TCP server debugging worksheet *Name* ____________________

1. SMTP – simple mail transfer protocol

OR: step-by-step guide to forging E-mail messages

SMTP is used by a client to transfer E-mail messages TO a server for delivery

Fill in the responses you see in the gaps

```
$ telnet ______________________ 25


HELO some.where.com

MAIL FROM:<>

RCPT TO:<your E-mail address>

DATA

From: womble@wimbledon.com
To: fred@flintstone.org
Subject: Greetings
Date: Mon, 17 Jun 96 11:24 PDT
(leave a blank line)
Hello!!
..Count the dots
.

QUIT
```

Now check your E-mail to see if the message has arrived (it may take a few seconds)

Things to notice about SMTP:

- Commands give both numeric result codes (for computers) and text messages (for humans)
- MAIL FROM and RCPT TO are the **message envelope** which gives the return address and delivery address, respectively. The "From:" and "To:" header lines in the message have no effect on the actual delivery
- You can send a message to multiple recipients – just repeat the RCPT TO line
- The DATA section is terminated by a period on a line of its own; any line which begins with a period must have an extra period inserted in front (which is removed upon delivery)
- You can send more messages in the same SMTP session by going back to MAIL FROM instead of typing QUIT

EXPERIMENT:

Connect again to a SMTP server and try the following commands (Not all servers implement them)

```
HELP
VRFY <username>        (Check if user exists)
EXPN <username>        (Expand mailing list)
```

2. POP3 – post office protocol, version 3

OR: how to read your E-mail without using an E-mail program!

POP3 allows a client to collect already-delivered mail FROM a server. It's the usual way a PC mail program will download messages for viewing locally

Make sure there is at least one message in your mailbox before starting.

Fill in the responses you see in the gaps

```
$ telnet ______________________ 110

USER your username

PASS your password (beware, it will echo!)

STAT

RETR 1000

RETR 1





QUIT
```

Don't worry: unless you use the DELE command, the message(s) you view will remain on the server.

Things to notice about POP3:

- Result messages are designed to be computer-readable, but simpler than SMTP: just "+OK" for success and "–ERR" for error
- Designed for use by computers not humans! But in emergency, people *have* been known to use this method for reading their mail…

EXPERIMENT:

While telnetted to the server, switch to another virtual console (e.g. Alt-F2),
type "netstat", and see if you can identify your TCP stream.
Does the POP3 server have a "HELP" command?
Does it matter whether commands are in upper or lower case?
What is the significance of the numbers given by the "STAT" command?

The full POP3 specification can be found at **ftp://ftp.internic.net/rfc/rfc1939.txt**