SNIFFER CIRCUIT DESCRIPTION

Author: C.R.Read
Date: 10/25/84
File: //users/crr/docs: sniffer

GENERAL DESCRIPTION

The SNIFFER circuit is an add-on daughter board to Nestar's IBM-PC NIC. Its purpose is to "massage" each data packet from the network before it reaches the RIM so that every data packet looks like a broadcast. This fools the RIM into accepting every data packet irrespective of its destination address (DID). Because of the operation of the RIM, only the first of the two DIDs need be zeroed, which fortunately leaves the second to be loaded into the buffer intact. As the data has been modified, the CRC check within the RIM will fail and the RI status bit will not be asserted, so that the SNIFFER must generate its own "Packet Received" signal. This signal may be either polled by software or may generate an interrupt, these alternatives being under software control.

CIRCUIT DESCRIPTION (see Figure 1)

The circuit is initialised by the IDLE PERIOD TIMEOUT CIRCUIT after 6.25uS of inactivity on the network. On ARCNET there is a guaranteed idle period between every transmission of 12.6uS. Reflections from an unterminated, maximum length (2000 feet) RG 62 cable will settle within 4.9uS. So detecting 6.25uS of inactivity will ensure that a reliable RESET signal is generated between every packet. The RESET signal is cleared by the first data bit on the RX serial data line into the RIM.
The START OF HEADER (SOH) DETECTOR discriminates between the wanted data packets and the other four unwanted types of packets which occur on ARCNET. [see Token Passing Protocol Boosts Throughput in Local Area Networks - by John A. Murphy - Electronics, September 8th, 1982]
The SOH DETECTED signal from this circuit initiates a 1 byte delay in the DID SYNC circuit which then generates a PACKET signal which is synchronous to the beginning of the DID byte. The DID BLANKING COUNTER generates the correct length blanking pulse (KILL) which is fed back to the NIC to gate out the DID byte into the RIM.
The PACKET signal is cleared by the RESET signal 6.25uS into the next idle period. The falling edge of PACKET then sets a latch which sets a flag or pulls an interrupt in the NIC to indicate that a complete packet has been received.

IDLE TIMEOUT CIRCUIT

This circuit behaves like a re-triggerable monostable with a period of 6.25uS. It comprises 2 cascaded divide by 5 counters followed by a divide by 2. The counter chain is cleared (active high reset) by the positive pulses on the RIMRX signal from the TRANSCEIVER which occur whenever there is activity in the network. After the last bit of a packet, the counter will start counting up but will lock-up when the count reaches 25 (half of full count) when the inverted MSB (RESET) will inhibit the 4 MHz clock. The RESET signal then will occur 25 x 0.25uS or 6.26uS after the last network activity.

DATA CLOCK GENERATOR

The data clock (CA) into the RIM is essentially a 5 MHz square wave, interrupted at the end of each byte by the data synchronisation signal (DSYNC) from the RIM. To generate a synchronous data clock (DCLK) for the sniffer the CA is divided by 2 by a J/K which is cleared by DSYNC. This produces a sequence of 9 pulses, in which the first 8 positive going edges occur in the middle of the data bits in the byte.

START OF HEADER DETECTOR

The first byte after the ALERT BURST (6 one-bits) is one of five packet-type control characters. For a DATA PACKET this character is an ASCII SOH which is unique in having 7 contiguous zeros. This is detected by shifting the inverted data from the TRANSCEIVER into an 8 bit shift register and ANDing 7 adjacent bits. The output of the AND gate is latched by the transceiver clock (CA) into a J/K. The output of this (SOH DETECTED) enables the DID synchronisation circuit. This circuit originally detected 4 contiguous ones of the ALERT BURST before recognising the SOH character, which accounts for the XOR data invertor. However this caused problems of "lost packets" and so was modified. [see the appendix - SNIFFER HARDWARE PROBLEMS].

DID SYNCHRONISATION CIRCUIT

After a SOH character has been recognised a check must be made that there are subsequent valid bytes, to eliminate false triggering by the idle period that follows one of the other types of packet. This is done by counting 2 further rising edges of the DSYNC signal. DSYNC clocks a D-type divide by 2 whose output then clocks a "1" into a latch. The output of this latch (PACKET) determines the start of the first DID byte.

DID BLANKING COUNTER

There are 9 data clock (DCLK) edges to every byte so the byte length signal is generated by clocking PACKET through a 9 bit shift register (an 8-bit S/R plus a F/F) with the negative edges of DCLK. The inverted output of this S/R is ANDed with PACKET to produce the blanking signal. This signal is then gated with the software controlled SNIFF signal to produce the KILL signal. KILL is fed back to the NIC to control the gate which blanks out the DID in the serial data line into the RIM. The SNIFF control allows the SNIFFER to behave like a normal NIC.

PACKET RECEIVED LATCH

The packet received signal (SNIFFINT) which flags the end of a data packet is generated by setting a latch with the falling edge of PACKET which will occur when the system is reset by the idle period timeout circuit. The output of the latch is also gated with SNIFF to generate SNIFFINT before being fed back to the NIC.

