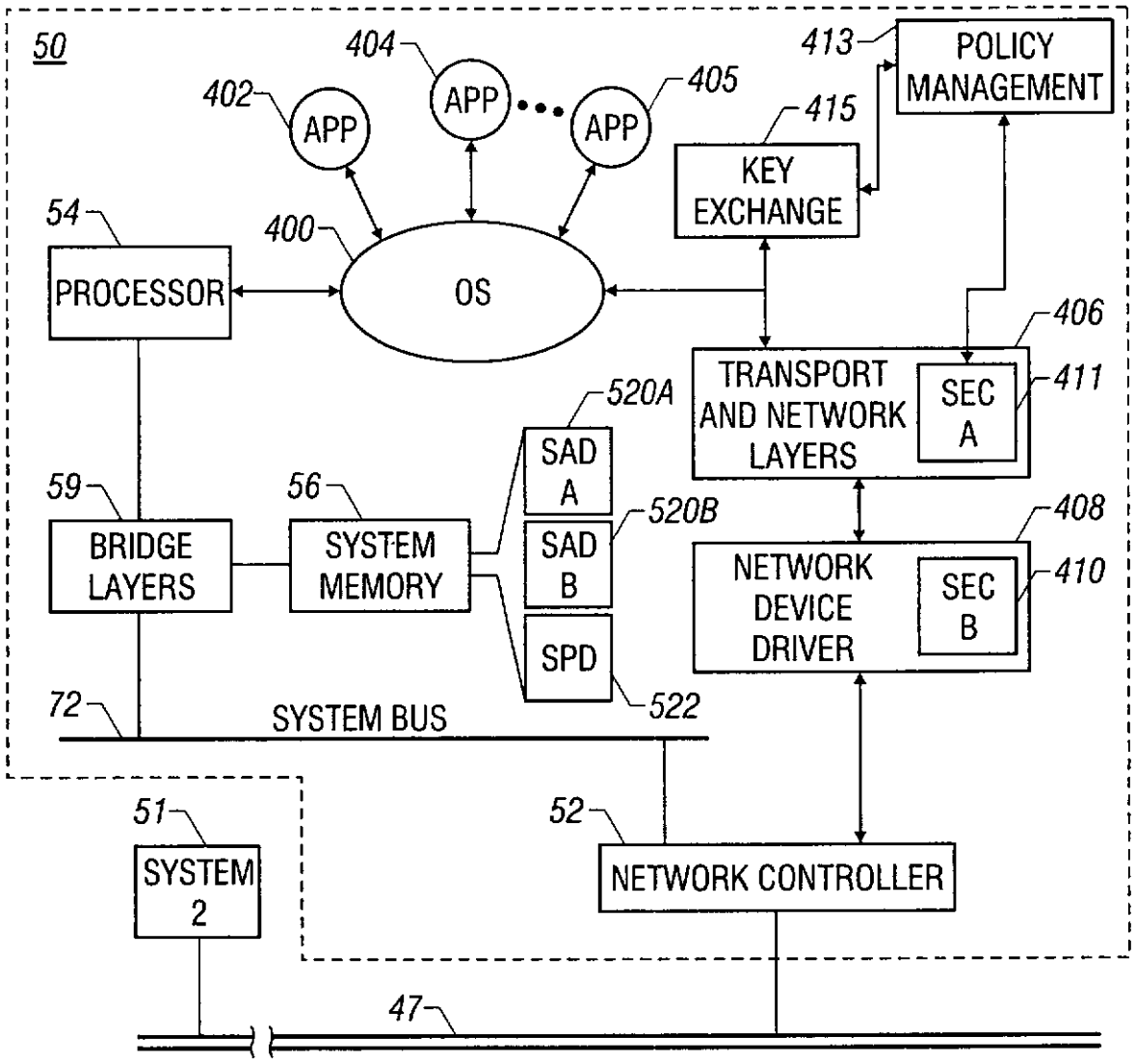

50
404
APP
402
APP
405
APP
413
POLICY MANAGEMENT
415
KEY EXCHANGE
54
PROCESSOR
400
OS
406
TRANSPORT AND NETWORK LAYERS
SEC A
411
520A
SAD A
59
BRIDGE LAYERS
56
SYSTEM MEMORY
520B
SAD B
408
NETWORK DEVICE DRIVER
SEC B
410
SPD
522
72
SYSTEM BUS
51
SYSTEM 2
52
NETWORK CONTROLLER
47

