实验报告

东北林业大学

信息与计算机科学技术实验中心

|  |
| --- |
| 一、实验目的  1、理解、验证常用网络命令的原理和功能。  2、掌握常用的网络命令使用方法，合理使用相关命令对网络进行管理与维护。 |
| 二、实验环境  计算机  windows7操作系统， |
| 三、实验内容及结果  内容：   1. 网络参数查询命令：IPCONFIG和IP地址相关计算 2. 网络测试命令：网络质量定性分析和网络故障检测 3. 路由表命令ROUTE 4. 网络端口查询命令：NETSTAT 5. 以太网络 ARP 表命令和MAC绑定 6. Tracert 追踪实验   具体要求：  1.IPCONFIG  阅读参考资料：按如下要求运行命令：  1）ipconfig /?  具体截图显示。  2）ipconfig  具体截图，并通过查阅解释默认网关的含义。  3）ipconfig /all  具体截图，本地网卡中的物理地址（mac）为多少？  2.PING命令  阅读参考资料：按如下要求运行命令：  1）ping 外网一台主机的IP（如ping www.baidu.com 可得到其IP地址再执行命令）;ping局域网一台主机的IP（旁边同学的）截图并对图中结果给与说明和解释。  2）ping 127.0.0.1 代表什么含义？  截图并对图中结果给与说明和解释。  3）ping 本机ip；  截图并对结果给与解释  将本机器的IP改成旁边同学机器IP，重新运行此命令。并解释结果。  4）ping 网关ip，截图。  5）ping /? 列表可供使用的参数。截图。  6）-t。引导ping继续测试远程主机直到按Ctrl+C中断该命令。验证截图。  7）-a。使ping -a命令就是可以通过ping它的IP地址,可以解析出主机名。这对解决DNS和Hosts文件问题是否有用？（hosts文件位置）  改过后ping [www.baidu1.com](http://www.baidu1.com)是什么结果。  8）-n count。缺省情况下，ping发送四个ICMP包到远程主机，可以使用-n参数指定被发送的包的数目。截图  9）-l length。使用-l参数指定ping传送到远程主机的ICMP包的长度。缺省情况下，ping 发送长度为32bytes的包，但是可指定最大字节数为8192bytes。截图。  10）-i ttl。设定Time To Live(存活时间)。用ttl 指定其值。（设置i，使其能访问本局域网，而访问外网基本会超时过期）。截图。  3.ROUTE命令  阅读学习材料，运行如下命令，截图并解释结果。  1）route print——本命令用于显示路由表中的当前项目，由于用ip地址配置了网卡，因此所有的这些项目都是自动添加的。截图验证。  2）delete——使用本命令可以从路由表中删除路由。  4.. 以太网络 ARP 表命令和MAC绑定  通过arp命令可以查看ARP高速缓存中的内容，可以清除缓存中的地址映射，建立新的地址映射常用命令选项：  1）arp -a用于查看高速缓存中的所有项目。  2）arp -a IP--如果你有多个网卡，那么使用arp -a加上接口的IP地址，就可以只显示与该接口相关的ARP缓存项目。  3）arp -s IP 物理地址——你可以向ARP高速缓存中人工输入一个静态项目。  4）arp -d IP--使用本命令能够人工删除一个静态项目。  5）如何绑定AMC地址和IP？（MAC绑定在校园网络中，最方便的捣乱方法就是盗用别人的IP地址，被盗用IP地址的计算机不仅不能正常使用校园网络，而且还会频繁出现IP地址被占用的提示对话框，给校园网络安全和用户应用带来极大的隐患。捆绑IP地址和MAC地址就能有效地避免这种现象。）  6. Tracert的使用  Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其它主机的路由。  命令格式：  tracert IP地址或主机名 [-d][-h maximumhops][-j host\_list] [-wtimeout]  参数含义：  -d 不解析目标主机的名字；  -h maximum\_hops 指定搜索到目标地址的最大跳跃数；  -j host\_list 按照主机列表中的地址释放源路由；  -w timeout 指定超时时间间隔，程序默认的时间单位是毫秒。  1）tracert –d [www.nefu.edu.cn](http://www.nefu.edu.cn)  2）tracert –d [www.baidu.com](http://www.baidu.com)  截图并做相应解释。  要求  1、记录实验内容。  2、分析各命令综合应用的场景。 |

