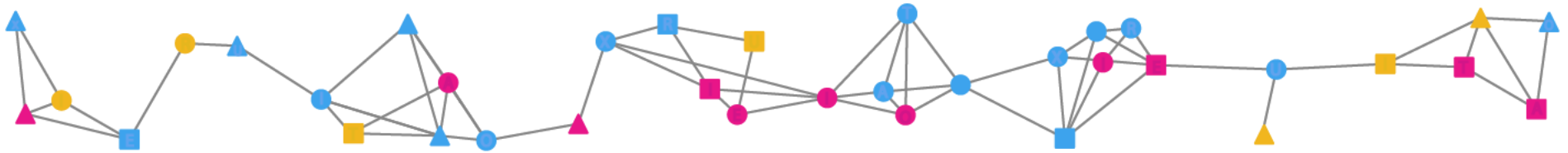


计算机网络

实验二 常用的网络命令

谢瑞桃
xie@szu.edu.cn
rtxie.github.io
计算机与软件学院
深圳大学

实验二 常用的网络命令

- 实验目的
  - 了解ping、ipconfig 、netstat、tracert、ARP、route、nslookup等常用网络工具的功能以及使用方法，并通过这些工具发现或者验证网络中的故障。

- 实验环境
  - 使用具有Internet连接的Windows操作系统。
  - Windows PowerShell 或者 Windows命令提示符(cmd.exe)，二选一。

实验内容

使用以下七种网络调试工具分析网络情况。

1. ipconfig
2. ping
3. netstat
4. tracert
5. ARP
6. nslookup
7. route

实验任务要求

- 请参考本讲义学习七种网络调试工具
- 理解每种工具的用途，以及使用方法
- 使用每种工具的各种指令
- 依照步骤完成实验内容1—7
- 对实验结果截图
- 撰写实验报告

实验报告撰写要求

- 使用教务处制作的实验报告模板
- 注意按进度填写实验时间和实验报告提交时间
- 填写模板中的每一部分
- 填写实验步骤时，做到条理清晰
- 注意截图清晰、美观
- 要求在演示操作步骤的截图上加标注，指出操作步骤和操作结果，没有会被扣分
- 实验报告只有截图，没有文字说明讲解会扣分
- 实验结果要有原理分析，否则会被扣分
- 出现一模一样的实验报告，均得零分

注意事项

- 如果提示“请求的操作需要提升”或“The requested operation requires elevation”，说明你没有权限运行该指令。你可以退出终端，选择“以管理员身份运行”该终端。

