

Embedding it better...



μTasker Document

- **Kirin3 M5225X Tutorial – Ethernet and the Simulator**

Table of Contents

1. Introduction.....	3
2. Getting Started	4
3. Testing on the Target.....	13
4. Compiling the Project for the Target.....	13
4.1. Compiling with GCC	15
5. Downloading the Code to the Target.....	16
6. Watchdog and Debugging	18
7. Specific Notes concerning the M5225X.....	19
8. A Tour through the Demo Web Server	20
8.1. Menu	20
8.2. LAN configuration	22
8.3. Serial Configuration	24
8.4. Statistics	25
8.5. I/O Page.....	26
8.6. Administration Side.....	26
8.7. Email Configuration Side	28
8.8. Dynamic Content Generation Side	29
9. Developing – Testing - Debugging	30
10. Off-Line Simulation.....	37
11. Conclusion.....	39

1. Introduction

µTasker is an operating system designed especially for embedded applications where a tight control over resources is desired along with a high level of user comfort to produce efficient and modular code.

The operating system is integrated with TCP/IP stack and important embedded Internet services alongside device drivers and system-specific project resources.

µTasker and its environment are essentially not hardware specific and can thus be moved between processor platforms with great ease and efficiency.

However the µTasker project setups are very hardware specific since they offer an optimal pre-defined (or a choice of pre-defined) configurations, taking it out of the league of “board support packages (BSP)” to a complete “project support package (PSP)”, a feature enabling projects to be greatly accelerated.

This tutorial will give you a flying start to using the µTasker on the COLDFIRE M5225X. It can be fully simulated using VisualStudio 6.0 or higher and can be run on the Freescale™ M52259EVB or M52259DEMO hardware, in which case the Codewarrior compiler and IDE with background debugger is assumed. Building the project using GCC is included as an optional post-build step when working in VisualStudio, but debugging with the GNU tool chain is not discussed. Both M52259DEMO and M52259EVB come with inbuilt background debuggers and are a cheap way to make acquaintance with this device. It is delivered with a special code limited version of the compiler, but this is adequate for the following tutorial and more besides!

Therefore there should be nothing standing in your way to getting your first, powerful embedded IP project up and running.

2. Getting Started

You are probably itching to see something in action and so why hang around. Let's start with something that will already impress you and your friends – no simple and basically useless demo which blinks an LED in a forever loop but something seriously professional and for real life projects very handy.

First I will assume that you have VisualStudio installed on your PC since we will first simulate everything – but don't worry, we are not going to see something attempting to interpret the instructions of the processor and requiring 2 minutes to simulate a couple of seconds of the application, instead we will see your PC operating in "real time" as the target processor. Your PC will not realise that the processor is simulated and so when you try contacting it by pinging it or browsing to it with your web browser, we will see that your PC will send IP frames to the network and will see answers on the network from the simulated device. Other PCs or IP enabled embedded devices on the network will also be able to communicate with the simulated device. You can also capture the frames using a sniffer tool (we will use Wireshark) for further analysis and playback.... Getting excited? In a few minutes you will see it in action!

If you haven't VisualStudio (6.0 or newer) then there are trial versions and the free Express version [<http://msdn.microsoft.com/vstudio/products/trial/or> <http://www.microsoft.com/express/>] and you can probably pick up a 6.0 version for very little cash on Ebay. VS 6.0 is adequate for our work as are the Express editions. It contains a world class C-compiler and editor as well as loads of other tools which make it a must, even for embedded work.

The simulator requires also WinPCap to be installed (from <http://www.winpcap.org>) which is an industry-standard tool for link-layer network access in Windows environments. It is also used by the network sniffer Wireshark, which every Ethernet designed really should have. Therefore it is simplest to install Wireshark since this includes WinPCap, saving a step, and making for simplest installation. Wireshark can be downloaded from <http://www.wireshark.org/> and is discussed towards the end of the document.

If you don't want to see the simulator in action – **which would be a big mistake as you will miss the opportunity to save many hours of your own project time later** – there is target code which can be loaded to the boards and will also run, as well as a software demo pack for the boards: <http://www.utasker.com/software/software.html>. A guide to loading these can be found at http://www.utasker.com/docs/M5223X/uTaskerV1.3_Kirin3_demo.PDF

You will find that the simulator is useful for most real embedded work. First, it allows testing things which you may not already have available as hardware (even if you have no evaluation board and cross compiler for it yet, you can start writing and testing your code) – it will allow you to use a matrix keyboard, LCD, I²C EEPROM or SPI FLASH (and more) connected to the virtual target without having to get your soldering iron out to connect it. And it is so accurate that you can then cross compile to the target and it will (almost certainly) work there as well. This is the last time I will say it ... ***don't make the BIG MISTAKE of taking a short cut when starting and diving into coding on the target.*** If you are an embedded SW professional you will be missing the chance of saving enough time in a year for a couple of months extra vacation. If you are a hobby user, you will be missing the change to get out more...!

So now I've said it and you have heard - so

...fasten your seat belts since we are about to roll

1. Simply copy the complete µTasker folder to your PC and go to `uTaskerV1.3\Applications\uTaskerV1.3`. This is a ready to run project directory showing a useful application using network resources (and more).
2. Move to the sub director `Simulator` and open the VisualStudio project workspace `uTaskerV1-3.dsw`. This project is in the VisualStudio 6.0 format to ensure compatibility and, if you have a higher version, simply say that it should be converted to the new format – no problems are involved and it should build with no warnings.
3. *Ensure that the compiler is set up for the M5223X target in the project's pre-compiler settings: look for the pre-processor define **_M5223X**. If instead you find that the project is set up for another target, eg. `_HW_NE64` or `_HW_SAM7X` simply overwrite this with **_M5223X**.*
4. Ensure that the project is configured for your target board in `config.h`: the define `_M5225X` should be set to select the M5225X family and then enable either `M52259EVb` if you are using the EVb, or else `M52259DEMO` for the demo board.

Build the project (use F7 as short cut) and you should find that everything compiles and links without any warnings.

5. I would love to be able to say “Execute” but there are a couple of things which have to be checked before we can do this. First of all, you will need to be connected to a network, meaning that your PC must have a LAN cable inserted and the LAN must be operational – either connected to another PC using a crossover cable or to a router or hub (wireless links tend not to work well but this may improve as the WinPCap capabilities get better with newer version).

Then we have to be sure that the network settings allow your PC to speak with the simulated device. The IP address must be within the local subnet:

Open the C-file `application.c` in the `uTaskerV1.3` project directory and check that the following default settings match your network settings (check what your PC uses in a DOS window with “`ipconfig`”)

```
static const NETWORK_PARAMETERS network_default = {
    (AUTO_NEGOTIATE | FULL_DUPLEX | RX_FLOW_CONTROL), // usNetworkOptions - see
                                                         driver.h for other possibilities
    {0x00, 0x00, 0x00, 0x00, 0x00, 0x00}, // ucOurMAC - our default MAC
    { 192, 168, 0, 3 }, // ucOurIP - our default IP address
    { 255, 255, 254, 0 }, // ucNetMask - our default network mask
    { 192, 168, 0, 1 } // ucDefGW - our default gateway
};
```

Just make sure that the network mask matches, that the device's IP address is within the local network and that the IP address defined doesn't collide with another one on the local network.

After making any modifications, simply compile the changes and we will be in business.

6. So now I can say EXECUTE (use F5 as short cut).

You will see the simulated device working away on your PC screen. There will also be one port output toggling away. Let's take a quick look at it. This is in fact the watchdog routine which is called every 200ms which is also toggling the output so that we can see that all is well (TC[0]).

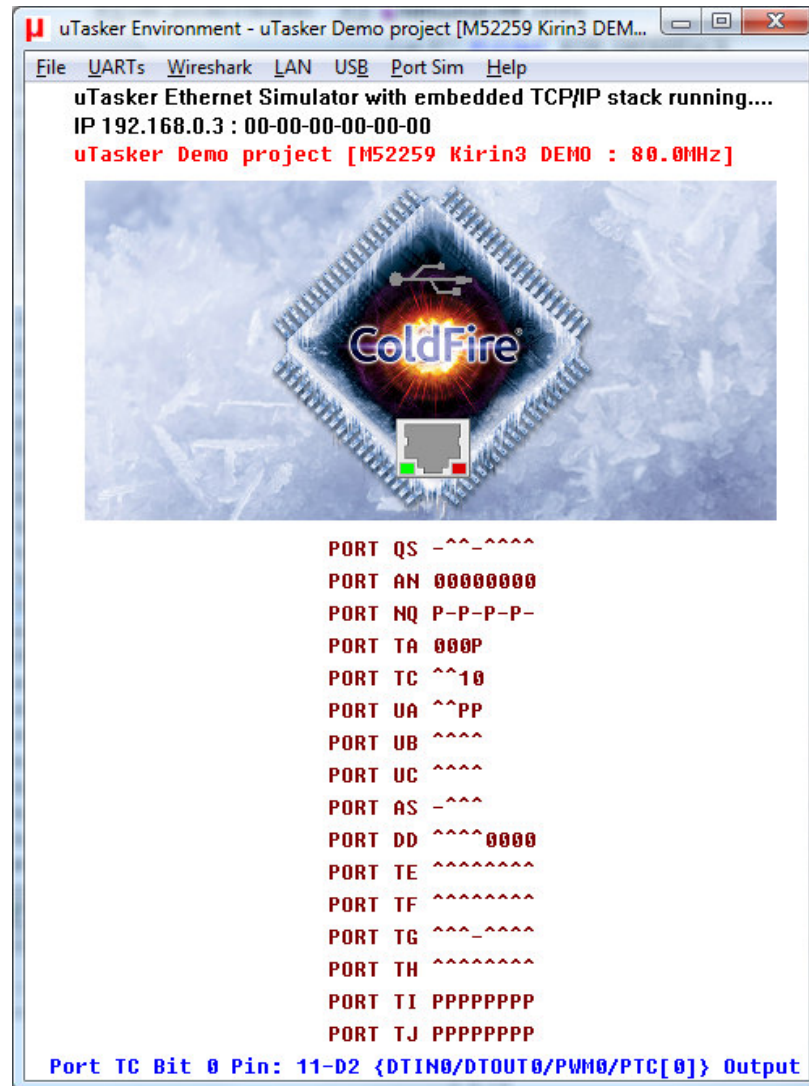


Figure 1. μTasker simulator running a M52259DEMO board

If you hover your mouse over the port which is toggling, or other available ones, you will see which pin number it has on the device, its name and present use as well as the possible peripheral functions which it can be programmed to perform. In the screen above this is seen by the line in blue at the bottom of the simulation window.

Open the file `uTasker\watchdog.c` (in the VisualStudio project manager). Put your cursor on the call to retrigger the watchdog "`fnRetriggerWatchdog()`" and hit the F9 key (set a break point). Almost immediately the program will halt and you can use F11 to step into the hardware specific routine responsible for triggering the watchdog and, in our case, also toggling the port output. The routine writes to the corresponding

device registers and returns. Remove the breakpoint and let the simulated device run again using F5.

