

设置 DNS 服务器时，在图 2.36 所示的窗口中选择“启用 DNS”，在“主机”栏中填入主机名(如 ourlab)，“域”栏可以不填。在“DNS 服务器搜索顺序”下面的栏目中填入 DNS 服务器的地址，如 202.117.128.2，然后单击“添加”按钮。最后单击“确定”按钮完成网络的配置。

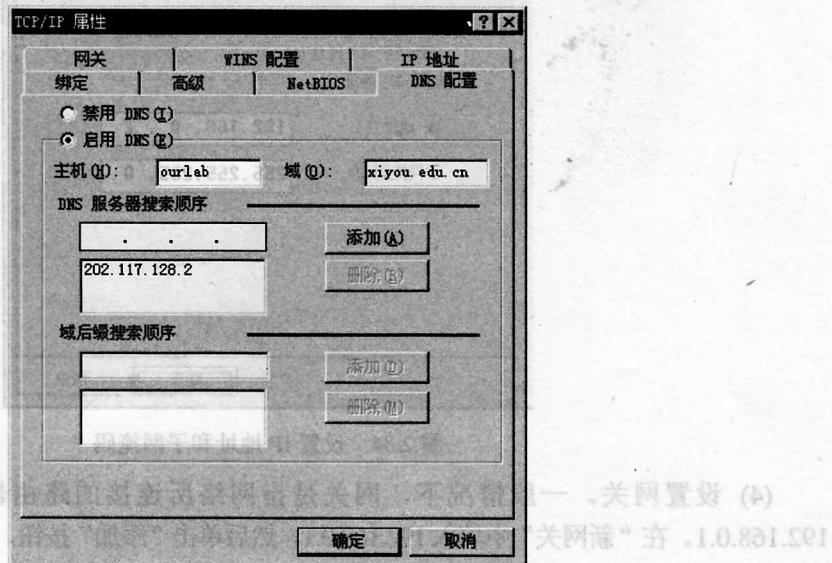


图 2.36 DNS 配置

(6) 在完成 TCP/IP 协议配置以后，就可以使用因特网提供的各种网络服务了，例如可以浏览网页、下载文件。

2.4 基本网络测试命令

2.4.1 基本网络测试命令简介

1. ping 命令

ping.exe 是个使用频率极高的实用程序，利用 ping 命令可以排除网卡、Modem、电缆和路由器等存在的故障。

ping 命令只有在安装了 TCP/IP 协议以后才可以使用。运行 ping 命令以后，在返回的黑屏窗口中会返回对方客户机的 IP 地址并表明 ping 连通对方的时间，如果出现信息“Reply from ...”，则说明能与对方连通；如果出现信息“Request timeout ...”，则说明不能与对方连通。

ping 命令是用于检测网络连通性、可到达性和名称解析等疑难问题的 TCP/IP 命令。根据返回的信息，可以推断 TCP/IP 参数的设置是否正确以及 TCP/IP 协议运行是否正常。

按照缺省设置，每发出一个 ping 命令就向对方发送 4 个网间控制报文协议 ICMP 的回送请求，如果网络正常，发送方应该得到 4 个回送的应答。ping 命令发出后得到以毫秒或

者纳秒为单位的应答时间，这个时间越短就越表示数据路由畅通；反之则说明网络连接不够畅通。

ping 命令显示的 TTL(Time To Live 存在时间)值，可以推算出数据包通过了多少个路由器。因此用 ping 命令来测试两台计算机是否连通非常有效。如果 ping 不成功，则可以认为故障出现在以下几个方面：网线、网卡和 IP 地址。

2. tracert 命令

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。该命令比较适用于大型网络。

tracert 命令通过递增“生存时间(TTL)”字段的值将“ICMP 回送请求”报文发送给目标主机，从而确定到达目标主机的路径。所显示的路径是源主机与目标主机间路径上的路由器的近侧接口列表。近侧接口是距离路径中的发送主机最近的路由器的接口。

