

This is going to be a basic introduction to network troubleshooting from the Windows command line. We will cover the commands and the more common options and switches for them. The last section will cover the telnet command and troubleshooting your e-mail using it.

We will start with the ping command, this is used to check if your computer can connect to another at the most basic level. The only requirements for ping to work are a connection to the other computer and its willingness to respond to the ping request. You can see the command syntax and options with this command:

```
C:\>ping /?
```

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] target_name
```

Options:

- t Ping the specified host until stopped.
To see statistics and continue - type Control-Break;
To stop - type Control-C.
 - a Resolve addresses to hostnames.
 - n count Number of echo requests to send.
 - l size Send buffer size.
 - f Set Don't Fragment flag in packet.
 - i TTL Time To Live.
 - v TOS Type Of Service.
 - r count Record route for count hops.
 - s count Timestamp for count hops.
 - j host-list Loose source route along host-list.
 - k host-list Strict source route along host-list.
 - w timeout Timeout in milliseconds to wait for each reply.
-

Your first attempt to try a ping should be to a site you know is going to answer, you can try a few yourself and find one you like or use my site:

```
C:\>ping -w 2000 stanmiller.info
```

```
Pinging stanmiller.info [209.217.36.7] with 32 bytes of data:
```

```
Reply from 209.217.36.7: bytes=32 time=1477ms TTL=237
< trimmed 3 more>
```

```
Ping statistics for 209.217.36.7:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 697ms, Maximum = 1477ms, Average = 912ms
```

You see two options above, the -w option with a time of 2000 milliseconds and a site to ping by name, stanmiller.info. The -w option is always a good idea when using the satellite, the designers of the ping command had much faster connections available and set the default timeout too short for our use.

The site name stanmiller.info is the one that the ping command will send the ping request to, since the Internet doesn't work using names stanmiller.info has to be translated to an IP number by the DNS (covered later) resolver. You can see this conversion on this line:

Pinging stanmiller.info [209.217.36.7] with 32 bytes of data:

That also tells you the amount of data that is being sent to the distant system, you can change that using the -l command. Using packets over about 1450 can result in the packets requiring special processing and giving unusual looking results, it is best to stay with the default unless you have a special reason to go larger.

The next thing you will see is a block of information about the responses from the other computer:

Reply from 209.217.36.7: bytes=32 time=1477ms TTL=237

The reply from is only important when you are pinging more than one system and you already know the packet size and the TTL is related to the number of other computers you had to pass through and unimportant to us. That leaves us with only two useful pieces of information, the fact that we got a response in the first place and how long it took to get that response.

The entire ping session is summarized when it completes or you terminate it with a Ctrl-C, the summary looks like this:

Ping statistics for 209.217.36.7:

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

Approximate round trip times in milli-seconds:

Minimum = 697ms, Maximum = 1477ms, Average = 912ms

If the connection is not overloaded or having other problems the Packets Lost should be 0, every packet that is lost in normal operation has to be resent and will slow down your communications. If you end the command early you may have one packet lost due to that. The approximate round trip times let you see how fast the other computer is responding without having to calculate the numbers from the individual responses above it.

If you are having problems with pinging by name you can add the -a option and try to ping by number, this will use the number you entered but will also attempt to look up the name of the system.

```
C:\>ping -a 192.168.0.1
```

Pinging dw6000.home [192.168.0.1] with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=2ms TTL=63

Here is a ping by number without the -a option for comparison:

```
C:\>ping 192.168.0.1
```

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=2ms TTL=63

The skipping of the name lookup makes working with ping much faster if you are having DNS problems or are pinging systems that do not have names.

Now lets look at several different amounts of time to wait for responses and what you will see in response to them. The first thing to notice is that the time isn't very exact as you can see from the -w 500 below, it still gets packets that are over 500 but misses others that were slightly longer.

