Inter-Office Memorandum

To	Distribution	Date	July 12, 1982
From	Andrew Birrell	Location	Palo Alto
Subject	Pupwatch	Organization	PARC/CSL

XEROX

Filed on: [Indigo]<Grapevine>Pupwatch>Pupwatch.bravo and Pupwatch.press

1. Introduction

Pupwatch is a program for observing PUP packets on your local Ethernet network. It will run on any computer that can run Alto/Mesa 6.0 or Cedar. Pupwatch operates by making the computer *promiscuous*, so that it will accept every well-formed Ethernet packet on the attached network. It then filters these packets to select only the packets which are from or to the particular PUP host currently being watched.

Pupwatch has a reasonable understanding of the common PUP packet types, the PUP Byte Stream Protocol and the Leaf "Sequin" protocol. On the display, Pupwatch shows you a summary of packets interactively as they arrive. By explicit command, you can cause Pupwatch to write a disk file containing details of the packets received.

2. User Interface

There are two entirely different user interfaces for Pupwatch: one on Altos (or machines emulating Altos) and one when running under Cedar.

2.1. Alto-Mesa

When it starts up, Pupwatch initialises its display, then prompts you with the message "Host (NLS-name or Net-address):". You should then type the PUP address of the host you want to watch. This may be a PUP address constant such as "3#17#" (note the second "#"), or it may be a Name Lookup Server text name such as "Ivy"; any socket number is ignored. Pupwatch will then display PUP packets it receives whose source or destination address matches the network number and host number you have given. Note that a network number is needed: Pupwatch is concerned with packets on the PUP Internet, not just Ethernet packets. The address you give need not be on your local network: if it is on another network, Pupwatch will perform the same filtering, to show you any packets addressed to or from that host which happen to pass through your local network. Unless you intervene, Pupwatch will now sit there forever showing you packets as it receives them. There are several commands you may type.

If you type a "?", Pupwatch will tell you the available commands. Typing a space causes Pupwatch to stop displaying packets; typing another space will cause it to continue. While Pupwatch is waiting for you to tell it to continue, it is still receiving packets and buffering them (subject to not getting more than 150 packets ahead of the last packet displayed); it will display

these packets when you let it continue. If you type an "h", Pupwatch will prompt you for a new host name; if you successfully give it a new host name, Pupwatch will re-initialise itself and watch for packets to or from that host. If you type "q" Pupwatch will terminate (returning to the disk or net executive as appropriate).

If you type an "s", Pupwatch will enter "slow" mode. In this mode it will wait for you to type a space after every 40 packets (so that packets don't go by faster than you can read them). If you type an "f", Pupwatch will leave "slow" mode and return to the default "fast" mode. If you type an "r", Pupwatch will replay buffered packets. Pupwatch retains at least the previous 150 packets, and up to 300. While replaying, Pupwatch is still receiving and buffering incoming packets (subject to not getting more than 150 packets ahead of the one being displayed). Using the "r" command causes Pupwatch to enter "slow" mode as if you had also given the "s" command.

If you type a "w" (and you are not running Pupwatch.boot), it will write a log of the buffered packets to the disk file "Pupwatch.log". The first use of this command commences writing at the start of Pupwatch.log; subsequent uses of this command during a single run of Pupwatch append to the file. Multiple uses of the "w" command will not cause a packet to be written to the file more than once. The details of the text written to the file for each packet are described below. Pupwatch.log is formatted with the assumption that you will look at it with a fixed pitch font. Printing it with Empress.run and the default font (Gacha 8) works well.

2.2. Cedar

The operations available when running under Cedar are basically the same as under Alto-Mesa. Instead of being invoked by keyboard commands, they are invoked by buttons. When it starts up under Cedar. Pupwatch initializes itself to watch the host that it is running on. You can change the host being watched by typing a host name or address constant in the text area following the "Host:" label then clicking "New Host". Click the "Pause" button to cause Pupwatch to stop displaying packets; this also causes the "Pause" button to change into a "Continue" button. The "Fast" and "Slow" buttons allow you to flip between "fast" and "slow" mode; the current mode is indicated by its button being gray. When Pupwatch pauses in "slow" mode, the "Pause" button changes into a "Continue" button. The "Write Log" button writes (or appends to) the disk log file; a viewer for the log file is created if necessary.

Two extra switches are available under Cedar. The "Yes" and "No" buttons following the "Broadcasts:" label control whether or not to display broadcast packets that would be received by the host being watched. The "Normal" and "Background" buttons following the "Priority:" label control the priority of the process that displays packets; using background causes less perturbation to processes on the machine where Pupwatch is running, but may cause the display process to get far enough behind that it misses packets. The current state of the "Broadcasts" and "Priority" decisions is indicated by the appropriate button being gray.