3. netstat 命令

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，可以统计目前总共有哪些网络连接正在运行。

具体地说，netstat 命令可以显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(对于 IP、ICMP、TCP 和 UDP 协议)以及 IPv6 统计信息(对于 IPv6、ICMPv6、通过 IPv6 的 TCP 协议以及通过 IPv6 的 UDP 协议)。使用 netstat 命令时如果不带参数，则显示活动的 TCP 连接。

4. ipconfig 命令

ipconfig 命令可用于显示当前所有的 TCP/IP 网络配置值，这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。另外，ipconfig 还可以刷新动态主机配置协议(DHCP)和域名系统(DNS)的设置。使用不带参数的 ipconfig 命令可以显示所有适配器的 IP 地址、子网掩码和默认网关。

2.4.2 基本网络测试命令在 Windows 2000 下的格式

1. ping 命令

(1) 格式：

```
ping [-t] [-a] [-n Count] [-l Size] [-f] [-i TTL] [-v TOS] [-r Count] [-s Count] [[-j HostList]]  
[-k HostList] [-w Timeout] TargetName
```

(2) 参数说明：

① -t：指定在中断前 ping 命令可以持续发送回送请求信息到目的地。按下 Ctrl+Break 组合键可中断并显示统计信息；按下 Ctrl+C 组合键则中断并退出 ping。

② -a：指定对目的 IP 地址进行反向名称解析。如果解析成功，ping 命令将显示相应的主机名。

③ -n Count：指定发送回送请求信息的次数，默认值为 4。

④ -l Size：指定发送的回送请求信息中“数据”字段的长度(以字节表示)，默认值为 32。Size 的最大取值是 65 527。

⑤ -f: 指定发送的回送请求信息带有“不要拆分”标志(所在的 IP 数据报头部标志位设为 1)。回送请求信息不能由目的地路径上的路由器进行拆分。该参数可用于检测并解决“路径最大传输单位(PMTU)”的故障。

⑥ -i TTL: 指定发送回送请求信息的 IP 报头中的 TTL 字段值, 其默认值是 32。TTL 的最大值是 255。

⑦ -v TOS: 指定发送回送请求信息的 IP 报头中的“服务类型(TOS)”字段值, 默认值是 0。TOS 被指定的范围为 0~255。

⑧ -r Count: 指定 IP 报头中的“记录路由”选项用于记录由回送请求信息和相应的回应答信息使用的路径。路径中的每个跃点都使用“记录路由”字段中的一个值。如果可能, 可以指定一个等于或大于来源地和目的地之间跃点数的 Count。Count 的最小值为 1, 最大值为 9。

⑨ -s Count: 指定 IP 报头中的“Internet 时间戳”选项用于记录每个跃点的回送请求信息和相应的回应答信息的到达时间。Count 的最小值为 1, 最大值为 4。

⑩ -j HostList: 指定回送请求信息对于在 HostList 中指明的中间目标集使用 IP 报头中的“松散源路由”选项。主机列表中的地址或名称的最大数为 9, 主机列表是一系列由空格分开的 IP 地址。

⑪ -k HostList: 指定回送请求信息对于在 HostList 中指明的中间目标集使用 IP 报头中的“严格源路由”选项。使用严格源路由时, 下一个中间目的地必须是直接可达的(必须是路由器接口上的邻居)。主机列表中的地址或名称的最大数为 9, 主机列表是一系列由空格分开的 IP 地址。

⑫ -w Timeout: 指定等待回应答信息响应的时间(以微秒为单位), 该回应答信息响应接收到的指定回送请求信息。如果在超时时间内未接收到回应答信息, 将会显示“请求超时”的错误信息。默认的超时时间为 4000 ms(4 s)。

⑬ TargetName: 指定目标, 可以是 IP 地址或主机名。

2. tracert 命令

(1) 格式:

`tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] TargetName`

(2) 参数说明:

