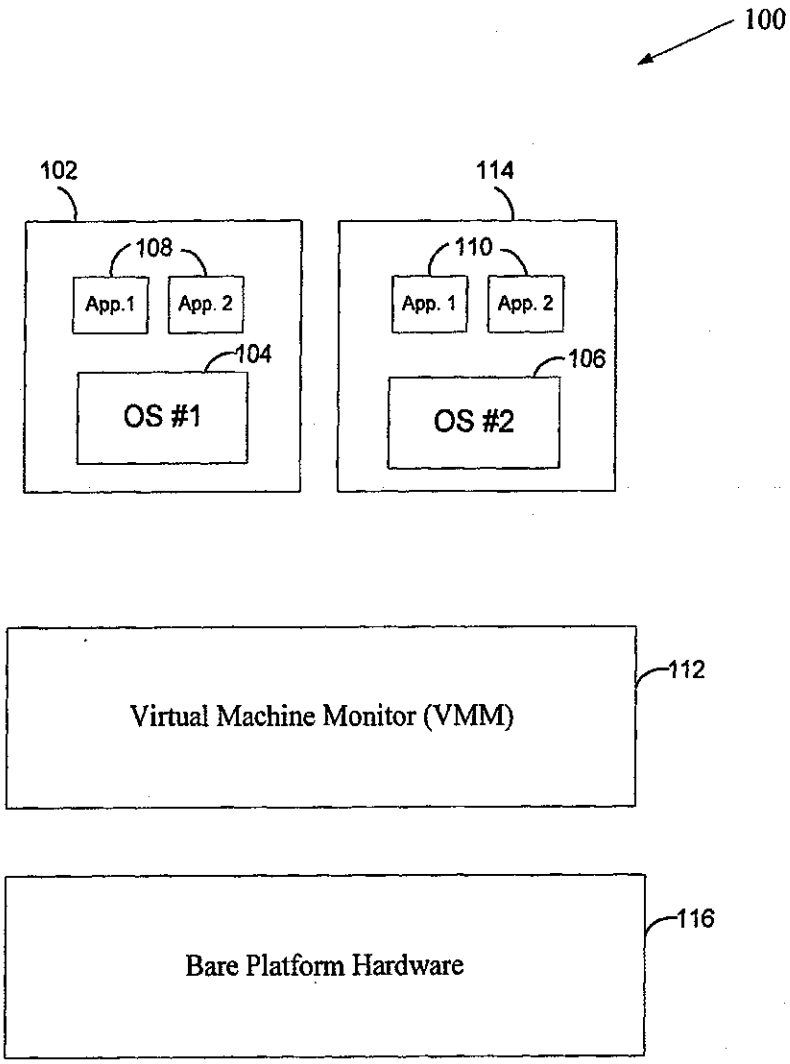

100
102
114
108
110
App.1
App. 2
App. 1
App. 2
104
106
OS #1
OS #2
Virtual Machine Monitor (VMM)
112
Bare Platform Hardware
116