FIG. 1A

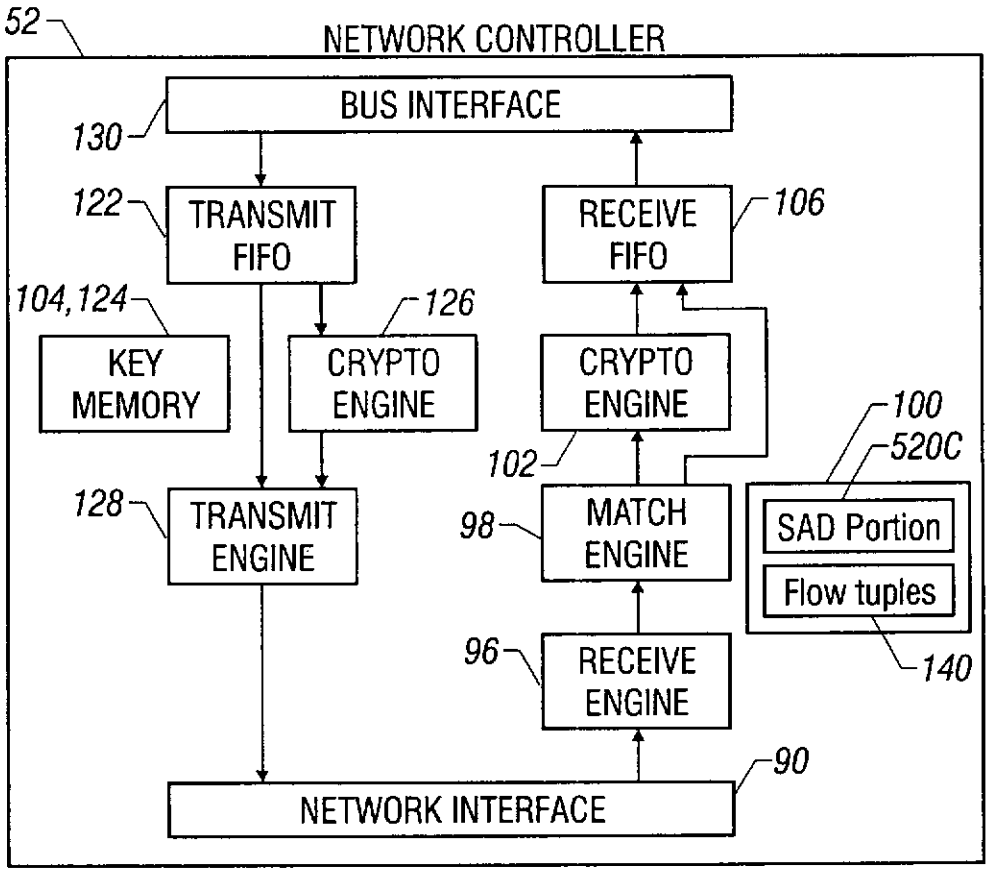

52
NETWORK CONTROLLER
BUS INTERFACE
130
122
TRANSMIT FIFO
RECEIVE FIFO
106
104,124
KEY MEMORY
126
CRYPTO ENGINE
CRYPTO ENGINE
100
520C
102
128
TRANSMIT ENGINE
98
MATCH ENGINE
SAD Portion
Flow tuples
140
96
RECEIVE ENGINE
90
NETWORK INTERFACE

FIG. 1B

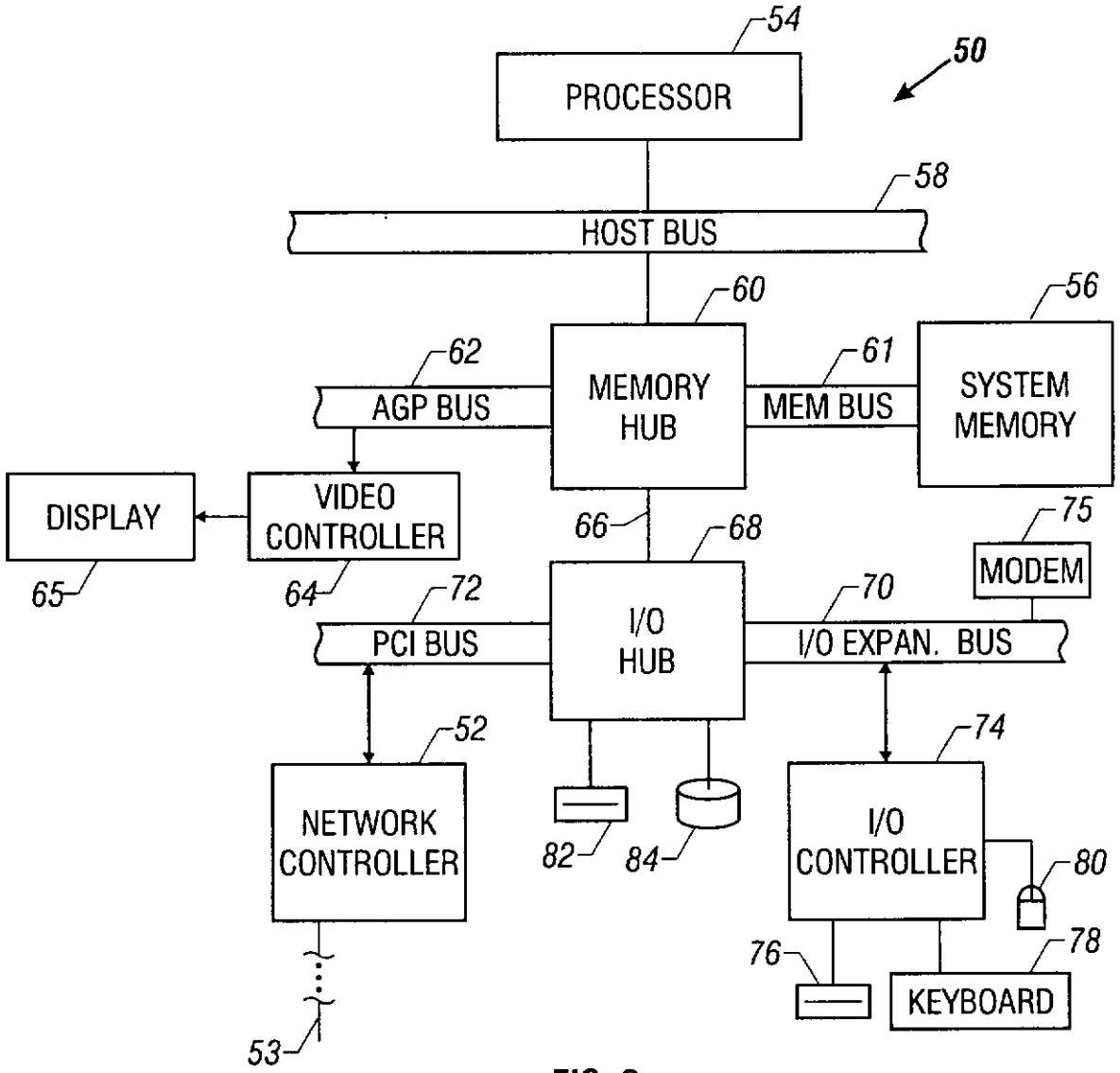

54
50
PROCESSOR
58
HOST BUS
60
56
62
61
AGP BUS
MEMORY HUB
MEM BUS
SYSTEM MEMORY
DISPLAY
VIDEO CONTROLLER
66
68
75
MODEM
65
64
72
70
PCI BUS
I/O HUB
I/O EXPAN. BUS
52
74
NETWORK CONTROLLER
82
84
I/O CONTROLLER
80
76
78
KEYBOARD
53

