

Foreign Node Capture

Network diagnostic

Wed, Jan 28, 1998

The Internet is a global network that permits access to any IRM or local station from anywhere. This note describes a method for capture of such network activities as an aid to security concerns.

The *SNAP* Task processes all IP communications, so it is a likely point of introducing a diagnostic for capturing foreign node frame activity. The information available from the message queue that is read by *SNAP* is the frame size, a pointer to the received frame, and the physical network addresses. *SNAP* processes the IP header, so it knows the location of the frame contents. To determine whether a frame is sent from a foreign source, the source IP address field in the IP header must be compared with the local node's IP address and subnet mask.

This diagnostic facility records the time of day along with the first part of the frame content, so as not to use too much memory. It uses a timer counter to establish the first frame received from the foreign node. If the counter is zero, the received frame is considered the first one. If the counter is nonzero (counting down), the frame is considered the last one. In either case, the timer counter is reset to the full time interval used.

When a frame is received, find the source IP address and test it for being foreign. If it is foreign, check if this IP address has been recorded previously and is now active; i.e., has a nonzero timer counter. (If the timer counter is zero, leave it alone, as it represents a complete record, albeit an older one.) If none is found, record a new first frame and set the counter. If one is found, record a new final frame and reset the counter to the full time interval. In this way, we should have a capsule summary of foreign frame activities. By examination of the frame contents, we can determine the nature of the foreign frame activities encountered.

How much data should be captured? Suppose we capture an 8-byte time-of-day of the usual format, followed by the first 56 bytes of the frame. With 20 bytes for the IP header, 8 bytes for a UDP header, it leaves 28 bytes of UDP datagram content. (If token ring is used, another 8 bytes is consumed by the *SNAP* header, so that only 20 bytes remain.) Since this diagnostic is meant only to capture foreign frame activity, the frame header is of little or no interest.

By using a fixed place in memory for this diagnostic, each station has a copy that can show what foreign nodes accessed the local node. Note that an access may be initiated by the local station, as there is no easy way to distinguish a generic request message. If the local node pings a foreign node, the foreign node's response will be entered into the buffer.

An example that shows the format of the foreign node capture buffer is as follows:

```

0576:006800 9801 2314 3823 0219 Date,time of first frame captured
0576:006808 4500 0028 C7C6 0000 First frame contents
0576:006810 3111 C429 83A9 70D4 Source IP address = 131.169.112.212
0576:006818 83E1 8576 1A90 1A90 UDP port# 6800
0576:006820 0014 A389 000C 0000 Classic reply message
0576:006828 0099 0000 28A2 0000
0576:006830 28A2 0000 E900 0000
0576:006838 FFFF B345 2845 1019

0576:006840 0006 0014 3841 1119 Time of last frame captured within period
0576:006848 4500 0076 C982 0000 Last frame contents
0576:006850 3111 C21F 83A9 70D4
0576:006858 83E1 8576 1A90 1A90
0576:006860 0062 A349 0030 0000 Classic reply message
0576:006868 0109 0000 0000 0000
0576:006870 0000 0000 5445 534C
0576:006878 4120 4952 4D2D 3120

```

This example shows the first record. The buffer is located at 00006800–00006FFF, so there is room for 16 of these 128-byte record structures. A record is built over a time interval that lasts as long as there are frames received within the countdown timer period, which is 30 seconds. When a timer period passes without receiving any more frames from the same IP address, the record is complete. Subsequent frames from the same IP address will cause a new record to be built. The buffer is treated as a circular buffer of 16 records, so that records will be lost when the 17th record has been opened.

The count of frames received from the node (whose IP address is found in the captured first frame's IP header) within the time interval of activity is in the first word in the second half (at 00006840 in the above example). The countdown timer is the next byte (at 00006842 above.) The next 5 bytes are the time-of-day hours, minutes, seconds, cycles, and half milliseconds. The year, month, and day are likely to be the same as in the first frame's time-of-day, which is complete.

There are a few variables in the SNAP Task that relate to this diagnostic work. At present, they can be found at 0004C612, but that may change in the future, if task stack sizes must be changed. Here is an example:

```
0004C612 0100 001E 0000 0002
```

The 0100 word is the byte offset into the buffer for the next record to be recorded. The 001E is the 30 second period value. If one needs to modify this period for a special experiment, simply change this word. Its contents provide the value used to reset the timer countdown words in each record. The last four bytes are the total record count. If this value is greater than 00000010, then the buffer has wrapped, and records have been overwritten. After resetting the system, these four words will be 0000 001E 0000 0000.