FIG. 1

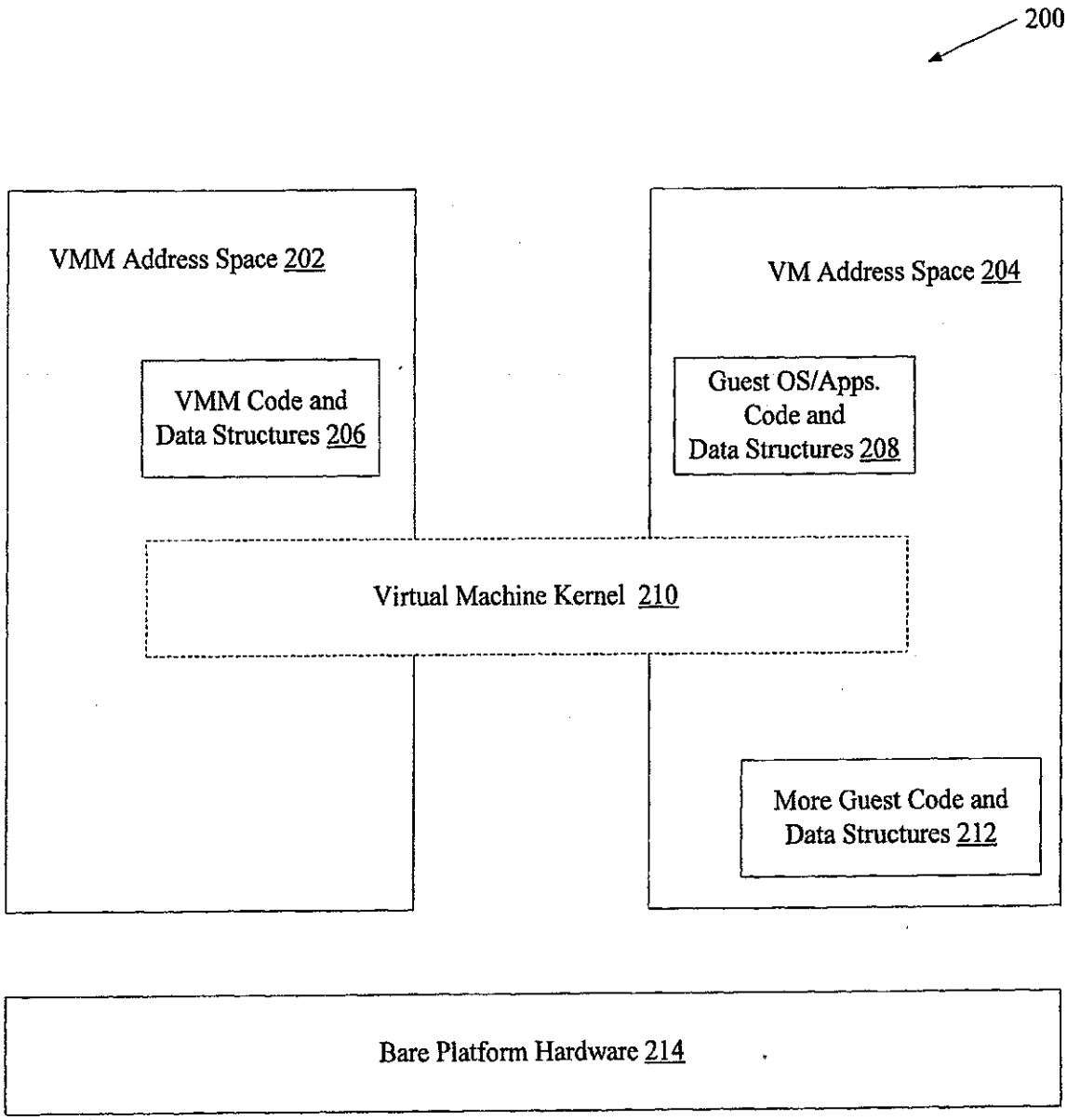

200
VMM Address Space 202
VMM Code and Data Structures 206
VM Address Space 204
Guest OS/Apps. Code and Data Structures 208
Virtual Machine Kernel 210
More Guest Code and Data Structures 212
Bare Platform Hardware 214