FIG. 2

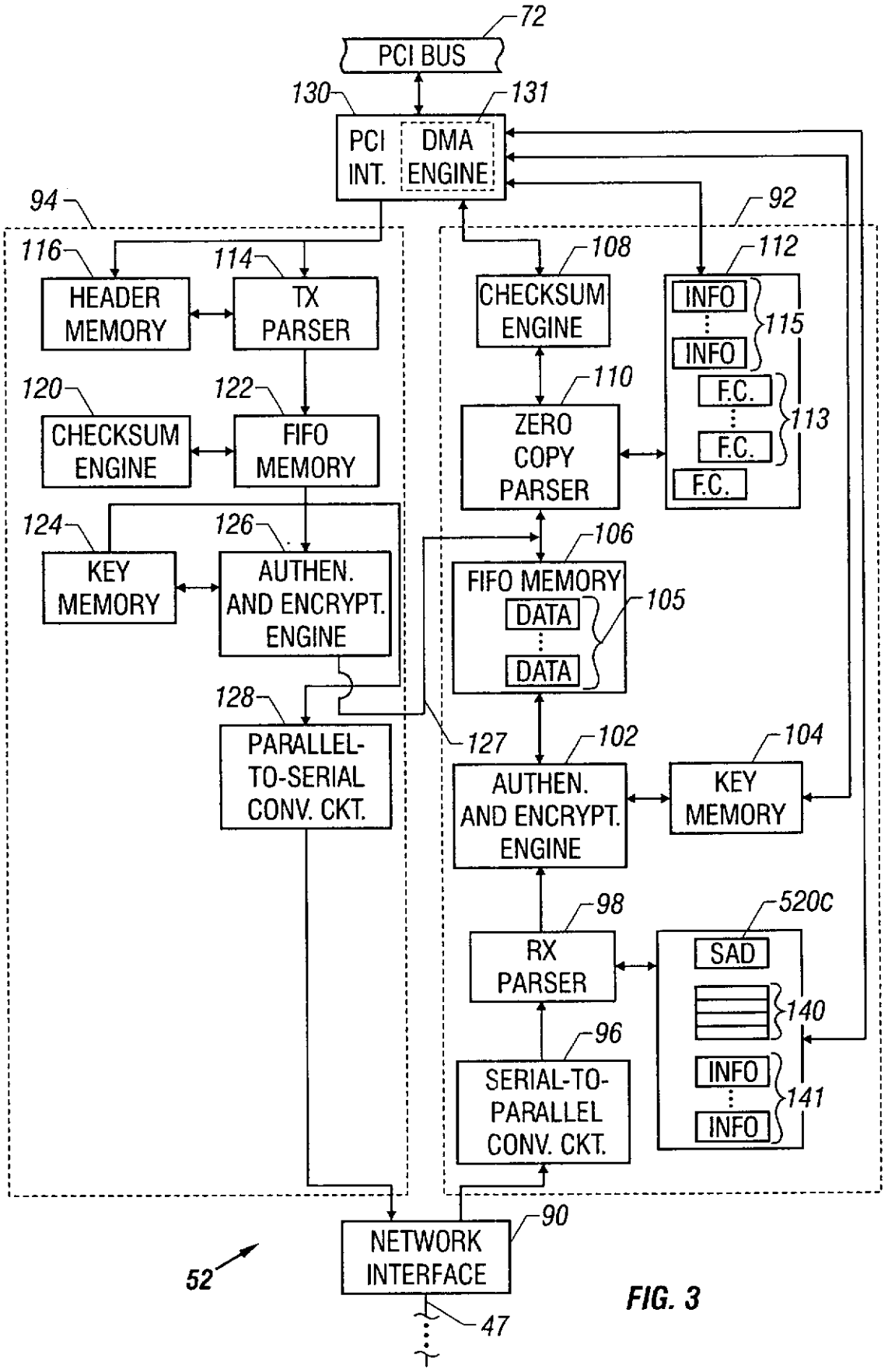

72
PCI BUS
130
131
PCI INT.
DMA ENGINE
94
92
116
114
108
112
HEADER MEMORY
TX PARSER
CHECKSUM ENGINE
INFO
INFO
115
120
122
110
CHECKSUM ENGINE
FIFO MEMORY
ZERO COPY PARSER
F.C.
F.C.
F.C.
113
124
126
106
KEY MEMORY
AUTHEN. AND ENCRYPT. ENGINE
FIFO MEMORY
DATA
DATA
105
128
127
102
104
PARALLEL-TO-SERIAL CONV. CKT.
AUTHEN. AND ENCRYPT. ENGINE
KEY MEMORY
98
520c
RX PARSER
SAD
140
96
INFO
INFO
141
SERIAL-TO-PARALLEL CONV. CKT.
90
NETWORK INTERFACE
52
47