```
>ping -w 500 stanmiller.info
```

Pinging stanmiller.info [209.217.36.7] with 32 bytes of data:

Request timed out.

Reply from 209.217.36.7: bytes=32 time=752ms TTL=237

Reply from 209.217.36.7: bytes=32 time=740ms TTL=237

Request timed out.

Another neat ping trick is the -f option that lets you see how big a packet of data your network will send. You normally don't care about this until you set up a local LAN and even then you'll be fine with the default MTU setting of 1500 in your router. If you want to check this you'll want to combine the -w -f and -l commands

```
C:\>ping -w 2000 -f -l 1800 192.168.0.1
```

Pinging 192.168.0.1 with 1800 bytes of data:

Packet needs to be fragmented but DF set.

The nslookup command will test the functions of your DNS name to IP address translation system, it does not test the portion of this function done inside the proxy or web accelerator. You start it with nslookup and it will show you the default name server. In this example it is the router I'm connected to, I get both the router name and its IP address since these are available from my DNS server, if you don't have that set up you will see just the address.

To see the available options enter a “?” and it will list them for you.

```
C:\>nslookup
```

Default Server: wrt55-ag.home

Address: 192.168.2.1

```
> ?
```

Commands: (identifiers are shown in uppercase, [] means optional)

NAME - print info about the host/domain NAME using default server

NAME1 NAME2 - as above, but use NAME2 as server

help or ? - print info on common commands

set OPTION - set an option

all - print options, current server and host

[no]debug - print debugging information
 [no]d2 - print exhaustive debugging information
 [no]defname - append domain name to each query
 [no]recurse - ask for recursive answer to query
 [no]search - use domain search list
 [no]vc - always use a virtual circuit
 domain=NAME - set default domain name to NAME
 srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
 root=NAME - set root server to NAME
 retry=X - set number of retries to X
 timeout=X - set initial time-out interval to X seconds
 type=X - set query type (ex. A,ANY,CNAME,MX,NS,PTR,SOA,SRV)
 querytype=X - same as type
 class=X - set query class (ex. IN (Internet), ANY)
 [no]msxfr - use MS fast zone transfer
 ixfrver=X - current version to use in IXFR transfer request
 server NAME - set default server to NAME, using current default server
 lserver NAME - set default server to NAME, using initial server
 finger [USER] - finger the optional NAME at the current default host
 root - set current default server to the root
 ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
 -a - list canonical names and aliases
 -d - list all records
 -t TYPE - list records of the given type (e.g. A,CNAME,MX,NS,PTR etc.)
 view FILE - sort an 'ls' output file and view it with pg
 exit - exit the program

>

This is the default display if you start it with no options, it is waiting for you to enter a command or server name after the “>” prompt.

```

C:\>nslookup
Default Server: wrt55-ag.home
Address: 192.168.2.1
>
  
```

If you give it a server to lookup on the command line you will get a response like this:

```

C:\>nslookup stanmiller.info
Server: wrt55-ag.home
Address: 192.168.2.1

Non-authoritative answer:
Name: stanmiller.info
Address: 209.217.36.7
>
  
```

If you give it a server to lookup and a server to use for the lookup on the command line you will get a

response like this, note that it isn't using your default server for the query:

```
C:\>nslookup stanmiller.info 4.2.2.2
Server: vns-c-bak.sys.gte.net
Address: 4.2.2.2
```

```
Non-authoritative answer:
Name: stanmiller.info
Address: 209.217.36.7
>
```

This is handy if your server is failing to find an address or if the address it is finding is wrong. That isn't all that uncommon as folks move machines around and change the addresses, the changes can take 24-48 hours to make it to all the local name servers.

Depending on your name server you may see responses like these where you get a single IP address or multiple IP addresses. It is perfectly fine for a name to translate into one or more IP address, that is done for load balancing on busy systems or to have a backup on line and ready to take over if the primary machine fails.

```
C:\>nslookup smtp.direcway.com
Server: wrt55-ag.home
Address: 192.168.2.1
```

```
Non-authoritative answer:
Name: smtp.direcway.com
Address: 66.82.4.76
```

```
C:\>nslookup smtp.direcway.com
Server: NSLU2-2
Address: 192.168.2.252
```

```
Non-authoritative answer:
Name: smtp.direcway.com
Addresses: 66.82.4.76, 66.82.4.75
```

The ipconfig command has a lot of different uses, we will go through the more common ones. As usual starting it with a “/?” will get you some basic help:

```
C:\>ipconfig /?
```

USAGE:

