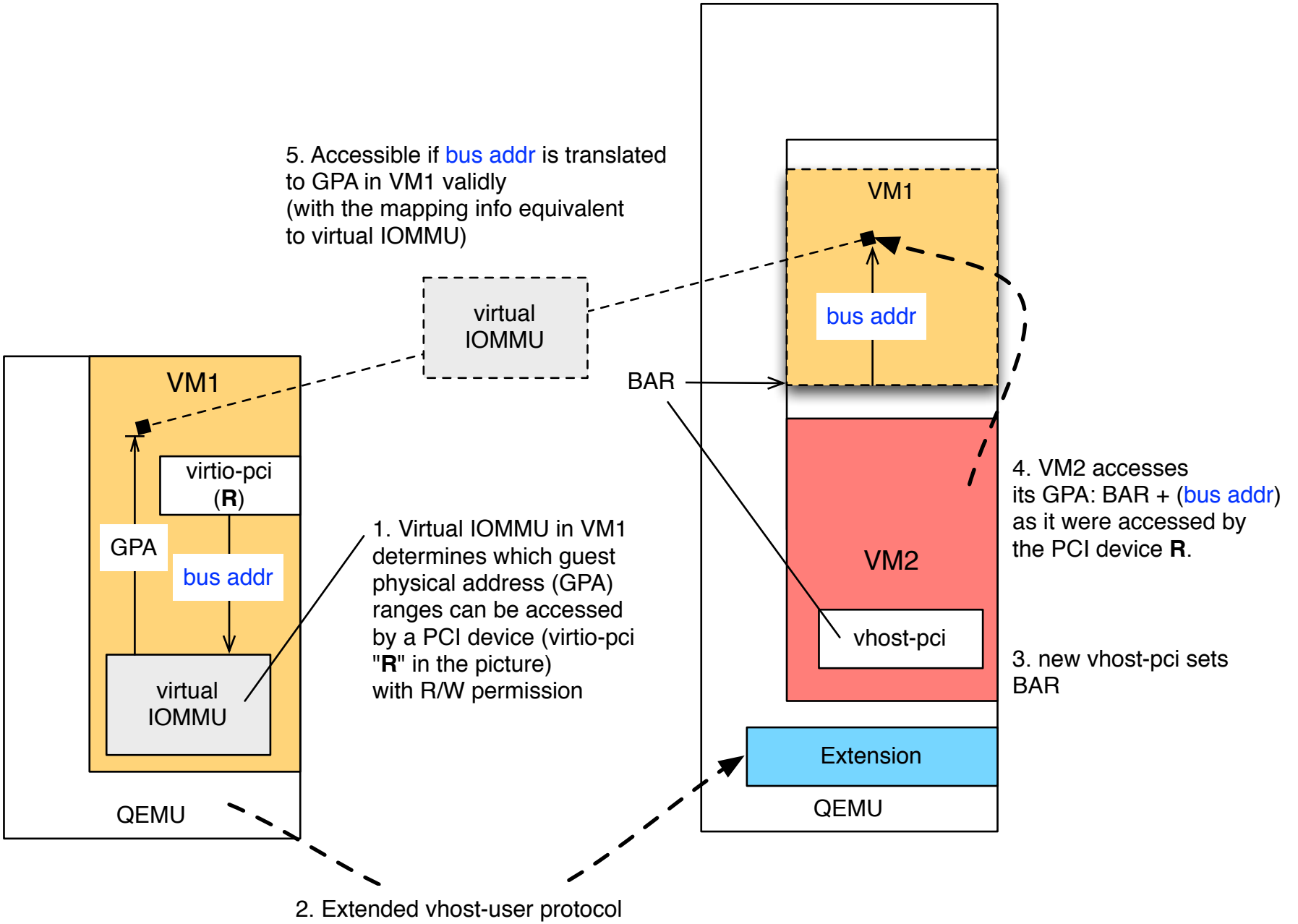
5. Accessible if bus addr is translated to GPA in VM1 validly (with the mapping info equivalent to virtual IOMMU)
virtual IOMMU
VM1
virtio-pci (R)
GPA
bus addr
virtual IOMMU
QEMU
1. Virtual IOMMU in VM1 determines which guest physical address (GPA) ranges can be accessed by a PCI device (virtio-pci "R" in the picture) with R/W permission
VM1
bus addr
BAR
VM2
vhost-pci
4. VM2 accesses its GPA: BAR + (bus addr) as it were accessed by the PCI device R.
3. new vhost-pci sets BAR
Extension
QEMU
2. Extended vhost-user protocol