7. OK. So at least you are convinced that it is really running our project code, but it is not exactly something to write home about.

Let's get down to more serious stuff:

There are some menu items in the µTasker environment simulation window. Open "LAN | Select working NIC" and select the network card you would like the simulator to use – don't worry, it will be shared with anything else which is already using it.

Open a DOS window and do the standard PING test - "ping 192.168.0.3" if you didn't need to change anything, or the IP address you defined if you did.

The simulated device should now be responding. That means that your PC has sent PING test messages to the network and received answers from some network device (or course our internal simulated device – but no one will know the difference).

You can also try sending the ping test from another PC on the network and it will also receive an answer.

If you have a network sniffer you can also record the data from the network – don't worry if you haven't used a network sniffer before because we will come back to this later on and use Wireshark to do the job.

Watch the LAN indicators on the processor's virtual LAN connector. The left one will blink green when a frame is received – if it is accepted by the device (matching address, broadcast or all when in promiscuous mode). The right one will blink red whenever the simulated device sends a frame to the network.

8. I suggest that you now close the µTasker environment simulation window using the 'normal' method `File | Exit` or by clicking on the close cross in the top right hand corner.

This standard termination will cause the selected NIC to be saved to a file in the project simulation directory called **NIC.ini** and so you will not have to configure it the next time you start the µTasker environment simulation.

9. Now I'm sure you are not yet satisfied with the progress, so let's execute the project again (short cut F5) and this time we will do something a bit more interesting. Start your web browser (Internet Explorer, Firefox, Chrome, etc.) and establish a connection with the simulated target: In the URL line type in <http://192.168.0.3> (assuming its address has not been changed) and hit the ENTER key. The web browser will request the start page on the web server, which will return the following page the first time used:

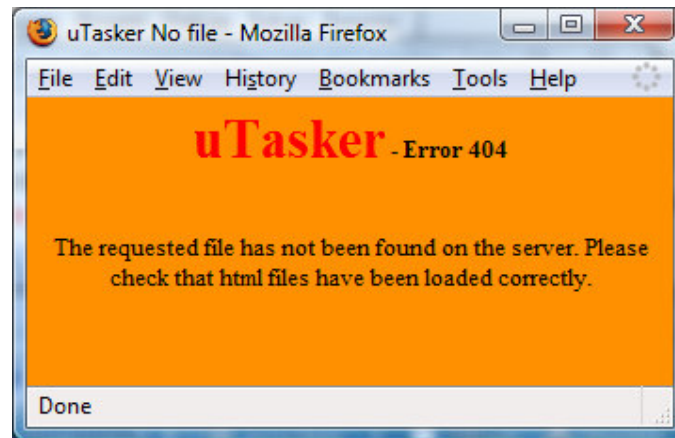


Figure 2. µTasker web server displaying that it has no web pages loaded

This is displaying that the page has not been found on the server, which is simply due to the fact that we haven't loaded any web pages to it yet, so we will do this as next step.

10. Take a look in the project directory
`uTaskerV1.3\Applications\uTaskerV1.3\WebPages\WebPagesM5225X`
and you will find the web pages prepared for the demo project. These are HTM, JPG and GIF files. It is possible to load these pages using FTP clients but these tend to work quite differently from another and require various setups before they work smoothly. See the following document for more information on this subject:
<http://www.utasker.com/docs/uTasker/uTaskerFTP.PDF>

This is the reason that working with simple DOS FTP tends to be the fastest and simplest method and the bat file `Copy_all.bat` even does all the work for you. Check that its content is set to use the correct IP address and then double-click the file to start the transfer of all of the web pages to the simulated target device. The transfer takes just a few seconds.

Then go back to the web browser window and make a refresh. Now you will see the start side and can navigate to a number of other pages.

Before we get into any more details about the web pages and their uses, please modify and save the Device ID (on the start page – default "KIRIN3") to any name of your choice and close the µTasker environment simulation window by using the normal exit method.

By doing this, the contents of the device's simulated FLASH (Flash is used to save the web pages in the file system and also any parameters, for example the device ID which you have modified) are saved to a file in the project simulation directory called **FLASH_M5223X.ini**. [The name is correct – all Coldfire FLASH files have the same name, irrespective of whether M52259, M52211, M52235 or other Coldfire processor is actually being used]

Now execute again (F5) and check that the loaded web pages are all there and that after a refresh of the start side also the device ID which you chose is correct.

Now you should understand the operation of the simulator; *on a normal exit it saves all present values and settings and on the next start the device has the saved FLASH contents as at the last program exit.* This is exactly how the real device works since, after a reset, its FLASH contents are as saved – I mean, that is what FLASH is all about.

If however you have modified FLASH contents and do not want them to be saved, you can always avoid this by quitting the debugger (short cut SHIFT F5) which causes the simulator to be stopped without performing the normal save process.

If you wish to start with a fresh device (with blank FLASH contents) then simply delete the **FLASH_M5223X.ini** file from the simulator directory...

11. There is one important setting which we should perform before continuing; that is to set a MAC address to our new device.

So browse to the “*LAN configuration side*”, where you will see that the default MAC address is 00-00-00-00-00-00. This works, but we really should set a new one – as long as we are not directly connected to the Internet any non-used value can be set. You make one up. For example set 00-11-22-33-44-55 (watch that the entry format is correct and always start with 00!) and then click on “modify / validate settings”. The entry field will be set inactive since it is no longer zero and cannot be changed a second time (should you want to reset the value before we commit it to (simulated) FLASH click on “Reset changes”, otherwise click on “Save changes”).

The device is commanded to be reset at this point after a short delay of about 2 seconds to allow it to complete the web page serving. The simulator will open a dialog box to indicate that it has been terminated with a reset:

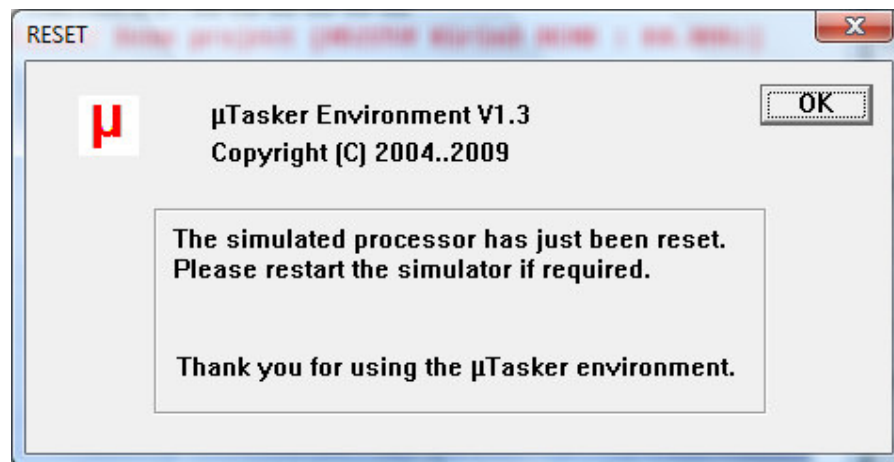


Figure 3. µTasker simulator indicating that the processor has just been reset

You can restart the simulator after the reset (which was interpreted as a normal program exit and so the changes to the FLASH have also be saved to the hard disk and will be restored on the next program start) by using F5 as normal.

12. You may have read on the LAN configuration side that the new setting should be validated within 3 minutes – this is a safety mechanism so that falsely set critical values do not leave a remote device unreachable and means that we should establish a connection within three minutes of the new start to verify that all is well, otherwise the device will automatically delete the newly set values, reload the original ones and can then be contacted as before, using the original settings. So we will now validate our new setting (new MAC) so that it will always be used in the future.

Refresh the web pages by clicking first on “*Go back to menu page*” and then “*Configure LAN Interface*” again.

You may well have a shock because it doesn't respond....but don't get worried because your PC is still trying to reach the IP address using the previous MAC address, which is no longer valid (hence an incorrectly configured device can become unreachable). In a DOS windows type in “arp -d” which will delete the PC's ARP table – which is mapping IP address to MAC addresses and then it will work on the second attempt. Vista PCs may not always accept this command so wait a couple of minutes before starting the simulator again, until its ARP table automatically times out.

The page will not allow any parameters to be modified and also the check box “*Settings validated*” shows that the device is waiting for the new values to be validated. To perform this, click on “*Modify / validate settings*”, after which the parameters will be displayed as validated. (*Don't forget to terminate the simulator normally later so that it is really the case*).

Should the 3 minutes have elapsed before you managed all that, the simulated device will again reset, clearing the temporary settings and reverting back to the initial MAC address. Just start the simulator again and repeat this step.

13. Now you may be thinking that it is all well and good having a web server running on a device, sitting somewhere on the Internet but you probably want to use the device for controlling something - in its simplest form by switching something on or off. Using a relay this could be something quite powerful which can also have really useful benefits; imagine browsing to your device and commanding it to open the blinds or turn on the lawn sprinkler...the list of possibilities is almost endless...
Look at the simulated M5225X and imagine that you have connected your lawn sprinkler to the output Port TC2. Presently it is at the state input '1' [signified by '^'], the default state when the software starts since there is a pull-up in the device. Now click on the link menu page to open an I/O window – it is shown in the following screen shot. Notice that the port TC2 is being displayed as an input and its digital value as active ('1') in its check box.

Do a quick test: Hover your mouse over the port TC bit 2 in the simulator – it will tell you which pin it is on your device. Now click – this has toggled the simulated input (each time you click, it will change state again) – leave it at the low state '0', displayed as 'v'. Now refresh the I/O web page by clicking in the Refresh button.

What is the web page now displaying? If it is behaving correctly it will of course be displaying the new port input state.

Now we can configure it as an output and control its state from the I/O page. See next page.