FIG. 3

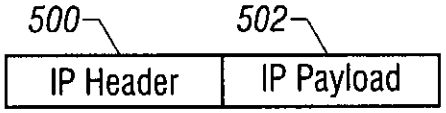
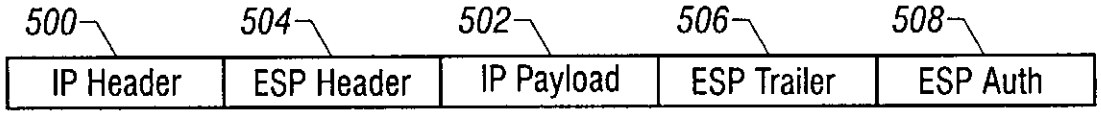
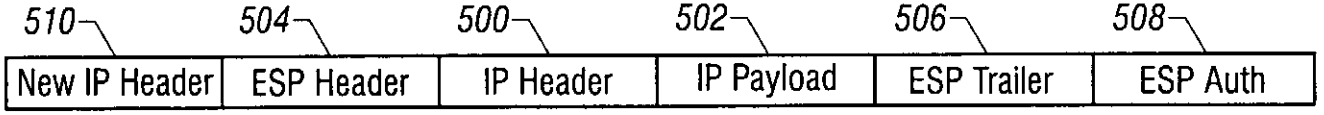


FIG. 4A



TRANSPORT MODE

FIG. 4B



TUNNEL MODE

FIG. 4C

20 JAN 2004

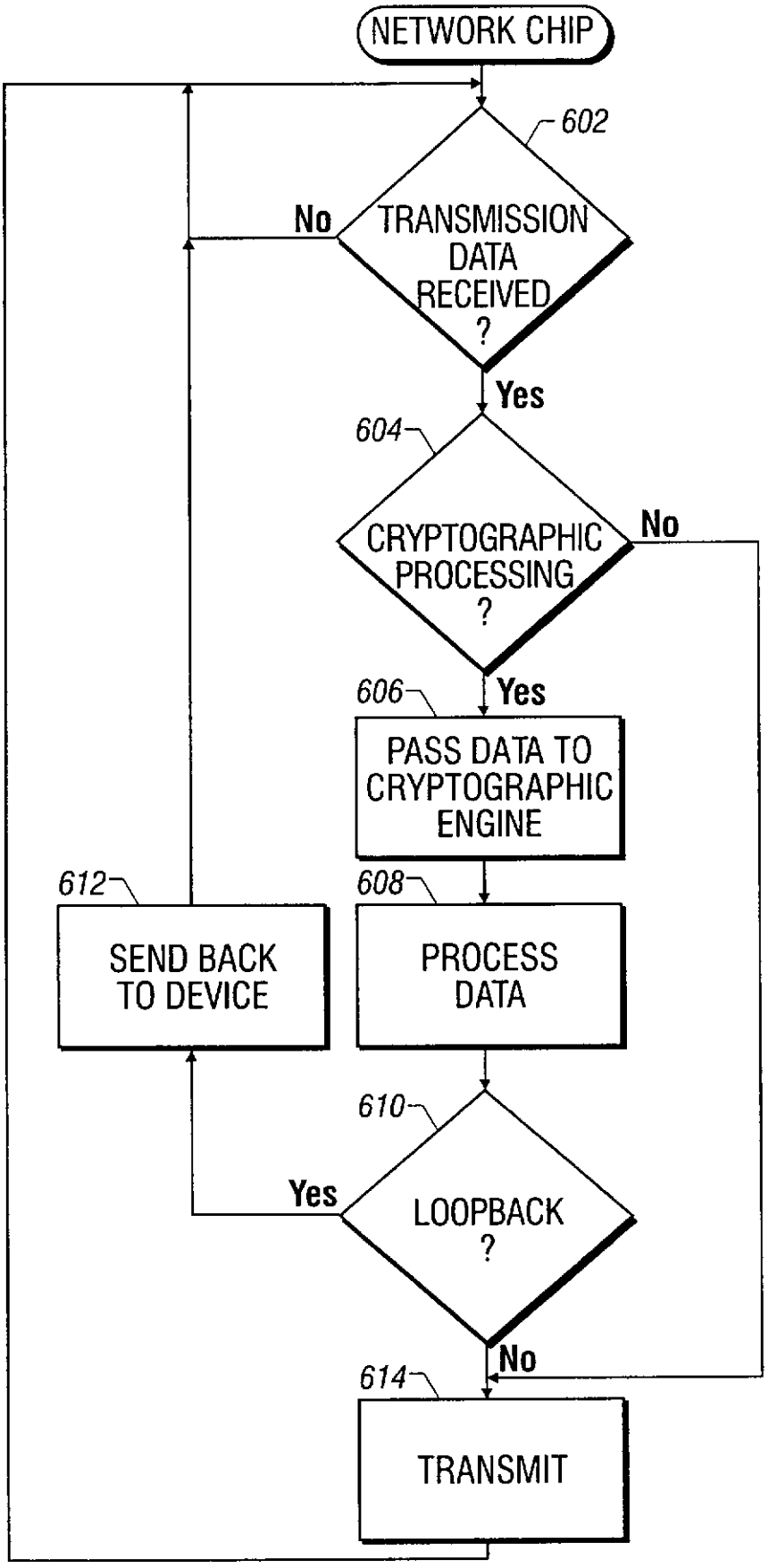

NETWORK CHIP
602
TRANSMISSION DATA RECEIVED ?
No
Yes
604
CRYPTOGRAPHIC PROCESSING ?
No
Yes
606
PASS DATA TO CRYPTOGRAPHIC ENGINE
608
PROCESS DATA
610
LOOPBACK ?
Yes
No
612
SEND BACK TO DEVICE
614
TRANSMIT

