



MEMORY MODEL

```
000000000000000000 - 00007fffffffffffff (=47 bits) user space, different per mm
hole caused by [47:63] sign extension
ffff800000000000 - fffff87fffffffffffff (=43 bits) guard hole, reserved for hypervisor
ffff880000000000 - fffffc7fffffffffffff (=64 TB) direct mapping of all phys. memory
ffffc80000000000 - fffffc8fffffffffffff (=40 bits) hole
ffffc90000000000 - fffffe8fffffffffffff (=45 bits) vmalloc/ioremap space
ffffe90000000000 - fffffe9fffffffffffff (=40 bits) hole
fffffea00000000000 - fffffeafffffffffffffff (=40 bits) virtual memory map (1TB)
... unused hole ...
fffffec00000000000 - ffffffbfffffffffffff (=44 bits) kasan shadow memory (16TB)
... unused hole ...
                vaddr_end for KASLR
ffffffe00000000000 - ffffffe7fffffffffffff (=39 bits) cpu_entry_area mapping
ffffffe80000000000 - ffffffefffffffffffff (=39 bits) LDT remap for PTI
fffffff00000000000 - ffffffff7fffffffffffff (=39 bits) %esp fixup stacks
... unused hole ...
ffffffffffef00000000 - fffffffffffefffffffffff (=64 GB) EFI region mapping space
... unused hole ...
ffffffffff800000000 - fffffffffff9fffffffff (=512 MB) kernel text mapping, from phys 0
fffffffffffa0000000 - ffffffffffffefffffffff (1520 MB) module mapping space
[fixmap start] - fffffffffff5fffff kernel-internal fixmap range
ffffffffff600000 - fffffffffff600fff (=4 kB) legacy vsyscall ABI
fffffffffffe00000 - fffffffffffefffffffffff (=2 MB) unused hole
```

https://www.kernel.org/doc/Documentation/x86/x86_64/mm.txt



MELTDOWN AND
SPECTRE

CONCLUSION

MEMORY MODEL

Virtual memory map with 4 level page tables:

```
000000000000000000 - 00007fffffffffffff (=47 bits) user space, different per mm
hole caused by [47:63] sign extension
ffff800000000000 - ffff87ffffffffffff (=43 bits) guard hole, reserved for hypervisor
ffff880000000000 - ffffc7ffffffffffff (=64 TB) direct mapping of all phys. memory
ffffc80000000000 - ffffc8ffffffffffff (=40 bits) hole
ffffc90000000000 - ffffe8ffffffffffff (=45 bits) vmalloc/ioremap space
ffffe90000000000 - ffffe9ffffffffffff (=40 bits) hole
fffffea00000000000 - ffffeaffffffffffffff (=40 bits) virtual memory map (1TB)
... unused hole ...
fffffec00000000000 - fffffbffffffffffff (=44 bits) kasan shadow memory (16TB)
... unused hole ...
                                vaddr_end for KASLR
ffffffe00000000000 - ffffffe7ffffffffffff (=39 bits) cpu_entry_area mapping
ffffffe80000000000 - ffffffefffffffffffff (=39 bits) LDT remap for PTI
fffffff00000000000 - ffffffff7fffffffffffff (=39 bits) %esp fixup stacks
... unused hole ...
fffffffef000000000 - ffffffffeffffffffffffff (=64 GB) EFI region mapping space
... unused hole ...
fffffffff800000000 - fffffffff9ffffffffffff (=512 MB) kernel text mapping, from phys 0
ffffffffffa0000000 - ffffffffffefffffffffff (1520 MB) module mapping space
[fixmap start]      - ffffffffffff5fffffff kernel-internal fixmap range
fffffffffffff600000 - fffffffffffff600ffff (=4 kB) legacy vsyscall ABI
fffffffffffffe00000 - ffffffffffffffffffffff (=2 MB) unused hole
```