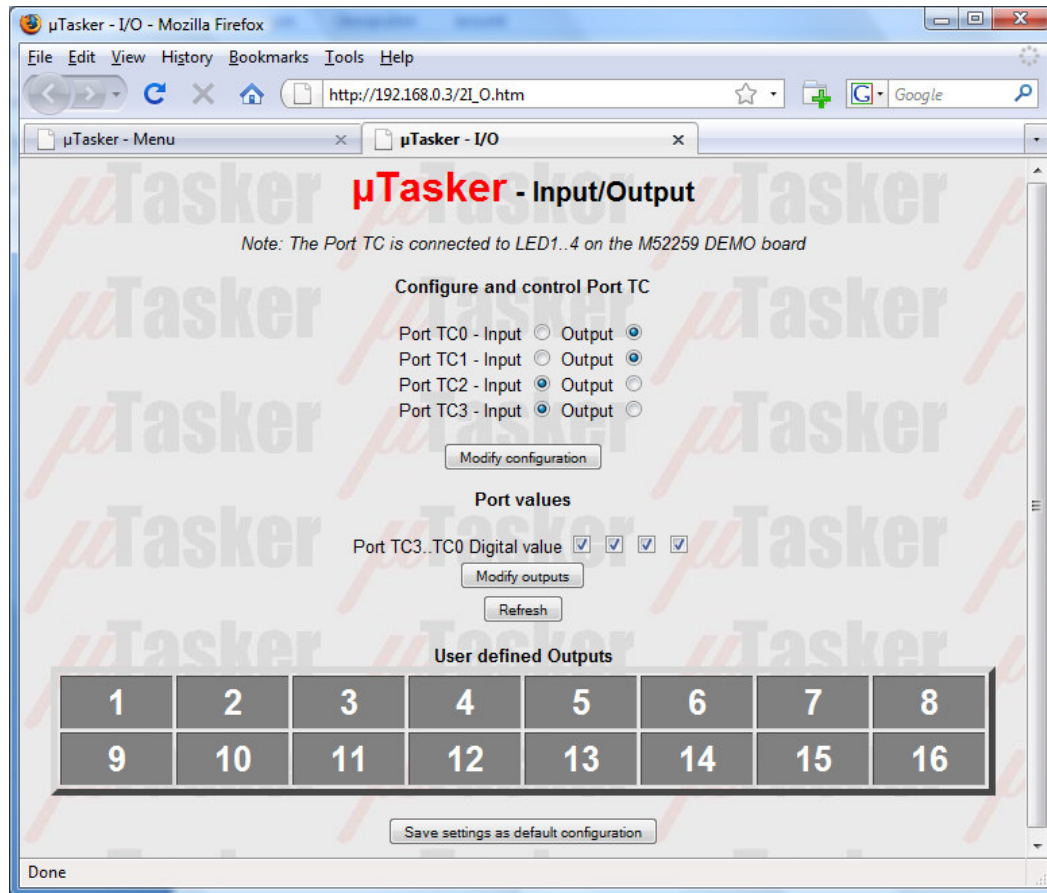


Figure 4. µTasker web server showing the I/O control page

Set TC2 to be an output, rather than an input and click on “*Modify configuration*”. Afterwards set the port state to ‘1’ by setting the third port value from the right and click on “*Modify outputs*”.

Watch the state of Port TC2 on the simulated device – you will see that the output is now set and now your lawn would get the water it has been waiting for!

Set the state to ‘0’ and it will be turned off. In this example web page, all of the 4 Port TC0..TC3 outputs can be controlled individually.

TC0 is used as a RUN LED in the demo project and so is configured as an output by default, as is TC1.

If you would like a certain setting to be returned after every reset of the device, simply save the setting by clicking on “*Save settings as default configuration*” and you will see that they are indeed set automatically when the device is started the next time.

The demo project includes also 16 user controllable outputs. These are automatically configured as outputs in the project code and can be seen as outputs with state ‘0’ when looking at the simulator – see the ports AN, TA and TD. If you now click on the user defined outputs on the I/O page you will see that they immediately toggle their port output and the state is either displayed as a grey button when ‘0’ or as red buttons when ‘1’. Also the present state of the 16 outputs can be saved as default states when the target starts the next time.

Note that these outputs can be mapped to any port and port bit in the demo project – it shows a useful example of flexible independent output control.

14. The last setting which we will change before taking a look at the project on the target hardware is to activate HTTP user authentication and disable the FTP server so that no one else without our password has entry to the web server and no sneaky person can change the web pages which we have just programmed...

Browse to the administration page, deactivate FTP and activate HTTP server authentication before selecting the action to “*Modify and save server settings*”. Finally click on “*Perform desired action*” and close your web browser..

Open the web browser again and enter the device’s address <http://192.168.0.3> (or your address) and this time you will need to enter the user name “ADMIN” and password “uTasker” to get in.

Try to do something with the FTP server (like transfer the file with *Copy_all.bat* or delete the file system contents with *delete_all.bat*) and you will find that it simply won’t work anymore. This is because it is no longer running in the simulated device and you can rest assured that no one out there will be able to change anything which you have loaded.

You probably noticed a button at the bottom of the administration page which allows a file to be searched for and uploaded to the target as a new software version. This is an example of using the HTTP POST method to transfer data to the embedded device. The µTasker project for the M5225X supports the upload of complete new software using this method (as well as by FTP and even USB), which is a very powerful feature!! We will test this later on the target and you will see that you will then be able to develop code for a real target on the internet, including uploading it from anywhere where you have web access to it!

I hope that the introduction has shown that we are dealing with something which is very simple to use but is also very powerful in features. There are lots of details which need to be learned to understand and use everything to its fullest capabilities and it is up to you to decide whether you want this or would like to simply use the µTasker and its capabilities as a platform for your own application development. In any case you have just learned the basics of a powerful tool which is not only great fun but can really save you lots of development time.

3. Testing on the Target

Up until now we have been using the simulator and hopefully you will agree too that it is a very useful tool. We have tested some quite useful code designed to run on the M5225X and done this in an environment enabling us to do embedded IP stuff in real time. We haven't actually done any debugging or added new code but you can probably already imagine the advantages of being able to write and test it on the PC before moving to the target.

At the same time you are probably thinking about how that will all work on the real device. Perhaps you are worried that it is all a show after all and the real device will remain as dead as a door nail or at the best crash every time the user breaths heavily. So let's prove that this is not the case by repeating the first part of the tutorial, but this time we will go live...

We will use the Freescale™ M52259EVB or the M52259DEMO (both will operate equivalently).

4. Compiling the Project for the Target

The first thing that we need to do is to compile the project for the target. This means that we will be cross compiling the code which we already have been testing with the simulator, using an assembler, a C-compiler and a linker. There are a number of such tools available and unfortunately they are not all compatible in every aspect, even if ANSI compatible. Basically there is always the chore of getting the thing to reset from the reset vector, meaning that the start-up code must be available and at the correct location. Then there are specialities concerning how we force certain code or variables to certain addresses or regions and how we need to define interrupt routines so that they are handled correctly. Sometimes there is also need for some special assembler code which does such things as setting the stack pointer or enabling and disabling interrupts.

The µTasker demo project for the M5225X is delivered with a Codewarrior project and also a make file for compiling with the GNU compiler. The Codewarrior compiler is a very good compiler, producing efficient code so is recommended for professional work. The evaluation boards are delivered with the Special edition of Codewarrior which is adequate for the full µTasker demo plus a substantial user application.

By the way, if you can't wait until you have installed the compiler or got your own project up and running, there is a file delivered with the µTasker which was compiled with the Codewarrior compiler and can be downloaded already...

Check out the following document for a high-level guide to testing the demo software on the board: http://www.utasker.com/docs/M5223X/uTaskerV1.3_Kirin3_demo.PDF

You can find the Codewarrior project file and the target file(s) in the sub-directory called `CodeWarrior_M5223X`:

`uTaskerV1.3_CW7.mcp` This is the Codewarrior V7.1.1 project work space. Codewarrior V7.1.1 or higher should be used with the M5225X

`bin\uTasker_full.elf.S19` This is the file which you can download to the target using either Codewarrior or CF-Flasher

`bin\uTasker_BM.elf.S19` This is a special version which requires the „Bare-Minimum“ boot-loader to first be installed, so we won't use it just yet.

`bin\H_Upload.bin` This is a binary version of the previous file, including a special header with check sum and coded key [generated by using the bat file `BM-Convert.bat` in the same directory]. This is the file which can be uploaded to the board via a standard web browser (as long as the board is prepared to receive it).
But more about all this later. We don't want to get ahead of ourselves!

Using Codewarrior you can open the µTasker project and compile the target **M5225X_ROM** (this is suitable for both the demo board and the evaluation board).

Note that the M52259 has 64k of RAM and so the size of code running there is quite limited. For this reason it is preferred to load to and debug from FLASH, since the amount of actual target debugging which we will need to do is very limited. That is what the µTasker simulator is all about, keeping the bulk of development work on the PC where it is much more efficient to perform.

Note that, even though 64k SRAM is available in the chip we are using in fact we will only use 32k of it for the demo. This means that the project will in fact even operate on the smallest M5225X chip.

There should be no warnings when compiling the project and afterwards the code can be loaded to the board as explained in the next sections – either from within Codewarrior using the Flash Programmer tool, or using CF Flasher.

4.1. Compiling with GCC

The project is delivered with a bat file and make file so that the project can be simply compiled with the GNU compiler. It is recommended to use the Codesourcery g++ build, which is available as a free Lite edition at <http://www.codesourcery.com/>

Compiling with GCC is also greatly simplified when working from VisualStudio by adding the step as a post build step to the normal simulator compile process. When the target Win32 uTasker M5223X plus GNU build is selected as active configuration the process will be executed as follows:

- The GCC directory GNU_Coldfire contains the bat file Build_M5223X.bat. This directory will be selected as working directory
- The bat file will be executed and starts the GCC make file make_uTaskerV1.3_GNU_M5223X. The bat file also contains a path to the GCC binaries on the local PC – *if no path variables have been configured when the GCC compiler was installed this path can be set manually to enable the make utility, compiler and linker to be found.*
- As additional steps the process creates files suitable for use with the boot loader and even generates a file containing boot loader and application for simple downloading to the target.

The following target files are generated during the GCC build step:

- uTaskerV1.3.s19: this is a stand-alone target which doesn't contain the boot loader
- uTaskerV1.3_BM.s19: this is a target containing boot loader and application.
- H_Upload.bin: this is a target which can be uploaded (eg. via HTTP POST) containing just the new application.

The GCC build is displayed in the log windows of VisualStudio and warnings or errors are counted by the VisualStudio compiler during the process.

5. Downloading the Code to the Target

The evaluation and demo boards include in-build BDM debuggers.

The M52259DEMO board contains an integrated background debugger (OSBDM), used for programming and testing, which is supported by CodeWarrior 7.1 with 7.1.1 patch. This software is delivered on the CD in the M52259DEMO board pack and should be installed before continuing (first the CW7.1, followed by the patch).

The M52259EVB has a connector for an external Background Debug Module (BDM) as well as an integrated P&E Micro BDM module.

Before downloading code to the target using Codewarrior V7.1 the correct BDM should be configured. In the target configuration setting ensure that the debugger setting suits the board used:

- When using the M52259DEMO board the “Connection” setting must be selected for `Coldfire v2-v4 JM60 OSBDM`
- When using the M52259EVB the “Connection” setting must be selected for `PEMICRO_USB`

Downloading can be performed within the Coldwarrior V7.1 environment by following these steps:

- Step 1: Compile the ROM project.
- Step 2: Connect the target board and your PC according to the manufacturer’s instructions.
- Step 3: Power on the evaluation board – its power LED should light (the demo board is powered via USB).
- Step 4: In the tools menu start the FLASH programmer.
- Step 5: Load settings – there is preconfigured files in the Codewarrior program directory called `MCF52259_INTFLASH.xml` which is suitable for both DEMO and EVB boards. This will prepare everything for the next steps.
- Step 6: First delete the FLASH contents using “Erase / Blank Check”. The first time you use this and in the case that you want to reset everything, you can delete all sectors which are available, which is the default erase setting. If you want to delete the demo program without also deleting any loaded web pages and other parameter settings, select the sectors up to 0x20fff. This will leave the file system block, starting at 0x21000 intact.