FIG. 5

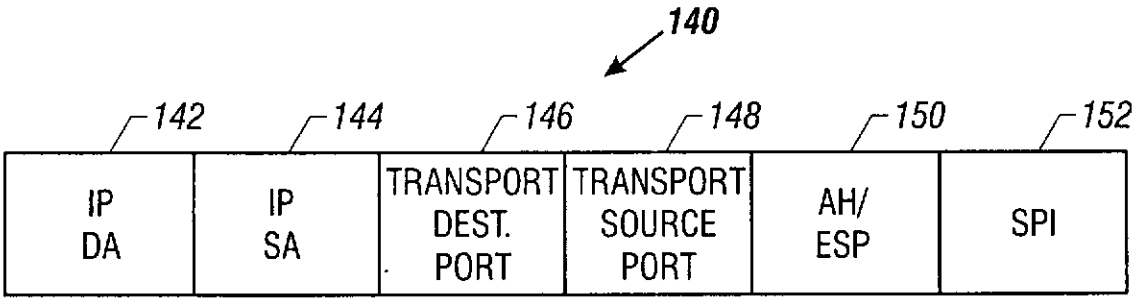

140
142
144
146
148
150
152
IP DA
IP SA
TRANSPORT DEST. PORT
TRANSPORT SOURCE PORT
AH/ ESP
SPI

FIG. 6

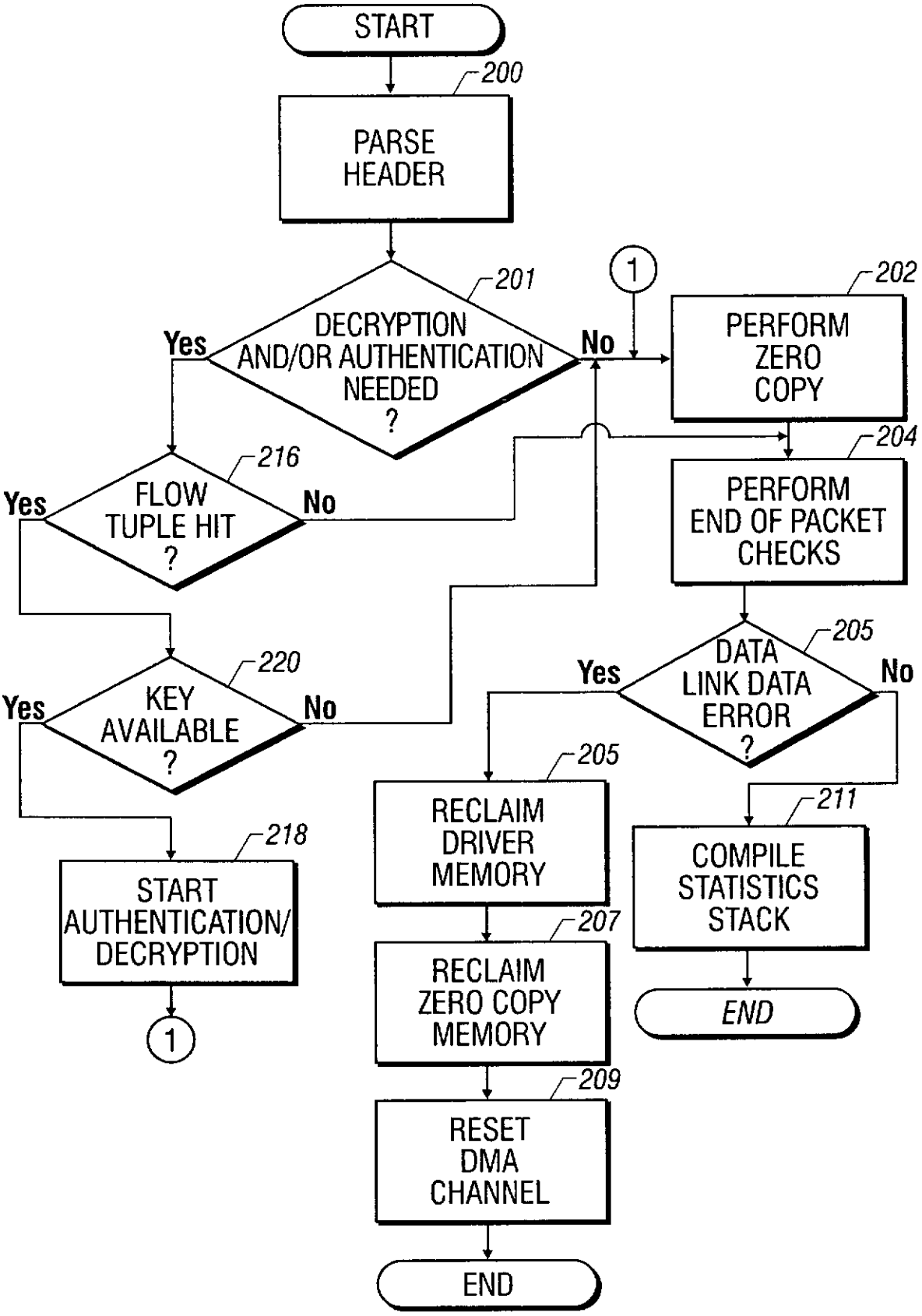

START
200
PARSE HEADER
201
DECRYPTION AND/OR AUTHENTICATION NEEDED ?
Yes
No
1
202
PERFORM ZERO COPY
204
PERFORM END OF PACKET CHECKS
205
DATA LINK DATA ERROR ?
Yes
No
211
COMPILE STATISTICS STACK
END
216
FLOW TUPLE HIT ?
Yes
No
220
KEY AVAILABLE ?
Yes
No
218
START AUTHENTICATION/ DECRYPTION
1
205
RECLAIM DRIVER MEMORY
207
RECLAIM ZERO COPY MEMORY
209
RESET DMA CHANNEL
END