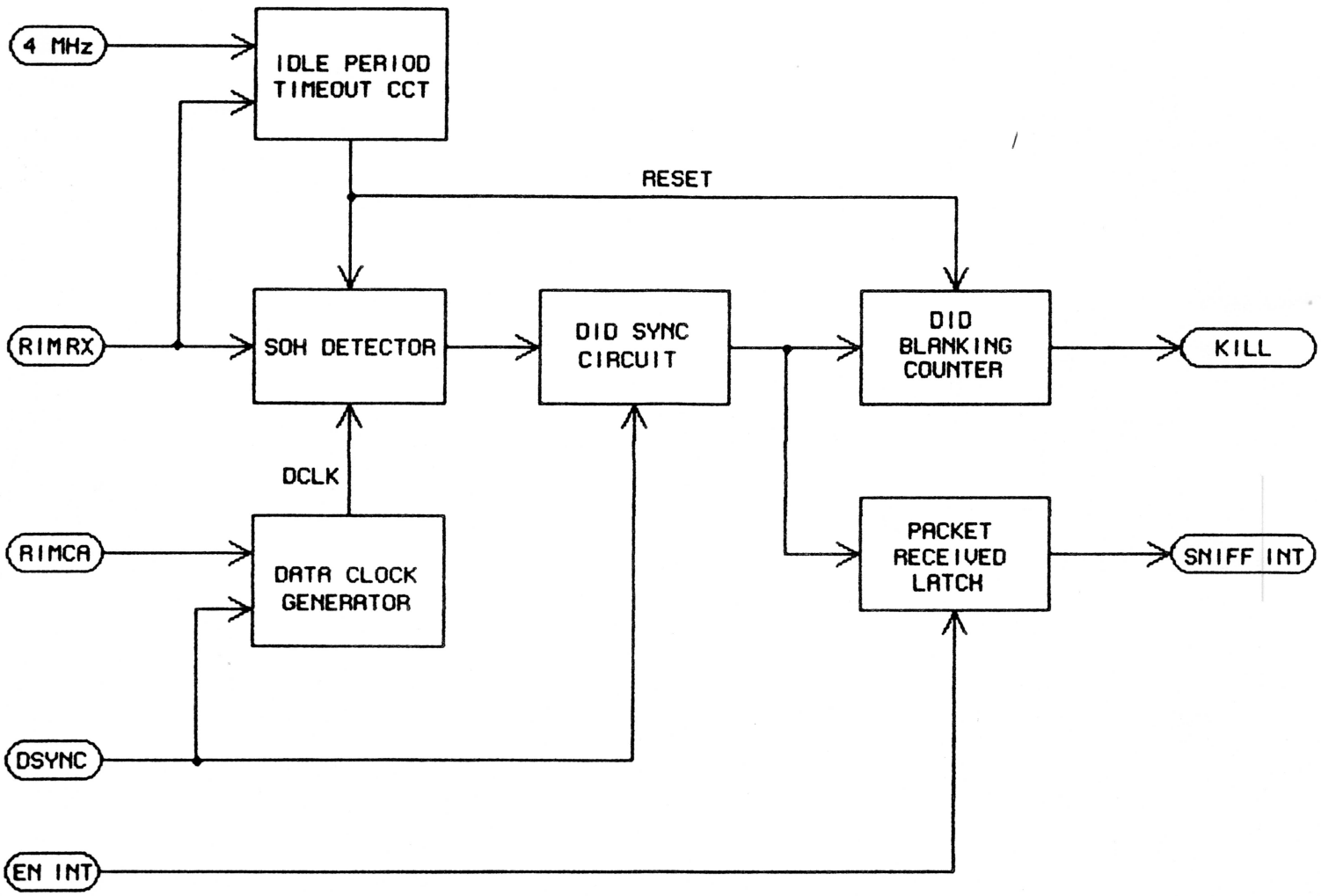


FIGURE 1 SNIFFER BLOCK DIAGRAM

APPENDIX - SNIFFER HARDWARE PROBLEMS

Author: Chris Read
Date: 6/4/84
File: //users/crr/docs:snifmods

INTRODUCTION

There are two hardware problems with the Sniffer hardware (revision - 001).
Firstly, certain sniffer addresses were known to produce false triggering, and it was thought that it occurred when the token was received.
Secondly, a small percentage of data packets were being missed by the Sniffer.

FALSE TRIGGERING

a) The data packet detection circuit looks for a string of 7 contiguous zeros after the ALERT burst. This will detect the Data Packet control character (SOH = $01) but none of the other 4 control characters (EOT,ENQ,ACK or NACK). Following the SOH DETECTED signal the circuit requires 2 rising edges of DSYNC (the byte synchronising signal from the RIM) to generate a PACKET DETECTED signal.
Because the SOH only looks for 7 contiguous zeros, a destination address (DID) of $80 or $01 in any Token or Free Buffer Enquiry will trigger the SOH detector circuitry. The RIM however will only generate one DSYNC pulse after the first (triggering) DID and so will not generate a PACKET DET interrupt signal.
BUT, if the token is addressed to the RIM it generates 2 extra DSYNC pulses and thus generates a false PACKET detected interrupt !

b) Again because the SOH detector only looks for 7 zeros, there will be a SOH DET at the end of EVERY data transmission after the data has ended. This normally doesn't matter because there are no DSYNCs.
However, two factors combine to produce false triggering.
If the last 6 or 7 bits of the Sniffer's station address are zero ($01, $02 or $03) then this final SOH will occur earlier and will just get caught by the first of the extra DSYNCs and then by the second extra DSYNC causing the false PACKET detection.

Various Sniffer station addresses were tried (eg C0,C1,11 & 81) but no problems were detected either when running the Sniffer program or observed on the Logic State Analyser. Only Sniffer station addresses $01, $02, $03 and $80 will cause false triggering when the token comes around.

MISSED PACKETS

The Sniffer ALERT detector circuit, which starts the packet detection sequence, looks for a sequence of 4 contiguous '1's following an IDLE timeout. This was chosen because it was thought that the RIM also triggered on the first 4 '1's and it would protect against spurious activity on the line.
However, the RIM sometimes triggers after only 2 or 3 bits of the Alert burst which causes it to drop it's DSYNC signal early, with unfortunate results.
The data clock of the Sniffer (DCLK) is generated by dividing the RIM's CA by 2 and gating it with DSYNC, so when DSYNC goes low DCLK is inhibited. So in the case where the RIM detects the Alert burst early, the ALERT detector circuit does not get the required number of clock pulses and thus fails to trigger.
There is one saving factor, which is that if DSYNC drops after only 3 bits of the Alert burst of a DATA PACKET, the next bit clocked into the Alert detector circuit will be the '1'(LSB) of the SOH character and so the circuit will trigger, although late. This reduces the probability of missing Data Packets (which are the only ones we are interested in).
The probability of an 'early' DSYNC seems to be dependent on the time delay between messages on the line and can be made to vary by changing the number of stations or the propagation delay in the line (by adding a HUB for example), it is therefore not predictable or controllable.

