据包上的 TTL 到达 0 时，路由器应该将“ICMP 已超时”的消息发送回源系统。Tracert 先发送 TTL 为 1 的回显数据包，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。路由通过检查中级路由器发送回的“ICMP 已超时”的消息来确定路由。不过，有些路由器可能丢弃包含过期 TTL 值的数据包，而 tracert 看不到。

1） **命令格式：**

tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name

2） **基本参数：**

- -d 指定不将地址解析为计算机名。
- -h maximum_hops 指定搜索目标的最大跃点数。
- -j computer-list 指定沿 computer-list 的稀疏源路由。
- -w timeout 每次应答等待 timeout 指定的微秒数。
- target_name 目标计算机的名称。

3） **练习示例：，自己截图**

最简单的一种用法如下：

C:\>tracert -d www.qz.zj.cn

Tracing route to www.qz.zj.cn [202.96.113.8]

over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	172.17.9.254
2	<1 ms	<1 ms	<1 ms	172.16.1.100
3	<1 ms	1 ms	<1 ms	61.153.55.69
4	1 ms	1 ms	<1 ms	202.96.113.8

Trace complete.

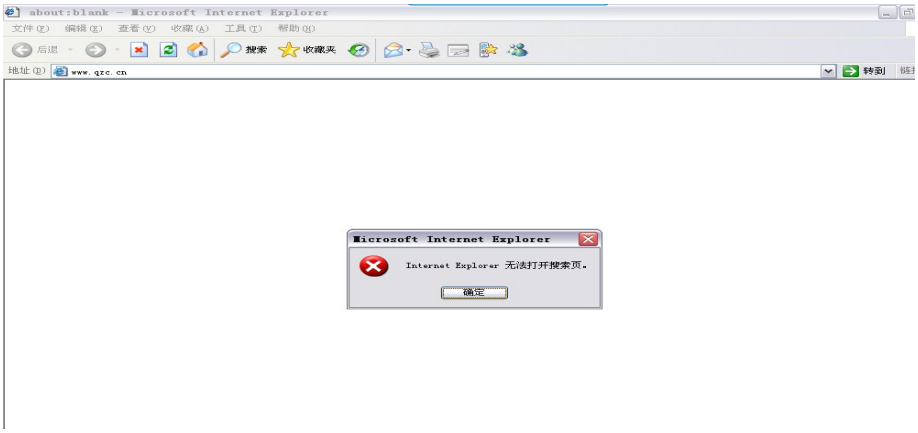
（四）. 实验要求：

1、通过实验熟悉上述 5 个常用网络命令的基本用法；

2、完成下面进阶练习：利用网络命令排解故障

当在一个局域网中突然发现我们的网络出现了中断，而物理层的设备经过检查又完全正常的情况下，这时我们就需要一些网络命令进行网络错误的排查。下面我们模拟一次网络排查的经过：利用 arp －s 完成错误的网关、DNS 的 IP 和 MAC 地址的绑定。

1）、打开 ie，发现不能上网了：



2）、首先检查本机的 ip 地址配置信息：我们用到了 ipconfig 命令：

```
C:\Documents and Settings\陈>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.17.9.178
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.17.9.254
```

3）、这样，我们得到了网关的 ip 信息：172.17.9.254，然后运用 PING 命令，查看我们与网关的连接是否正常：

```
C:\Documents and Settings\陈>ping 172.17.9.254

Pinging 172.17.9.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.9.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

4）、从 icmp 包回馈的信息我们看到，本机到网关包全部 loss，说明问题基本锁定在了 172.17.9.0 这个网段的内部.接下来，我们用 ARP 命令查看 ip 和 mac 的对应关系表：

```
C:\Documents and Settings\陈>arp -a

Interface: 172.17.9.178 --- 0x20002
  Internet Address      Physical Address      Type
  172.17.9.253          00-11-25-3f-97-97     dynamic
  172.17.9.254          c0-cc-8b-29-18-01     static
```

5）、运用 ARP-a 命令之后我们发现了问题：网关的 ip mac 被绑定了，而且绑定了错误的 mac 地址，这有两种可能性，1、人为操作失误造成的 2、网络病毒发作造成的。于是，我们又用 ARP-d 这条命令删除了 ARP 缓存中的所有记录：

```
C:\Documents and Settings\陈>arp -d

C:\Documents and Settings\陈>arp -a

Interface: 172.17.9.178 --- 0x20002
  Internet Address      Physical Address      Type
  172.17.9.254          00-0a-8b-99-c8-0a     dynamic
```

6)、接下来继续 PING 网关 ip 地址：

```
C:\Documents and Settings\陈>ping 172.17.9.254

Pinging 172.17.9.254 with 32 bytes of data:

Reply from 172.17.9.254: bytes=32 time<1ms TTL=255
Reply from 172.17.9.254: bytes=32 time<1ms TTL=255
Reply from 172.17.9.254: bytes=32 time<1ms TTL=255
Reply from 172.17.9.254: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.9.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7)、说明问题得以排除，本机和网关之间的连接得到修复。打开浏览器，上网正常。

四、思考题：

1、 结合本实验中进阶实验内容，概括总结出现网络故障时，可使用哪些命令进行初步的故障侦查，给出一般的流程。