实验内容

1. ipconfig
2. ping
3. netstat
4. tracert
5. ARP
6. nslookup
7. route

1. ipconfig 简介

- ipconfig 可用于显示主机当前的IPv6地址、 IPv4地址、 子网掩码和默认网关。

1. ipconfig 使用方法

1) ipconfig

- 当不带任何参数选项使用时，它显示每个接口的IP地址、子网掩码和默认网关。

2) ipconfig /all

- 当使用all选项时，显示完整配置信息，包括DNS 服务器、DHCP服务器、IP地址获得租约的时间、IP地址租约过期的时间等。

3) ipconfig /release

- 释放（归还）所有接口的租用IPv4地址。

4) ipconfig /renew

- 更新所有接口的IPv4地址。多数情况下网卡将被重新赋予和以前所赋予的相同的IP地址，但租约过期时间会更新。

实验内容

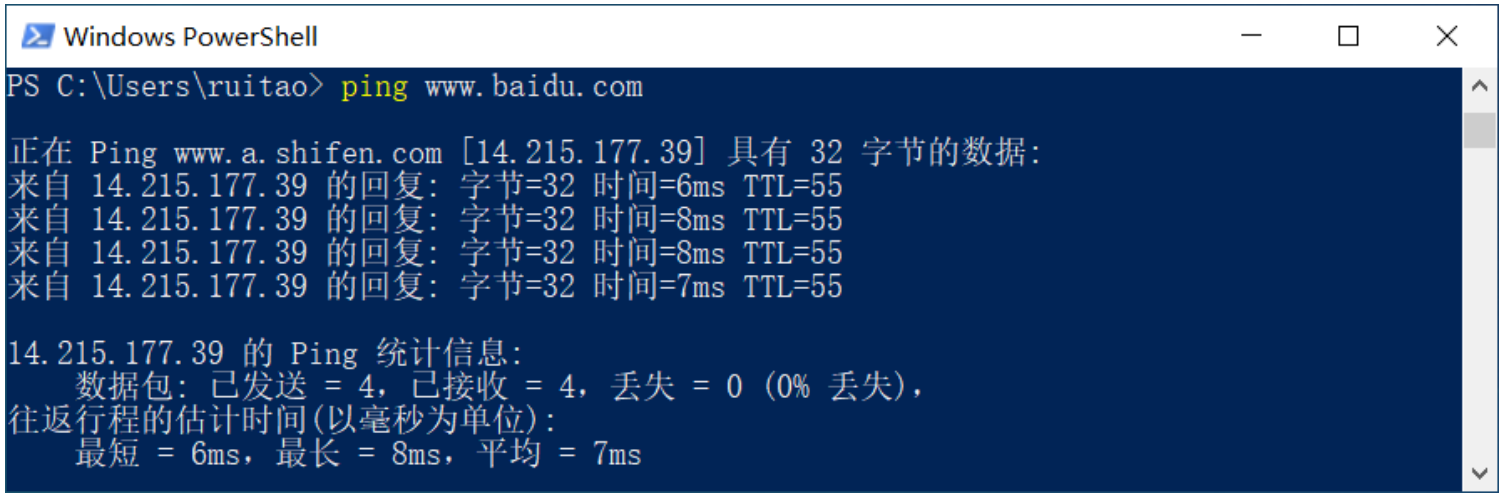
1. ipconfig
2. ping
3. netstat
4. tracert
5. ARP
6. nslookup
7. route

2. ping 简介

- ping是一个测试程序，用于确定本地主机是否能与另一台主机发送或接收数据报。如果ping运行正确，就可以排除发送与接收方网络层以下的故障。

2. ping 简介

- 按缺省设置，运行ping命令时发送4个ICMP（网络控制报文协议）回显请求，每个含32字节数据。若正常，应收到4个回显应答。
- ping显示发送回显请求到收到回显应答之间的时间间隔，单位为毫秒。



2. ping 简介

- ping 还能显示TTL（Time To Live），即生存时间。
- 通过TTL值推算数据报已经通过了多少个路由器：“TTL起始值”减去所接收的回显应答中的“TTL值”。
- “TTL起始值”是多少呢?
  - 比返回TTL稍大的一个2的次方数。

2. ping 简介

- 不同的操作系统中“TTL起始值”不同。

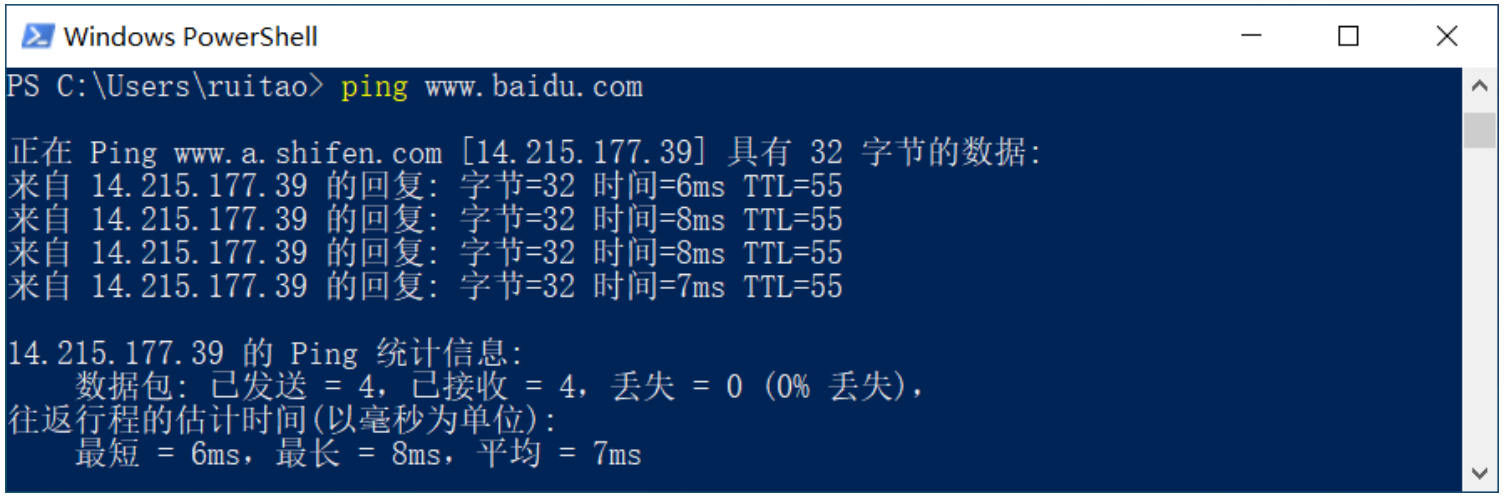
https://web.archive.org/web/20150206054041/http://www.binbert.com/blog/2009/12/default-time-to-live-ttl-values/