FIG. 7

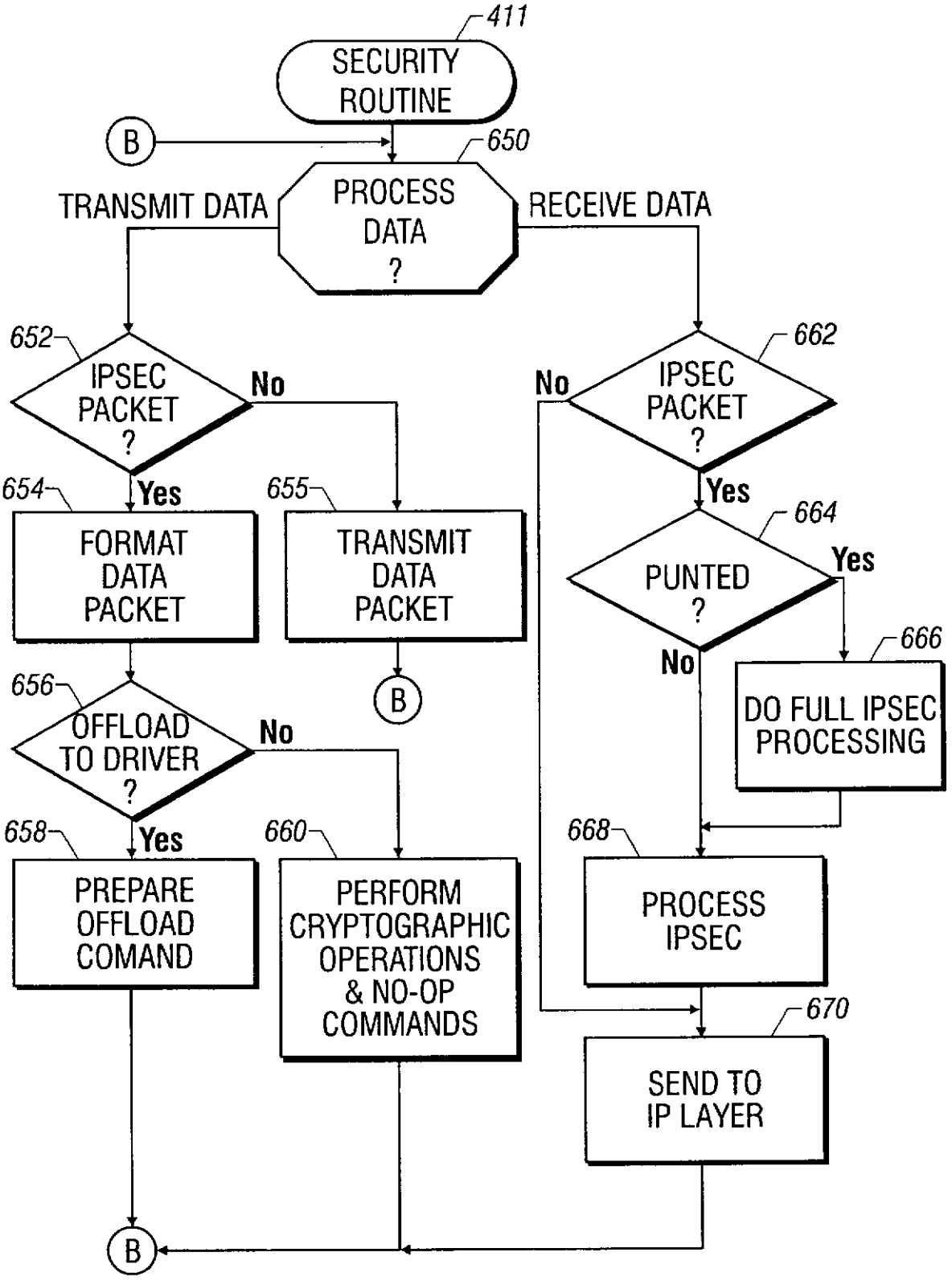

411
SECURITY ROUTINE
B
650
PROCESS DATA ?
TRANSMIT DATA
RECEIVE DATA
652
IPSEC PACKET ?
No
Yes
654
FORMAT DATA PACKET
655
TRANSMIT DATA PACKET
B
656
OFFLOAD TO DRIVER ?
No
Yes
658
PREPARE OFFLOAD COMAND
660
PERFORM CRYPTOGRAPHIC OPERATIONS & NO-OP COMMANDS
662
IPSEC PACKET ?
No
Yes
664
PUNTED ?
Yes
No
666
DO FULL IPSEC PROCESSING
668
PROCESS IPSEC
670
SEND TO IP LAYER
B