Closing the Pupwatch viewer has no effect on Pupwatch's state; it continues as if it was open. Destroying the Pupwatch viewer takes your machine out of promiscuous mode. It isn't sensible to run two instances of Pupwatch at one time.

3. Displayed Packets

Each packet displayed occupies a single line. Typical lines might look like:

```
1234: from 60#354#234 [aData,to:37064,L:52]   as??ghjk
```

```
40:     to 60#354#234 [ack,to:37014,pups:5]
123s: from 3#14#532   [mailCheckL,Birrell.PA]
```

The first number is the number of milliseconds that elapsed between receiving the previous packet and receiving this one. If this number would be greater than 9999, it is displayed as the number of seconds (for example "123s"). Intervals greater than 999 seconds are given as "long". The time interval is in decimal; all other numbers in Pupwatch are in octal. The clock used for this interval timing has a period of about 42 minutes; wrap-around of this clock is not detected. The time is followed by either "from" or "to" then an address of the form "a#b#c", where "a#b#" is the source or destination host of the packet (the destination or source is the host that you are watching), and "c" is the bottom 8 bits of the corresponding socket number. Then in square brackets is a summary of the packet. The summary always starts with the packet type, then has various details depending on the type. For many packets, the number of data bytes in the packet is given in the form "L:123". For packets involved in the PUP Byte Stream Protocol, these details include the bottom 16 bits of the sequence number at which this packet *ends*. For packets of type "data" or "aData", the packet summary is followed by the first few characters from the data part of the packet (with non-printing characters replaced by "?").

4. Logged Packets

When you use the "w" command, Pupwatch writes three lines to the log for each presently buffered packet that hasn't so far been logged. Typical lines might look like:

```
1234: from 60#354#234 [aData,to:37064,L:52] ID=432,37012 from=554,16234 to=6642,123
                                            as<0><1>ghjkeirukhfiekrhfg<15>pierutyzx
                                            141 163 0 1 145 150 152 153 145 151 162
```

The first line contains the time interval, the source or destination, and the packet summary as given for displayed packets. The remainder of the first line contains the PUP packet ID, source socket number and destination socket number, each written as a pair of 16 bit octal numbers. The second line contains up to the first 50 characters of the data part of the packet, with non-printing characters replaced by "<octal-number>". The third line contains up to the first 25 data bytes of the packet as octal numbers.

5. Limitations

Pupwatch can buffer up to 300 packets, although it will only buffer up to 150 packets ahead of the one currently being displayed (to ensure that the "replay" facility works). If it runs out of buffering space and this might cause it to ignore a packet to or from the host being watched, then the message "Packet(s) lost" is displayed (or logged) when that point in the packet sequence is reached. On an Alto (or Alto emulator), although Pupwatch's Ethernet driver tries hard to avoid missing packets it will occasionally miss packets that are successfully received by other hosts (because Pupwatch must inspect *every* packet on the local Ethernet). Pupwatch does not detect this happening. Running under Cedar, the Ethernet driver should see all packets, unless insufficient processor time is available to it. When Pupwatch is running under Cedar to watch the host it is running on, Pupwatch guarantees to see all packets received by the Pup socket level or Cedar's RPC runtime. Pupwatch will not receive PUP packets having more than 532 data bytes.

6. Released Versions

Pupwatch is available in four versions: Pupwatch.boot, Pupwatch.run, Pupwatch.bcd and Pupwatch.df. Each version has its advantages. Pupwatch.boot is network bootable on Altos (or Alto emulators), but it does not have the disk logging facility. Pupwatch.run needs to be invoked from the Alto disk executive. Pupwatch.bcd runs on Altos and is much smaller than Pupwatch.run, but you need to have Runmesa.run and Mesa.image on your disk. Use Pupwatch.df to run Pupwatch under Cedar.

Pupwatch.boot is installed on the Ivy boot server; on network 3, it may be booted by name from the network executive, or by booting an Alto while holding down the "backspace" and "L" keys. The availability of Pupwatch.boot on other networks depends on it being installed there by gateway or IFS administrators. Pupwatch is boot file number 40; it may be copied from [Ivy]<System>Boot>40-Pupwatch.boot. The other Alto versions may be copied from [Indigo]<Grapevine>Pupwatch>Pupwatch.run and Pupwatch.bcd. The Cedar version can be obtained by using Bringover to fetch the public file from [Indigo]<Cedar>Top>Pupwatch.df.

7. Maintenance

Pupwatch will be maintained at a leisurely pace for as long as it is useful to CSL. If you have comments, suggestions (including requests for interpretation of extra protocols) or bug reports, send a message to LaurelSupport.pa.

Last edit: July 12, 1982 3:22 PM