① -d: 防止 tracert 试图将中间路由器的 IP 地址解析为它们的名称。这样可加速显示 tracert 的结果。

② -h MaximumHops: 指定在搜索目标的路径中跃点的最大数, 默认值为 30。

③ -j HostList: 指定回送请求信息对于在 HostList 中指明的中间目标集使用 IP 报头中的“松散源路由”选项。主机列表中的地址或名称的最大数为 9, 主机列表是一系列由空格分开的 IP 地址。

④ -w Timeout: 指定等待“ICMP 已超时”或“回应答”信息的时间(以毫秒为单位)。如果在超时时间内未收到信息, 则显示一个星号(*)。默认的超时时间为 4000 ms(4 s)。

⑤ TargetName: 指定目标, 可以是 IP 地址或主机名。

3. netstat 命令

(1) 格式:

```
netstat [-a] [-e] [-n] [-s] [-p Protocol] [-r] [Interval]
```

(2) 参数说明:

① -a: 显示所有有效连接的信息，包括已建立的连接(Established)，也包括监听连接请求(Listening)的那些连接，以及计算机侦听的 TCP 和 UDP 端口。

② -e: 显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些数据既有发送的数据报数量，也有接收的数据报数量。该选项可以用来统计一些基本的网络流量，并可以与选项-s 结合使用。

③ -n: 显示所有已建立的有效的 TCP 连接，但是，只以数字形式表现地址和端口号，却不尝试确定名称。

④ -s: 分别显示各个协议的统计数据。默认情况下，显示 TCP、UDP 和 IP 协议的统计信息。如果应用程序(如 Web 浏览器)运行比较慢，或者不能显示 Web 页之类的数据，就可以使用该选项来查看所显示的信息。可以使用选项 -p 指定协议集。

⑤ -p Protocol: 显示 Protocol 所指定的协议的连接。在这种情况下，Protocol 可以是 TCP 或 UDP。如果该选项与选项-s 一起使用来显示协议的统计信息，则 Protocol 可以是 TCP、UDP 或 IP。

⑥ -r: 显示本机路由表的信息。

⑦ Interval: 每隔 Interval 秒重新显示一次选定的信息。按 Ctrl+C 组合键可停止重新显示统计信息。如果省略该参数，netstat 将只打印一次选定的信息。

4. ipconfig 命令

(1) 格式:

```
ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns] [/registerdns]
[/showclassid Adapter] [/setclassid Adapter [ClassID]]
```

(2) 参数说明:

① /all: 显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下，ipconfig 只显示 IP 地址、子网掩码和各个适配器的默认网关值。适配器可以代表物理接口(例如安装的网络适配器)或逻辑接口(例如拨号连接)。

② /renew [Adapter]: 更新所有适配器(不带 Adapter 参数)，或特定适配器(带有 Adapter 参数)的 DHCP 配置。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上使用。要指定适配器名称，请键入使用不带参数的 ipconfig 命令显示的适配器名称。

③ /release [Adapter]: 发送 Dhcrelease 消息到 DHCP 服务器，以释放所有适配器(不带 Adapter 参数)或特定适配器(带有 Adapter 参数)的当前 DHCP 配置并丢弃 IP 地址配置。该参数可以禁用配置为自动获取 IP 地址的适配器的 TCP/IP。要指定适配器名称，请键入使用不带参数的 ipconfig 命令显示的适配器名称。

④ /flushdns: 清理并重设 DNS 客户解析器缓存的内容。如有必要，在 DNS 疑难解答期间，可以使用该选项从缓存中丢弃否定性缓存记录和任何其他动态添加的记录。

⑤ /displaydns: 显示 DNS 客户解析器缓存的内容，包括从本地主机文件预装载的记录。

以及由计算机解析的名称查询而最近获得的任何资源记录。DNS 客户服务在查询配置的 DNS 服务器之前使用这些信息快速解析被频繁查询的名称。

⑥ /registerdns: 初始化计算机上配置的 DNS 名称和 IP 地址的手动动态注册。可以使用该参数对失败的 DNS 名称注册进行疑难解答或解决客户和 DNS 服务器之间的动态更新问题，而不必重新启动客户计算机。TCP/IP 协议高级属性中的 DNS 设置可以确定 DNS 中注册了哪些名称。

