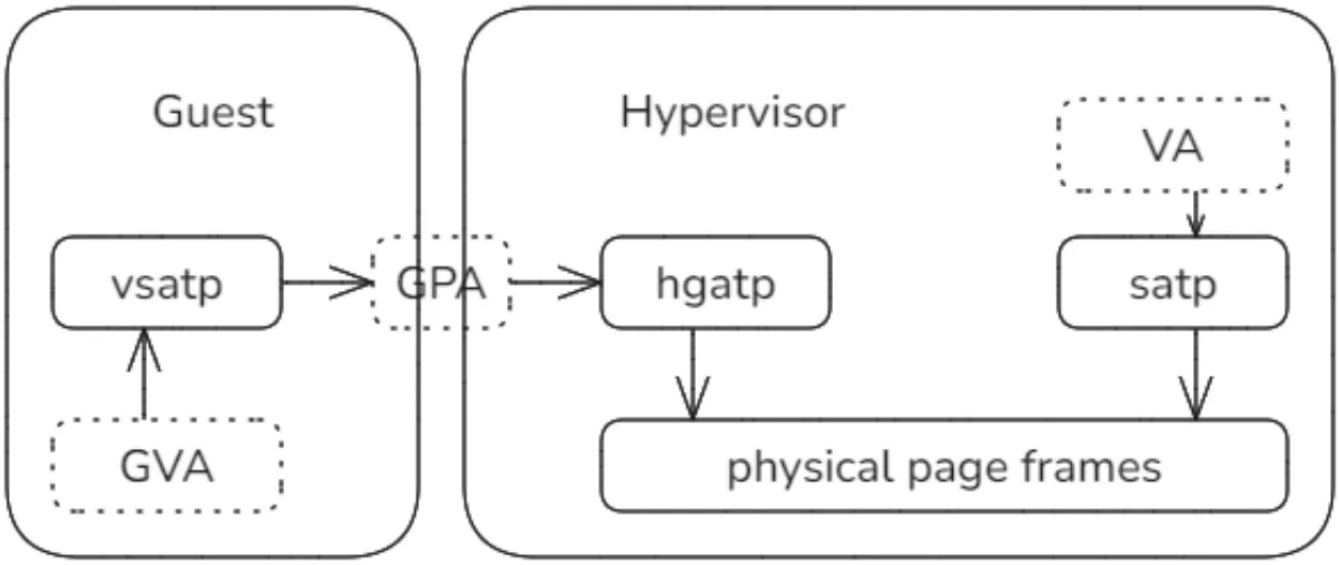
Hypervisor地址空间管理基础

H_2_0 GuestAspace——两阶段地址映射原理和具体实现



- hgatp相对于satp在根页表级扩展了2位，总数达到41位

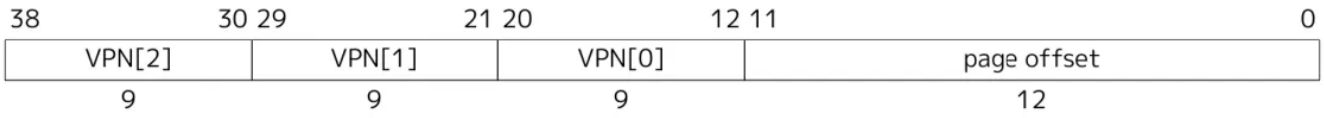


Figure 60. Sv39 virtual address.

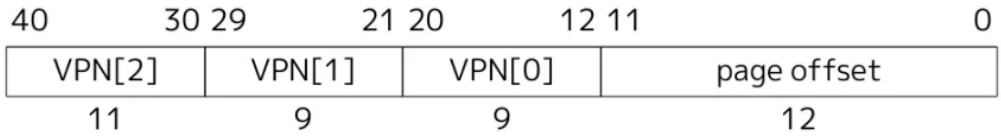
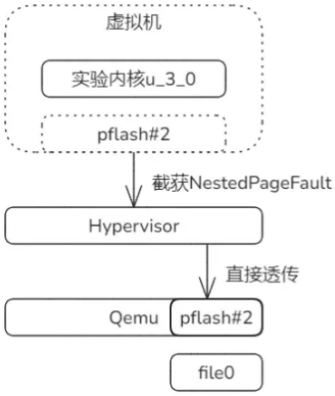
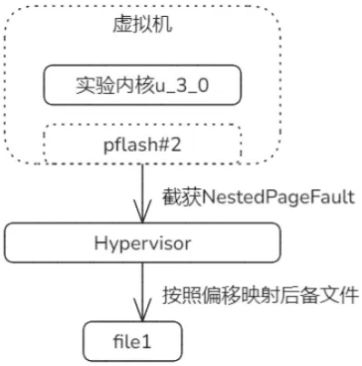


Figure 108. Sv39x4 virtual address (guest physical address).

设备模拟和透传(默认)两种模式的实现



用map_linear直接映射
qemu(宿主平台)的pflash#2的地址区域



用map_alloc申请页帧完成映射
从file1中加载内容填充页帧

课后练习——设备模拟和透传(默认)两种模式的实现

模拟可以理解为文件mmap，透传的做法类似于缺页映射。

```
68
69      loop {
70          match vcpu_run(&mut arch_vcpu) {
71              Ok(exit_reason: AxVCpuExitReason) => match exit_reason {
72                  AxVCpuExitReason::Nothing => {}
73                  NestedPageFault { addr: VirtAddr, access_flags: MappingFlags } => {
74                      debug!("addr {:#x} access {:#x}", addr, access_flags);
75                      // assert_eq!(addr, 0x2200_0000.into(), "Now we ONLY handle pflash#2.");
76                      // let mapping_flags = MappingFlags::from_bits(0xf).unwrap();
77                      // // Passthrough-Mode
78                      // let _ = aspace.map_linear(addr, addr.as_usize().into(), 4096, mapping_flags);
79
80                      // Pretend to load file to fill buffer.
81                      let mut buf: [u8; 4] = [0; 4];
82                      let mut file: File = File::open(path: "/sbin/pflash.img").unwrap();      You, 36秒钟前 • Uncommitted changes
83                      file.read_exact(&mut buf);
84
85                      aspace.map_alloc(start: addr, size: 4096, mapping_flags, populate: true);
86                      aspace.write(start: addr, &buf);
87                  }
88                  _ => {
89                      panic!("Unhandled VM-Exit: {:?}", exit_reason);
90                  }
91              },
92              Err(err: AxError) => {
93                  panic!("run VCpu get error {:?}", err);
```

```
问题 1  输出  终端  GITLENS

终端

  d8888888888 888     Y88b.    Y8b.     Y88b. .d88P Y88b  d88P
d88P     888 888      "Y8888P  "Y8888   "Y88888P"   "Y8888P"

arch = riscv64
platform = riscv64-qemu-virt
target = riscv64gc-unknown-none-elf
smp = 1
build_mode = release
log_level = warn

Try to access dev region [0xFFFFFFC022000000], got 0x646C6670
Got pflash magic: pfld
zjz@zjz:~/arceos/oscamp/arceos$
```