常用网络命令的认识与应用

一 实验目的

了解和掌握几个实用的网络命令会有助于更好地使用和维护网络，这里介绍 4 个基本的基于 windows 操作系统的网络命令。

二 实验内容

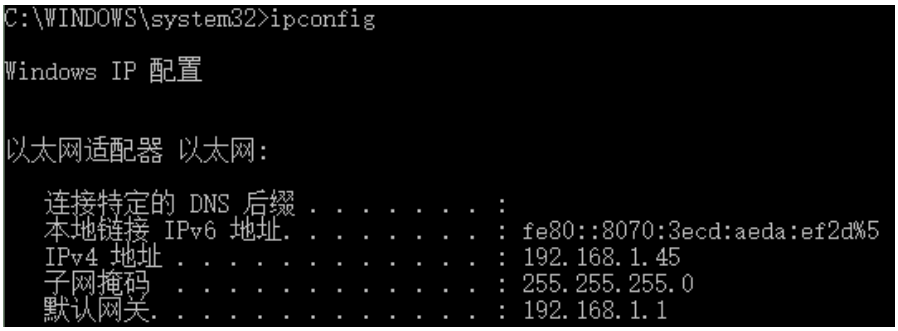
打开你自己电脑(Windows 操作系统)的命令提示符(cmd)。

1. ipconfig

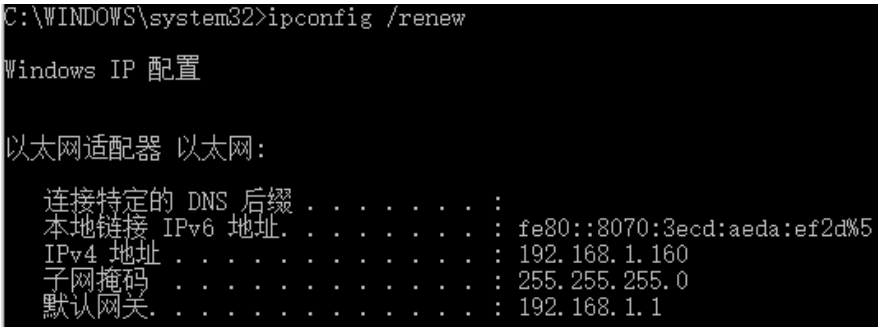
ipconfig 命令用来显示主机当前的 TCP/IP 协议的配置信息、刷新动态主机配置协议(DHCP) 和域名系统 (DNS) 设置。其常用的参数格式如下：

1. **ipconfig** ： 显示绑定到 TCP/IP 的适配器的 IP 地址、子网掩码和默认网关。
2. **ipconfig /?** ： 参数查询
3. **ipconfig /all** ： 显示本机 TCP/IP 配置的详细信息
4. **ipconfig /release** ： DHCP 客户端手工释放 IP 地址
5. **ipconfig /renew** ： DHCP 客户端手工向服务器刷新请求
6. **ipconfig /flushdns** ： 清除本地 DNS 缓存内容
7. **ipconfig /displaydns** ： 显示本地 DNS 内容
8. **ipconfig /registerdns** ： DNS 客户端手工向服务器进行注册

例如，我们可以通过 ipconfig 命令查看本机以太网适配器的相关信息：



我们还可以通过参数”release”和”renew”来释放和重新获取新的 ip 地址：



2. ping

ping 是一个最常用的网络连通性检查命令。ping 通过发送 4 个 echo_request 的 ICMP 数据包给目的主机（一定要记住 ping 是基于 ICMP 的哦）,并接收应答信息来确定两台计算机之间的网络是否连通。当网络运行中出现故障时，采用这个实用程序来预测故障和确定故障源是非常有效的。如果执行 ping 不成功，则可以预测故障出现在以下几个方面：网线是否连通，网络适配器配置是否正确，IP 地址是否可用等；如果执行 ping 成功而网络仍无法使用，那么问题很可能出在网络系统的软件配置方面。不过如果 ICMP 数据包因为某些原因(如防火墙的过滤)不能到达目的端或是目的端不能回答或是回应给挡下来了，Ping 也不能顺利完成，但并非代表网络连通故障。ping 成功只能保证当前主机与目的主机间存在一条连通的物理路径。其命令格式及参数含义如下：