```
ipconfig [/? | /all | /renew [adapter] | /release [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] ]
```

where

Physical Address. : 00-14-22-DC-5A-03

Ethernet adapter Wireless Network Connection:

Connection-specific DNS Suffix . :
Description : Intel(R) PRO/Wireless 2915ABG Network Connection
Physical Address. : 00-13-CE-45-91-BC
Dhcp Enabled. : Yes
Autoconfiguration Enabled : Yes
IP Address. : 192.168.2.12
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.2.1
DHCP Server : 192.168.2.1
DNS Servers : 192.168.2.1
 192.168.2.252
 4.2.2.2
 198.77.116.8
Lease Obtained. : Sunday, January 15, 2006 9:16:13 AM
Lease Expires : Monday, January 16, 2006 9:16:13 AM

Key items to look for here are the connection statuses, the addresses of your machine, gateway and DNS servers and the subnet mask. That should match your network, 255.255.255.0 is the normal one and rarely changed.

If you are using DHCP one of the simple fixes is the combination of the “/release” and “/renew” commands. That will generate the following information that will let you see if DHCP is working for you. If you have more than one connection this will work on and show info for each of them, you can see I have my Ethernet cable unplugged and my WiFi connected to an access point.

C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

Media State : Media disconnected

Ethernet adapter Wireless Network Connection:

Connection-specific DNS Suffix . :
IP Address. : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway :

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

Media State : Media disconnected

Ethernet adapter Wireless Network Connection:

Connection-specific DNS Suffix . :
IP Address. : 192.168.2.12
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.2.1

Here following the /renew command you see my WiFi router assigning my laptop the basic information it needs to connect to the internet.

This is a trimmed down version of the response to the /displaydns command, it shows the information about DNS, name to IP address conversion that Windows is saving internally. It will not show the information that your DNS server or your modem are storing locally or what the proxy or web accelerator are using for anything but the initial conversion to an IP number. You should always see the first and last entries here as they are part of your computers internal network.

C:\>ipconfig /displaydns

Windows IP Configuration

1.0.0.127.in-addr.arpa

Record Name : 1.0.0.127.in-addr.arpa.
Record Type : 12
Time To Live : 593806
Data Length : 4
Section : Answer
PTR Record : localhost

escapees.com

Record Name : escapees.com
Record Type : 1
Time To Live : 82546
Data Length : 4
Section : Answer
A (Host) Record . . . : 207.70.132.65

localhost

Record Name : localhost
Record Type : 1
Time To Live : 593806
Data Length : 4

C:\>ipconfig /flushdns Purges the DNS Resolver cache, you can use this if the DNS lookup has been misbehaving. It will remove any bad entries and allow you to start fresh without having to reboot your PC. Rebooting the modem may still be needed if it was the source of the errors.

Tracert will trace the path that an Internet Protocol (IP) packet takes to its destination from your computer. It does this by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination. Tracert works by manipulating the Time to Live (TTL). By increasing the TTL and then each router decrementing as it sends it along to the next router, you will have a hop count from your source to your destination. A router hop would be a packet sent from one router to another router – that's a hop. When the TTL on the packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

The list displayed contains information on the routers in the path between your computer and the destination you entered. One thing that is very important to remember is that near-side interfaces are used when reporting. The near-side interface is the interface of the router that is closest to the sending host in the path.

The way tracert works is, once launched and utilized is that it will report (print out) a list in the order in which it heard back from each host that it passed on its way to its intended destination. We will start out with the list of options:

C:\>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:

- d Do not resolve addresses to hostnames.
 - h maximum_hops Maximum number of hops to search for target.
 - j host-list Loose source route along host-list.
 - w timeout Wait timeout milliseconds for each reply.
-

As usual on the satellite link we need to add the timeout delay, 2000 is usually good but 3000 or more may be needed on a slow networking day. It starts off by converting the name you entered to an IP address and then works its way down each computer in the path giving the IP address and attempting to find a matching name. Not finding a name is not important to this process but having one present sure makes the results easier to read.

In this list you will see several "*" entries, they indicate that the target machine did not respond to the request (similar to a ping) in the time allotted.

C:\>tracert -w 3000 stanmiller.info

Tracing route to stanmiller.info [209.217.36.7]
over a maximum of 30 hops:

1 1 ms 1 ms 1 ms WRT55-AG.home [192.168.2.1]

