MEMORANDUM

To: F.E.Heart

From: B.Cosell

Subject: Network Reliability

Date: 4 October 1971

I have been thinking about how to make our IMP recovery procedure more effective. Much IMP downtime can be eliminated by merely providing an operator at the NCC more often. The hope was that by providing that operator with a little education and a devilishly clever set of procedures we would be able to make him self-reliant for nearly all IMP outages. To actually achieve that goal, unfortunately, would require an immense education and a set of procedures much too complicated and non-deterministic to be constructable, much less usable.

There are two distinct types of analysis done on broken IMPs: diagnosis and confirmation. The first consists of taking a potentially "new" crash and figuring out what went wrong. This is beyond the scope of one not intimate with the program. The second type consists of recognizing the crash at hand as one from a set of known, likely types of crashes. All but the simplest of these are beyond the abilities of an operator. When told where to look and what to expect, he would be able to observe that a particular bit in a particular region of memory was dropped (a common problem), but he wouldn't be able to guess that a machine broke because of a dropped bit, much less determine which registers were dropping which bits. At some level or another, software people will have to intervene to understand what is happening in a crash.

The way to achieve the parallel goals of getting the IMP back on the air quickly while still allowing a detailed analysis of the failure is to provide a core dumping facility. The operator, if he can't quickly understand a given problem, should be able to save the clues by dumping all of core somewhere, then reloading and restarting. Programmers could then post mortem from the core dump at their leisure.

I have spoken to several of our hardware people and they unanimously believe that failing memories will be a chronic problem with the network. This problem is important because it often takes several hours of poking to find out what bit was dropped where, and it is not even easy to determine that a dropped bit was the cause of the problem. No matter how we decide to proceed on these issues, some mechanism for quickly scanning all of memory and determining if there are any dropped bits will have to be built.

Any such mechanism is constrained in several ways. First, the mechanism must work while the affected IMP is not on the net. Hence, either the mechanism must be in the affected IMP, or the contents of the IMP's core must be sent to the mechanism. Since part of the mechanism will have to be a correct core image to compare against, the alternative of sending the core load to the mechanism is the reasonable alternative. Punching out all of a core image on paper tape via an IMP teletype has been shown to be unfeasible. Hence, the core load must be sent over the network. The mechanism will have to incorporate sufficient storage capacity to accept and save several core loads, at 24K each. The mechanism, therefore, will need some sort of bulk storage device attached to it. Once again, two alternatives present themselves. The first is to attach a disc or mag tape unit, or other recorder, to the NCC, or some other network machine at BBN, and have it store the core loads; the second is to use some operating system's bulk store. Either alternative can be made to work. The large system approach is the more attractive, however, because it would be easier to use, more powerful, and more flexible.

If, for the large system, we were to choose the PDP-1, we would gain further advantages. A major one is the ease of building the software. Since the PDP-1 would not be burdened with being a "server" host, there would be no need to implement Host protocol and then gimmick up its NCP to handle the core receiver. We can declare the PDP-1 the "Network Analysis Center" whose sole purpose on the net is to provide a tool for our use. In addition to its basic analysis facility, including a symbolic debugger and core verifier, the NAC can perform such functions as IMP and TIP re-loads, patch distribution, etc. It could also provide the "interrogation" facility that seems so difficult to build into the NCC. All of these are quite easy once the initial connection to the network is established. Later, we could even decide to implement HOST or TELNET protocol if we wanted, but this would not be necessary to the NAC activities. A further consideration is that we might be able to convince ARPA to defray some of the PDP-1's operating costs.

With the NAC in operation, a core load would be dumped over the network directly to it and then later analyzed at great depth. Because of the PDP-1's nearly infinite drum capacity, this deferred analysis could include archiving snapshots of problems too difficult to be understood for examination weeks or months later in conjunction with the core loads of other crashes suspected to be similar.

The core dumper could be initiated by the NCC operator and could even be automatically initialed by the watchdog timer. If some problem which is watchdog-timer-correctable crops up, we could be working on locating it right away without either having to wait for a complete failure or having to run the machine without the watchdog timer on. Thus, we could plan on always, even in times of crisis, having the watchdog timers operative.

Providing the PDP-1 as a tool for helping us run the network more effectively is a generally good thing, and has many specific advantages. It will certainly be adequate to the task. The FASTRAND makes storage considerations no problem. Since it will not be essential to network operation, we may consider not merely its percentage down time, but the product of its probability of being down with the probability of a failure in the net. A crude calculation indicates that we would miss a core load once every few months, so reliability is no problem. I recommend that we immediately begin coordinating an effort to get the PDP-1 on the net with our efforts to provide more comprehensive operator coverage.

BC/jm

cc: HKR
WRC
RA
SMO
DCW
MJT
JMcQ