# PetaLinux SDK User Guide

## *QEMU System Simulation Guide*

**UG982 (v2013.04) April 22, 2013**

XILINX®

# Revision History

| Date | Version | Notes |
|---|---|---|
| 2009-11-27 | 1.1 | Initial version for SDK 1.1 release |
| 2010-11-26 | 1.3 | Updated for PetaLinux SDK 1.3 release and PowerPC support |
| 2011-04-03 | 2.1 | Updated for PetaLinux SDK 2.1 release (AXI device and CPU models |
| 2012-08-03 | 3.1 | Updated for PetaLinux SDK 3.1 release |
| 2012-09-03 | 12.9 | Updated for PetaLinux SDK 12.9 release |
| 2012-12-17 | 2012.12 | Updated for PetaLinux SDK 2012.12 release |
| 2013-04-22 | 2013.04 | Updated for PetaLinux SDK 2013.04 release |

XILINX

# Table of Contents

# About this Guide

This guide describes how to use the QEMU System Simulator included with PetaLinux SDK. The system simulator in PetaLinux SDK has the unique capability to configure automatically the simulation model to match the architecture of your target hardware system.

The ability to test and develop your software stack in a simulated environment allows your software and hardware design efforts to greatly improve parallelism, reducing overall development time.

- As of PetaLinux SDK v2013.04, Zynq and MicroBlaze (little-endian) architectures are supported.

Please note: readers of this document are assumed to have basic Linux knowledge such as how to run simple Linux commands.

# PetaLinux Software Simulation with QEMU

The `petalinux-qemu-boot` tool is used to boot a PetaLinux kernel image in the system simulator.

## Prerequisites

This guide assumes that the following prerequisites have been satisfied:

- PetaLinux SDK and at least one PetaLinux BSP has been installed.
- You know how to build PetaLinux software image (Please refer to the *PetaLinux SDK Getting Started Guide (UG977)* ).
- Your workstation has `tftpd` server running.
- There exists a `"/tftpboot"` directory on your workstation and all users have read/write permissions to it.
- PetaLinux working environment has been setup in each command console you use with PetaLinux. Run the following command to check whether the PetaLinux environment has been setup on the command console:

  ```
  $ echo $PETALINUX
  ```

  If the PetaLinux working environment has been setup, it should show the path to the installed PetaLinux. If it shows nothing, please refer to the section Environment Setup in the *PetaLinux SDK Getting Started Guide (UG977)* document to setup the environment.

## Boot Recently Built Linux Image

If no argument is given, `petalinux-qemu-boot` boots the most recently built Linux image (from the `"$PETALINUX/software/petalinux-dist/image.elf"` system image).

1. Build the PetaLinux software image
2. After the software image has been successfully built, run `petalinux-qemu-boot` on the command console:

   ```
   $ petalinux-qemu-boot
   ```

3. Watch the console, you will see the Linux boot process, ending with a login prompt:

```
Mounting devpts:
Mounting all filesystem
Setting hostname:
Bringing up network interfaces:
GEM: lp->tx_bd ffdfb000 lp->tx_bd_dma 2e833000 lp->tx_skb ef1cb4c0
GEM: lp->rx_bd ffdfc000 lp->rx_bd_dma 2e83b000 lp->rx_skb ef1cb2c0
GEM: MAC 0x00350a00, 0x000002b2, 00:0a:35:00:b2:02
udhcpc (v1.14.3) started
Sending discover...
Sending select for 192.168.10.2...
Lease of 192.168.10.2 obtained, lease time 864000
adding dns 192.168.1.1
adding dns 192.168.1.254
Starting portmap:
Starting uWeb server:

Welcome to
 _____       _            _      _
| ___ \     | |          | |    (_)
| |_/ / ___ | |_   __ _ | |     _  _ __    _   _ __  __
|  __/ / _ \| __| / _‘ || |    | || ’_ \ | | | |\ \/ /
| |   |  __/| |_ | (_| || |____| || | | || |_| | >  <
\_|    \___| \__| \__,_|\_____/|_||_| |_| \__,_|/_/\_\


on Xilinx-ZC702-14.5


Xilinx-ZC702-14.5 login:
```

Figure 1: Boot PetaLinux Linux Image with QEMU

You may see slightly different output from the above example, it depends on the Linux image you test.