FIG. 2

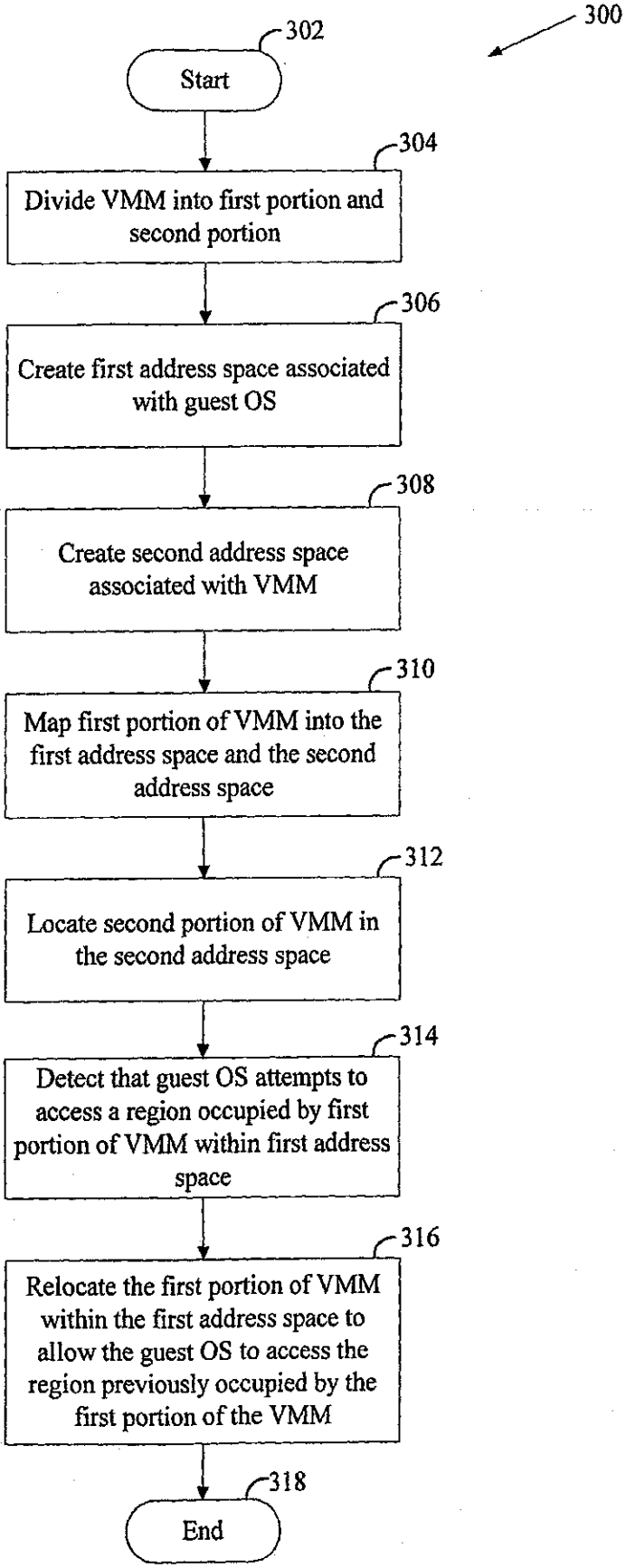

300
302
Start
304
Divide VMM into first portion and second portion
306
Create first address space associated with guest OS
308
Create second address space associated with VMM
310
Map first portion of VMM into the first address space and the second address space
312
Locate second portion of VMM in the second address space
314
Detect that guest OS attempts to access a region occupied by first portion of VMM within first address space
316
Relocate the first portion of VMM within the first address space to allow the guest OS to access the region previously occupied by the first portion of the VMM
318
End