Alternatively if you should want to delete the contents of the file system and reset FLASH parameters then all sectors from 0x21000 can be deleted...

- Step 7: Program / Verify. Here the actual code download is performed. If the file is already entered, the download can be started simply by pressing “Program” button. If a different file is to be programmed then this should first be prepared by enabling “Use Selected File” and setting the path.

At the time of writing the CF Flasher doesn't support the M5225X nor the OSBDM. If the loader is updated in the future the following guide should be valid:

- Step 1: Connect the BDM between the target board and your PC according to the manufacturer's instructions.
- Step 2: Power on the evaluation board – its power LED should light (the demo board is powered via USB).
- Step 3: Start the CF Flasher and set the target configuration to M52259DEMO or M52259EVB and select the BDM you are using in "BDM Communication". Click on OK.
- Step 4: Select "Erase".
The first time you use this and in the case that you want to reset everything, you can delete all sectors which are available, which is the default erase setting – "Erase entire FLASH". If you want to delete the demo program without also deleting any loaded web pages and other parameter settings, select "Erase from sector 0..x". This will leave the file system block, starting at 0x21000 intact.

Alternatively if you should want to delete the contents of the file system and reset FLASH parameters then all sectors from 0x21000 can be deleted...in this case select "Erase from sector x..y".

- Step 5: Now program by clicking on "Program" and select the file to be loaded, which will be `uTasker_full.elf` in the demo project (assuming the Codewarrior target is used). Start the programming, whereby you can also check the verify box so that the loaded program is also automatically checked for accuracy. Since the download doesn't take long I tend to verify to be absolutely sure...

You should be done within a few minutes....

Now you can either click on the Debug button in Codewarrior 7.1 (the little green bug on the green arrow) or just press the reset button on the board so that it starts working (*this may not work with the M52259DEMO since due to the OSBDM debugger – it can however be powered via the processor's USB interface to enable stand-alone operation*).

Make sure that the board is connected to the network and give it a test run.

Are you surprised that it behaves the same as the simulator? You shouldn't really be because that is exactly what the simulator is all about. It allows you to test your real code in real time and, once it is working as you want it to, you can simply transfer it to the real target. In fact you will find that your real target is not really necessary for most of your development work. Develop on the simulator and ship on the target – that is the way to do things really efficiently.

Note that the I/O page allows the LEDs and port lines on the I/O port connector on the M52259EVB or the M52259DEMO board to be controlled and the state of these to be displayed. Two LEDs are set as outputs by default. If TC0 is reconfigured to be an input, the blinking LED will no longer light.

6. Watchdog and Debugging

Before you get down to detailed work and debugging on the target there is one important topic which must be explained. It concerns the watchdog.

The watchdog is a hardware timer which is used to monitor the correct operation of the processor. It has the capability that it, when activated, can detect a serious program error (unintentional forever loop or some other unrecoverable condition) and reset the processor so that it restarts and clears this otherwise serious fault state.

The watchdog timer is configured in the µTasker demo project and is normally active and will cause a reset if it is not actively retriggered within a period of 2 seconds. Whether it actually runs and its exact characteristics can in fact be set up in the file `app_hw_m5223x.h`.

Here is the code which is responsible for its configuration. It can be found in `M5223X.c`:

```
INIT_WATCHDOG_LED(); // allow user configuration of a blink LED
INIT_WATCHDOG_DISABLE();
if (!WATCHDOG_DISABLE()) {
    #if defined BACKUP_WATCHDOG_TIMER // {78} the BWT is used in preference to core watchdog
        CONFIGURE_BACKUP_WATCHDOG();
    #else
        CWCR = CONFIGURE_WATCHDOG; // allow user configuration of internal watch dog timer
    #endif
} else {
    CWCR = WATCHDOG_DISABLED;
}
```

The actual code which is inserted here is defined in the project specific set-up file `app_hw_m5223x.h`. The following is an extract from the M52259DEMO configuration, which is however not identical to the M52259EVb configuration in every aspect.

```
#define INIT_WATCHDOG_LED() DDRTC |= PORT_TC_BIT0
```

This is configuring the BLINK-LED, which is toggled by the watchdog task each time it retriggers the watchdog. It can be set to a different port output or completely removed by deleting the defined code to the right of `INIT_WATCHDOG_LED()`.

```
(PNQPAR &= ~(ALT_2_FUNCTION_Q << BIT_1_Q_SHIFT)) // ensure IRQ1 is an input (SW2 on demo board)
```

This configures the IRQ1 pin as an input and

```
#define WATCHDOG_DISABLE() !((PORTIN_SETNQ & PORT_NQ_BIT1)) // pull this input down to disable watchdog
```

reads the state of the IRQ1 pin to determine whether the watchdog should be activated or disabled.

When the watchdog is enabled, the code is a little more complicated – if you search for the `define CONFIGURE_BACKUP_WATCHDOG()` you will see what I mean... It enables and configures the Backup Watchdog Timer (BWT).

What should however be clear here is that the watchdog is normally configured but can be modified, or completely removed, in a certain application and can also be disabled by applying a '0' to the IRQ1 input at start-up. *The IRQ1 pin is connected to the push button SW2 on the M52259DEMOboard and this can be held down when powering up the board to effectively disable the watchdog operation.*

The BWT is used in preference to the Core Watchdog timer since its operation is more reliable. It doesn't rely on an interrupt to command a reset of the hardware if the watchdog fires. Once started, it also retains its mode of operation over a software reset.

The important point for debugging comes now.... when working with the BDM the watchdog timer should always be disabled. If the watchdog timer is not disabled it will fire as soon as the code runs into a break point when you want to debug something and will immediately cause the debugging session to fail. That is the main reason why you will probably want to disable it occasionally using the input trick.

Of course it should be clear that you can completely disable it in your project, although this is not normally advisable due to its important function.

Finally there is a third technique which can also be used quite easily which I will describe here for completeness.

1. Set a break point on the code in `M5223X.c`
`if (!WATCHDOG_DISABLE()) {`
2. Start the debugger running.
3. The code will immediately break at the above line. At the moment the watchdog is not running so it doesn't cause a difficulty.
4. Position the cursor at the line after
`CONFIGURE_BACKUP_WATCHDOG();`
5. Right click and choose the debugger command "Set program counter". This will move the program execution to this line which will not enable the watchdog.
6. Let the code continue to run as normal and then afterwards any code debugging will operate without watchdog interference.

Note that (due to the operation of the BWT) it is necessary to power off the board to stop it from operating if it were to be started once.

7. Specific Notes concerning the M5225X

The M5225X devices do not suffer from the "Internal FLASH Speculation Address Qualification" errata as the M5223x family. For this reason the workaround (see errata sheet MCF52235DE, Rev. 1 11/2006) is removed when building for this target.

The M5225X devices do not have an internal EPHY and so do not suffer from the auto-negotiation errata.

The complete M52259 demo project (HTTP, FTP, TELNET, UART, USB etc.) requires about 87k of FLASH for code. Although the M52259 has 64k internal SRAM the demo project is configured to utilise only 32k of this. This means that the demo project will operate correctly on any of the M5225X devices, the smallest being the M52252 and M52256, with 256k internal FLASH and 32k internal SRAM.

8. A Tour through the Demo Web Server

Now that you have the possibility to simulate the demo and also run it on the target hardware it is time to take a more detailed look at what it does and then how it all works. The demo is designed to give you a practical platform to use as a basis for your own developments so it would be good to know how it can be best modified to suite your own needs.

8.1. Menu

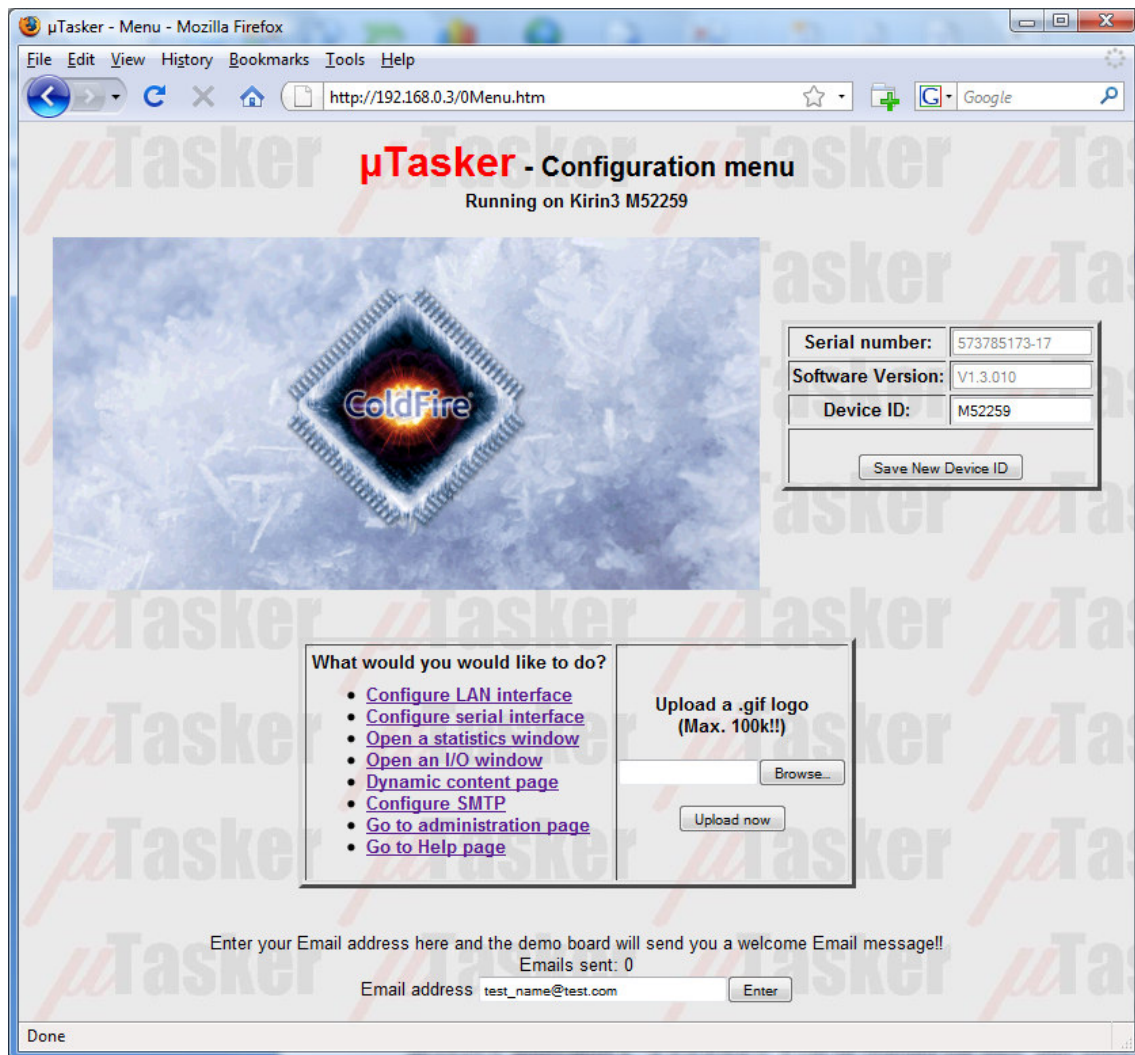


Figure 5. µTasker web server showing the menu page

Serial number – this is a decimal representation of the MAC address programmed in the device. Since the MAC address is normally unique it can serve also as a serial number if required. Notice that the serial number is displayed in grey and cannot be modified (disabled).