ENABLING THE SNIFFER IN THE MIDDLE OF A DATA PACKET

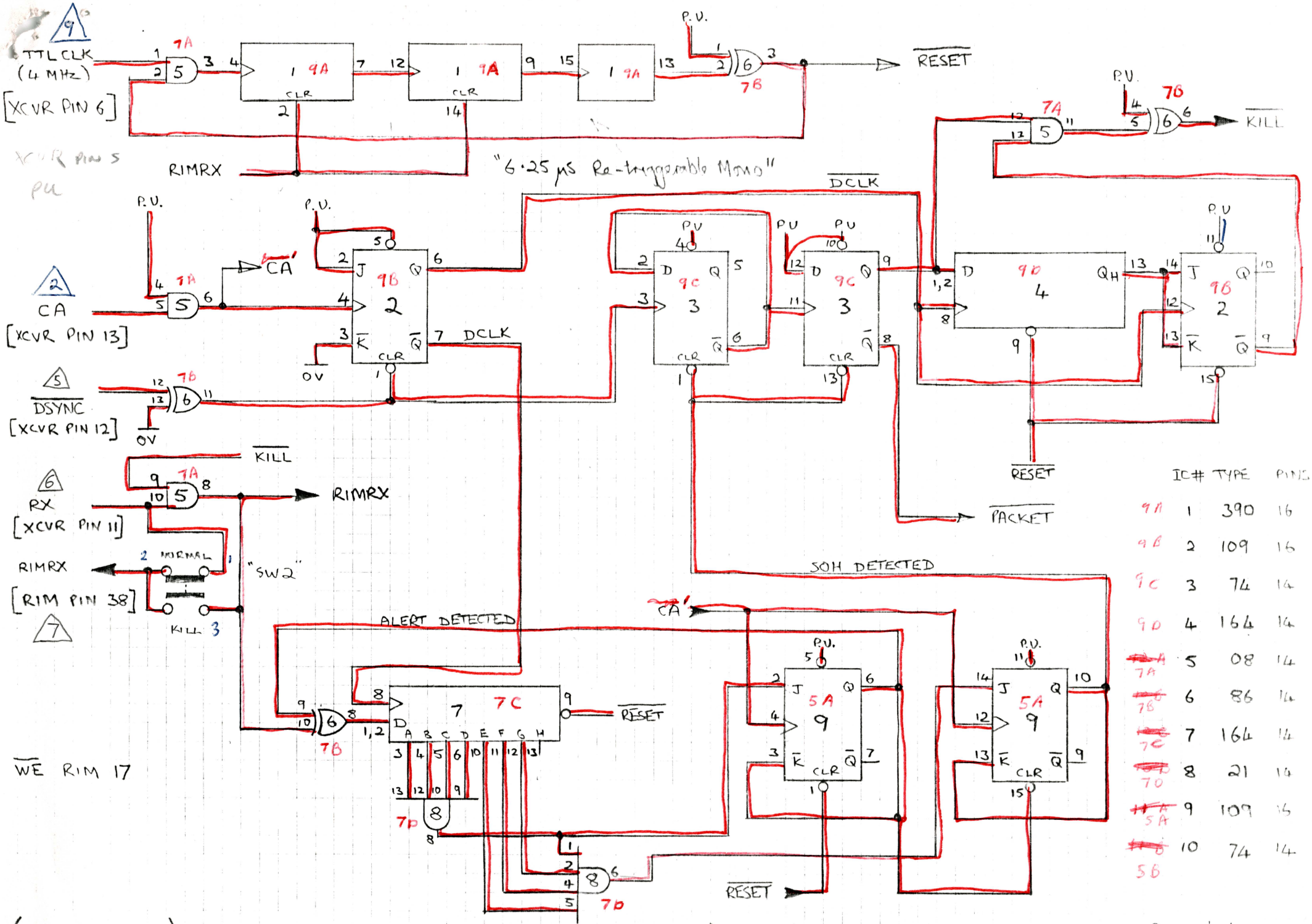
I was thought that if the Sniffer was enabled in the middle of a data packet then the sequence '4 x ones' followed some time later by '7 x zeros' was likely to occur and cause false triggering.
This cannot happen because the ALERT and SOH detection must occur within the first 3 bytes otherwise the KILL signal will not be generated and therefore the RIM will not be fooled into thinking it had a broadcast. It will therefore not generate DSYNC pulses after the 4th byte.

RECOMMENDATIONS

The problem of false triggering only occurs with adresses $01, $02, $03 & $80 and therefore can be prevented by prohibiting them.
The problem of missing data packets due to 'early' DSYNC pulses can be solved by a simple modification to the circuit (see below).
This modification will enable the ALERT detector immediatly after any activity on the line (ie when the RESET signal is lifted). This should be safe against spurious pulses on the line because of the 2 stage filtering in the HYBRID and the TRANCEIVER.

HARDWARE MODIFICATION

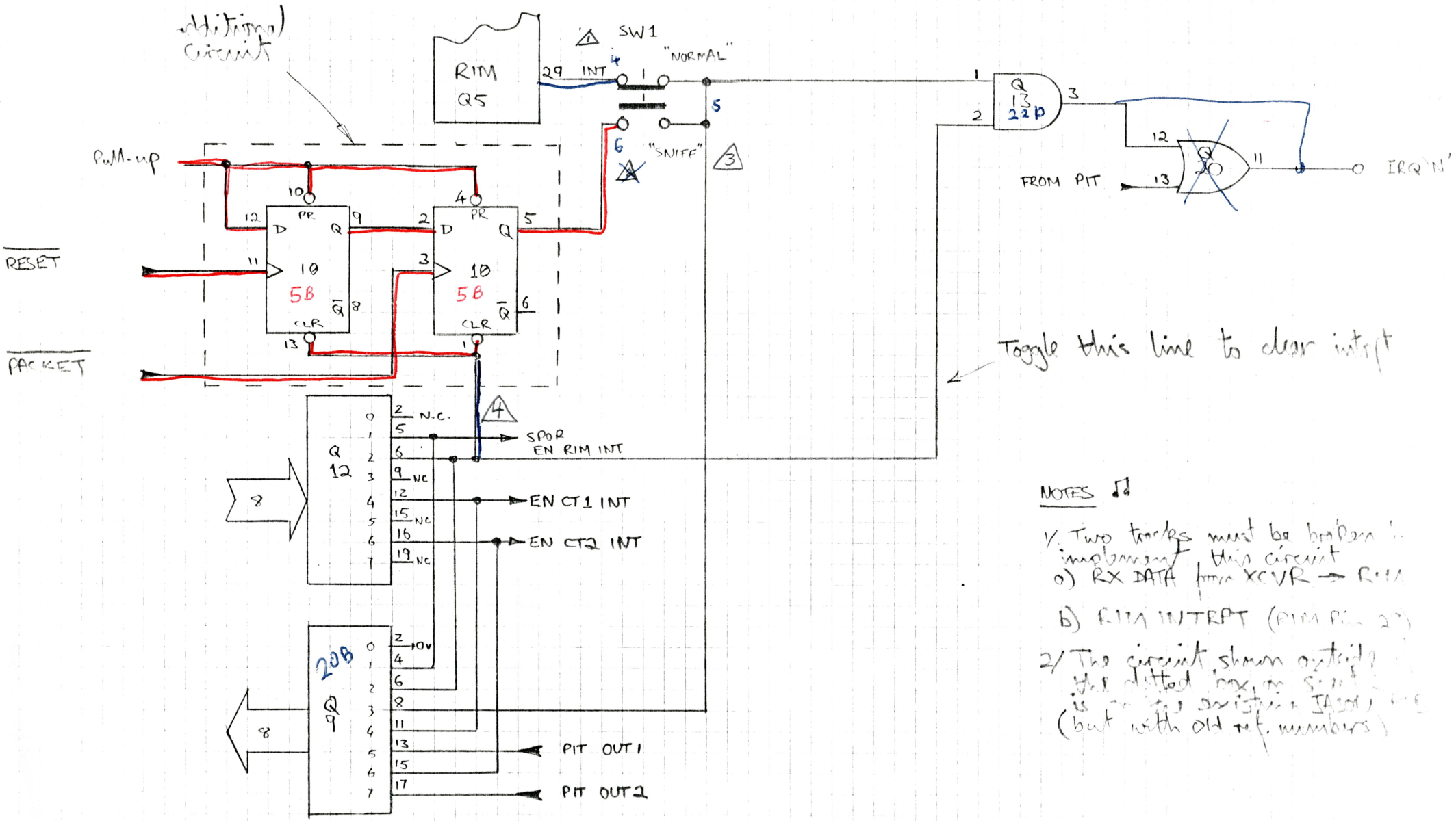
Cut trace between IC 3 pin 2 and IC 6 pins 1,8 just above IC 3 pins 1,2.
Link IC3 pin 2 to pull-up on IC 3 pin 11.
This modification may be possible on potted versions (by carefully removing the potting under IC 3) and can easily be done on un-potted boards.
This modification has been incorporated into the -002 revision of the PC boards.