4. Login to the virtual system when you see the login prompt on the simulator console.
5. Try some Linux commands such as `ls`, `ifconfig`, `cat /proc/cpuinfo` and so on. They behave the same as on real hardware.
6. To exit the simulator, press `Ctrl+A` then `X`.

## Direct Boot a Specific Linux Image

`petalinux-qemu-boot` can also boot a specific Linux image, using the `image` option (`-i` or `--image`):

```
$ petalinux-qemu-boot -i <path-to-Linux-image-file>
```

e.g.:

```
$ petalinux-qemu-boot -i images/image.elf
```

**WARNING:** *`petalinux-qemu-boot` can only boot ELF images*

## Direct Boot a Linux Image with Specified DTB

Device Trees (DTB files) are used to describe the hardware architecture and address map to the Linux kernel. The PetaLinux system simulator also uses DTB files to dynamically configure the simulation environment to exactly match your hardware model.

If no DTB file option is provided, as in the previous two examples, `petalinux-qemu-boot` extracts the DTB file from the given ELF image. Alternatively, you can specify a particular DTB file by giving the DTB command option (`-d` or `--dtb`) as follows:

```
$ petalinux-qemu-boot -d <path-to-DTB-file>
```

e.g. for a MicroBlaze system:

```
$ petalinux-qemu-boot -d linux-2.6.x/arch/microblaze/boot/system.dtb
```

## QEMU boot Linux Image via U-boot

In addition to the kernel, it is also possible to boot via the u-boot bootloader in QEMU. This is useful for example to prepare and test custom u-boot command scripts or other settings. It is even possible to replicate the u-boot / tftpboot / Linux kernel boot process, all inside QEMU!

**WARNING:** *This feature requires `sudo` access on the local machine to setup the QEMU virtual network, and does not work with the `--noroot` option.*

1. Boot u-boot with QEMU by running `petalinux-qemu-boot` as follows on the command console:

   ```
   $ petalinux-qemu-boot -u
   ```

   If no DTB file is specified with the `--dtb` option, and there is no DTB file embedded in the ELF file (such as with the `"u-boot.elf"` image), then the most recently compiled DTB is used instead. For MicroBlaze this is:

   ```
   $PETALINUX/software/linux-2.6.x/arch/microblaze/boot/system.dtb
   ```

2. Watch the console, you will see the u-boot booting messages.
3. Hit any key to stop auto boot when you see `'Hit any key to stop autoboot:'` on the console. e.g:

```
U-Boot 2011.06
Xilinx Zynq Platform

DRAM:  1 GiB
MMC:   SDHCI: 0
Using default environment

In:    serial
Out:   serial
Err:   serial

Net:   XGem.e000b000

U-BOOT for Xilinx-ZC702-14.5

Resetting PHY...

PHY reset complete.

Waiting for PHY to complete autonegotiation.
PHY claims autonegotiation complete...
GEM link speed is 100Mbps
BOOTP broadcast 1
DHCP client bound to address 192.168.10.2
Hit any key to stop autoboot:  0
U-Boot-PetaLinux>
```

Figure 2: QEMU U-boot

4. Run u-boot command `print` on the QEMU console to check whether the u-boot variable `serverip` has been set to the right TFTP server from which to download the Linux image:

   ```
   U-Boot-PetaLinux> print serverip
   ```

   By default, this should be `192.168.10.1` - the address of your Linux workstation in the QEMU virtual subnet. If this value is not correct, run u-boot command set to change it on the QEMU console:

   ```
   U-Boot-PetaLinux> set serverip <TFTP serverip IP>
   ```

5. Run the `netboot` command to boot the virtual processor via TFTP over the virtual network:

   ```
   U-Boot-PetaLinux> run netboot
   ```

6. Watch the QEMU console, you should see the Linux image booting messages.

7. When you see the Linux login prompt on the QEMU console, login to start using Linux on a virtual processor.

# Going Further

## Running QEMU without sudo access

By default QEMU requires `sudo` access to the local machine. This access is required for setting up the virtual networking between the local machine and the emulated system.