⑦ /showclassid Adapter: 显示指定适配器的 DHCP 类别 ID。要查看所有适配器的 DHCP 类别 ID，可以使用星号(*)通配符代替 Adapter。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上使用。

⑧ /setclassid Adapter [ClassID]: 配置特定适配器的 DHCP 类别 ID。要设置所有适配器的 DHCP 类别 ID，可以使用星号(*)通配符代替 Adapter。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上使用。如果未指定 DHCP 类别 ID，则会删除当前类别 ID。

2.4.3 实验 ping 命令的使用

1. 实验要求

- (1) 掌握 ping 命令的使用方法。
- (2) 能够灵活应用 ping 命令的各种参数来检测网络连通性、可到达性和名称解析等问题。

2. 实验环境

相互连通的计算机多台，构成简单的局域网；该局域网与因特网连通。

3. 实验过程和主要步骤

(1) 回环测试：这个 ping 命令被送到本地计算机 IP 软件。在 DOS 提示符下输入回环测试的 ping 命令，正常情况下可以看到来自本机的应答信息，如图 2.37 所示。这一命令可以用来检测 TCP/IP 的安装或运行存在的某些最基本的问题。

```
C:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<10ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.37 直接利用 IP 地址回环测试

localhost 是 127.0.0.1 的别名，我们也可以利用 localhost 来进行回环测试，如图 2.38 所示。每台计算机都应该能够将名称 localhost 转换成地址 127.0.0.1，如果不能做到这一点，则表示主机文件(Host)中存在问题。

```
C:\>ping localhost

Pinging computer [127.0.0.1] with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<10ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.38 利用 localhost 进行回环测试

(2) ping 本机 IP: 这个命令使用本地计算机所配置的 IP 地址。如果我们在 ping 命令中加上参数-t, 本地计算机应该始终对该 ping 命令作出应答(如图 2.39 所示, 这里只给出了 6 次应答信息); 否则, 说明本地计算机的 TCP/IP 安装或配置存在问题。

```
C:\>ping -t 222.24.12.31

Pinging 222.24.12.31 with 32 bytes of data:

Reply from 222.24.12.31: bytes=32 time<10ms TTL=128
```

图 2.39 ping 本机 IP

(3) ping 局域网内其他主机 IP: 该命令对局域网内的其他主机发送回送请求信息。如果能够收到对方主机的回送应答信息, 表明本地网络中的网卡和传输媒体运行正常, 如图 2.40 所示。

```
C:\>ping 222.24.12.35

Pinging 222.24.12.35 with 32 bytes of data:

Reply from 222.24.12.35: bytes=32 time<10ms TTL=128

Ping statistics for 222.24.12.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.40 ping 局域网内其他主机 IP

如果显示“请求超时”, 不能收到对方主机的回送应答信息, 则表明局域网的连通性存在问题, 原因可能有子网掩码不正确、网卡配置错误或传输媒体不正常等, 如图 2.41 所示。

```
C:\>ping 222.24.12.32

Pinging 222.24.12.32 with 32 bytes of data:

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

Ping statistics for 222.24.12.32:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.41 请求超时

(4) ping 网关: 如果能够收到应答信息, 则表明网络中的网关路由器运行正常, 如图 2.42 所示。

```
C:\>ping 222.24.12.1

Pinging 222.24.12.1 with 32 bytes of data:

Reply from 222.24.12.1: bytes=32 time<10ms TTL=255

Ping statistics for 222.24.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.42 ping 网关

(5) ping 域名服务器: 如果能够收到应答信息, 则表明网络中的域名服务器运行正常, 如图 2.43 所示。

```
C:\>ping 202.117.128.2

Pinging 202.117.128.2 with 32 bytes of data:

Reply from 202.117.128.2: bytes=32 time<10ms TTL=253

Ping statistics for 202.117.128.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.43 ping 域名服务器