(SHEET 1 of 2)

TRANSMIT AND RECEIVE TOTALISER (TART) (NEE SNIFFER)

SPR 11/8/82



NOTES

1/ Two tracks must be broken to implement this circuit
a) RX DATA from XCVR → RIM
b) RIM INTRPT (RIM Pin 29)

2/ The circuit shown outside the dotted box is in the existing IA (but with old ref. numbers)

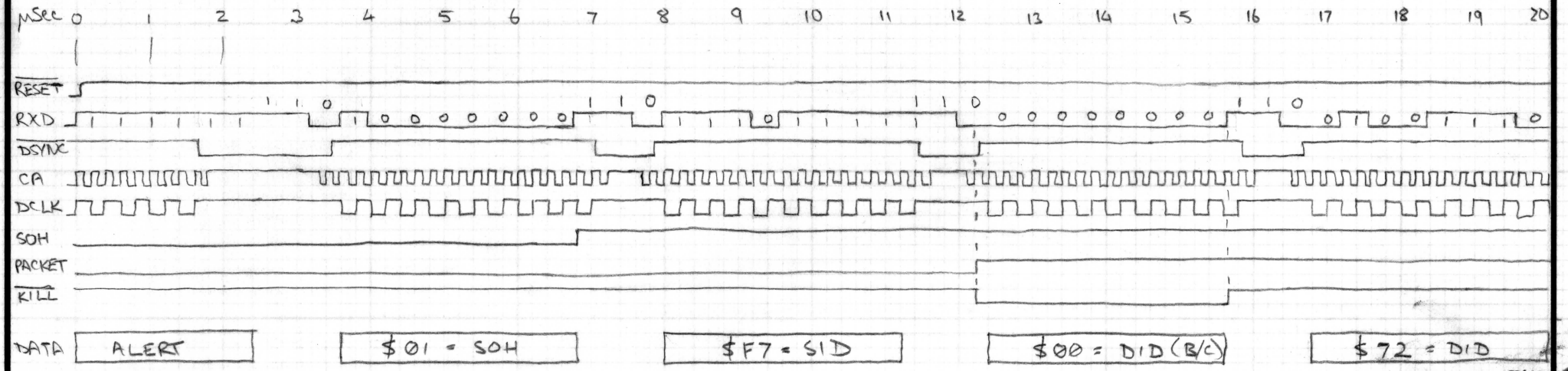
(SHEET 2 of 2)

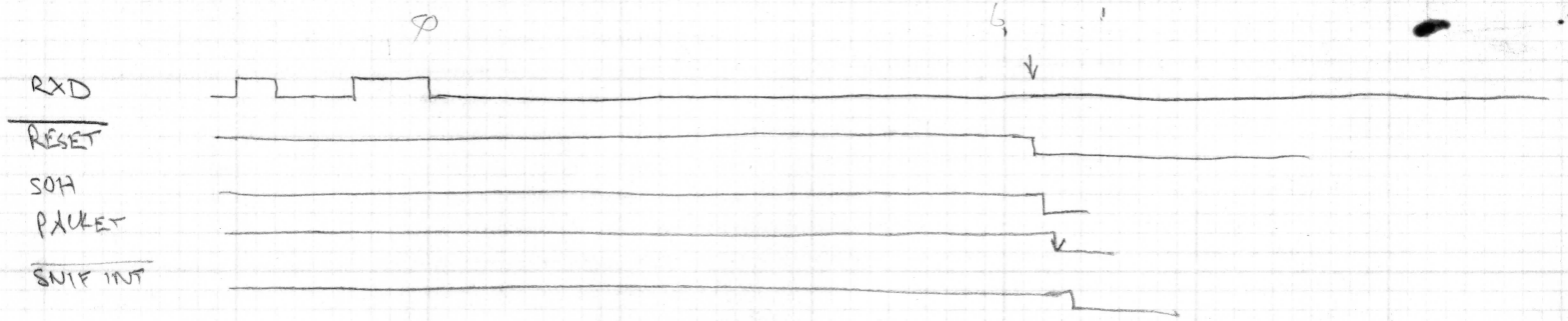
TART END OF PACKET INTERRUPT

12/10/82

REVISIONS			
LTR	DESCRIPTION	DATE	APPROVED

200 nS / Div





NOTE THE FIRST 'DID' IS CLAMPED TO ZERO WHICH FOOLS THE RIM INTO THINKING IT IS A BROADCAST. THE SECOND DID IS LOADED INTO RAM BY THE RIM WHERE IT CAN BE READ