Software version – this is a string which is defined in `application.h`. It is also disabled so that it cannot be modified via the web side.

Device ID – this is a string defined in the `cParameters` structure in `application.c`. The default value can be set in code and also modified via the web page. When ‘*Save new device ID*’ is clicked, the new value is also saved to a parameter block in the internal flash so that it remains valid after the next reset or power up.

Menu – There are links to several other web pages allowing specific configurations to be displayed and modified.

Email address – If you have configured the demo project to support SMTP (`#define USE_SMTP` in `config.h`) then it is possible to enter an email address and send a test email to it. This entry is disabled if the support is not active in the project.

Note that it is necessary to configure some SMTP settings before an email can actually be sent – the default settings will not work since they are fictive and will not correspond with your email provider. Full details to the SMTP and its use in the µTasker demo project are given in the document <http://www.utasker.com/docs/uTasker/uTaskerSMTP.PDF>

Logo and upload field – The Coldfire logo was uploaded to the file system as a GIF file when the files were loaded. It is possible to change this logo for a different GIF file by selecting a GIF and pressing the “*Upload now*” button. The GIF may be up to 100k in size.

8.2. LAN configuration

This side is a very critical side since it allows important Ethernet settings to be modified. The first time the device is started, the default MAC address – defined in the `cParameters` structure in **application.c** - is 0-0-0-0-0-0. It can be changed just once, after which it is displayed as disabled. This is because it is normally necessary to program a new device with a unique MAC address which should normally never be changed again. (*See the short discussion about MAC addresses at the bottom of this section for some details about how they are obtained.*)

The IP address, subnet mask and default gateway IP address can be modified as long as the device is not set to DHCP operation. If they are first modified and then the device is set to DHCP mode, they represent preferred settings to be requested during the DHCP procedure or for use as a last resort if no DHCP server is available.

The Ethernet speeds of 10M, 100M or auto-negotiation (full or half-duplex) can be set.

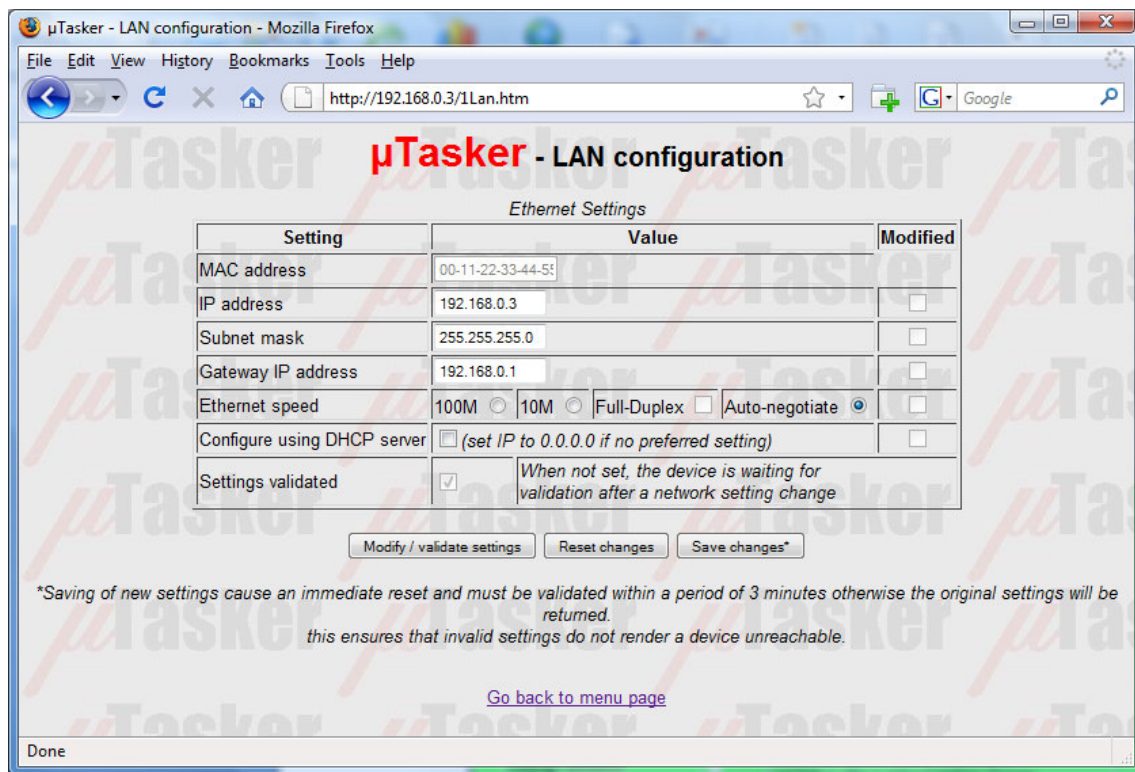


Figure 6. µTasker web server showing the LAN configuration page

Values, which are not disabled, can be modified and accepted by clicking on “Modify / validate settings” and changed values are indicated by a check box in the configuration table. They have not yet been committed to memory and the previous setting can be returned by clicking on “Reset changes”.

Once you are sure that the modifications are correct, they are saved to flash memory by clicking on “Save changes”. This will cause also a reset of the device after a delay of about 1 second and it will be necessary to establish a new connection to the device using its new settings and validate the changes.

So why make it so complicated? Well it is simply to be sure that you have not modifying something which will render the device unreachable. For example, you may have changed its Ethernet speed from 100M to 10M although it is connected to a hub which only supports 100M and, to make matters worse, the device is not simply sitting on your office desk at arm's length but is at a customer's site several hours drive away. It would be a nasty situation if you had just lost contact with the equipment and have to somehow get it back on line although everyone at the customer's site has already left for a long weekend...

So this is where the validation part comes in. After the reset, the device sees that there are new settings in memory but also that these are only provisional (not validated) - the original values are also still available. These new values are nevertheless used for a 'trial-period' and a timer of three minutes duration started. It is now your job to establish a new web server connection to the device, using the new settings and to click on "Modify / validate settings". If you do this the check box names "Settings validated" will be checked, the new parameters are validated in flash and the old ones deleted. This in the knowledge that the new values are also really workable ones – how would you otherwise have been able to validate them?

Imagine however that a change really rendered the device unreachable – for example the LAN speed was really incompatible or you made a mistake with the subnet mask. After three minutes without validation, the provisional values are deleted from flash and, after a further automatic reset, the original settings are used again. After a short down period you can then connect as before the change and perform the modifications again, though correcting the previous mistake. There is therefore no danger of loosing contact with the device, even when a 'silly' mistake is made.

Some notes about MAC addresses

If you are using your own device behind a router and it is not visible to the 'outside world' you can in fact program any MAC address that you like because it is in a private area. It just has to be unique in this private area. (This is also valid for a device sitting in a Demilitarized Zone- DMZ)

If however you are selling a product or the device is sitting directly on the Internet then it must have a world wide unique MAC address which has to be purchased from IEEE. It is purchased either as a block (IAB) of 4k MAC addresses at a cost of about \$500, or if you are going to produce a large number of pieces of equipment you can purchase a unique company ID (OUI) of 16Million for about \$1'600 (plus \$2'000 if you don't want the OUI to be registered on the public listing).

It is then your responsibility to manage the assignment of these addresses in your own products.

The registration page is at: <http://standards.ieee.org/regauth/index.html>

For any one just wanting to make one or two pieces of equipment for hobby use it is a bit much to pay \$500 for a bunch of MAC addresses and use just one or two of them. Unfortunately it is no allowed to sell the rest on to people in similar situation because a block must always remain with the individual or organisation purchasing it.

One trick which is often used is to find out what the MAC address is in an old NIC from an old PC which is being scrapped. This MAC address is then used in your own piece of equipment and the old NIC destroyed. You can then be sure that the MAC address is unique and can not disturb when used for any imaginable application.

8.3. Serial Configuration

This web page allows the debug interface UART in the M5225X to be set. See the USB demo document for some more details on this interface:

http://www.utasker.com/docs/uTasker/uTaskerV1.3_USB_Demo.PDF

µTasker - Serial configuration - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168. ...

µTasker - Serial configuration

Serial port

Serial speed	19200		
Parity	<input type="radio"/> Even	<input type="radio"/> Odd	<input checked="" type="radio"/> None
Data	<input checked="" type="radio"/> 8 bits	<input type="radio"/> 7 bits	
Stop bits	<input checked="" type="radio"/> 1	<input type="radio"/> 1.5	<input type="radio"/> 2
Flow control	<input type="radio"/> RTS/CTS	<input checked="" type="radio"/> XON/XOFF	<input type="radio"/> NONE
Flow control buffer levels	Flow OFF (%) 80	Flow ON (%) 20	

Modify serial port setting

Reset changes

Save changes

[Go back to menu page](#)

Done

Figure 7. µTasker web server showing the serial interface configuration page

8.4. Statistics

The statistics window opens in a separate window and displays a table of the number of Ethernet frames counted by the Ethernet task. These are classified according to whether they were transmitted, received for the local IP address or received as broadcast frames and divided into IP protocol types. Since the values can continue to change, the user can update the window by clicking on the “Refresh” button. It is also possible to reset the counters if desired by clicking on “Reset frame stats”.

The contents of the ARP cache is also displayed and can be cleared by clicking on “Delete ARP entries”. These are equivalent to the DOS commands `arp -a` to display the local ARP cache and `arp -d` to delete it. Notice that when the ARP cache is deleted via the web page there will always remain one entry, this being the PC which commanded the deletion of the ARP table and updated the table. Due to the network activity it will always immediately be re-entered...