(6) ping 远程 IP 地址: 如西安邮电学院校园网服务器的 IP 地址为 202.117.128.8, 缺省状态下如果能够收到 4 个应答, 则表示成功地使用了默认网关, 如图 2.44 所示。

```
C:\>ping 202.117.128.8
Pinging 202.117.128.8 with 32 bytes of data:
Reply from 202.117.128.8: bytes=32 time<10ms TTL=126

Ping statistics for 202.117.128.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.44 ping 远程 IP 地址

(7) ping 域名地址：如果这里出现故障，可能是因为 DNS 服务器的 IP 地址配置不正确或 DNS 服务器有故障，如图 2.45 所示。

```
C:\>ping www.xiyou.edu.cn
Pinging www.xiyou.edu.cn [202.117.128.8] with 32 bytes of data:
Reply from 202.117.128.8: bytes=32 time<10ms TTL=126

Ping statistics for 202.117.128.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.45 ping 域名地址

如果上面所列出的所有 ping 命令都能正常运行，那么本地计算机基本上具备了进行本地和远程通信的功能。但是，这些命令的成功并不表示本地主机的所有网络配置都没有问题，例如，某些子网掩码错误可能无法用这些方法检测到。

(8) 如果需要验证 IP 地址为 222.24.12.40 的目的主机，并且解析目的主机的名称，可以在 ping 命令中使用参数 -a，如图 2.46 所示。

```
C:\>ping -a 222.24.12.40
Pinging STUDENT [222.24.12.40] with 32 bytes of data:
Reply from 222.24.12.40: bytes=32 time<10ms TTL=128

Ping statistics for 222.24.12.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.46 利用 ping 命令解析目的主机的名称

(9) 假设目的主机的 IP 地址为 222.24.12.35，如果需要返回 6 个应答信息，并且应答信息“数据”字段为 1000 字节，则可以在 ping 命令中使用如图 2.47 所示的参数。

```
C:\>ping -n 6 -l 1000 222.24.12.35
Pinging 222.24.12.35 with 1000 bytes of data:
Reply from 222.24.12.35: bytes=1000 time<10ms TTL=128

Ping statistics for 222.24.12.35:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 2.47 带有两个参数的 ping 命令

(10) 如果需要验证 IP 地址为 202.117.128.8 的目的主机，并记录 2 个跃点的路由，则可以在 ping 命令中使用参数 -r，如图 2.48 所示。

```
C:\>ping -r 2 202.117.128.8
Pinging 202.117.128.8 with 32 bytes of data:
Reply from 202.117.128.8: bytes=32 time=15ms TTL=126
Route: 222.24.63.2 ->
202.117.128.70
Reply from 202.117.128.8: bytes=32 time<10ms TTL=126
Route: 222.24.63.2 ->
202.117.128.70
Reply from 202.117.128.8: bytes=32 time<10ms TTL=126
Route: 222.24.63.2 ->
202.117.128.70

Ping statistics for 202.117.128.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 3ms
```

图 2.48 记录路由的 ping 命令

2.4.4 实验 tracert 命令的使用

1. 实验要求

掌握 tracert 命令的使用方法，并能灵活应用这一命令的各种参数。

2. 实验环境

相互连通的计算机多台，构成简单的局域网；该局域网与因特网连通。

3. 实验过程和主要步骤

- (1) 如果要跟踪到达西安邮电学院校园网服务器(www.xiyou.edu.cn)的路径，可以使用如图 2.49 所示的 tracert 命令。

```
C:\>tracert www.xiyou.edu.cn
Tracing route to www.xiyou.edu.cn [202.117.128.8]
over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms 222.24.12.1
2 <10 ms <10 ms <10 ms 222.24.63.1
3 <10 ms <10 ms <10 ms XIYOU-SRUXIVSVR [202.117.128.8]

Trace complete.
```