```

2 * * * Request timed out.
3 * * * Request timed out.
4 1245 ms 839 ms 799 ms dpc6682026130.direcpc.com [66.82.26.130]
5 612 ms 689 ms 669 ms dpc6682017089.direcpc.com [66.82.17.89]
6 699 ms 629 ms 679 ms dpc6682016069.direcpc.com [66.82.16.69]
7 841 ms 749 ms 719 ms dca-edge-13.inet.qwest.net [65.113.48.89]
8 712 ms 619 ms 709 ms dca-core-01.inet.qwest.net [205.171.209.73]
9 833 ms 749 ms 690 ms dcx-core-02.inet.qwest.net [205.171.209.114]
10 703 ms 740 ms 739 ms dcp-brdr-02.inet.qwest.net [205.171.251.38]
11 717 ms 917 ms 720 ms sl-st21-ash-6-0.sprintlink.net [144.232.19.17]
12 704 ms 679 ms 689 ms sl-bb26-rly-6-0.sprintlink.net [144.232.20.135]
13 * 797 ms 619 ms sl-bb25-rly-13-0.sprintlink.net [144.232.14.169]
14 620 ms 609 ms 780 ms sl-bb21-rly-11-0.sprintlink.net [144.232.14.157]
15 662 ms 639 ms 669 ms sl-bb21-atl-6-0.sprintlink.net [144.232.20.176]
16 671 ms 709 ms 629 ms sl-bb22-atl-15-0.sprintlink.net [144.232.12.150]
17 716 ms 669 ms 679 ms sl-bb23-fw-13-0.sprintlink.net [144.232.8.67]
18 1004 ms 669 ms 799 ms sl-bb21-fw-13-0.sprintlink.net [144.232.11.245]
19 708 ms 639 ms 690 ms sl-gw35-fw-8-0.sprintlink.net [144.232.11.254]
20 733 ms 960 ms 689 ms sl-ethoscomm-3-0.sprintlink.net [144.232.236.34]
21 868 ms 750 ms 839 ms smtp3.catalog.com [209.217.36.7]

```

Trace complete.

Here is a quick example of the -d switch which removes the name lookups for the hops along the way, this can save time on longer paths or when you have slow connections like we do over the sat link.

```
C:\>tracert dw6000.home
```

```
Tracing route to dw6000.home [192.168.0.1]
over a maximum of 30 hops:
```

```

1 1 ms <1 ms <1 ms WRT55-AG.home [192.168.2.1]
2 2 ms 2 ms 2 ms dw6000.home [192.168.0.1]

```

Trace complete.