If the virtual networking is not required you can run QEMU with `--noroot`. This will allow QEMU to execute without `sudo` access, and emulate the target system without networking.

```
$ petalinux-qemu-boot --noroot
```

In this mode the network device will appear however it will not be able to communicate with the host.

## Specifying the QEMU Virtual Subnet

By default, PetaLinux uses `192.168.10.*` as the QEMU virtual subnet. If it has been used by your local network or other virtual subnet, you may wish to use another subnet. You can configure PetaLinux to use other subnet settings for QEMU by running `petalinux-qemu-boot` as follows on the command console:

**WARNING:** *This feature requires `sudo` access on the local machine, and does not work with the `--noroot` option.*

```
$ petalinux-qemu-boot --subnet <subnet gateway IP>/
    <number of the bits of the subnet mask>
```

e.g., to use subnet `192.168.20.*`:

```
$ petalinux-qemu-boot --subnet 192.168.20.0/24
```

## Access Internet with QEMU

By default, the Linux boot via QEMU cannot access the Internet or other network addresses outside the virtual QEMU network.

**WARNING:** *This feature requires `sudo` access on the local machine, and does not work with the `--noroot` option.*

`petalinux-qemu-boot` provides an option to allow QEMU access the Internet:

```
$ petalinux-qemu-boot --iptables-allowed
```

This command will add a rule to the iptables FORWARD chain to allow traffic from the QEMU virtual subnet to `eth0` to any destination. This rule will be deleted when the QEMU is terminated.

If you test the pre-built MicroBlaze software image with QEMU, you can run `petalinux-boot-prebuilt` as follows to allow QEMU access the Internet:

```
$ petalinux-boot-prebuilt -p <reference platform> -q --qboot-args
    --iptables-allowed
```

Please note that the use of the `--iptables-allowed` option does modify your PC firewall rules and state. While every effort is made to restore any changes to the state, it is not guaranteed to restore the state. If you have any doubt, or you are in a secure networking environment, **DO NOT USE THIS OPTION**.

## Debugging the Linux Kernel in QEMU

You can debug the MicroBlaze Linux Kernel inside QEMU, using the GDB debugger. The default TCP port for MicroBlaze QEMU is `9000`:

1. Launch QEMU with the currently built Linux by running the following command:

   ```
   $ petalinux-qemu-boot
   ```

2. Open another command console and go to the Linux directory:

   ```
   $ cd $PETALINUX/software/petalinux-dist/linux-2.6.x
   ```

3. Start GDB on the vmlinux kernel image in command mode inside `"linux-2.6.x"` directory:

   ```
   $ microblazeel-xilinx-linux-gnu-gdb vmlinux
   ```

   You should see the `gdb` prompt. e.g.:

   ```
   GNU gdb (crosstool-NG 1.18.0) 7.4.50.20120403-cvs
   Copyright (C) 2012 Free Software Foundation, Inc.
   License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
   This is free software: you are free to change and redistribute it.
   There is NO WARRANTY, to the extent permitted by law. Type "show copying"
   and "show warranty" for details.
   This GDB was configured as "--host=i686-build_pc-linux-gnu --target=microblazeel-xilinx-linux-gnu".
   For bug reporting instructions, please see:
   <http://www.gnu.org/software/gdb/bugs/>...
   ```

4. Attach to the QEMU target in GDB by running the following GDB command:

   ```
   (gdb) target remote :9000
   ```

5. To let QEMU continue execution:

   ```
   (gdb) continue
   ```

6. You can use `Ctrl+C` to interrupt the kernel and get back the GDB prompt.

7. You can set break points and run other GDB commands to debug the kernel.

It may be helpful to enable kernel debugging in the kernel configuration menu (**petalinux-config-kernel** > **Kernel hacking** > **Kernel debugging**), so that kernel debug symbols are present in the image.