图 2.49 跟踪到达服务器(www.xiyou.edu.cn)的路径

- (2) 在跟踪过程中，为了防止将每个 IP 地址解析为它的名称，可以在 tracert 命令中使用参数 -d，如图 2.50 所示。

```
C:\>tracert -d www.xiyou.edu.cn
Tracing route to www.xiyou.edu.cn [202.117.128.8]
over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms 222.24.12.1
2 <10 ms <10 ms <10 ms 222.24.63.1
3 <10 ms <10 ms <10 ms 202.117.128.8

Trace complete.
```

图 2.50 带有-d 参数的 tracert 命令

2.4.5 实验 netstat 命令的使用

1. 实验要求

熟练掌握 netstat 命令的使用方法，并能够灵活应用 netstat 命令的各参数来检测本地主机各端口的网络连接情况。

2. 实验环境

相互连通的计算机多台，构成简单的局域网；该局域网与因特网连通。

3. 实验过程和主要步骤

(1) 如果需要显示所有有效连接(包括 TCP 和 UDP 两种)的信息，可以在 netstat 命令中使用参数 -a，这里包括已建立的连接(Established)，也包括监听连接请求(Listening)的那些连接，以及计算机侦听的 TCP 和 UDP 端口。图 2.51 中省略了部分信息。

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	computer:echo	computer:0	LISTENING
TCP	computer:discard	computer:0	LISTENING
...
TCP	computer:563	computer:0	LISTENING
TCP	computer:1025	computer:0	LISTENING
...
TCP	computer:9996	computer:0	LISTENING
TCP	computer:netbios-ssn	computer:0	LISTENING
UDP	computer:echo	**	
UDP	computer:discard	**	
...
UDP	computer:1032	**	
UDP	computer:1034	**	
UDP	computer:1035	**	
...

图 2.51 带有参数 -a 的 netstat 命令

(2) 可以在 netstat 命令中使用参数 -e 来显示关于以太网的统计数据，如图 2.52 所示。

Interface Statistics		
Received	2191233	742146
Bytes	2808	2532
Unicast packets	8749	121
Non-unicast packets	0	0
Discards	0	0
Errors	798	
Unknown protocols		

图 2.52 带有参数 -e 的 netstat 命令

(3) 如果需要显示已建立的有效的 TCP 连接，可以在 netstat 命令中使用参数-n，如图 2.53 所示。

```
C:\>netstat -n
Active Connections

Proto Local Address          Foreign Address        State
TCP   222.24.12.31:139      222.24.12.35:1395    ESTABLISHED
```

图 2.53 带有参数 -n 的 netstat 命令

(4) 如果需要显示 TCP 或 UDP 的统计信息, 可以使用如图 2.54 和图 2.55 所示的 netstat 命令。

```
C:\>netstat -s -p tcp
TCP Statistics

Active Opens          = 86
Passive Opens         = 50
Failed Connection Attempts = 0
Reset Connections     = 31
Current Connections   = 1
Segments Received     = 2994
Segments Sent          = 2694
Segments Retransmitted = 0

Active Connections

Proto Local Address          Foreign Address        State
TCP   computer:7080          computer:1143        TIME_WAIT
TCP   computer:7080          computer:1150        TIME_WAIT
TCP   computer:netbios-ssn   IS~WL70:1381       ESTABLISHED
TCP   computer:1146          202.117.128.240:http TIME_WAIT
TCP   computer:1148          202.117.128.240:http TIME_WAIT
TCP   computer:1153          202.117.128.240:http TIME_WAIT
TCP   computer:1155          202.117.128.240:http TIME_WAIT
```

图 2.54 利用 netstat 命令显示 TCP 的统计信息

```
C:\>netstat -s -p udp
UDP Statistics

Datagrams Received     = 1322
No Ports               = 3125
Receive Errors          = 0
Datagrams Sent          = 558

Active Connections

Proto Local Address          Foreign Address        State
```