OS/Device	Version	Protocol	TTL
AIX		TCP	60
AIX		UDP	30
AIX	3.2, 4.1	ICMP	255
BSDI	BSD/OS 3.1 and 4.0	ICMP	255
Compa	Tru64 v5.0	ICMP	64
Cisco		ICMP	254
DEC Pathworks	V5	TCP and UDP	30
Foundry		ICMP	64
FreeBSD	2.1R	TCP and UDP	64
FreeBSD	3.4, 4.0	ICMP	255
FreeBSD	5	ICMP	64
HP-UX	9.0x	TCP and UDP	30
HP-UX	10.01	TCP and UDP	64
HP-UX	10.2	ICMP	255
HP-UX	11	ICMP	255
HP-UX	11	TCP	64
Irix	5.3	TCP and UDP	60
Irix	6.x	TCP and UDP	60
Irix	6.5.3, 6.5.8	ICMP	255
juniper		ICMP	64
MPE/IX (HP)		ICMP	200
Linux	2.0.x kernel	ICMP	64
Linux	2.2.14 kernel	ICMP	255
Linux	2.4 kernel	ICMP	255
Linux	Red Hat 9	ICMP and TCP	64
MacOS/MacTCP	2.0.x	TCP and UDP	60
MacOS/MacTCP	X (10.5.6)	ICMP/TCP/UDP	64
NetBSD		ICMP	255
Netgear FVG318		ICMP and UDP	64
OpenBSD	2.6 & 2.7	ICMP	255
OpenVMS	07.01.2002	ICMP	255
OS/2	TCP/IP 3.0		64
OSF/1	V3.2A	TCP	60
OSF/1	V3.2A	UDP	30
Solaris	2.5.1, 2.6, 2.7, 2.8	ICMP	255
Solaris	2.8	TCP	64
Stratus	TCP_OS	ICMP	255
Stratus	TCP_OS (14.2-)	TCP and UDP	30
Stratus	TCP_OS (14.3+)	TCP and UDP	64
Stratus	STCP	ICMP/TCP/UDP	60
SunOS	4.1.3/4.1.4	TCP and UDP	60
SunOS	5.7	ICMP and TCP	255
Ultrix	V4.1/V4.2A	TCP	60
Ultrix	V4.1/V4.2A	UDP	30
Ultrix	V4.2 – 4.5	ICMP	255
VMS/Multinet		TCP and UDP	64
VMS/TCPware		TCP	60
VMS/TCPware		UDP	64
VMS/Wollongong	1.1.1.1	TCP	128
VMS/Wollongong	1.1.1.1	UDP	30
VMS/UCX		TCP and UDP	128
Windows	for Workgroups	TCP and UDP	32
Windows	95	TCP and UDP	32
Windows	98	ICMP	32
Windows	98, 98 SE	ICMP	128
Windows	98	TCP	128
Windows	NT 3.51	TCP and UDP	32
Windows	NT 4.0	TCP and UDP	128
Windows	NT 4.0 SP5-		32
Windows	NT 4.0 SP6+		128
Windows	NT 4 WRKS SP 3, SP 6a	ICMP	128
Windows	NT 4 Server SP4	ICMP	128
Windows	ME	ICMP	128
Windows	2000 pro	ICMP/TCP/UDP	128
Windows	2000 family	ICMP	128
Windows	Server 2003		128
Windows	XP	ICMP/TCP/UDP	128