TOLERANCES UNLESS OTHERWISE SPECIFIED		
FRACTIONS	DEC	ANGLES
±	±	±

APPROVALS	DATE
DRAWN	
CHECKED	

SNIFFER WAVEFORMS

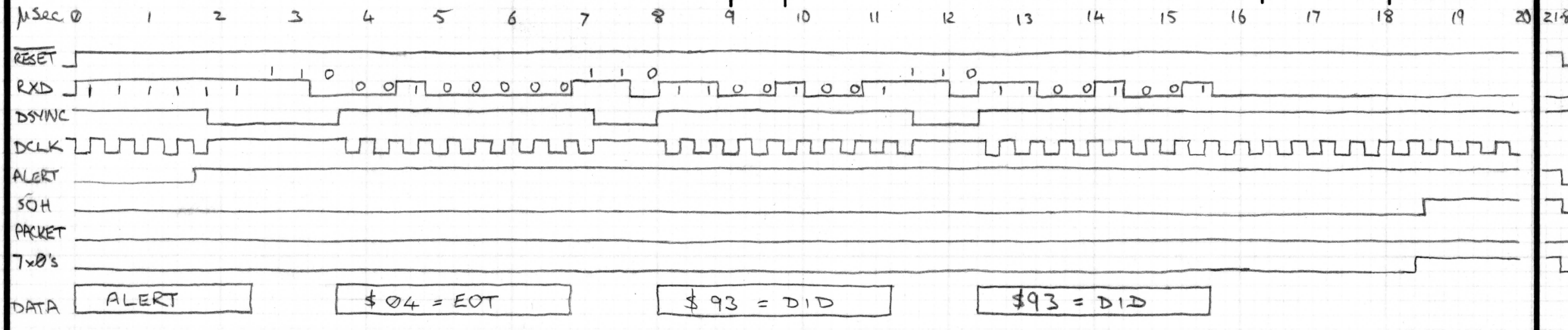
'SNIFFED' DATA PACKET

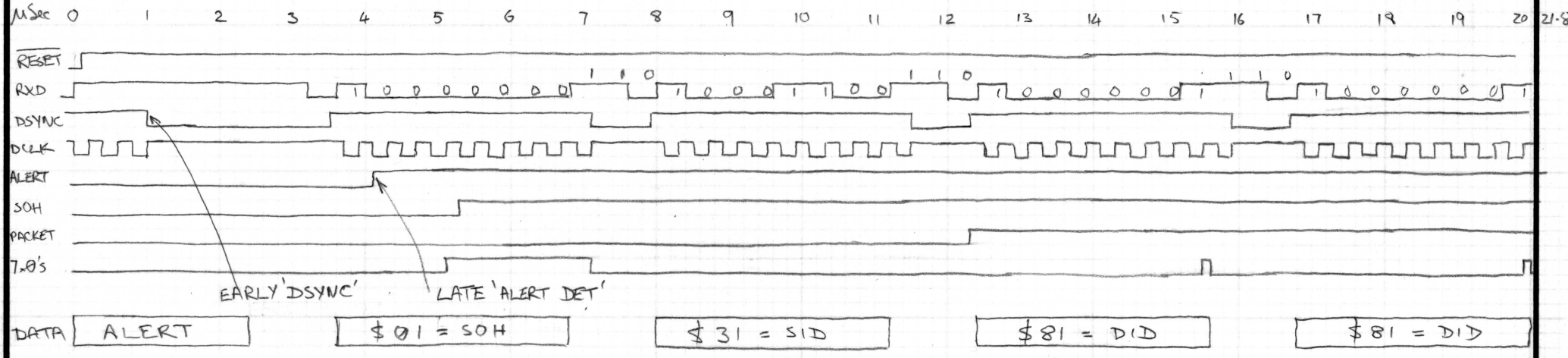
SCALE	SIZE	DRAWING NO.
	A	

DO NOT SCALE DRAWING

REVISIONS			
LTR	DESCRIPTION	DATE	APPROVED

SCALE = 200μS / div





NOTE 'DSYNC' DROPS AFTER ONLY 3 RISING EDGES OF 'DCLK' HOWEVER, AS THE LSB OF 'SOH' IS A '1' THERE ARE STILL 4 CONTIGUOUS '1's CLOCKED INTO THE SHIFT REG. SO 'ALERT DET' IS SET JUST IN TIME TO TRIGGER 'SOH'

TOLERANCES UNLESS OTHERWISE SPECIFIED
FRACTIONS ± DEC ± ANGLES ±

APPROVALS	DATE
DRAWN	
CHECKED	

SNIFFER WAVEFORMS

UPPER = TOKEN PASS TO NON-SNIFFER STN

LOWER = DATA PACKET TO NON-SNIFFER STN

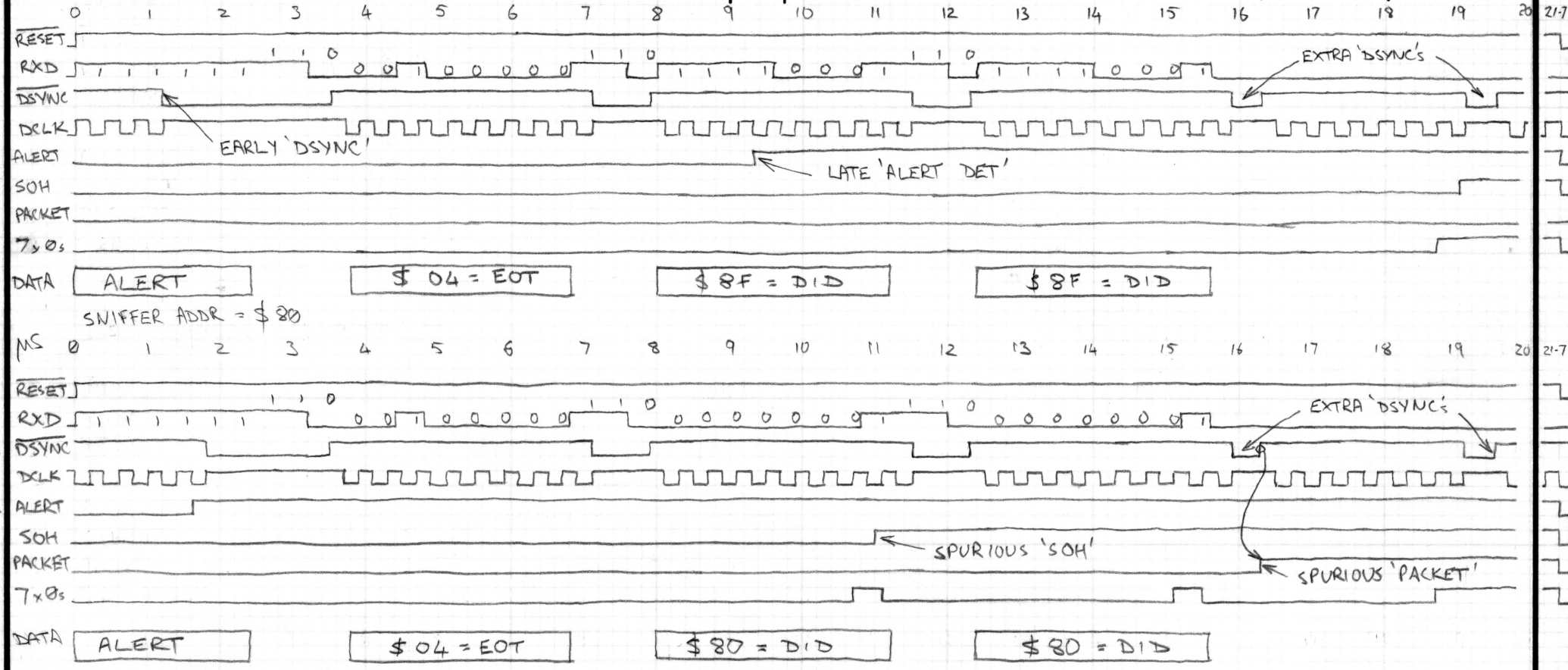
SCALE | SIZE A | DRAWING NO.

DO NOT SCALE DRAWING | SHEET 2 of 3

REVISIONS			
LTR	DESCRIPTION	DATE	APPROVED

SCALE = 200 uS / div

SNIFFER ADDR = $8F



SNIFFER ADDR = $80

NOTE LOWER W/F SHOWS SPURIOUS 'PACKET' SIGNAL CAUSED BY SEVEN CONTIGUOUS '1's IN AN ADDRESS GENERATING A SPURIOUS 'SOH'. THE EXTRA 'DSYNC' PULSES OCCUR WHEN THE RIM RECEIVES THE TOKEN & THEY CLOCK 'PACKET'

NOTE UPPER W/F SHOWS HOW 'DSYNC' DROPPING BEFORE 4 x '1's OF THE 'ALERT' CAUSES 'ALERT DET' TO BE GENERATED LATE. 'ALERT DET' WILL NOT BE GENERATED AT ALL IF THERE ARE NOT 4 CONTIGUOUS '1's IN THE DIDs OF A TOKEN.

TOLERANCES UNLESS OTHERWISE SPECIFIED		
FRACTIONS	DEC	ANGLES
±	±	±

APPROVALS	DATE
DRAWN	
CHECKED	

SNIFFER WAVEFORMS (RECEIVING TOKEN)

UPPER W/F STN ADDR = $8F

LOWER W/F STN ADDR = $80 (BAD)

SCALE	SIZE	DRAWING NO.
	A	

DO NOT SCALE DRAWING

SHEET 3 of 3

Hints for using the sniffer.