图 2.55 利用 netstat 命令显示 UDP 的统计信息

(5) 如果需要显示关于路由表的信息,可以在 netstat 命令中使用参数 -r, 如图 2.56 所示。

```
C:\>netstat -r
Route Table
Interface List
0x1 ..... MS TCP Loopback interface
0x1000003 ...00 0d 56 64 f5 65 ..... Broadcom 440x 10/100 Integrated Controller

Active Routes:
Network Destination     Netmask      Gateway       Interface   Metric
          0.0.0.0     0.0.0.0    222.24.12.1  222.24.12.35    1
         127.0.0.0   255.0.0.0    127.0.0.1    127.0.0.1    1
        222.24.12.0  255.255.255.0  222.24.12.35  222.24.12.35    1
      222.24.12.35  255.255.255.255    127.0.0.1    127.0.0.1    1
      222.24.12.255 255.255.255.255    222.24.12.35  222.24.12.35    1
        224.0.0.0     224.0.0.0    222.24.12.35  222.24.12.35    1
      255.255.255.255 255.255.255.255    222.24.12.35  222.24.12.35    1
Default Gateway:        222.24.12.1

Persistent Routes:
None
```

图 2.56 带有参数 -r 的 netstat 命令

2.4.6 实验 ipconfig 命令的使用

1. 实验要求

掌握 ipconfig 命令各参数的使用方法,并能够利用这一命令显示 TCP/IP 网络配置值、刷新动态主机配置协议(DHCP)和域名系统(DNS)设置。

2. 实验环境

相互连通的计算机多台,构成简单的局域网;该局域网与因特网连通。

3. 实验过程和主要步骤

(1) 如果需要显示所有适配器的基本 TCP/IP 配置,可以使用不带参数的 ipconfig 命令,如图 2.57 所示。

```
C:\>ipconfig
Windows 2000 IP Configuration

Ethernet adapter 本地连接:

Connection-specific DNS Suffix . .
IP Address . . . . . 222.24.12.31
Subnet Mask . . . . . 255.255.255.0
Default Gateway . . . . . 222.24.12.1
```

图 2.57 不带参数的 ipconfig 命令

(2) 如果需要显示所有适配器的完整 TCP/IP 配置,可以在 ipconfig 命令中使用参数 /all,如图 2.58 所示。

```
C:\>ipconfig /all
Windows 2000 IP Configuration

Host Name ..... computer
Primary DNS Suffix ..... .
Node Type ..... Hybrid
IP Routing Enabled ..... No
WINS Proxy Enabled ..... No

Ethernet adapter 本地连接:

Connection-specific DNS Suffix : .
Description : Broadcom 440x 10/100 Integrated Controller
Physical Address : 00-0D-56-64-D6-F5
DHCP Enabled ..... No
IP Address ..... : 222.24.12.31
Subnet Mask ..... : 255.255.255.0
Default Gateway..... : 222.24.12.1
DNS Servers ..... : 202.117.128.2
```

图 2.58 利用 ipconfig 命令显示完整的 TCP/IP 配置

(3) 清理并重设 DNS 客户解析器缓存的内容，可以通过在 ipconfig 命令中使用参数 /flushdns 来实现，如图 2.59 所示。

```
C:\>ipconfig /flushdns
Windows 2000 IP Configuration

Successfully flushed the DNS Resolver Cache.
```

图 2.59 带有参数/flushdns 的 ipconfig 命令

(4) 如果需要显示 DNS 客户解析器缓存的内容，可以在 ipconfig 命令中使用参数 /displaydns，如图 2.60 所示。

```
C:\>ipconfig /displaydns
Windows 2000 IP Configuration

localhost.

Record Name ..... localhost
Record Type ..... 1
Time To Live ..... 31530702
Data Length ..... 4
Section ..... Answer
A (Host) Record ..... 127.0.0.1

1.0.0.127.in-addr.arpa.

Record Name ..... 1.0.0.127.in-addr.arpa
Record Type ..... 12
Time To Live ..... 31530702
Data Length ..... 4
Section ..... Answer
PTR Record ..... localhost
```

图 2.60 带有参数/displaydns 的 ipconfig 命令