FIG. 8

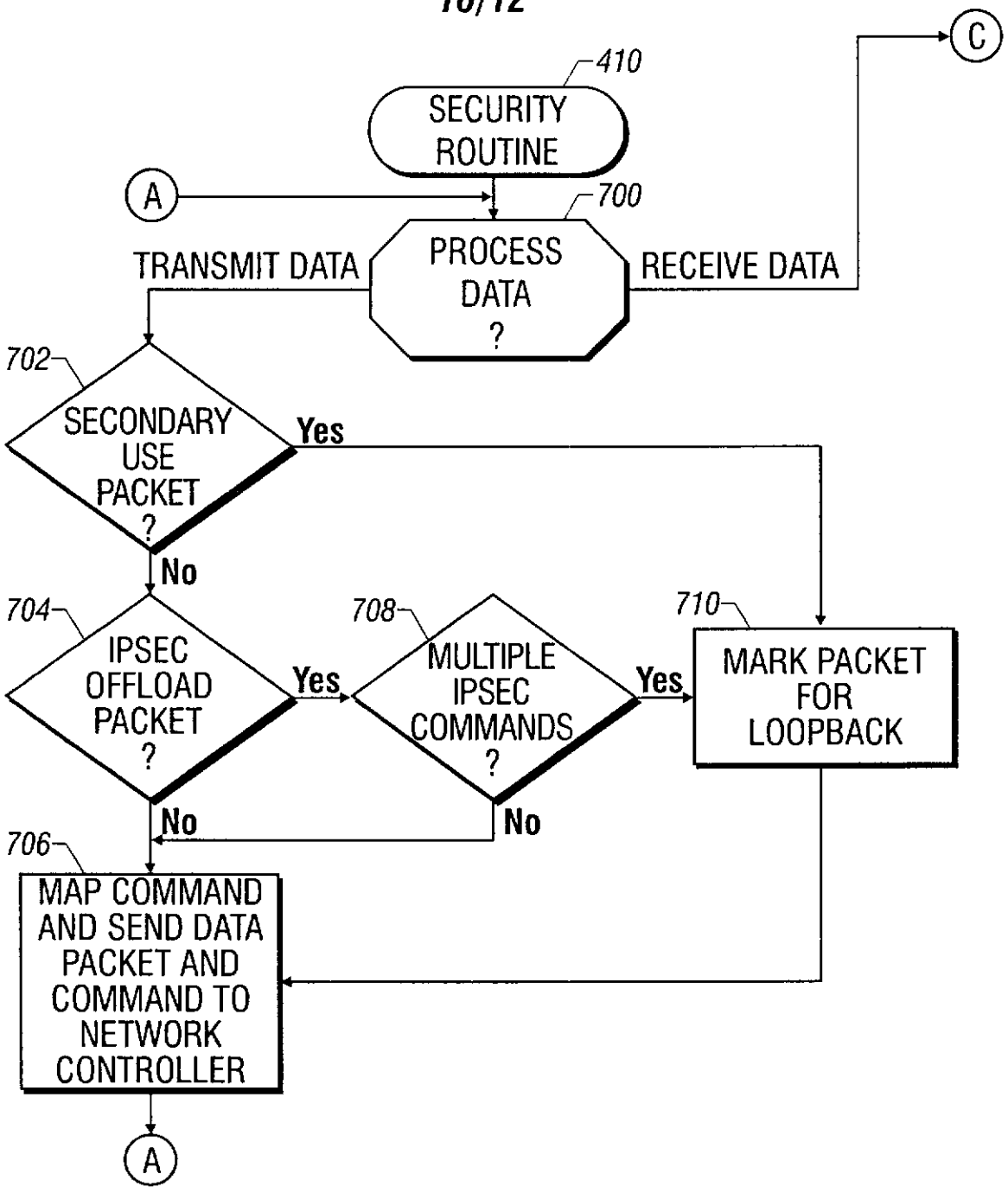

410
SECURITY ROUTINE
A
700
PROCESS DATA ?
TRANSMIT DATA
RECEIVE DATA
C
702
SECONDARY USE PACKET ?
Yes
No
704
IPSEC OFFLOAD PACKET ?
Yes
708
MULTIPLE IPSEC COMMANDS ?
Yes
No
No
710
MARK PACKET FOR LOOPBACK
706
MAP COMMAND AND SEND DATA PACKET AND COMMAND TO NETWORK CONTROLLER
A

