

Author : Muhammad Imran
Date: 12-02-2026
Module : RISCv Arch Test
Section: RISCv Arch Test
Task Name: Task 2

Github link: [RISCv Arch Test- Task 2](#)

Task Description:

This test creates and configures two memory regions with different constraints and verifies them. One follows the TOR addressing method with '**X**' permissions and other follows the NAPOT addressing method with '**R**' permissions. PMP checks are also applied on the existing memory regions created in the previous tasks. Load , Stores and Executes accesses are tested from the lower privilege modes on these configured memory regions and verified that configured PMP restrictions are working correctly. Each access gives the appropriate access fault. At the end the same restrictions are also set for Machine mode setting the lock bit of each PMP region and appropriate access faults are again tested and verified for Machine mode. Trap handler for corresponding access faults is also added to the trap vector to address the access faults.

Memory Regions:

The linker script defines multiple memory sections. Two new PMP test regions are created:

TOR Section

Label: `._tor_section`
Start: `._tor_start` (4KB aligned)
End: `._tor_end` (4KB aligned)
Contains a single nop instruction and a ret instruction.

NAPOT Section

Label: `._napot_section`
4KB aligned
Contains a single word `._word 0x0`.

Other memory sections exist as usual among them stack is not configured for PMP
PMP checks:

PMP_configurations:

The `_start` function calls `pmp_config` to initialize PMP entries in which at first existing memory region is configured as follows:

- **Region 0 (pmpaddr0):** `.text.init` configured as **TOR**, initially OFF. for this region the lower bound is addresses towards 0 and upper bound is the address of the `.text.init` section. It is shifted 2 bit right because pmpaddr reg stores word aligned address.

```
21 core 0: 0x80000040 (0xfbc28293) addi t0, t0, 00
22 core 0: 3 0x80000048 (0xfbc28293) x5 0x80000000
23 core 0: 0x8000004c (0x0022d293) srli t0, t0, 2
24 core 0: 3 0x8000004c (0x0022d293) x5 0x20000000
25 core 0: 0x80000050 (0x3b029073) csrw pmpaddr0, t0
26 core 0: 3 0x80000050 (0x3b029073) c944_pmpaddr0 0x20000000
27 core 0: 0x80000054 (0x00000293) li t0, 0
```

- **Region 1 (pmpaddr1):** Mapped from `_end` of `.bss` to top of memory as **TOR** with all permissions.

```
34 core 0: 3 0x80000060 (0xfa428293) x5 0x80002000
35 core 0: 0x80000064 (0x0022d293) srli t0, t0, 2
36 core 0: 3 0x80000064 (0x0022d293) x5 0x20000800
37 core 0: 0x80000068 (0x3b129073) csrw pmpaddr1, t0
38 core 0: 3 0x80000068 (0x3b129073) c945_pmpaddr1 0x20000800
39 core 0: 0x8000006c (0x00f00313) li t1, 15
```

- **Region 2 (pmpaddr2): TOR SECTION** Configured as TOR region with execute-only permission

```
52 core 0: 3 0x80000084 (0xf8028293) x5 0x80003000
53 core 0: 0x80000088 (0x0022d293) srli t0, t0, 2
54 core 0: 3 0x80000088 (0x0022d293) x5 0x20000c00
55 core 0: 0x8000008c (0x3b229073) csrw pmpaddr2, t0
56 core 0: 3 0x8000008c (0x3b229073) c946_pmpaddr2 0x20000c00
57 core 0: 0x80000090 (0x00c00313) li t1, 12
```

- **Region 2 (pmpaddr3): NAPOT Section** Configured as NAPOT region with read-only permission

```
70 core 0: 3 0x800000a8 (0xf5c28293) x5 0x80003000
71 core 0: 0x800000ac (0x1ff00313) li t1, 511
72 core 0: 3 0x800000ac (0x1ff00313) x6 0x000001ff
73 core 0: 0x800000b0 (0x0022d293) srli t0, t0, 2
74 core 0: 3 0x800000b0 (0x0022d293) x5 0x20000c00
75 core 0: 0x800000b4 (0x0062e2b3) or t0, t0, t1
76 core 0: 3 0x800000b4 (0x0062e2b3) x5 0x20000dff
77 core 0: 0x800000b8 (0x3b329073) csrw pmpaddr3, t0
78 core 0: 3 0x800000b8 (0x3b329073) c947_pmpaddr3 0x20000dff
79 core 0: 0x800000bc (0x01900393) li t2, 25
```

Actual Output:

After switching to the supervisor mode

Performing RWX in TOR Region

READ/LOAD access fault

```
150 core 0: 1 0x8000010c (0xef828293) x5 0x80002000
151 core 0: 0x80000110 (0x0002a303) lw t1, 0(t0)
152 core 0: exception trap_load_access_fault, epc 0x80000110
153 core 0: tval 0x80002000
154 core 0: >>>> trap_vector
155 core 0: 0x80000014 (0x342022f3) csrr t0, mcause
156 core 0: 3 0x80000014 (0x342022f3) x5 0x00000005
157 core 0: 0x80000018 (0x00800313) li t1, 8
```