FIG. 3

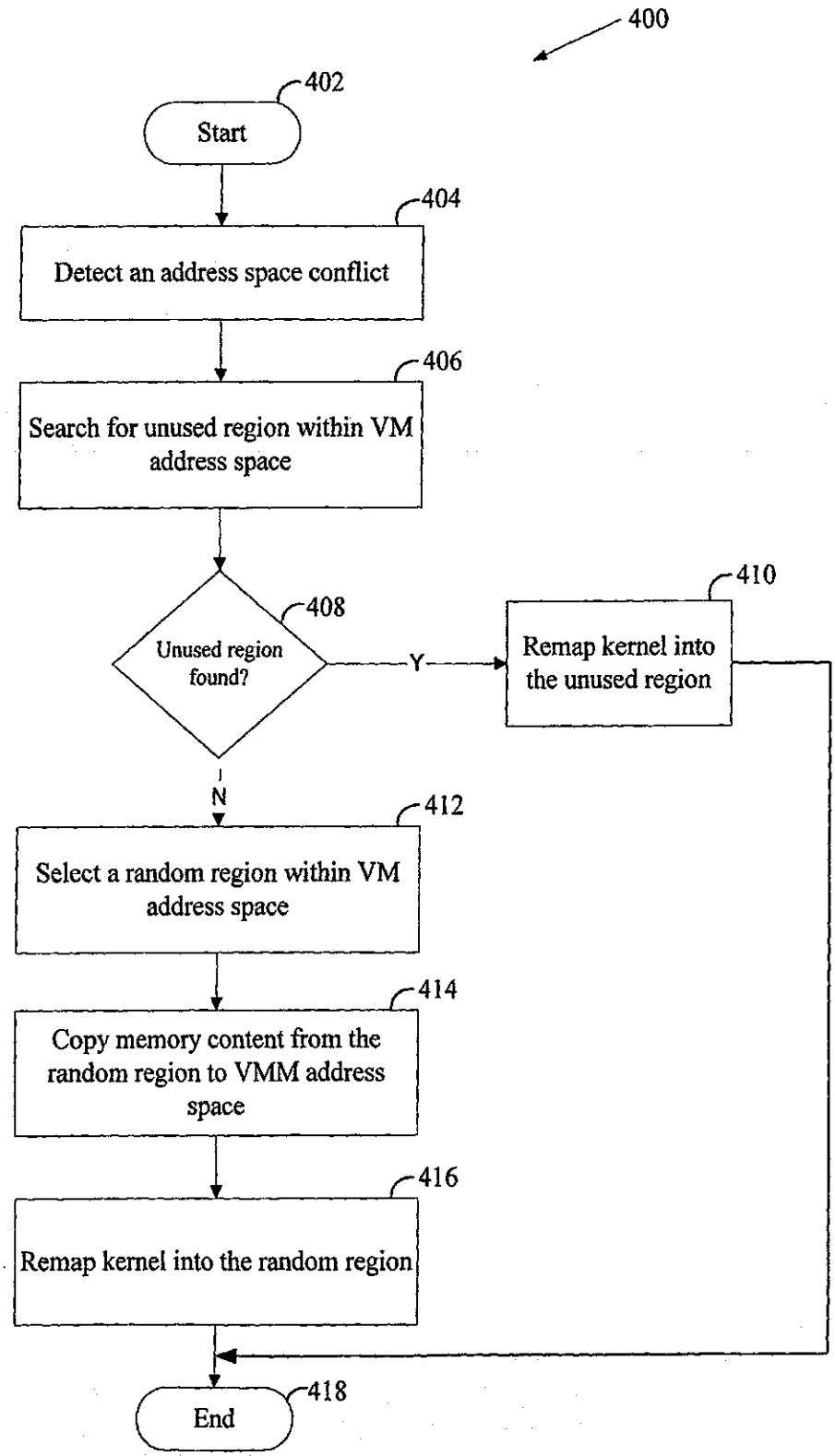

400
402
Start
404
Detect an address space conflict
406
Search for unused region within VM address space
408
Unused region found?
Y
410
Remap kernel into the unused region
N
412
Select a random region within VM address space
414
Copy memory content from the random region to VMM address space
416
Remap kernel into the random region
418
End