The Sniffer board can be placed in any IBM slot and will work in any 64k, basic PC with at least 1 disk drive. The only restriction in the layout in the host machine is that there must be at least 64k of expansion memory contiguous with the 64k on the main system board (i.e. address starting at segment $1000). The expansion memory need not be declared by the switches as the expansion memory is found by the sniffer initialisation routine. The sniffer can also work as an ordinary NIC so before using it the switches at the top of the board must be turned on (towards the front of the PC). Also the memory segmnent where the card is placed must be set to $D200 or else it will not respond to software commands.

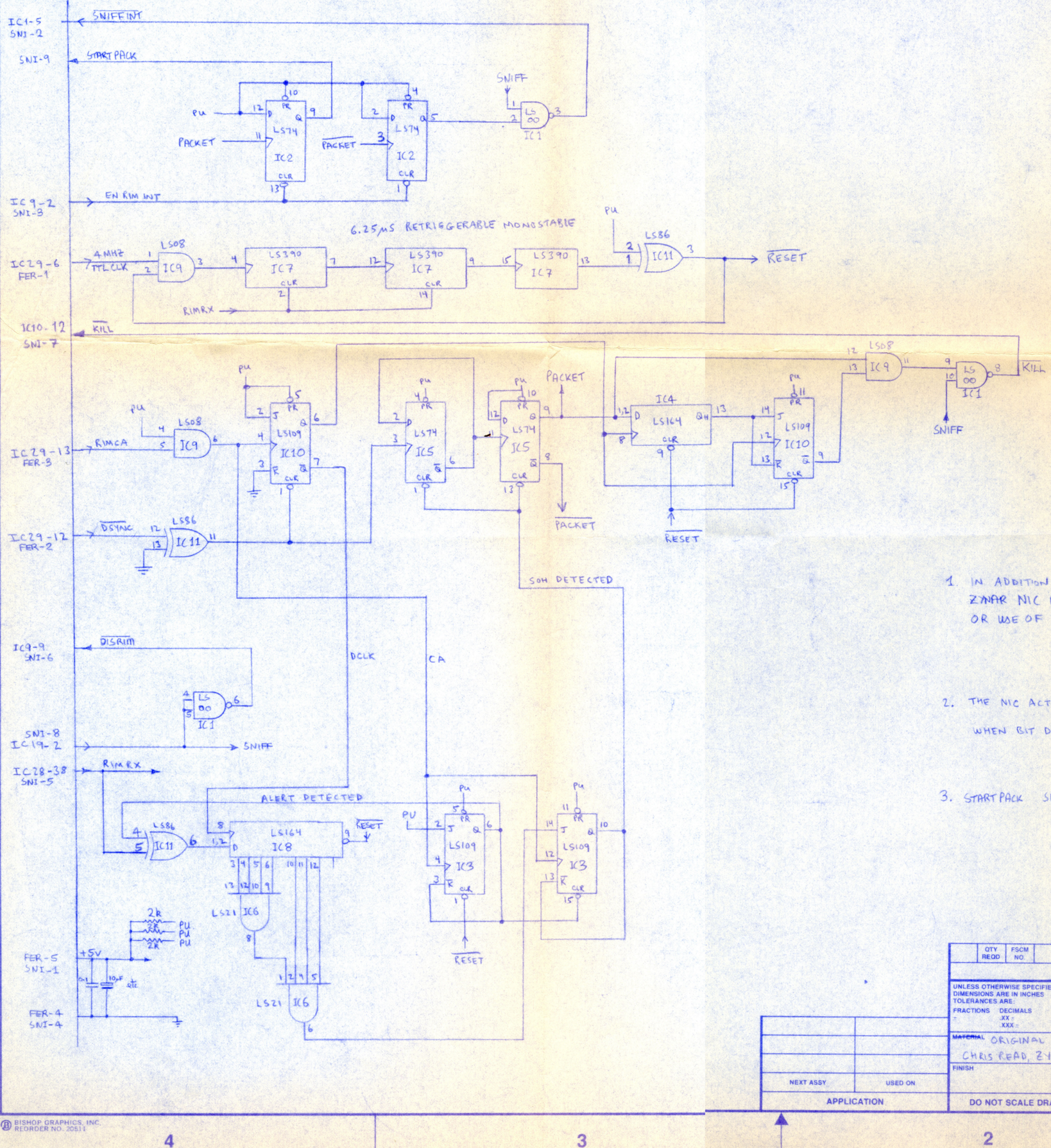
To start the board running the Sniffer software disk is placed in the boot disk drive and the machine turned on. After a few whirs and skraunches the user will be required to indicate whether short or long frames are expected. Untill the new RIM's arrive the answer to this will always be 'short'. The sniffer board is then initialised and the number of packets it should hang around for is requested, if 0 is entered the whole of RAM will be filled (each frame takes up 512 bytes so a 256k RAM card will take 512 frames). Pressing any key will cause the receive process to terminate with however many frames it already received safely stored away. When the receive operation finishes, either by pressing a key or else when the required number of packets have been received, the last received frame number is indicated to the user. Working back from this enables the inspection of frame headers and data of all received packets. A displayed menu of choices is given allowing different frames or data to be displayed. The sniffer can be restarted at any point in the display routines and frames then received will be placed after the frames already received in RAM. Should the whole of RAM be filled the program bombs out and tells you so, the sniffer will then have to be restarted and places the new frames at the start of RAM again.

The speed of the sniffer is such that all normal activity in a network can be captured without missing any data or complete frames. However there is a statistical possibility if two adjacent stations send data on the same token 'round', and the first sends a frame with greater than 200 data bytes while the second sends minimum data (50 bytes of header only) that the first packet will have some of its data overwritten by the second frame before it is safely stored away in RAM, though the header will be preserved intact.

JHAR

5th november 1982

IBM PC NIC



REVISIONS				
ZONE	REV.	DESCRIPTION	DATE	APPROVED
	A	MODIFY TO USE ZYNAR REV B BOARD ADOPT LS00 FOR NC/SNIFFER EXCHANGE	10.25.83	
	B	ADD SNI-9 & CHANGE USAGE OF IC2	11.10.83	
	C	ALERT Det. Cct changed (IC3/2 → PU)	8.9.83	10/17/84

1. IN ADDITION TO THE 12 CONNECTIONS TO THE HEADERS OF THE REV B ZYNAR NIC (IBM PC), IC 19-2 MUST BE CONNECTED VIA FLYING LEAD OR USE OF ONE POWER CONNECTION PIN (FER-5 OR SNI-1)

2. THE NIC ACTS NORMALLY AT POWER ON, AND BECOMES A SNIFFER ONLY WHEN BIT D0 (LSB) OF THE CONTROL REGISTER (XXX0802) IS SET ON.