1. TTL起始值为比接收TTL稍大的一个2的次方数，这种推测不一定对。
2. 255是最大值，因为TTL字段最多8位。

2. ping 简介

- 举例：返回TTL值为55，那么可以推算发送方(14.215.177.39)数据报的TTL值为64，经过9个路由器(64-55)，最终到达接收方。
- 注意传输方向：192.168.2.178<——14.215.177.39



2. ping使用方法

1) ping 127.0.0.1

- 这个Ping命令被送到本地计算机的IP协议层。如果出错，则表示TCP/IP的安装或运行存在某些问题。

2) ping 本机IP （通过ipconfig查询）

- 这个命令被送到本计算机所配置的IP地址。如果出错，则表示本地配置或安装存在问题。

3) ping 网关IP（通过ipconfig查询）

- 这个命令如果应答正确，表示局域网中的网关路由器正在运行并能够作出应答。

2. ping使用方法

4) ping 某个域名 (例如www.baidu.com)

- 对某个域名执行Ping命令，本地计算机必须先通过DNS服务器将域名转换成IP地址。如果出现故障，则表示DNS服务器的IP地址配置不正确或DNS服务器有故障。

5) ping 远程IP

- 如收到4个应答，表示成功使用了缺省网关。对于拨号上网用户则表示能够成功的访问Internet（但不排除ISP的DNS会有问题）。

2. ping使用方法

6) ping命令的常用参数选项:

- `ping IP -t`

连续对IP地址执行Ping命令，直到被用户以Ctrl + C中断。

- `ping IP -l size`

指定Ping命令中的数据长度为size字节，缺省为32字节。

- `ping IP -n count`

执行count次数的Ping命令，缺省为4次。

7) Ping命令的参数用法查询：`ping`

8) 请利用TTL计算源节点与目的节点之间的路由器数量。

实验内容

1. ipconfig
2. ping
3. netstat
4. tracert
5. ARP
6. nslookup
7. route

3. netstat 简介和使用方法

- 用于显示与 IP、TCP、UDP 和 ICMP 协议的统计信息，用于检验本机各端口网络连接情况。

1）`netstat -s`

- 显示每个协议的统计信息。默认情况下，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息。

2）`netstat -e`

- 显示以太网统计信息。

3. netstat使用方法

3) netstat -r

- 显示路由表，以及接口列表。

4) netstat -a

- 显示所有连接和侦听端口。所显示的状态有：已建立（ESTABLISHED）、正在监听（LISTENING）、TCP握手（SYN_SENT）等。

5) netstat -n

- 显示所有活动连接，并且以数字形式显示地址和端口号。

实验内容

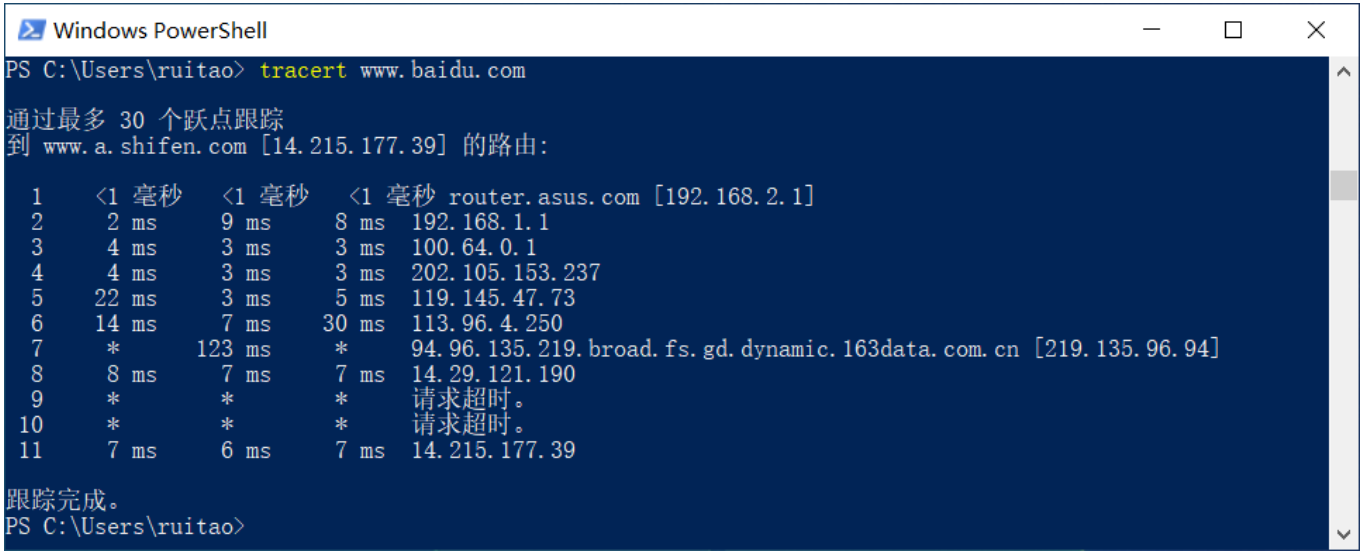
1. ipconfig
2. ping
3. netstat
4. tracert
5. ARP
6. nslookup
7. route