FIG. 4

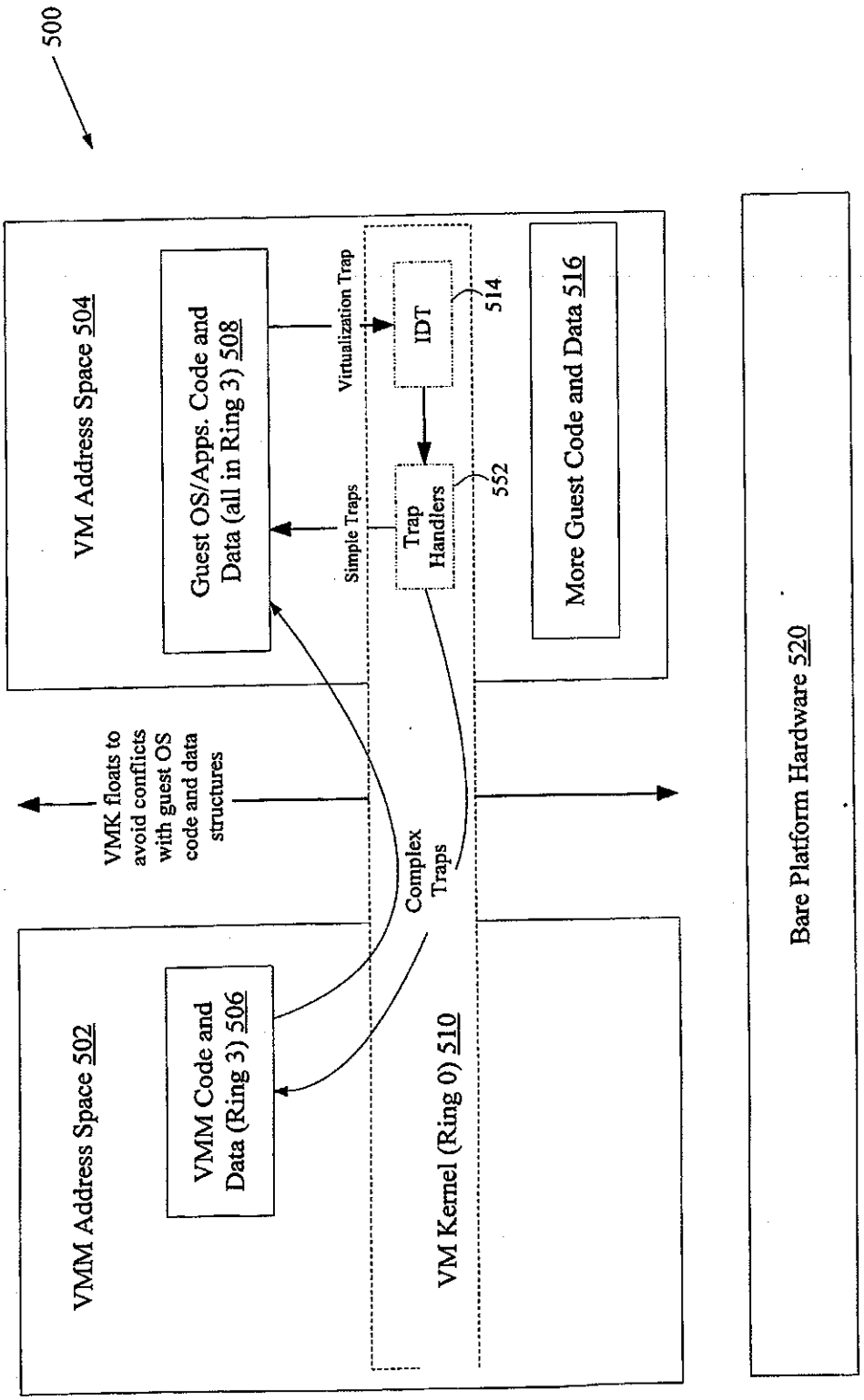

500
VM Address Space 504
Guest OS/Apps. Code and Data (all in Ring 3) 508
Virtualization Trap
IDT
514
Simple Traps
Trap Handlers
552
More Guest Code and Data 516
VMK floats to avoid conflicts with guest OS code and data structures
Complex Traps
VMM Address Space 502
VMM Code and Data (Ring 3) 506
VM Kernel (Ring 0) 510
Bare Platform Hardware 520