3. STARTPACK SIGNAL IS UNUSED, ADDED SIMPLY FOR FUTURE USE IF DESIRED.

PROPRIETARY INFORMATION
NESTAR SYSTEMS, INCORPORATED

QTY REQD	FSCM NO.	PART OR IDENTIFYING NO.	NOMENCLATURE OR DESCRIPTION	MATERIAL SPECIFICATION

PARTS LIST

NEXT ASSY	USED ON
APPLICATION	

UNLESS OTHERWISE SPECIFIED DIMENSIONS ARE IN INCHES
TOLERANCES ARE:
FRACTIONS ± DECIMALS .XX ± .XXX ± ANGLES ±

MATERIAL ORIGINAL BY CHRIS READ, ZYNAR
FINISH
DO NOT SCALE DRAWING

CONTRACT NO.

APPROVALS	DATE
DRAWN L. SHUSTEK	9/26/83
CHECKED	
ISSUED	

NESTAR SYSTEMS INCORPORATED

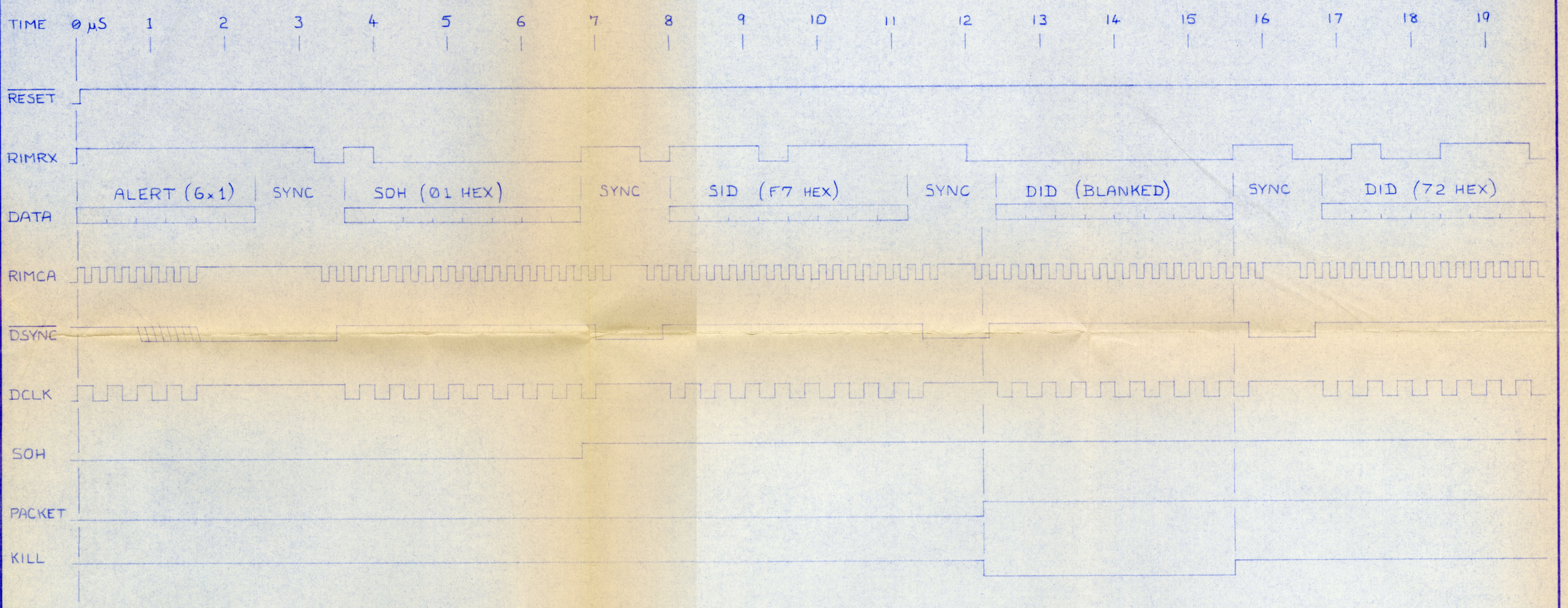
SNIFFER

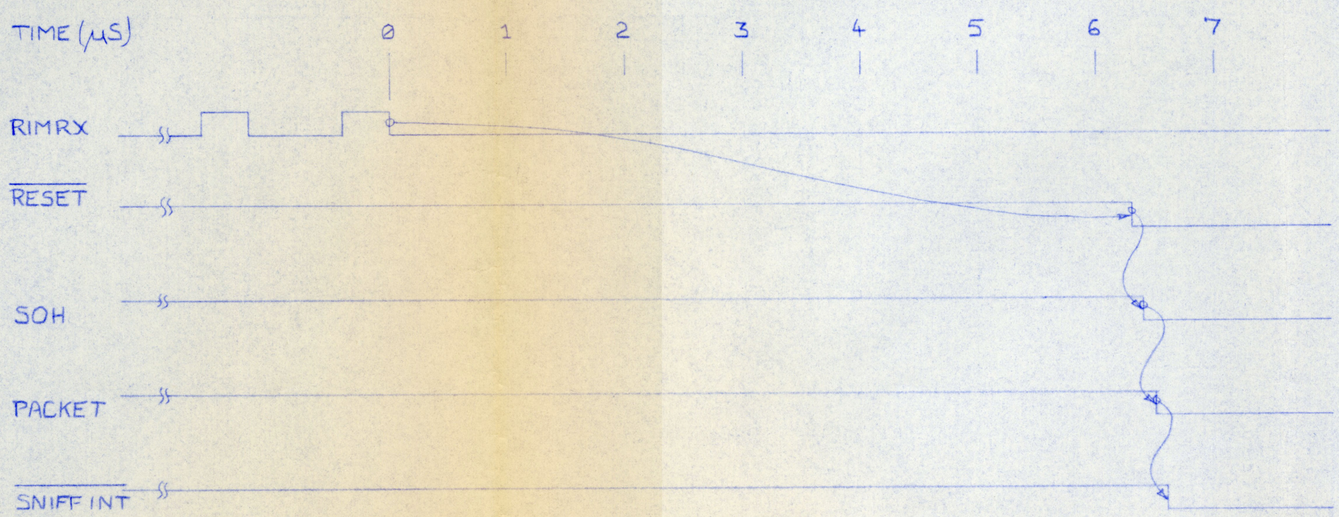
SIZE	FSCM NO.	DWG. NO.	REV.
C			C

SCALE | SHEET 1 of 1

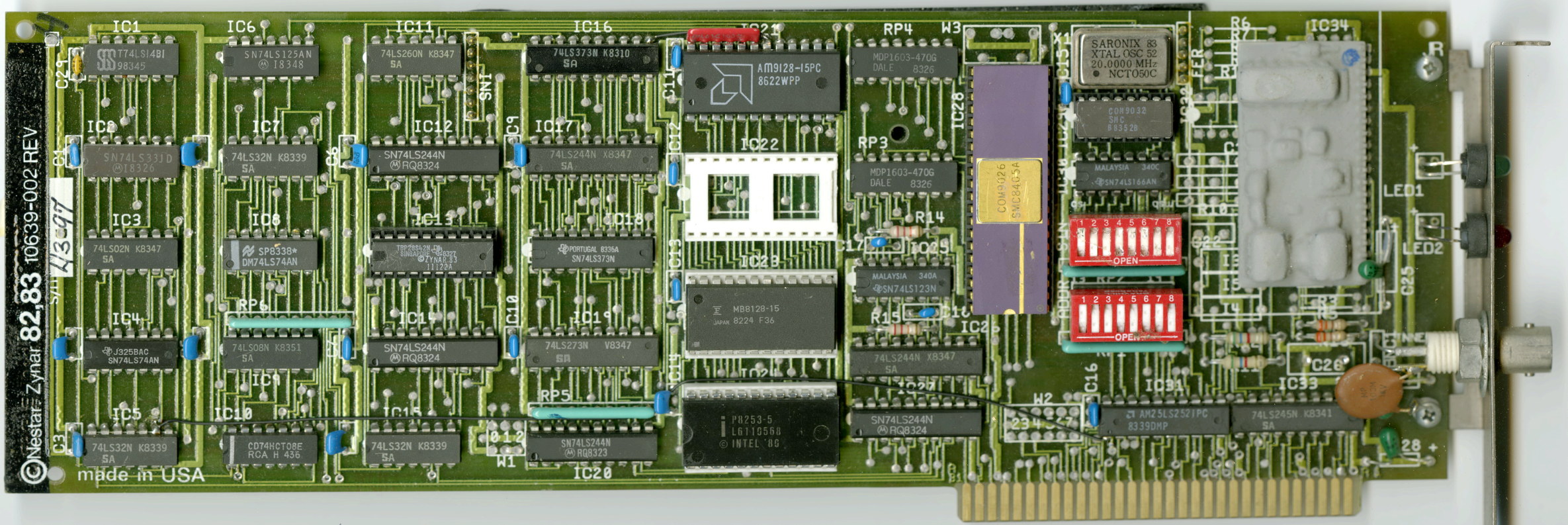
DWG. NO. SH REV.

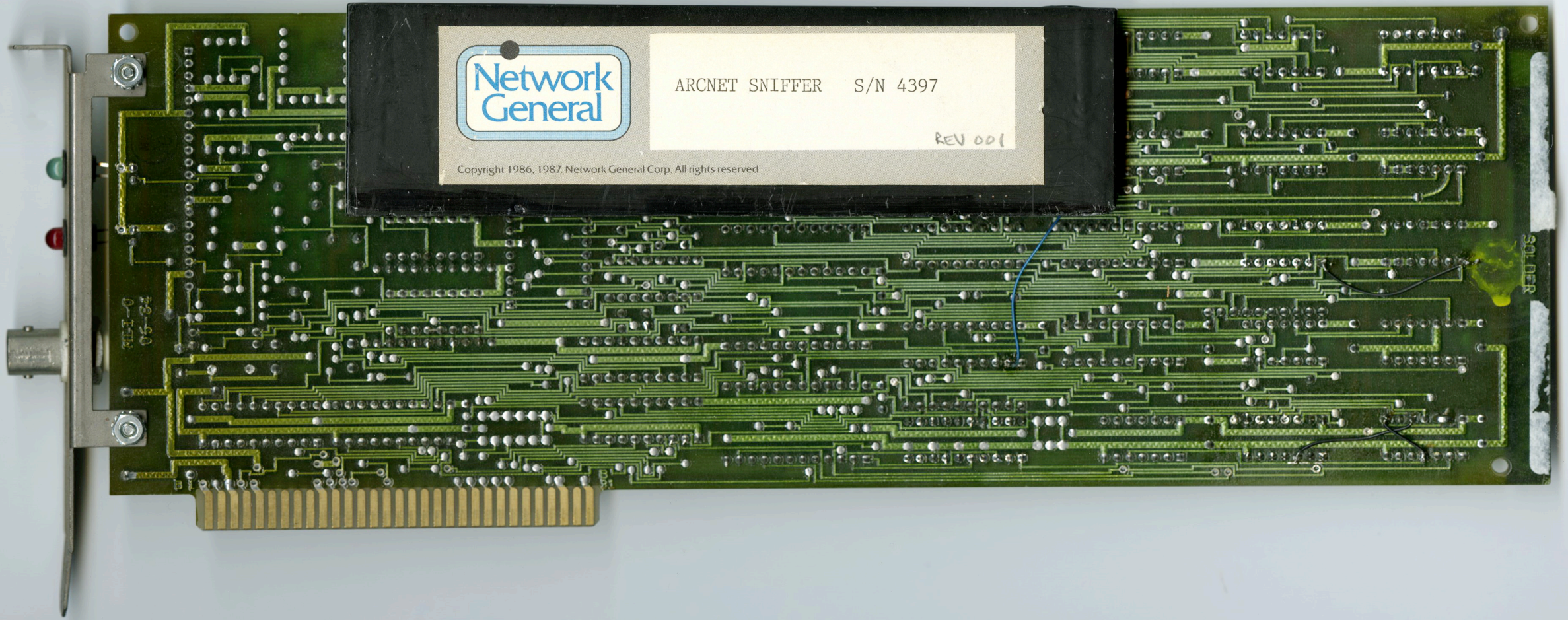
REVISIONS			
LTR	DESCRIPTION	DATE	APPROVED





TOLERANCES UNLESS OTHERWISE SPECIFIED FRACTIONS DEC ANGLES ± ± ±		NESTAR SYSTEMS INCORPORATED	
