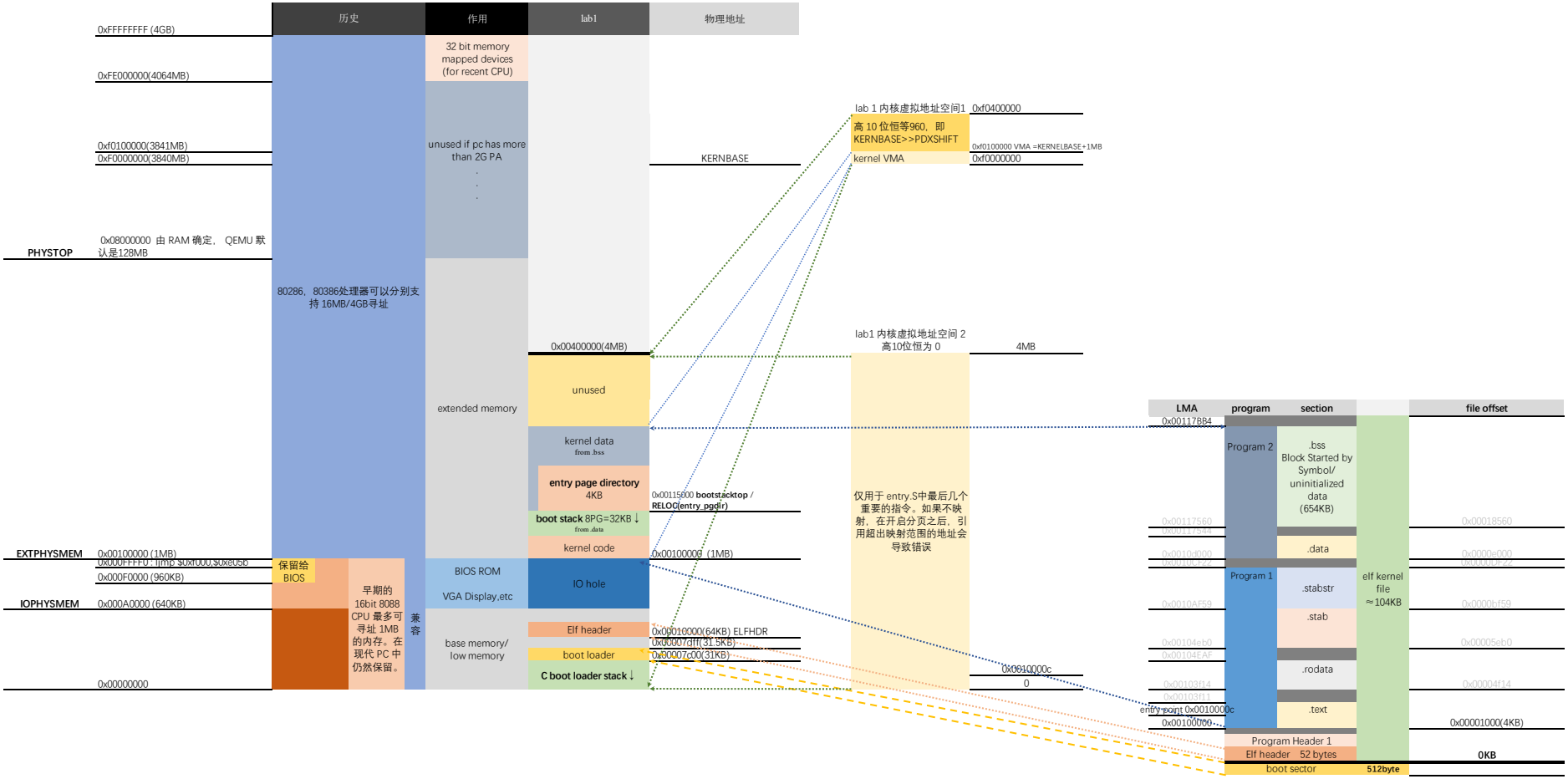
历史
作用
lab1
物理地址
0xFFFFFFFF (4GB)
0xFE000000(4064MB)
0xf0100000(3841MB)
0xF0000000(3840MB)
0x08000000 由 RAM 确定， QEMU 默认是128MB
PHYSTOP
EXTPHYSMEM
0x00100000 (1MB)
0x000FFFF0 : jmp $0xf000,$0xe05b
0x000F0000 (960KB)
IOPHYSMEM
0x000A0000 (640KB)
0x00000000
80286，80386处理器可以分别支持 16MB/4GB寻址
保留给BIOS
早期的16bit 8088 CPU 最多可寻址 1MB 的内存。在现代 PC 中仍然保留。
兼容
32 bit memory mapped devices (for recent CPU)
unused if pc has more than 2G PA
extended memory
BIOS ROM
VGA Display,etc
base memory/ low memory
KERNBASE
0x00400000(4MB)
unused
kernel data
from .bss
entry page directory 4KB
0x00115000 bootstacktop / RELOC(entry_pgdir)
boot stack 8PG=32KB ↓
from .data
kernel code
0x00100000 (1MB)
IO hole
Elf header
0x00010000(64KB) ELFHDR
0x00007fff(31.5KB)
boot loader
0x00007c00(31KB)
C boot loader stack ↓
lab 1 内核虚拟地址空间1
0xf0400000
高 10 位恒等960，即 KERNBASE>>PDXSHIFT
0xf0100000 VMA =KERNELBASE+1MB
kernel VMA
0xf0000000
lab1 内核虚拟地址空间 2
高10位恒为 0
4MB
仅用于 entry.S中最后几个重要的指令。如果不映射，在开启分页之后，引用超出映射范围的地址会导致错误
0x0010000c
0
LMA
program
section
file offset
0x00117BB4
Program 2
.bss
Block Started by Symbol/ uninitialized data (654KB)
0x00117560
0x00018560
0x00117534
0x00110000
.data
0x0000e000
0x00010C52
0x0000bf22
Program 1
.stabstr
0x0010AF59
0x0000bf59
.stab
0x00104eb0
0x00005eb0
0x00104EAF
.rodata
0x00103f14
0x00004f14
0x00103f11
entry point 0x0010000c
.text
0x00100000
0x00001000(4KB)
Program Header 1
Elf header 52 bytes
0KB
boot sector
512byte
elf kernel file ≈104KB