4. tracert 简介

- tracert命令可以用来跟踪数据报使用的路由(路径)，并列出所经过的每个路由器上所花费的时间。因此，tracert一般用来检测故障的位置。
- 用法：只需在tracert后面跟一个IP地址或主机名。
- 举例：`tracert www.baidu.com`
- 我们已经知道利用ping返回的TTL数可以计算两个节点之间经过了多少个路由器。请将该结果与tracert结果对比，看看是否一致。

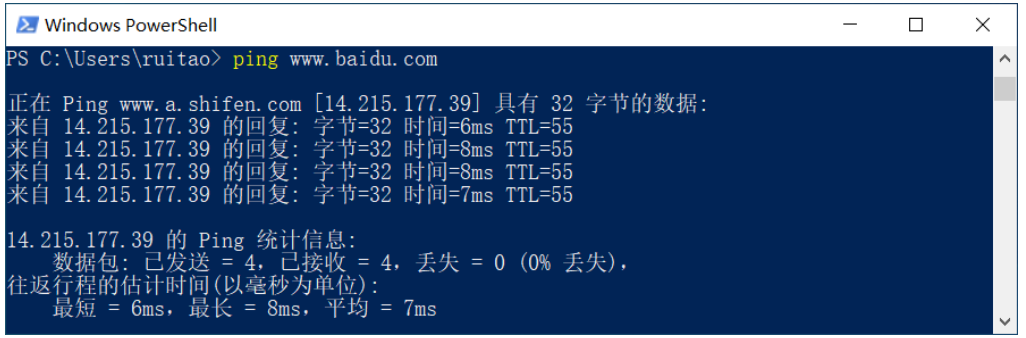
4. tracert 使用举例一

- 此次运行经过了10个IP路由器。其中前两个路由器位于局域网内，因为192.168.x.x是局域网私有地址。最后一行是所访问的Web服务器。
- 注意传输方向：192.168.2.178——>14.215.177.39