APPROVALS	DATE	SNIFFER TIMING	
DRAWN	10/27/84		
CHECKED		SCALE —	SIZE C / DRAWING NO.
		DO NOT SCALE DRAWING	SHEET 1 OF 1


©Nestar Zynar 82,83 10639-002 REV
made in USA
IC1
IC6
IC11
IC16
IC21
RP4
W3
IC2
IC7
IC12
IC17
IC22
RP3
IC28
IC3
IC8
IC13
IC18
IC23
R14
IC4
RP6
IC14
IC19
IC24
R15
IC29
IC5
IC10
IC15
IC20
RP5
W1
W2
IC31
IC33
IC34
R6
LED1
LED2
C26
C25
X1
SARONIX 83
XTAL OSC 52
20.0000 MHz
NCTO50C
AM9128-15PC
8622WPP
MB8128-15
P8253-5
INTEL '86
COM9026
SMC8463A
COM9032
SMC
8352B
MDP1603-470G
DALE 8326
SN74LS244N
RQ8324
74LS373N K8310
74LS260N K8347
SN74LS125AN
74LS32N K8339
74LS244N X8347
74LS273N V8347
74LS245N K8341
AM25LS2521PC
8339DMP
SN74LS123N
SN74LS166AN
MALAYSIA 340A
MALAYSIA 340C
PORTUGAL 8336A
SN74LS373N
SP8338*
DM74LS74AN
74LS02N K8347
74LS08N K8351
CD74HCT08E
RCA H 436
SN74LS33JD
OPEN


Network General
ARCNET SNIFFER S/N 4397
REV 001
Copyright 1986, 1987. Network General Corp. All rights reserved