|  |
| --- |
| 四、实验过程分析与讨论  1.简单介绍PING命令。（工作在哪一层，发送的是哪一层的报文）  2. TTL值表示一个包被转发的范围。具体有设置哪些值，有什么含义？  3.什么是环回地址。有什么特点？  4.PING局域网内其他ip不通，可能是什么问题？  实验过程出现的问题及解决的方案 |
|  |
| 五、指导教师意见    指导教师签字：  年 月 日 |

参考内容：

**1）IPCONFIG**

Windows系统下实用小程序ipconfig ，用于显示当前的tcp/ip配置的设置值。这些信息一般用来检验人工配置的tcp/ip设置是否正确。但是，如果你的计算机和所在的局域网使用了动态主机配置协议（dynamic hostconfiguration protocol，dhcp），这个程序所显示的信息也许更加实用。这时，ipconfig可以让你了解你的计算机是否成功的租用到一个ip地址，如果租用到则可以了解它目前分配到的是什么地址。了解计算机当前的ip地址、子网掩码和缺省网关实际上是进行测试和故障分析的必要项目。

最常用的选项：

ipconfig /? 列表可供使用的参数。

ipconfig——当使用ipconfig时不带任何参数选项，那么它为每个已经配置了的接口显示ip地址、子网掩码和缺省网关值。

ipconfig /all——当使用all 选项时，ipconfig能为dns 和wins 服务器显示它已配置且所要使用的附加信息（如ip地址等），并且显示内置于本地网卡中的物理地址（mac）。如果ip地址是从dhcp服务器租用的，ipconfig将显示dhcp服务器的ip地址和租用地址预计失效的日期。

**2） ping命令**

ping 是个使用频率极高的实用程序，用于确定本地主机是否能与另一台主机交换（发送与接收）数据报。根据返回的信息，你就可以推断tcp/ip参数是否设置得正确以及运行是否正常。需要注意的是：成功地与另一台主机进行一次或两次数据报交换并不表示tcp/ip配置就是正确的，你必须执行大量的本地主机与远程主机的数据报交换，才能确信tcp/ip的正确性。

简单的说，ping就是一个测试程序，如果ping运行正确，你大体上就可以排除网络访问层、网卡、modem的输入输出线路、电缆和路由器等存在的故障，从而减小了问题的范围。但由于可以自定义所发数据报的大小及无休止的高速发送，ping 也被某些别有用心的人作为ddos（拒绝服务攻击）的工具。按照缺省设置，windows上运行的ping命令发送4个icmp（网间控制报文协议）回送请求，每个32字节数据，如果一切正常，你应能得到4个回送应答。ping能够以毫秒为单位显示发送回送请求到返回回送应答之间的时间量。如果应答时间短，表示数据报不必通过太多的路由器或网络连接速度比较快。ping还能显示ttl（time to live存在时间）值，TTL值表示一个包被转发的范围。

有以下转换：0，限制在同一主机 1， 限制在同一子网 32， 限制在同一节点 64，限制在同一区域（region）128，限制在同一大陆（continent）255，。

通过ping检测网络故障的典型次序。正常情况下，当你使用ping命令来查找问题所在或检验网络运行情况时，你需要使用许多ping命令，如果所有都运行正确，你就可以相信基本的连通性和配置参数没有问题；如果某些ping命令出现运行故障，它也可以指明到何处去查找问题。下面就给出一个典型的检测次序及对应的可能故障：

ping 127.0.0.1——这个ping命令被送到本地计算机的ip软件，该命令永不退出该计算机。如果没有做到这一点，就表示tcp/ip的安装或运行存在某些最基本的问题。

ping 本机ip——这个命令被送到你计算机所配置的ip 地址，你的计算机始终都应该对该ping命令作出应答，如果没有，则表示本地配置或安装存在问题。出现此问题时，局域网用户请断开网络电缆，然后重新发送该命令。如果网线断开后本命令正确，则表示另一台计算机可能配置了相同的ip地址。

