# USRP Host Performance Tuning Tips and Tricks

## Contents

**AN-088**

This application note provides various tips and tricks for tuning your host computer for best performance when working with USRP devices.

Ensure your CPU governor is set to `performance`. This can be done with the Linux utility `cpufrequtils`.

Install `cpufrequtils` with the command below:

```
sudo apt install cpufrequtils
```

You can then set the CPU governor to `performance` per core by issuing the command:

```
sudo cpufreq-set -c $core_number -g performance
```

To set the CPU governor to `performance` for all cores:

```
for ((i=0;i<$(nproc --all);i++)); do sudo cpufreq-set -c $i -r -g performance; done
```

You can then verify that the CPU governor has been set by running the command:

```
cpufreq-info
```

When UHD spawns a new thread, it may try to boost the thread's scheduling priority. If setting the new priority fails, the UHD software prints a warning to the console, as shown below. This warning is harmless; it simply means that the thread will retain a normal or default scheduling priority.

```
UHD Warning:
    Unable to set the thread priority. Performance may be negatively affected.
    Please see the general application notes in the manual for instructions.
    EnvironmentError: OSError: error in pthread_setschedparam
```

To address this issue, non-privileged (non-root) users need to be given special permission to change the scheduling priority. This can be enabled by creating a group `usrp`, adding your user to it, and then appending the line `@usrp - rtprio 99` to the file `/etc/security/limits.conf`.

```
sudo groupadd usrp
sudo usermod -aG usrp $USER
```

Then add the line below to end of the file `/etc/security/limits.conf`:

```
@usrp - rtprio  99
```

You must log out and log back into the account for the settings to take effect. In most Linux distributions, a list of groups and group members can be found in the `/etc/group` file.

There is further documentation about this in the User Manual at the link below.

- Threading Notes section of the User Manual

This applies to USRP devices connected via Ethernet, such as the N200, N210, N300, N310, N320, N321, X300, X310, E320.

Note that these settings will not persist across a reboot.

```
sudo sysctl -w net.core.wmem_max=33554432
sudo sysctl -w net.core.rmem_max=33554432
sudo sysctl -w net.core.wmem_default=33554432
sudo sysctl -w net.core.rmem_default=33554432
```

This applies to Ethernet connected USRPs (N2xx, N3xx, X3xx, E320).

For 1 Gigabit connections, the MTU should be set to `1500`.

For 10 Gigabit connections, the MTU should be set to `9000`.

It is important to set the value and **not** leave it is `automatic`

This applies to Ethernet connected USRPs using a 10 Gb interface (X3xx, N3xx, E320).

Increasing the Ring Buffers on the NIC may help prevent flow control errors at higher rates.

```
sudo ethtool -G <interface> tx 4096 rx 4096
```

DPDK is supported on N3xx, X3xx and E320 USRPs. DPDK replaces the traditional Linux networking stack with a low overhead user-land based driver. Additional details of using DPDK can be found in the UHD Manual located at the following link: https://files.ettus.com/manual/page_dpdk.html

In some applications which require the highest possible CPU performance per core, disabling hyper-threading can provide roughly a 10% increase in core performance, at the cost of having fewer core threads. Hyper-threading is disabled within the BIOS and how to do this varies by motherboard manufacturer. With other techniques listed here, disabling hyper-threading should only be done as a last resort to eek absolute maximum performance from the CPU.

In some cases, disabling the KPTI protections for the Linux Kernel can increase performance by 10-15%. It is important to note the ramification making this modification can have. This modification is only recommended for systems that absolutely require the best performance and are not connected to the internet.

- https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)
- https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)

Disabling KPTI protections can be done by adding the lines below to your `/etc/default/grub` file at `GRUB_CMDLINE_LINUX_DEFAULT=""`

```
pti=off spectre_v2=off l1tf=off nospec_store_bypass_disable no_stf_barrier
```

After modifying the `grub` file, run the following command to update your configuration and reboot:

```
sudo update-grub
```