```
C:\>tracert -d dw6000.home
```

```
Tracing route to dw6000.home [192.168.0.1]
over a maximum of 30 hops:
```

```

1 1 ms 1 ms 1 ms 192.168.2.1
2 2 ms 2 ms 2 ms 192.168.0.1

```

Trace complete.

I included this for completeness but it isn't much use since it will not work if any host in the path refuses to respond to the ping requests and most DW hosts refuse blocking the test.

Pathping is a TCP/IP based utility (command-line tool) that provides useful information about network latency and network loss at intermediate hops between a source address and a destination address. It does this by sending echo requests via ICMP and analyzing the results. ICMP stands for Internet Control Message Protocol. ICMP is an extension to the Internet Protocol (IP - part of the TCP/IP protocol suite) defined by [RFC 792](#). ICMP supports packets containing error, control and informational messages. Pathping will send multiple echo request messages to each router between what you are attempting to ping – the source address. If your destination is across a WAN link then it's certain that you will be using some form of router, most likely two, which would mean that you could test pathping across a two hop network – two router hops. A typical network diagram is seen in the following illustration.

Another command of little use unless you are using a 4000 and ICS is route, it shows and manipulates network routing tables in your computer. The two options of interest are -f to clear the cache of any routes it has saved and the PRINT command to show what is being saved for internal use.

ROUTE [-f] [-p] [command [destination]
[MASK netmask] [gateway] [METRIC metric] [IF interface]

- f Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.
- p When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. Ignored for all other commands, which always affect the appropriate persistent routes. This option is not supported in Windows 95.

command One of these:

- PRINT Prints a route
- ADD Adds a route
- DELETE Deletes a route
- CHANGE Modifies an existing route

destination Specifies the host.

MASK Specifies that the next parameter is the 'netmask' value.

netmask Specifies a subnet mask value for this route entry.

If not specified, it defaults to 255.255.255.255.

gateway Specifies gateway.

interface the interface number for the specified route.

METRIC specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database file NETWORKS. The symbolic names for gateway are looked up in the host name database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard, (wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only matching destination routes are printed. The '*' matches any string,

and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Diagnostic Notes:

Invalid MASK generates an error, that is when (DEST & MASK) != DEST.

Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1

The route addition failed: The specified mask parameter is invalid.

(Destination & Mask) != Destination.

Examples:

> route PRINT

> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2

destination^ ^mask ^gateway metric^ ^
Interface^

If IF is not given, it tries to find the best interface for a given gateway.

> route PRINT

> route PRINT 157* Only prints those matching 157*

> route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

CHANGE is used to modify gateway and/or metric only.

> route PRINT

> route DELETE 157.0.0.0

> route PRINT

C:\>route print

Interface List

0x1 MS TCP Loopback interface

0x2 ...00 14 22 dc 5a 03 Broadcom 440x 10/100 Integrated Controller - Pac

ket Scheduler Miniport

0x3 ...00 13 ce 45 91 bc Intel(R) PRO/Wireless 2915ABG Network Connection

- Packet Scheduler Miniport

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.2.1	192.168.2.12	25
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.2.0	255.255.255.0	192.168.2.12	192.168.2.12	25
192.168.2.12	255.255.255.255	127.0.0.1	127.0.0.1	25
192.168.2.255	255.255.255.255	192.168.2.12	192.168.2.12	25
224.0.0.0	240.0.0.0	192.168.2.12	192.168.2.12	25
255.255.255.255	255.255.255.255	192.168.2.12	2	1
255.255.255.255	255.255.255.255	192.168.2.12	192.168.2.12	1

Default Gateway: 192.168.2.1

Persistent Routes:

None

Other commands I'm skipping over:

C:\>arp Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

C:\>netsh Is a command line interface to the options usually set from the control panel network connection properties.

You can use a command line to start the FTP protocol to get a remote file but it is quite aggravating compared to using one of the graphical FTP programs. I'll only hit on the very basics of using it here since most of us will never be forced to use it.

First, start the ftp program from the directory where you want the file you are getting to be placed. Connect to the server where the file is and give it your user name and password. Next if it is not a text file you are moving switch to binary mode for the transfer or your file will be mangled. You will then have to change to the directory where the file you want is located on the server and get the file. A typical session would look like this, user typing underlined:

```
C:\>ftp
ftp open stanmiller.info
connected to stanmiller.info
Please enter the user name.
user: xxxxx
Please enter the password.
password: *****
```

```
ftp binary
switching to binary mode
```

```
ftp dir
<< directory listed here >>
```

```
ftp get test.fil
<< file transfer confirmation and speed >>
```

```
ftp quit
```

The last command I'll cover is telnet, it is a simple one to use and has many uses for both your equipment and for checking remote equipment. It is considered obsolete by most security conscious folks and is replaced by SSH or another secure protocol. For the uses I'll cover it is adequate and safe enough to use.

What telnet does is similar to the command window under Windows, it opens a window where you can enter commands, see information or run programs that are compatible with a text interface. We will start off with the standard "show me the help" command and then cover the options most commonly used.

```
C:\>telnet /?
```

telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]

- a Attempt automatic logon. Same as -l option except uses the currently logged on user's name.
- e Escape character to enter telnet client prompt.
- f File name for client side logging
- l Specifies the user name to log in with on the remote system. Requires that the remote system support the TELNET ENVIRON option.
- t Specifies terminal type. Supported term types are vt100, vt52, ansi and vtnt only.

host Specifies the hostname or IP address of the remote computer to connect to.

port Specifies a port number or service name.

Of the above list the host and port are the ones you will most often need, you only need to enter the port when you are not connecting to the standard port, # 23.

You can get an additional list of options if you enter telnet with no other information and then t the prompt enter a “?” and press enter.

This would open a standard telnet session and request your username and password if I hadn't turned off my telnet service:

```
C:\>telnet stanmiller.info
```

This command will connect to the Escapees RV club's mail transfer machine on port 25 which is used by the SMTP (Simple Mail Transfer Protocol) to accept mail messages for forwarding to another user or system.