## More about petalinux-qemu-boot

This guide has introduced the most commonly used modes and options of `petalinux-qemu-boot`. To learn more, run it with the `--help` option:

```
$ petalinux-qemu-boot --help
```

The detailed explanation of each option will be shown on the console.

# Virtual IO

## Networking

### Default Mode

`petalinux-qemu-boot` runs in `sudo` mode by default. In this mode it creates a tap networking device on the host and runs QEMU with the tap networking backend. In this mode, QEMU and the host can directly transmit and recieve network packets.

### User Mode

If `petalinux-qemu-boot` is run with `--noroot` option, or if user does not have `sudo` access, `petalinux-qemu-boot` will run in normal user mode. In this mode, QEMU runs without any non default networking options. In this mode, it does not permit any network traffic between the host and guest. However using QEMU, you can redirect a port on the host to a port on the guest (similar to NAT). This is avaliable via the `--qemu-args` options. E.g.:

| QEMU options switch | Purpose | Accessing guest from host |
|---|---|---|
| `-tftp /path-to-your-home-directory` | Sets up a TFTP server to the specified directory | |
| `-redir tcp:10021:10.0.2.15:21` | Redirects port 10021 on the host to port 21 (ftp) in the guest | `host> ftp localhost 10021` |
| `-redir tcp:10023:10.0.2.15:23` | Redirects port 10023 on the host to port 23 (telnet) in the guest | `host> telnet localhost 10023` |
| `-redir tcp:10080:10.0.2.15:80` | Redirects port 10080 on the host to port 80 (http) in the guest | Type `http://localhost:10080` in the web broswer |
| `-redir tcp:10022:10.0.2.15:22` | Redirects port 10022 on the host to port 22 (ssh) in the guest | Run `ssh -P 10022 localhost` on the host to open a SSH session to the target |

## Serial Ports

By default, `petalinux-qemu-boot` searches for the `stdout` serial device in the DTS file and passes the `--serial mon:stdio` option to QEMU for this serial device. It uses `--serial /dev/null` for all other serial devices described in the DTS.

## Storage

By default, `petalinux-qemu-boot` does not use any backing files for any storage devices (e.g. Flash).

### SD Card

**IMPORTANT:** *This section only describes features avaliable in QEMU for Zynq.*

The following section describes how to attach a block device for non-volatile SD card storage in QEMU.

Ensure that the SD device tree node in the platforms DTS file is valid. The node should have the `compatible` property which contains `generic-sdhci`. See the example below.

```
ps7_sd_0: ps7-sdio@e0100000 {
        clock-frequency = <50000000>;
        compatible = "xlnx,ps7-sdio-1.00.a", "generic-sdhci";
        interrupt-parent = <&ps7_scugic_0>;
        interrupts = < 0 24 4 >;
        reg = < 0xe0100000 0x1000 >;
        xlnx,has-cd = <0x1>;
        xlnx,has-power = <0x0>;
        xlnx,has-wp = <0x1>;
        xlnx,sdio-clk-freq-hz = <0x2faf080>;
} ;
```

And then you can use the `-sd` QEMU option to tell the QEMU the SD card backing block device. E.g.

```
$ petalinux-qemu-boot --qemu-args "-sd <SD card backing block device>"
```

## USB

**IMPORTANT:** *This section only describes features avaliable in QEMU for Zynq. Also note that only USB Host mode is supported in QEMU.*