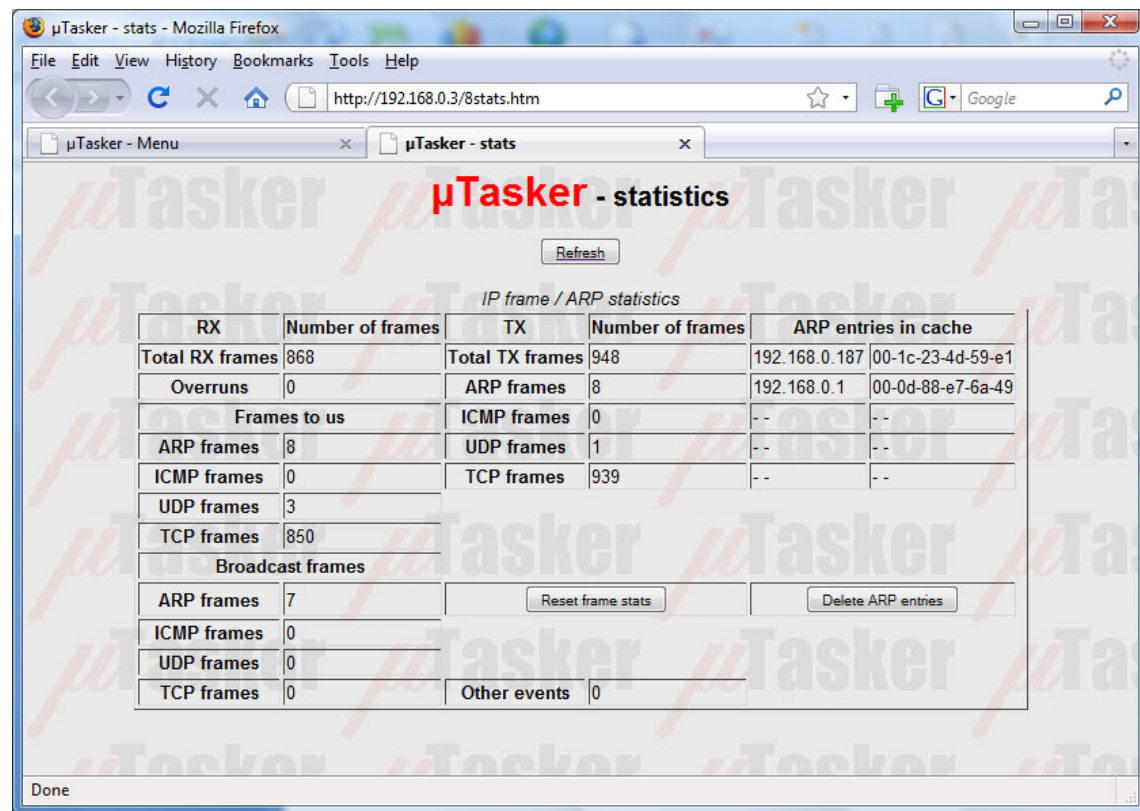


Figure 8. µTasker web server showing the statistics page

8.5. I/O Page

The I/O window was discussed in step 11 of the tutorial and will not be discussed in any more detail here.

8.6. Administration Side

On this page the FTP server can be activated and deactivated. See also step 12 of the tutorial.

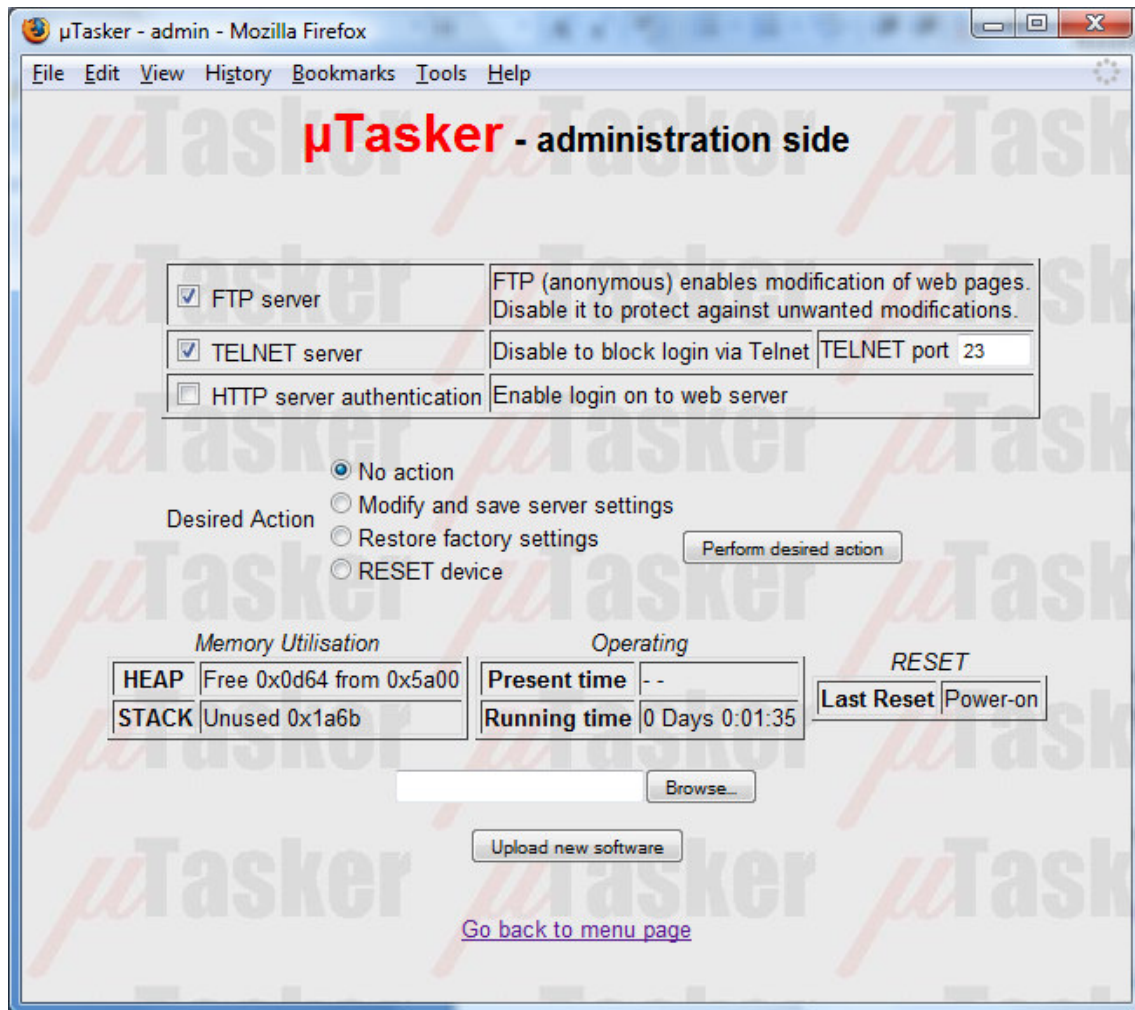


Figure 9. µTasker web server showing the administration page

The HTTP server can be configured to require basic authentication, meaning that it requests the user name and password when a new connection is established. These values are contained in the default settings in `application.c`.

A TELNET server can also be enabled or disabled, including setting it to a particular port number.

The previous three settings are modified and saved by setting the desired action to “*Modify and save server settings*” and clicking on “*Perform desired action*”.

A further action is “*Restore factory settings*” which returns the default settings as defined in `application.c`. This also provokes a reset of the device and if the default settings cause the network values to be modified it will automatically start a three minute validation period meaning that it will also be necessary to establish a connection using the ‘factory settings’ and validate them before the original ones will become permanent. This is again to ensure that there is no danger of losing contact with a remote device. Note that the MAC address is not reset since the Mac address should always remain unchanged in the device.

The last action is a simple reset of the device.

Memory Utilisation

HEAP – the used heap and the maximum defined heap are displayed. Note here that the simulator will often display that more heap is used as needed in the real target due to the fact that some variables will be of different sizes when running on a PC compared to an embedded target. It allows the real use on the target to be monitored and the user can then optimise the amount of heap allocated to just support the worst case.

STACK – the amount of stack which has not been used (safety margin) is measured and displayed. As long as the value remains larger than 0 the system is not experiencing any memory difficulties. A value of zero indicates a critical situation and must be reviewed. The simulator however doesn’t perform this stack monitoring and will always display zero; its use is on the target where resources need to be monitored carefully.

The methods used for the memory monitoring are detailed in the µTasker main documentation.

Present Time – If the demo project is configured to collect the timer from a time server, this displays the present time. The time may also be available if the device which the µTasker is operating on processes a RTC.

Running Time - The time since the device started, or since the last reset, is displayed. This is useful when monitoring a remote device to ensure that it is indeed operating stably since a watchdog reset due to a software error would allow the device to remove but possibly not enable its occurrence to be readily detected.

Last Reset – The last reset cause is displayed. This can (for example) be due to a power up, a software reset, an external reset or a watchdog reset.

8.7. Email Configuration Side

The SMTP configuration can be performed on this web page corresponding to the email provider's requirements.

For more details see the document

<http://www.utasker.com/docs/uTasker/uTaskerSMTP.PDF>

µTasker - Email Setup - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.0.3/4EmailSetup.htm

µTasker - Email configuration

SMTP server requires authentication ☐

User name

User password

User's Email address

SMTP server address

SMTP server IP address

Save settings

[Go back to menu page](#)

