 # Author : Muhammad Imran
 # Date: 18-02-2026
 # Module : RISCV Arch Test
 # Section: RISCV Arch Test
 # Task Name: Task 7

Github: Task 7

Test Description:

This test verifies the behavior of the Smepmp in RISC-V systems by evaluating how the mseccfg.MML bit affects Machine mode execution and memory access permissions when PMP (Physical Memory Protection) rules are configured. The test begins execution in Machine mode and intentionally manipulates the mseccfg register to observe system behavior before and after enabling MML. It explores what happens when executable permissions are assigned to a locked PMP region and examines whether Machine mode can still access memory once lockdown is activated. Additionally, the test validates how RLB (Rule Locking Bypass) enables modification of locked PMP entries prior to final lockdown. The experiment confirms that once MML is set, Machine mode becomes subject to PMP rules and can no longer bypass them. Load and store operations targeting protected regions should generate access faults, which are then handled by the trap vector. The test ensures that proper exception handling occurs and that the system continues execution as expected.

Output Explanation:

The test starts in Machine mode and sets mtvec to the trap_vector. RLB (bit 2 of mseccfg) is enabled first to allow modification of locked PMP entries.

```
19   core   0: 0x80000040 (0x00400293) li      t0, 4
20   core   0: 3 0x80000040 (0x00400293) x5  0x00000004
21   core   0: 0x80000044 (0x74729073) csrw    mseccfg, t0
22   core   0: 3 0x80000044 (0x74729073) c1863_mseccfg 0x00000004
```

A TOR (Top Of Range) PMP region entry is created using pmpaddr0.

```
24   core   0: 3 0x80000048 (0x00001297) x5  0x80001048
25   core   0: 0x8000004c (0xfc828293) addi    t0, t0, -56
26   core   0: 3 0x8000004c (0xfc828293) x5  0x80001010
27   core   0: 0x80000050 (0x0022d293) srli    t0, t0, 2
28   core   0: 3 0x80000050 (0x0022d293) x5  0x20000404
29   core   0: 0x80000054 (0x3b029073) csrw    pmpaddr0, t0
30   core   0: 3 0x80000054 (0x3b029073) c944_pmpaddr0 0x20000404
```

pmpcfg0 is set to 0x8C (L=1, TOR, X=1, W=0, R=0), creating a locked executable-only region

```
31   core   0: 0x80000058 (0x08c00293) li      t0, 140
32   core   0: 3 0x80000058 (0x08c00293) x5  0x0000008c
33   core   0: 0x8000005c (0x3a029073) csrw    pmpcfg0, t0
34   core   0: 3 0x8000005c (0x3a029073) c928_pmpcfg0 0x0000008c
```

After PMP configuration, mseccfg.MML is set

```
34   core   0: 3 0x8000005c (0x3a029073) c928_pmpcfg0 0x0000008c
35   core   0: 0x80000060 (0x7470d073) csrwi   mseccfg, 1
36   core   0: 3 0x80000060 (0x7470d073) c1863_mseccfg 0x00000001
37   core   0: 0x80000064 (0x00000013) nop
38   core   0: 3 0x80000064 (0x00000013)
```

Once MML is enabled, Machine mode obey PMP rules. NOP instruction will execute successfully because the rule specifies the only executable machine mode region. but

A load (lw) instruction attempts to read from the protected region — expected load access fault.

```
core   0: 3 0x80000070 (0xfd428293) x5  0x80000040
core   0: 0x80000074 (0x0002a303) lw      t1, 0(t0)
core   0: exception trap_load_access_fault, epc 0x80000074
core   0:           tval 0x80000040
core   0: >>>>  trap_vector
core   0: 0x80000010 (0x342022f3) csrr    t0, mcause
```

A store (sw) instruction attempts to write — expected store access fault.

```
core   0: 3 0x80000080 (0xfc428293) x5  0x80000040
core   0: 0x80000084 (0x0072a023) sw      t2, 0(t0)
core   0: exception trap_store_access_fault, epc 0x80000084
core   0:           tval 0x80000040
core   0: >>>>  trap_vector
core   0: 0x80000010 (0x342022f3) csrr    t0, mcause
```

Finally the test exit in machine mode by writing '1' to tohost.

Answering the Test Questions

Setting mseccfg.MML at the start?

if MML is set before PMP configuration, Machine mode immediately becomes restricted. Since no PMP rule matches the current code region, instruction access fault occurs instantly.

adding an executable M-mode-only or locked shared region?why?solution
Once locked and MML is enabled, Machine mode must obey the rule. If read/write permissions are not granted, load/store faults occur as observed; this can be solved by enabling RLB first. RLB allows modification of locked PMP entries before final lockdown. After configuration is complete, MML is set to enforce protection permanently.