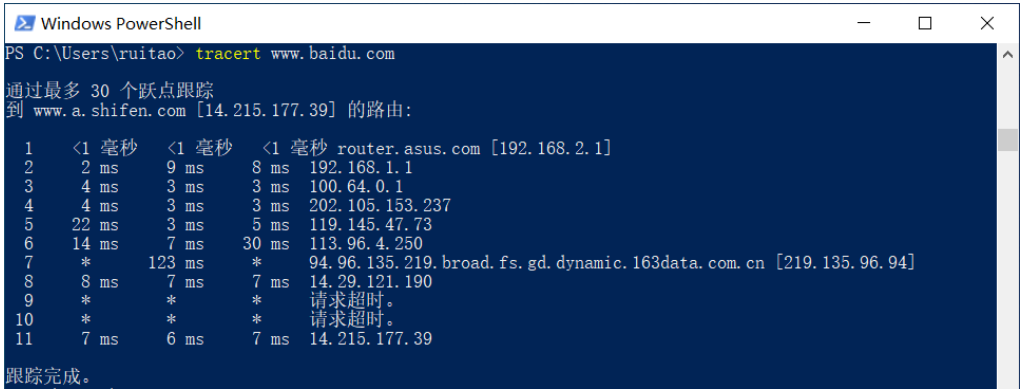


4. tracert 使用举例一

- 对比ping和tracert
- ping传输方向：192.168.2.178<——14.215.177.39
- 9个路由器



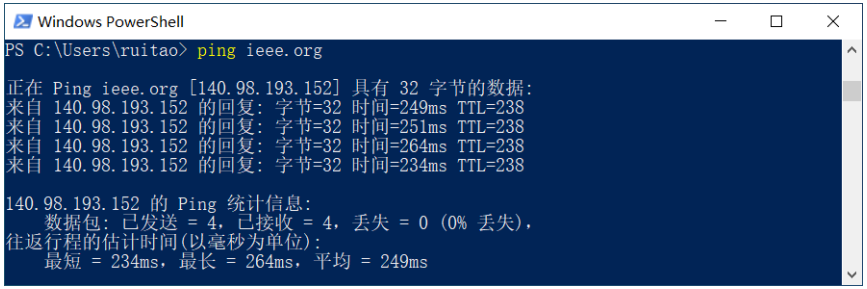
- tracert传输方向：192.168.2.178——>14.215.177.39
- 10个路由器