Done

Figure 10. µTasker web server showing the Email configuration page

8.8. Dynamic Content Generation Side

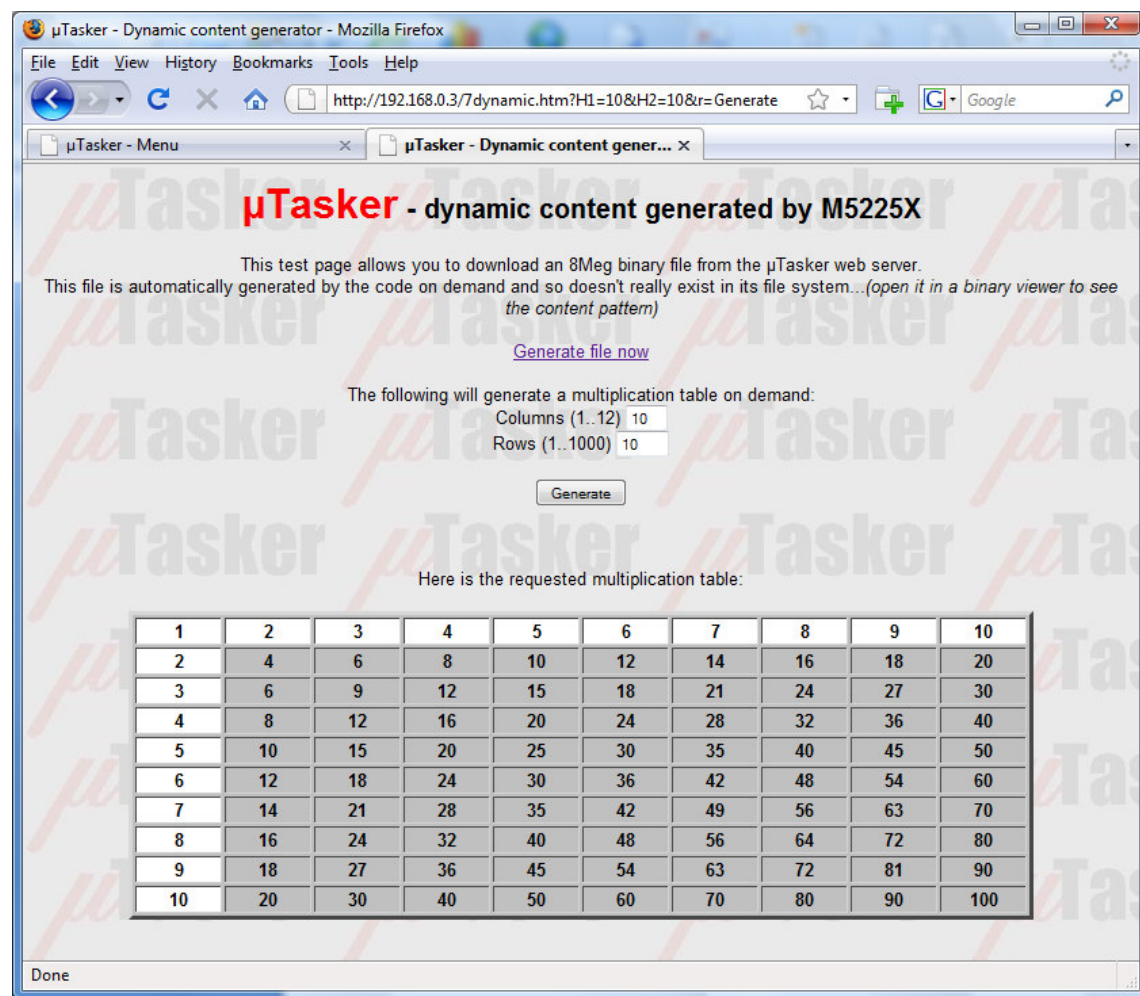
This web page contains two different demonstrations.

The first allows downloading an 8MByte test file from the board, which is generated on demand.

The second enables the user to configure the dimensions for a multiplication table which is generated on demand by the board.

For full details of this operation see the document

http://www.utasker.com/docs/uTasker/uTaskerV1.3_Content_Generation.PDF



µTasker - dynamic content generated by M5225X

This test page allows you to download an 8Meg binary file from the µTasker web server. This file is automatically generated by the code on demand and so doesn't really exist in its file system...*(open it in a binary viewer to see the content pattern)*

[Generate file now](#)

The following will generate a multiplication table on demand:

Columns (1..12)
Rows (1..1000)

Here is the requested multiplication table:

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	12	14	16	18	20
3	6	9	12	15	18	21	24	27	30
4	8	12	16	20	24	28	32	36	40
5	10	15	20	25	30	35	40	45	50
6	12	18	24	30	36	42	48	54	60
7	14	21	28	35	42	49	56	63	70
8	16	24	32	40	48	56	64	72	80
9	18	27	36	45	54	63	72	81	90
10	20	30	40	50	60	70	80	90	100

Done

9. Developing – Testing - Debugging

The demo project is designed to demonstrate a typical use of the operating system and TCP/IP stack. It is useful in itself as a starting point for many applications and this section looks at the support for developing, testing and debugging your own applications.

Until now you haven't actually had to develop anything since the project is delivered fully functional. To develop your own project it will be necessary to make configuration changes to suit your own use, to modify existing code and add new code of your own. To learn more about these aspects it is possible to study the documentation about the µTasker operating system and protocol stack. A more hands on approach is also possible by letting the demo project run and walking through the code parts which you are interested in – we did this briefly at the start of the demo but didn't linger to discuss any details. Here we will check out the advantages of the simulator by looking in more depth at a rather more complicated debugging session.

Debugging is performed for a number of reasons. It is a natural consequence of the test phase where unexpected program behaviour is experienced and the causes and reasons need to be understood before correcting the code. It is often also an integral part of the test phase itself when code reviews are performed, exception handling is to be exercised or software validation is required. The simulator allows a high degree of tests to be performed in comfort before going to the target testing phase, where such reviews would be rather more complicated.

So let's test something in the demo project. We'll test the simple PING ECHO utility which we already used once and we'll see how we can get to know the software in a very convenient and efficient manner. We will see how we can manipulate the operation to test and validate special cases and to make corrections in the code (and verify them too). First we will work ON LINE with the simulator, meaning that the simulator will be running effectively in real time and we will capture and analyse events. Afterwards we will see how to do the same OFF LINE, using a recording of the first case (which could also be a recording made when using a real target).

Introducing Wireshark

If you are using the µTasker then you will certainly be wanting to make use of its network capabilities and a tool to monitor network activity is essential. These are often called Network Sniffers since they can monitor, record and analyse network activity by watching what happens on the local Ethernet connection. The µTasker was designed with and around Wireshark (previously called Ethereal), a free and powerful network Sniffer. You can download this from <http://www.wireshark.org/>

If you haven't this program then don't delay – download it and install it and then we will get down to some work.

Now do the following steps:

1. Start the demo project simulation as described in the first tutorial.
2. Open a DOS window and prepare the PING command “ping 192.168.0.3”.
3. Start Wireshark and start monitoring the traffic on your local network (Capture | Start -> OK).
4. Enter return in the DOS windows so that the PING test is started.
5. Wait until the PING test has completed; there are normally 4 test messages sent.
6. Stop the Wireshark recording and save it to the directory
Applications\TaskerV1.3\Simulator\Ethereal\ with the name ping.eth

At this stage you can also look at the contents of the Wireshark recording and you will see something like the following:

No.	Time	Source	Destination	Prot	Info
1	0.437770	192.168.0.100	Broadcast	ARP	Who has 192.168.0.3? Tell 192.168.0.100
2	0.439926	00:11:22_33:44:55	192.168.0.100	ARP	192.168.0.3 is at 00:11:22:33:44:55
3	0.439933	192.168.0.100	192.168.0.3	ICMP	Echo (ping) request
4	0.449898	192.168.0.3	192.168.0.100	ICMP	Echo (ping) reply
5	1.441345	192.168.0.100	192.168.0.3	ICMP	Echo (ping) request
6	1.441650	192.168.0.3	192.168.0.100	ICMP	Echo (ping) reply
7	2.442782	192.168.0.100	192.168.0.3	ICMP	Echo (ping) request
8	2.442915	192.168.0.3	192.168.0.100	ICMP	Echo (ping) reply
9	3.444225	192.168.0.100	192.168.0.3	ICMP	Echo (ping) request
10	3.444344	192.168.0.3	192.168.0.100	ICMP	Echo (ping) reply

It is also very possible that there are other frames on the network from other computers or your own computer talking with others, and it is possible to perform many filtering functions to remove these either from the visible display or from the recording file – just look in the Wireshark Help.

Here my PC has the local address 192.168.0.102 and initially doesn't know how to find the destination 192.168.0.3. An ARP resolve is sent and the simulator responds to it, informing at which MAC address its IP can be found at.

The ping test is repeated four times, each time receiving a reply from the simulator.

So let's see in some more detail how we can check the operation of this procedure and we will begin at the deepest point in the code, the receiving interrupt routine in the Ethernet driver, which is called when a complete Ethernet frame has been received.

In the VisualStudio project, locate the file `M5223X.c` (in `hardware\M5223X\`) and search for the Ethernet reception interrupt routine called `fec_rx_frame_isr()`. Position the cursor over the first bracket after the interrupt subroutine definition and press F9 to set a break point there.

It may be that you will find the code stopping at this break point before starting the ping test, which is probably because the code is receiving broadcast frames from your network. If this happens before you start the ping test just press F5 to let it run again (which you may have to repeat if there is a lot of activity...).

Repeat the ping test from the DOS window and the execution will stop at the breakpoint which you set in the interrupt routine. Since there will be no answer to the ping test because our code has been stopped, the ping test(s) will fail, but we don't worry about that since we have caught the event which we are going to use to analyse the flow through the driver, memory, the operating system and the ICMP routine. Now we can get to know the code in as much detail as we want.....and since we are working with the M5223X, this will also give us the opportunity to look at some of its internal registers on the way.

A. Interrupt routine

```
__interrupt void fec_rx_frame_isr(void)
{
#ifdef _WINDOWS
    EIR &= ~RXF;
#else
    EIR = RXF;                // Reset interrupt flag
#endif
    iInterruptLevel++;        // ensure interrupts remain blocked
    fnWrite( INTERNAL_ROUTE, (unsigned char*)EMAC_RXA_int_message, HEADER_LENGTH);
                                // Inform the Ethernet task
    iInterruptLevel--;
}
```

The simulator has just received a frame for our MAC address or a broadcast address (the simulator doesn't disturb us with foreign MAC addresses when the EMAC in the M5223X has not be set up for promiscuous operation) and here we are in the interrupt routine. Now don't forget that this is the real code which will operate on your target and if this doesn't work properly it will also not work properly on your target.

We see that such routines are necessarily quite hardware specific. In fact the M5223X interrupt routine is very simple and has only to clear the interrupt flag which is performed on the target by writing a '1' to the corresponding bit. The simulator uses a slightly different technique and clears the bit as is normally performed in a variable. The register EIR (Ethernet Interrupt event Register) can be found in the data sheet to the device if you would like to learn more about its details and it exists in the simulated M5223X, where it can be looked at as follows.

Double click on EIR in the code and search for it using "search in files", ensuring that the search path starts at the highest level in the µTasker project, and using the search files of type *.c and *.h.

It will be found in the code at several locations but also in the file M5223X.h, where it is defined as:

```
#define EIR *(volatile unsigned long *) (EMAC_BASE_ADD + 0x4)
where EMAC_BASE_ADD is also defined locally twice:
#define EMAC_BASE_ADD ((unsigned char *) (&ucM5223X.SimEMAC)) and
#define EMAC_BASE_ADD (IPSBAR + 0x1000)
```

On the target, the register is located at an offset of 0x1000 from the IPSBAR (0x40000000) = 0x40001000 and when simulating it can be found in a structure called ucM5223X.

Double click on the word ucM5223X so that it becomes highlighted and then drag it into the watch window (Shift F9 opens a quick watch window). Expand the structure by clicking on the cross to the left of the name and you will see the various internal peripheral divided into sub-blocks. EMAC_ISR is in the sub-block SimEMAC so we also expand this sub-structure by clicking on the cross left of its name. If only the EMAC peripheral block is of interest this

block can be dragged alone to the watch windows by selecting ucM5223X.SimEMAC and dragging this to there.