WRITE/STORE access FAULT

```
186 core 0: 1 0x8000011c (0xee828293) x5 0x80002000
187 core 0: 0x80000120 (0x0072a223) sw t2, 4(t0)
188 core 0: exception trap_store_access_fault, epc 0x80000120
189 core 0: tval 0x80002004
190 core 0: >>>> trap_vector
191 core 0: 0x80000014 (0x342022f3) csrr t0, mcause
192 core 0: 3 0x80000014 (0x342022f3) x5 0x00000007
193 core 0: 0x80000018 (0x00800313) li t1, 8
```

NO INSTRUCTION Access FAULT

```
core 0: 0x80000124 (0x6dd010ef) jal pc + 0x1edc
core 0: 1 0x80000124 (0x6dd010ef) x1 0x80000128
core 0: 0x80002000 (0x00000013) nop
core 0: 1 0x80002000 (0x00000013)
core 0: 0x80002004 (0x00008067) ret
core 0: 1 0x80002004 (0x00008067)
core 0: 0x80000128 (0x00003297) auipc t0, 0x3
core 0: 1 0x80000128 (0x00003297) x5 0x80003128
```

Performing RWX in NATOP Region

NO READ/LOAD access fault

```
core 0: 0x80000128 (0x00003297) auipc t0, 0x3
core 0: 1 0x80000128 (0x00003297) x5 0x80003128
core 0: 0x8000012c (0xed828293) addi t0, t0, -296
core 0: 1 0x8000012c (0xed828293) x5 0x80003000
core 0: 0x80000130 (0x0002a303) lw t1, 0(t0)
core 0: 1 0x80000130 (0x0002a303) x6 0x00000000 mem 0x80003000
core 0: 0x80000134 (0x00500393) li t2, 5
core 0: 1 0x80000134 (0x00500393) x7 0x00000005
```

WRITE/STORE access FAULT

```
core 0: 1 0x8000013c (0xec828293) x5 0x80003000
core 0: 0x80000140 (0x0072a223) sw t2, 4(t0)
core 0: exception trap_store_access_fault, epc 0x80000140
core 0: tval 0x80003004
core 0: >>>> trap_vector
core 0: 0x80000014 (0x342022f3) csrr t0, mcause
core 0: 3 0x80000014 (0x342022f3) x5 0x00000007
```

INSTRUCTION Access FAULT

```
core 0: 0x80000144 (0x6bd020ef) jal pc + 0x2ebc
core 0: 1 0x80000144 (0x6bd020ef) x1 0x80000148
core 0: exception trap_instruction_access_fault, epc 0x80003000
core 0: tval 0x80003000
core 0: >>>> trap_vector
core 0: 0x80000014 (0x342022f3) csrr t0, mcause
core 0: 3 0x80000014 (0x342022f3) x5 0x00000001
core 0: 0x80000018 (0x00800313) li t1, 8
```

Going back to Machine mode using ECALL in S-mode

```
core 0: 0x80000224 (0x30200073) mret
core 0: 3 0x80000224 (0x30200073) c768_mstatus 0x00000080 c784_mstatush 0x00000000
core 0: 0x80000148 (0x00000073) ecall
core 0: exception trap_supervisor_ecall, epc 0x80000148
core 0: >>>> trap_vector
core 0: 0x80000014 (0x342022f3) csrr t0, mcause
core 0: 3 0x80000014 (0x342022f3) x5 0x00000009
core 0: 0x80000018 (0x00800313) li t1, 8
```

Switching back to Machine mode, the same PMP restrictions apply. Appropriate access faults are generated when attempting unauthorized access.

Trap occurred in machine mode too

```
core 0: 0x80000150 (0xeb428293) addi    t0, t0, -332
core 0: 3 0x80000150 (0xeb428293) x5    0x80002000
core 0: 0x80000154 (0x0002a303) lw      t1, 0(t0)
core 0: exception trap_load_access_fault, epc 0x80000154
core 0:          tval 0x80002000
core 0: >>>> trap_vector
core 0: 0x80000014 (0x342022f3) csrr    t0, mcause
core 0: 3 0x80000014 (0x342022f3) x5    0x00000005
```

```
core 0: 3 0x80000160 (0xea428293) x5    0x80002000
core 0: 0x80000164 (0x0072a223) sw      t2, 4(t0)
core 0: exception trap_store_access_fault, epc 0x80000164
core 0:          tval 0x80002004
core 0: >>>> trap_vector
core 0: 0x80000014 (0x342022f3) csrr    t0, mcause
core 0: 3 0x80000014 (0x342022f3) x5    0x00000007
core 0: 0x80000018 (0x00800313) li      t1, 8
```

```
12 core 0: 3 0x8000023c (0x30200073) c768_mstatus 0x00000080 c784_mstatush 0x00000000
13 core 0: 0x80000168 (0x699010ef) jal    pc + 0x1e98
14 core 0: 3 0x80000168 (0x699010ef) x1    0x8000016c
15 core 0: 0x80002000 (0x00000013) nop
16 core 0: 3 0x80002000 (0x00000013)
17 core 0: 0x80002004 (0x00008067) ret
18 core 0: 3 0x80002004 (0x00008067)
19 core 0: 0x8000016c (0x0f80006f) j      pc + 0xf8
```

Reference:

Physical Memory Protection: Privileged Architecture v1.12, Sec 3.7