

Hands On Session On Qemu Simulator

- **Step 1 :** First of all how to access HPC cluster ?

Open terminal and run this command:

ssh -X riscv-sim@10.0.0.153



Figure 1: Interface of HPC Cluster

- **Step 2:** Run command in the terminal:
`cd demo_simulators/`
- **Step 3:** Create directory of your name:
`mkdir qadeer`
- **Step 4:** Write & Compile Your Hello World RISC-V Program with Debug Symbols:
Use the -g flag to include debug symbols when compiling your RISC-V code.
`riscv64-unknown-elf-gcc -g -o my_program my_program.c`
- **Step 5 :** Run QEMU with RISC-V 64-bit:
`qemu-riscv64 ./my_program`
- **Step 6:** To connect with gdb and debug it
`qemu-system-riscv64 -machine virt -nographic -kernel my_program -s -S`

- **Explanation:**

-machine virt: Specifies a virtual RISC-V machine.

-nographic: Disables graphical output (useful for kernel debugging).

-kernel my_kernel.elf: Specifies the kernel or program you want to run.

-s: Starts QEMU with a GDB server listening on port 1234.

-S: Stops QEMU at startup, waiting for GDB to connect.

Now Open New Terminal and run:

```
riscv64-unknown-elf-gdb ./my_program
```

- **Step 7:** Inside GDB, connect to QEMU:

```
target remote localhost:1234
```

- **Step 8: Debugging with GDB**

- You can set breakpoints on specific functions or lines:

```
break main
```

- View the RISC-V registers:

```
info registers
```

- Continue execution in QEMU from within GDB:

```
continue
```

- Quit GDB:

```
quit
```

Tasks

Task 1: Write a c code of swapping variables and debug it on gdb & qemu. Show to the instructor.