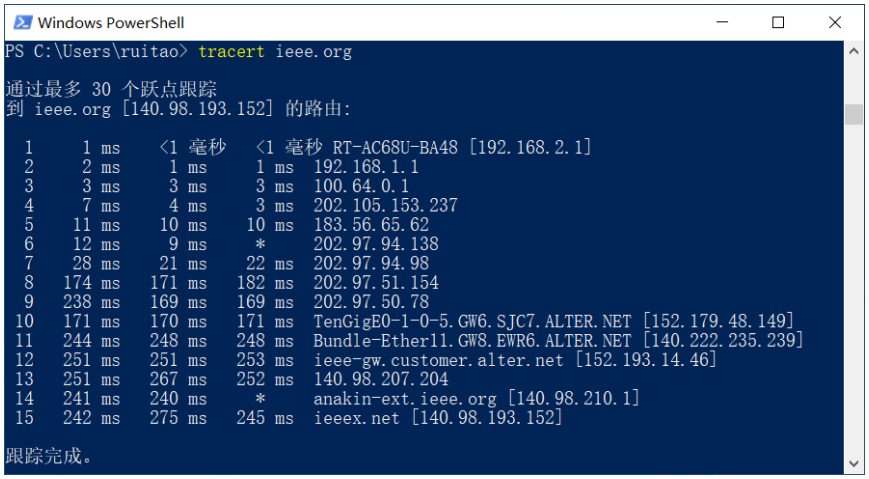
两个方向经过的路由很可能不同

4. tracert 使用举例二

- 对比ping和tracert
- ping传输方向：192.168.2.178<——140.98.193.152
- 255-238=17个路由器



- tracert传输方向：192.168.2.178——>140.98.193.152
- 14个路由器



两个方向经过的路由很可能不同

实验内容

1. ipconfig
2. ping
3. netstat
4. tracert
5. ARP
6. nslookup
7. route

5. ARP(地址转换协议) 简介

- 显示和修改地址解析协议(ARP)使用的“IP 到物理”地址转换表。
- ARP协议用于确定对应IP地址的网卡物理地址。

5. ARP使用方法

1) arp -a

- 通过询问当前协议数据，显示当前 ARP 项。如果不止一个网络接口使用 ARP，则显示每个 ARP 表的项。

2) arp -a inet_addr

- 如果有多个网卡，那么使用arp -a加上接口IP地址inet_addr，就可以只显示与该接口相关的ARP缓存项目。

5. ARP使用方法

3) `arp -d inet_addr`

- 删除 inet_addr 指定的主机对应的条目。
- 使用arp -a inet_addr检查是否删除成功。

4) `arp -s inet_addr eth_addr`

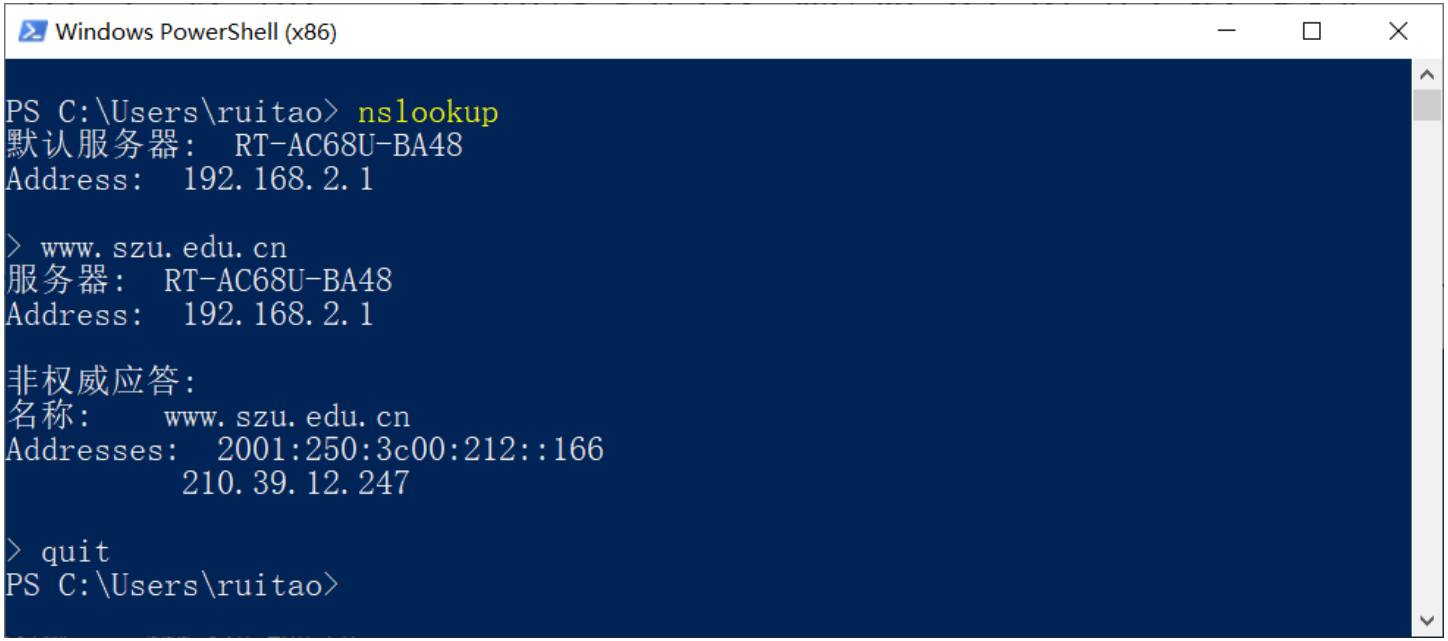
- 添加 Internet 地址 inet_addr 与物理地址 eth_addr 的关联条目。物理地址是用连字符分隔的 6 个十六进制字节。
- 请把之前删除的条目加回来，再用arp -a inet_addr检查是否添加成功。

实验内容

1. ipconfig
2. ping
3. netstat
4. tracert
5. ARP
6. nslookup
7. route

6. nslookup 简介和使用方法

- 用于查询一台机器的IP地址对应的域名。
- 举例：



实验内容

1. ipconfig
2. ping
3. netstat
4. tracert
5. ARP
6. nslookup
7. route

7. route 简介和使用方法

操作网络路由表。

1) `route print`

- 观察路由表的构成。

2) `route delete inet_addr`

- 删除路由。
- 其中，inet_addr是“网络目标”ip地址。
- 请选择路由表里的一条路由信息，将其删除。
- 删除前请记录下来，稍后会用。
- 删除以后，请用route print查看是否成功。

7. route 使用方法

3) route add inet_addr_1 inet_addr_2

- 添加路由。
- 其中，inet_addr_1是网络目标IP地址， inet_addr_2是网关地址。
- 请添加之前删除的路由。
- 添加以后，请用route print查看是否成功。

恭喜你已完成实验