1. To access your USB device (e.g. USB Flash Drive) you will need to make sure the USB device tree node in the platforms DTS is valid. See the example below.

```
ps7_usb_0: ps7-usb@e0002000 {
        compatible = "xlnx,ps7-usb-1.00.a";
        dr_mode = "host";
        interrupt-parent = <&ps7_scugic_0>;
        interrupts = < 0 21 4 >;
        phy_type = "ulpi";
        reg = < 0xe0002000 0x1000 >;
        xlnx,usb-reset = "MIO 7";
} ;
```

2. Get the Vendor ID and the Product ID of the USB device using the `lsusb` command on the host.

3. Use `-usb -usbdevice host:<VendorID>:<ProductID>` QEMU option to enable QEMU USB host support and attach the specified device.

```
$ petalinux-qemu-boot --qemu-args "-usb -usbdevice host:<VENDORID>:<PRODUCTID>"
```

# Troubleshooting

This section describes some common issues you may experience when creating and testing user application, and ways to solve them.

| Problem/Error Message | Description and Solution |
|---|---|
| QEMU failed to get IP address. | ***Problem Description:***<br>This is most likely because your firewall blocking DHCP requests.<br><br>***Solution:***<br>use `ifconfig` to assign an IP belonging to the QEMU virtual subnet to the system on the QEMU console:<br><br>`# ifconfig eth0 <system IP>`<br><br>e.g., to use `192.168.10.3`:<br><br>`# ifconfig eth0 192.168.10.3`<br><br>Alternatively, contact your system administrator to allow DHCP request to your workstation. |
| (gdb) target remote W.X.Y.Z:9000<br>:9000: Connection refused. | ***Problem Description:***<br>GDB failed to attach the QEMU target. This is most likely because the port `9000` is not the one QEMU is using.<br><br>***Solution:***<br>1. Check your QEMU console to make sure QEMU is running.<br>2. Try port `9001` on the GDB console:<br>`(gdb) target remote :9001`<br><br>The PetaLinux always tries to use port `9000` for QEMU GDB. If the port has been used, it will increase the port number by 1 until it can get a free port. |

# QEMU Supported Xilinx IP Models

The QEMU simulator supports a limited number of Xilinx IP models.

- Zynq-7000 ARM Cortex-A9 CPU
- Zynq-7000 ARM Cortex-A9 MPCore
- MicroBlaze CPU (little-endian AXI)
- Xilinx Zynq Triple Timer Counter
- Xilinx Zynq DDR Memory Controller
- Xilinx Zynq DMA Controller
- Xilinx Zynq Static Memory Controller (NAND/NOR Flash)
- Xilinx Zynq SD/SDIO Peripheral Controller
- Xilinx Zynq Gigabit Ethernet Controller
- Xilinx Zynq USB Controller (Host support only)
- Xilinx Zynq UART Controller
- Xilinx Zynq SPI Controller
- Xilinx Zynq QSPI Controller
- Xilinx Zynq I2C Controller
- Xilinx AXI Timer and Interrupt controller peripherals
- Xilinx AXI External Memory Controller connected to parallel flash
- Xilinx AXI DMA Controller
- Xilinx AXI Ethernet
- Xilinx AXI Ethernet Lite
- Xilinx AXI UART 16650 and Lite
- Xilinx AXI SPI

By default, QEMU will disable any devices for which there is no model available. For this reason it is not possible to use QEMU to test your own customized IP Cores.

# Additional Resources

## References

- PetaLinux SDK Application Development Guide (UG981)
- PetaLinux SDK Board Bringup Guide (UG980)
- PetaLinux SDK Eclipse Plugin Guide (UG979)
- PetaLinux SDK Firmware Upgrade Guide (UG983)
- PetaLinux SDK Getting Started Guide (UG977)
- PetaLinux SDK Installation Guide (UG976)
- PetaLinux SDK QEMU System Simulation Guide (UG982)