ping 局域网内其他ip——这个命令应该离开你的计算机，经过网卡及网络电缆到达其他计算机，再返回。收到回送应答表明本地网络中的网卡和载体运行正确。但如果收到0个回送应答，那么表示子网掩码（进行子网分割时，将ip地址的网络部分与主机部分分开的代码）不正确或网卡配置错误或电缆系统有问题。

ping 网关ip——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。

ping 远程ip——如果收到4 个应答，表示成功的使用了缺省网关。

下面是ping命令的语法：

ping /? 列表可供使用的参数。

ping命令可用的参数说明如下：

-t。引导ping继续测试远程主机直到按Ctrl+C中断该命令。

-a。使ping -a命令就是可以通过ping它的IP地址,可以解析出主机名，这对解决DNS和Hosts文件问题是有用的。

-n count。缺省情况下，ping发送四个ICMP包到远程主机，可以使用-n参数指定被发送的包的数目。

-l length。使用-l参数指定ping传送到远程主机的ICMP包的长度。缺省情况下，ping 发送长度为32bytes的包，但是可指定最大字节数为8192bytes。

-f。使ping 命令在每个包中都包含一个Do Not Fragment(不分段)的标志，它禁止包(packet)经过的网关把packet分段。

-i ttl。设定Time To Live(存活时间)。用ttl 指定其值。

destination-list。指定ping的主机。

**3） ROUTE**

route就是用来显示、人工添加和修改路由表项目的。

大多数主机一般都是驻留在只连接一台路由器的网段上。由于只有一台路由器，因此不存在使用哪一台路由器将数据报发表到远程计算机上去的问题，该路由器的ip地址可作为该网段上所有计算机的缺省网关来输入。但是，当网络上拥有两个或多个路由器时，你就不一定想只依赖缺省网关了。实际上你可能想让你的某些远程ip地址通过某个特定的路由器来传递，而其他的远程ip则通过另一个路由器来传递。

在这种情况下，你需要相应的路由信息，这些信息储存在路由表中，每个主机和每个路由器都配有自己独一无二的路由表。大多数路由器使用专门的路由协议来交换和动态更新路由器之间的路由表。但在有些情况下，必须人工将项目添加到路由器和主机上的路由表中。

一般使用选项：

route print——本命令用于显示路由表中的当前项目，由于用ip地址配置了网卡，因此所有的这些项目都是自动添加的。

route add——使用本命令，可以将可信路由项目添加给路由表。例如，要添加目标为10.41.0.0，子网掩码为255.255.0.0，下一个跃点地址为10.27.0.1的路由，执行以下命令：

route add 10.41.0.0 mask 255.255.0.0 10.27.0.1

route change——你可以使用本命令来修改数据的传输路由，不过，你不能使用本命令来改变数据的目的地。下面这个例子可以将数据的路由改到另一个路由器，它采用一条包含3个网段的更直的路径：

route add 209.98.32.33 mask 255.255.255.224 202.96.123.250 metric 3 route delete——使用本命令可以从路由表中删除路由。例如：route delete 209.98.32.33

**4） 以太网络 ARP 表命令和MAC绑定**

通过arp命令可以查看ARP高速缓存中的内容，可以清除缓存中的地址映射，建立新的地址映射常用命令选项：

arp -a或arp -g--用于查看高速缓存中的所有项目。-a和-g参数的结果是一样的，多年来-g一直是UNIX平台上用来显示ARP高速缓存中所有项目的选项，而 Windows用的是arp -a（-a可被视为all，即全部的意思），但它也可以接受比较传统的-g选项。

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

arp -s IP 物理地址——你可以向ARP高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。

arp -d IP--使用本命令能够人工删除一个静态项目。

MAC绑定在校园网络中，最方便的捣乱方法就是盗用别人的IP地址，被盗用IP地址的计算机不仅不能正常使用校园网络，而且还会频繁出现IP地址被占用的提示对话框，给校园网络安全和用户应用带来极大的隐患。捆绑IP地址和MAC地址就能有效地避免这种现象。

**8) Tracert的使用**

Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其它主机的路由。