FIG. 9A

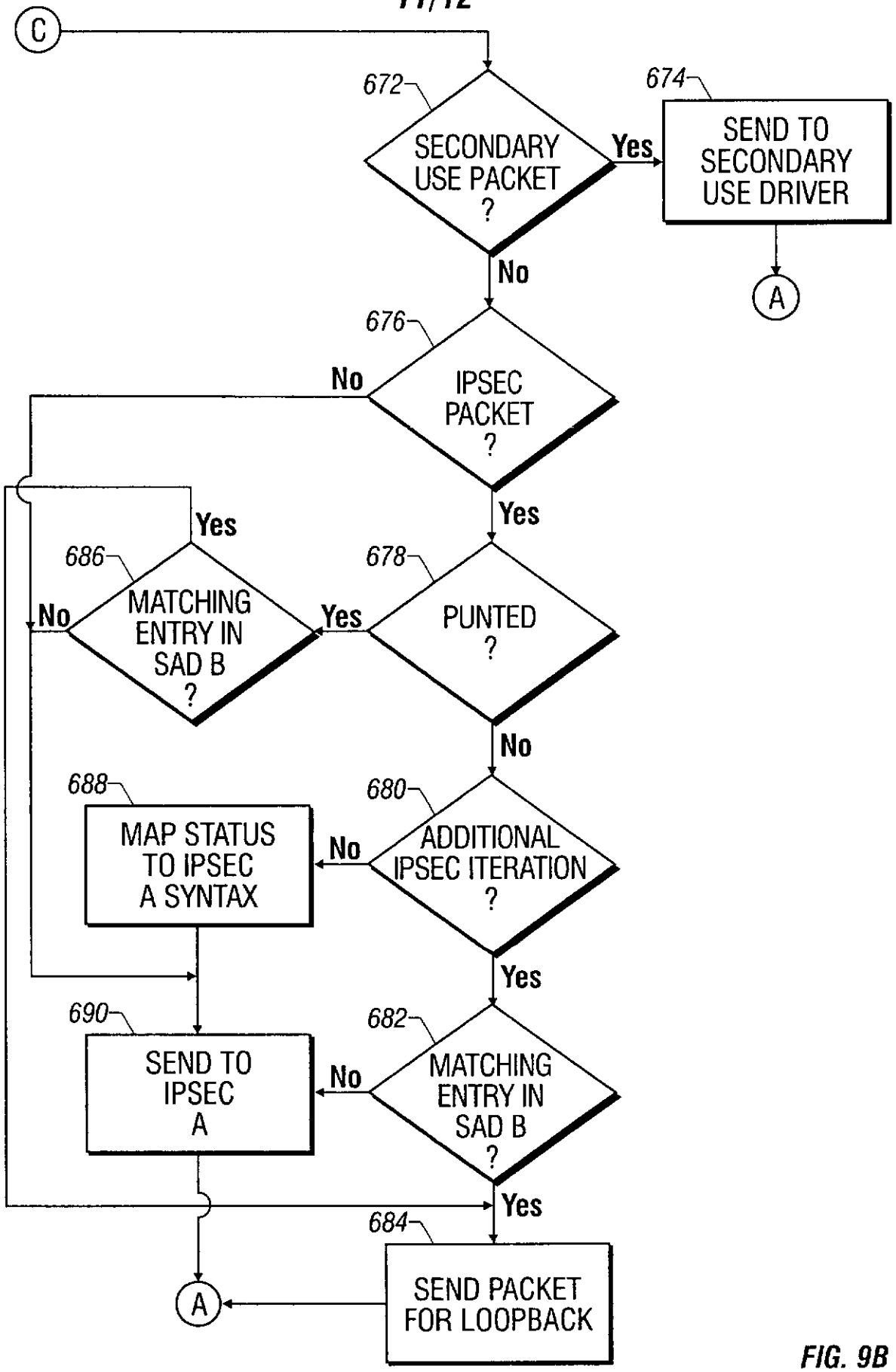

C
672
SECONDARY USE PACKET ?
Yes
674
SEND TO SECONDARY USE DRIVER
A
No
676
IPSEC PACKET ?
No
Yes
Yes
686
MATCHING ENTRY IN SAD B ?
No
Yes
678
PUNTED ?
No
688
MAP STATUS TO IPSEC A SYNTAX
No
680
ADDITIONAL IPSEC ITERATION ?
Yes
690
SEND TO IPSEC A
No
682
MATCHING ENTRY IN SAD B ?
Yes
684
SEND PACKET FOR LOOPBACK
A

FIG. 9B

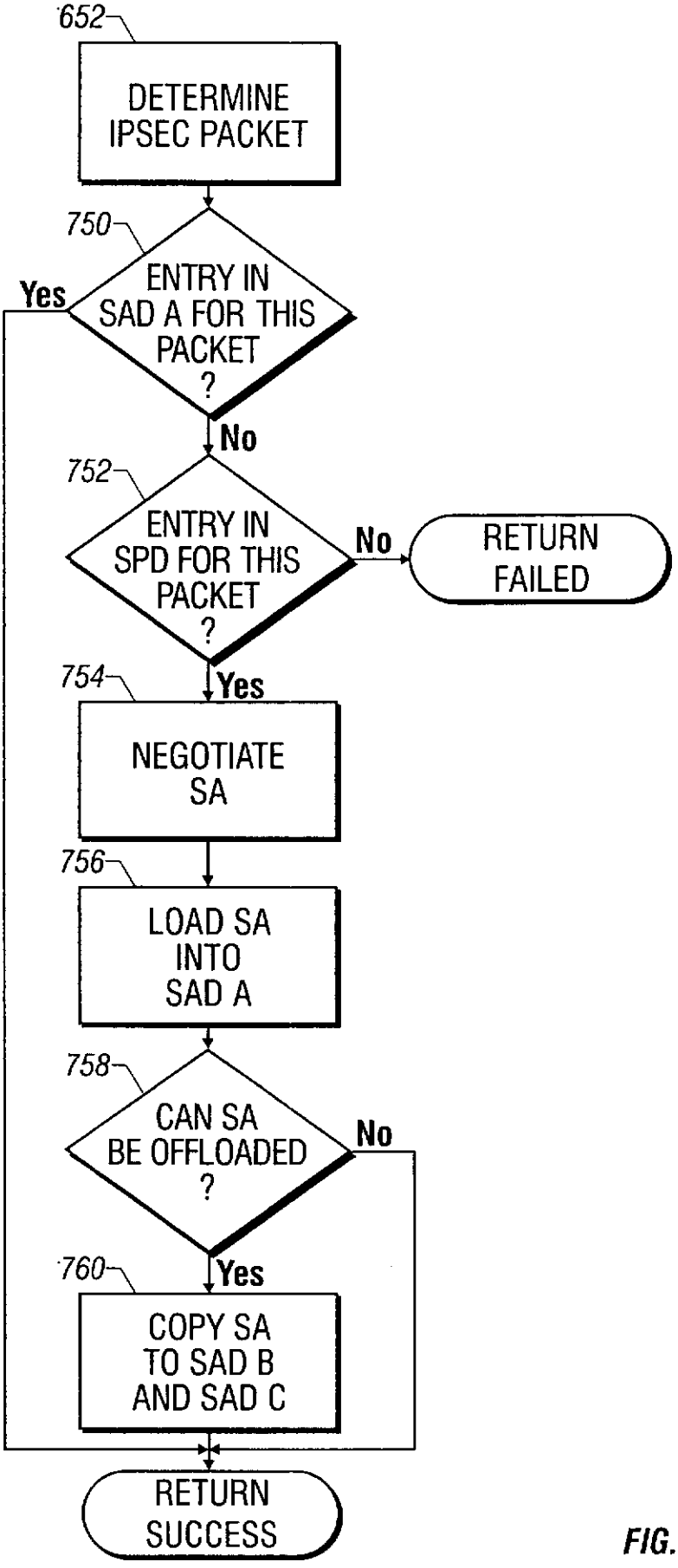

652
DETERMINE IPSEC PACKET
750
ENTRY IN SAD A FOR THIS PACKET ?
Yes
No
752
ENTRY IN SPD FOR THIS PACKET ?
No
RETURN FAILED
Yes
754
NEGOTIATE SA
756
LOAD SA INTO SAD A
758
CAN SA BE OFFLOADED ?
No
Yes
760
COPY SA TO SAD B AND SAD C
RETURN SUCCESS

FIG. 10