FIG. 5

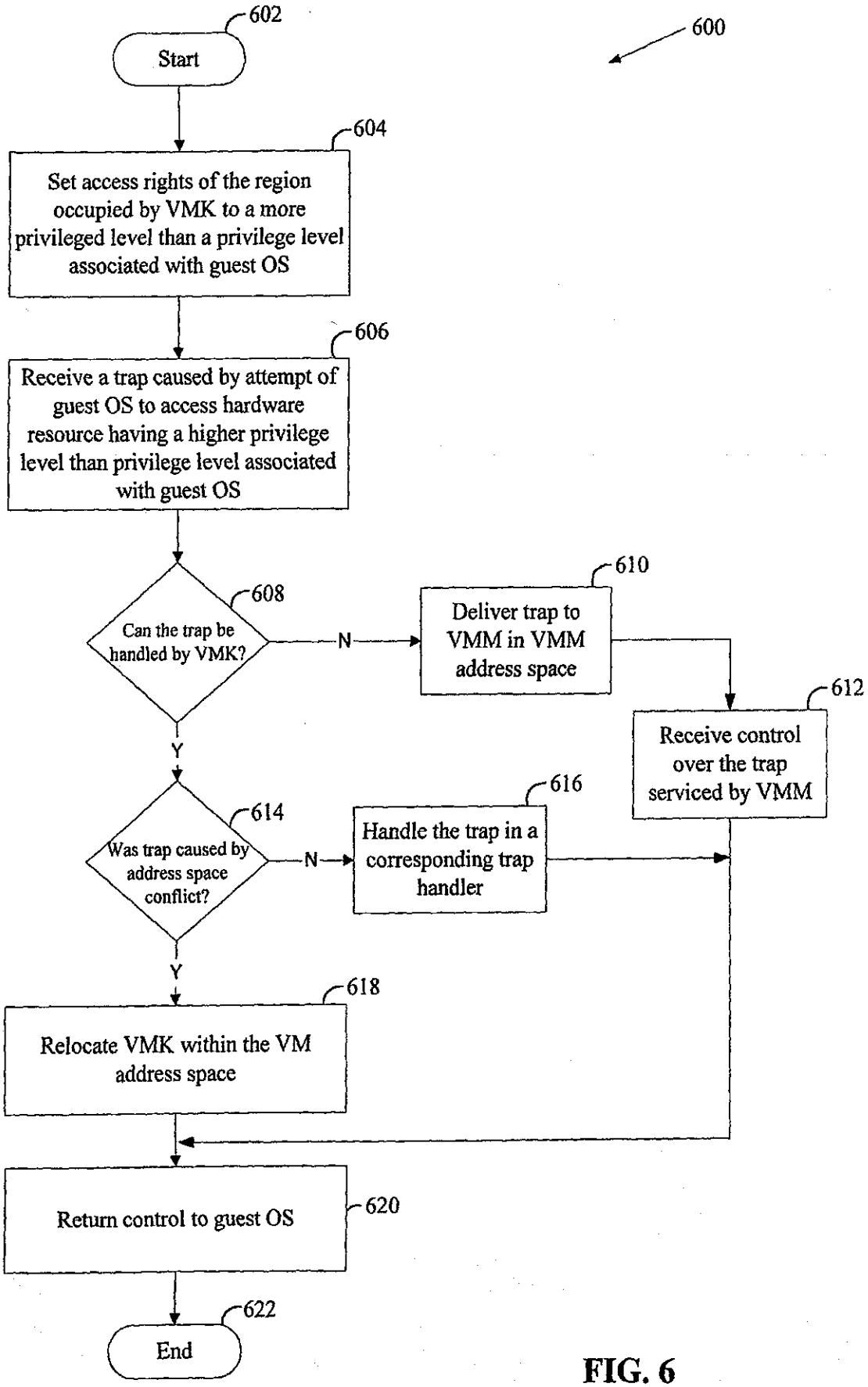

600
602
Start
604
Set access rights of the region occupied by VMK to a more privileged level than a privilege level associated with guest OS
606
Receive a trap caused by attempt of guest OS to access hardware resource having a higher privilege level than privilege level associated with guest OS
608
Can the trap be handled by VMK?
N
610
Deliver trap to VMM in VMM address space
612
Receive control over the trap serviced by VMM
Y
614
Was trap caused by address space conflict?
N
616
Handle the trap in a corresponding trap handler
Y
618
Relocate VMK within the VM address space
620
Return control to guest OS
622
End

FIG. 6

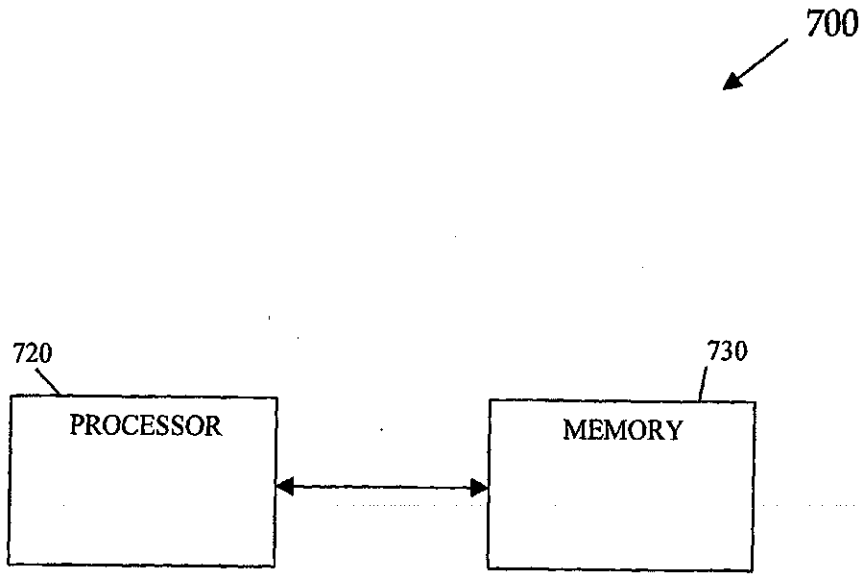


FIG. 7