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
-t ：Ping 指定的计算机直到手动中断(Ctrl+C)。
-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 size ：发送包含由 size 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 host-list :利用 host-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 host-list :利用 host-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。
-4、-6 ：表示强制使用 IPv4 或者 IPv6。
target_name：表示目标主机的名称或者 IP 地址。
```

例如，我们可以通过命令”ping www.baidu.com”测试本机是否可以连接外网；使用”-n”设置发送的 ECHO 数据包数量。

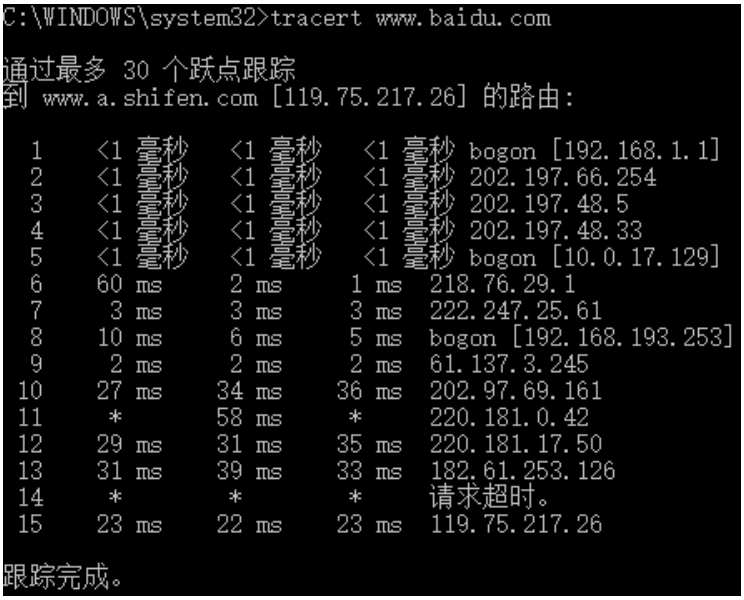
还有其他有趣的参数选项同学们可以在本机上进行有趣的尝试。

3. tracert

tracert 命令也是我们通常用到的 ICMP 程序工具，功能是判定数据包到达目的主机所经过的路径、显示数据包经过的中继节点清单和到达时间。tracert 命令对我们判断数据包的路由路线非常有用，命令格式及参数选项如下：

```
1. tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr]
   [-4] [-6] target_name
2. -d ：表示不将地址解析成主机名。
3. -h maximum_hops ：表示搜索目标的最大跃点数。
4. -j host-list ：表示与主机列表一起的松散源路由（仅适用于 IPv4）
5. -w timeout ：表示等待每个回复的超时间（以毫秒为单位）
6. -R ：表示跟踪往返行程路径（仅适用于 IPv6）
7. -S srcaddr ：表示要使用的源地址（仅适用于 IPv6）
8. -4、-6 ：表示强制使用 IPv4 或者 IPv6。
9. target_name ：表示目标主机的名称或者 IP 地址。
```

我们以命令”tracert www.baidu.com”为例，可以看到 192.168.1.1 是到达了我们的上行路由，然后 202.197.X.X 是中南大学的网段，10.0.17.129 是长沙教育网的内网，接下来的 4 个地址都是长沙电信机房的地址，然后经由中国电信的骨干网(202.97.69.161)就到达北京(220.181.X.X)了，直至最后到达百度的数据中心(119.75.217.26)。其中 IP 地址的相关信息可以在网站 http://ip.tool.chinaz.com/上进行查询。



Tracert 运行结果

查询 ip 地址信息

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，命令格式及参数含义如下:

```
1. netstat [-r] [-s] [-n] [-a]
2.
3. -r 显示本机路由表的内容;
4. -s 显示每个协议的使用状态(包括 TCP 协议、UDP 协议、IP 协议);
5. -n 以数字表格形式显示地址和端口;
6. -a 显示所有主机的端口号。
```

以参数-r 为例，我们可以查看本机路由表的内容：

大家可以把其他的参数都尝试一下，看看自己所在网络的整体使用情况。

三 思考

1. Linux 系统中类似于 ipconfig 的命令是什么？
2. 对于同一目的主机，tracert 命令所追踪到的路由路径是否都是完全一样的？为什么？
3. 根据各个命令所使用的协议尝试了解其工作原理。