```
C:\>telnet mail.escapees.com 25
```

When it connects you will see a prompt like this to warn you that you are not on a “standard” port 23 telnet connection:

```
220 mail.escapees.com (IMail 8.22 11343-51) NT-ESMTP Server X1
```

This command will connect to the Escapees RV club's mail transfer machine on port 110 which is used by the POP (Post Office Protocol) to deliver mail messages to your machine.

```
C:\>telnet mail.escapees.com 110
```

```
+OK X1 NT-POP3 Server mail.escapees.com (IMail 8.22 202693-8)
```

The same thing but for DirecWay's mail servers:

```
C:\> telnet smtp.direcway.com 25
```

```
220 a34-mta02.direcway.com -- Server ESMTP (iPlanet Messaging Server 5.2 HotFix 1.25 (built Mar 3 2004))
```

```
C:\> telnet pop3.direcway.com 110
```

Putting the telnet command to work and doing something that we may need to do from time to time involves the SMTP mail system or the POP server storing our incoming mail. I copied these sections from the Internet documents that specify the protocols and cleaned them up a bit to make them clearer.

Using a telnet command to port 25 of your mail server you can send a test message and see the actual progress of the transactions as they happen, this is handy when your mail client stops working and tosses up an error message that makes no sense. You connect using telnet and send yourself a message and if it goes correctly you know the problem is not your mail server but something on your machine instead.

D. Scenarios

This section presents complete scenarios of several types of SMTP sessions. In the examples, "C:" indicates what is said by the SMTP client, and "S:" indicates what is said by the SMTP server.

D.1 A Typical SMTP Transaction Scenario

This SMTP example shows mail sent by Smith at host bar.com, to Jones, Green, and Brown at host foo.com. Here we assume that host bar.com contacts host foo.com directly. The mail is accepted for Jones and Brown. Green does not have a mailbox at host foo.com.

```
S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: RCPT TO:<Green@foo.com>
S: 550 No such user here
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel
```

If your machine won't receive mail you can do a similar thing with the POP (Post Office Protocol) server. Depending on your mail client and virus program some malformed, usually virus or spam messages can get stuck to the point you can't delete them or get anything newer out of your inbox on the server. Depending on your mail server you might be able to get the administrator to find and clear the offending message or to clear your whole inbox (all unread messages will be lost) or tell you to get a new mail or virus program as it isn't their problem. Of the three if you are lucky enough to get the first response all you have to do is wait until they get-round-toit. Using this method you can fix it in a couple minutes yourself.

POP3 Command Summary

Minimal POP3 Commands:

USER name valid in the AUTHORIZATION state
PASS string
QUIT

STAT valid in the TRANSACTION state
LIST [msg]
RETR msg
DELE msg
NOOP
RSET
QUIT

POP3 Replies:

+OK
-ERR

Note that with the exception of the STAT, LIST, and UIDL commands, the reply given by the POP3 server to any command is significant only to "+OK" and "-ERR". Any text occurring after this reply may be ignored by the client.

10. Example POP3 Session

S: = Server

C: = Client (mail program or telnet to port 110)

```
S: <wait for connection on TCP port 110>
C: <open connection>
S: +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C: USER name
S: +OK
C: PASS string
S: +OK user's maildrop has 2 messages (320 octets)
C: STAT
S: +OK 2 320
C: LIST
S: +OK 2 messages (320 octets)
S: 1 120
```

S: 2 200
S: .
C: RETR 1
S: +OK 120 octets
S: <the POP3 server sends message 1>
S: .
C: DELE 1
S: +OK message 1 deleted
C: RETR 2
S: +OK 200 octets
S: <the POP3 server sends message 2>
S: .
C: DELE 2
S: +OK message 2 deleted
C: QUIT
S: +OK dewey POP3 server signing off (maildrop empty)
C: <close connection>