In the sub-block you will see all of the EMAC registers listed in the order in which they occur in memory as well as showing their present values. Step the code (F10) and you will see that the content of EIR is change as the code resets the interrupt flag before sending an internal message defined by

```
static const unsigned char EMAC_RXA_int_message[ HEADER_LENGTH ] = { 0, 0 ,  
TASK_ETHERNET, INTERRUPT_EVENT, EMAC_RXA_INTERRUPT };    // define fixed interrupt  
event
```

This internal message is sent to TASK_ETHERNET to inform that a frame has been received and is as such a method used by the operating system to wake up this Ethernet task. If you want to, you can also step into the write function to see the internal workings of how it wakes up the receiver task but I will assume here that all is working well and will just move to TASK_ETHERNET to see it actually receiving this interrupt message.

Before doing the next step, remove the break point in the interrupt routine by setting the cursor to its line and hitting F9.

B. Receive Task

Now open the file ethernet.c in the project directory TCP/IP and set the cursor to the bracket after the tasks routine `void fnTaskEthernet(TTASKTABLE *ptrTaskTable)`

With a right click, the menu item “Run to cursor” can be executed and you will see that this task is indeed started immediately since the program execution stops at this line.

Step slowly through the code using F10 and observe that the task reads the contents and interprets it as an INTERRUPT_EVENT. It calls fnEthernetEvent() to learn about the length of the received frame and to get a pointer to it – use F11 to step into this routine if you would like to see its internal workings, which I will not discuss here apart from to say that the EMAC in the M5223X uses buffer descriptors to coordinate Ethernet frames in RAM. These buffers were configured when the Ethernet interface was initialised and the routine retrieves the relevant information about where the frame is and how long it is...

You will see that the pointer to the frame is called rx_frame and it is defined as a pointer to an ETHERNET_FRAME. Now, as we all know, a pointer is just a pointer – but the fact that it is defined as a pointer to a certain structure will help us greatly to interpret the contents of the received frame. We will first look at the frame as it is in memory and then how it looks in the debugger as a structure.

C. Receive Frame

Let's start with simply looking at the raw data which we have just received from the Ethernet. Do this by placing `rx_frame` in a watch windows and expanding it so that the length of the frame (`frame_size`) and the pointer to the data (`ptEth`) are visible. `ptEth` has a value which you can double click on and insert to the clip board before pasting it into the address field of a memory display window (if this windows is not yet visible, activate it in the debug menu). Now you will see the raw Ethernet frame in memory – note that this is in the local computer's memory and the address of its location has nothing to do with the storage place on the real target. However its location is governed by the buffer descriptors in an analogue fashion to the operation in real device.

Now it is not exactly easy to understand the data but you should just be able to make out the MAC address at the beginning and the content of the ping test usually consists of `abcdefghijklmnop...` which is easily recognised. (Warning: it is possible that the frame which you actually captured is not the ping test but some other network activity, or even an ARP frame if the PC sending the ping had to re-resolve its MAC address. If this happens to be the case, set a break point at the location which the program is at and let it run again and hopefully it will come to this location the next time with the correct contents...).

Go back to the watch windows where the structure of `rx_frame` is being displayed and expand the sub-structure `ptEth`. This will start making life rather easier since it is showing us that the Ethernet frame is made up of a destination MAC address, a source MAC address, an Ethernet frame type and some data. Expand each sub-structure to see their exact contents, although it is not yet worth expanding the data field since we don't know what protocol its contents represent so it will not be displayed any better at the moment.

The screenshot shows a debugger interface with two main panes. The left pane displays the structure of `rx_frame` and its sub-structures. The right pane shows a memory dump starting at address `0x00457c1e`.

Name	Wert
<code>rx_frame</code>	<code>{...}</code>
<code>frame_size</code>	<code>0x004a</code>
<code>ptEth</code>	<code>0x00456a40</code>
<code>ethernet_destination_MAC</code>	<code>0x00456a40 ""</code>
<code>[0x0]</code>	<code>0x00 ''</code>
<code>[0x1]</code>	<code>0x00 ''</code>
<code>[0x2]</code>	<code>0x00 ''</code>
<code>[0x3]</code>	<code>0x00 ''</code>
<code>[0x4]</code>	<code>0x00 ''</code>
<code>[0x5]</code>	<code>0x00 ''</code>
<code>ethernet_source_MAC</code>	<code>0x00456a46 ""</code>
<code>[0x0]</code>	<code>0x00 ''</code>
<code>[0x1]</code>	<code>0x0b 'I'</code>
<code>[0x2]</code>	<code>0xdb 'Ù'</code>
<code>[0x3]</code>	<code>0xe6 'æ'</code>
<code>[0x4]</code>	<code>0x90 'I'</code>
<code>[0x5]</code>	<code>0x2b '+'</code>
<code>ethernet_frame_type</code>	<code>0x00456a4c "I"</code>
<code>[0x0]</code>	<code>0x08 'I'</code>
<code>[0x1]</code>	<code>0x00 ''</code>
<code>ucData</code>	<code>0x00456a4e "E"</code>

Adresse:	0x00457c1e
00457C1E	45 00 00 3C E...<
00457C22	9D 2D 00 00 ...
00457C26	80 01 1B DA ...U
00457C2A	C0 A8 00 66 A...f
00457C2E	C0 A8 00 03 A...
00457C32	00 00 51 5C ...Q\
00457C36	02 00 02 00
00457C3A	61 62 63 64 abcd
00457C3E	65 66 67 68 efgh
00457C42	69 6A 6B 6C ijkl
00457C46	6D 6E 6F 70 mnop
00457C4A	71 72 73 74qrst
00457C4E	75 76 77 61 uvwa
00457C52	62 63 64 65 bcde
00457C56	66 67 68 69 fghi
00457C5A	41 43 41 43 ACAC
00457C5E	41 43 41 43 ACAC
00457C62	41 43 41 43 ACAC
00457C66	41 00 00 20 A...
00457C6A	00 01 00 00
00457C6E	00 00 00 00
00457C72	00 00 00 00
00457C76	00 00 00 00
00457C7A	00 00 00 00
00457C7E	00 00 00 00
00457C82	00 00 00 00
00457C86	00 00 00 00
00457C8A	00 00 00 00
00457C8E	00 00 00 00

D. Frame protocol

Step slowly using F10 and you will see that the frame is checked for the ARP protocol, which it won't be if it is the ping request which we are analysing. It then calls fnHandleIP(), which we will enter using F11 since all such TCP/IP frames are built on the IP protocol.

After a couple of basic checks of IP frame validity, the pointer received_ip_packet is assigned to the data part of the received frame. Again this structure is very valuable to us since it can be dragged into the watch windows and now we suddenly understand how the IP fields are constructed. We can expand any field we want to see, such as the IP address of the source sending the IP frame. *Note that when looking at IP frames it may be worth requesting the debugger to display the contents in decimal rather than in hexadecimal by using right click and then selecting the display mode. The IP addresses are then better understandably and afterwards you can set the mode back to hexadecimal display since it is better for most other data fields.*

Name	Wert
received_ip_packet	0x00456a4e
version_header_length	69 'E'
differentiatedServicesField	0 ''
total_length	0x00456a50 ""
[0x0]	0 ''
[0x1]	60 '<'
identification	0x00456a52 "I0"
[0x0]	157 'I'
[0x1]	48 '0'
fragment_offset	0x00456a54 ""
[0x0]	0 ''
[0x1]	0 ''
time_to_live	128 'I'
ip_protocol	1 'I'
ip_checksum	0x00456a58 "IXA"
[0x0]	27 'I'
[0x1]	215 'x'
source_IP_address	0x00456a5a "A"
[0x0]	192 'A'
[0x1]	168 ''
[0x2]	0 ''
[0x3]	102 'f'
destination_IP_address	0x00456a5e "A"
[0x0]	192 'A'
[0x1]	168 ''
[0x2]	0 ''
[0x3]	3 'I'
ip_options	0x00456a62 "I"

Adresse: 0x00457c1e	
00457C1E	45 00 00 3C E..<
00457C22	9D 2D 00 00 .-..
00457C26	80 01 1B DA ...U
00457C2A	C0 A8 00 66 A..f
00457C2E	C0 A8 00 03 A...
00457C32	00 00 51 5C ..Q\
00457C36	02 00 02 00
00457C3A	61 62 63 64 abcd
00457C3E	65 66 67 68 efgh
00457C42	69 6A 6B 6C ijkl
00457C46	6D 6E 6F 70 mnop
00457C4A	71 72 73 74qrst
00457C4E	75 76 77 61 uvwa
00457C52	62 63 64 65 bcde
00457C56	66 67 68 69 fghi
00457C5A	41 43 41 43 ACAC
00457C5E	41 43 41 43 ACAC
00457C62	41 43 41 43 ACAC
00457C66	41 00 00 20 A...
00457C6A	00 01 00 00
00457C6E	00 00 00 00
00457C72	00 00 00 00
00457C76	00 00 00 00
00457C7A	00 00 00 00
00457C7E	00 00 00 00
00457C82	00 00 00 00
00457C86	00 00 00 00
00457C8A	00 00 00 00
00457C8E	00 00 00 00
00457C92	00 00 00 00
00457C96	00 00 00 00
00457C9A	00 00 00 00
00457C9E	00 00 00 00
00457CA2	00 00 00 00
00457CA6	00 00 00 00
00457CAA	00 00 00 00
00457CAE	00 00 00 00

If you continue to step through the routine you will see that the IP frame is interpreted to see whether we are being addressed, it may cause our ARP cache to be updated and the checksum of the IP frame will also be verified. To return without stepping all the way you can use SHIFT F11 to return to the ETHERNET task code, where the protocol type is checked.

E. ICMP Handling

Note that each protocol type can be individually activated or deactivated in config.h. ICMP frames are only handled when the define `USE_ICMP` is set. If your project doesn't want to support ICMP then it can be simply removed...

Step into the ICMP routine (`fnHandleICP()`) by using F11. You will see that there is also a checksum in the ICMP field which is verified and the structure `ptrICP_frame` allows the ICMP fields to be comfortably viewed in the watch window.

Our frame should be of type `ECHO_PING`, which can also be individually deactivated in your project if you want to support ICMP but do not want the ping test to be replied to.

The received frame is sent back, after modifying a few fields, using the call `fnSendIP()`. I don't want to go into details about how the IP frame I constructed – you can see this in detail by stepping into the routine and observing what happens – but I should mention how the frame is sent out over the Ethernet since this is again a low level part which uses the M5223X registers again. Very briefly you should understand that the M5223X has been set up with one or more transmission buffers into which the data is copied. The data is set up to respect the ICMP, IP and Ethernet layers as we observed in the received message and, once completely ready, the transmission is activated.

This transmission activation takes place in the file `M5223X.c` in the function `fnStartEthTx()` so search for it and set a break point there. Once the program reaches this point it will stop and you can see which registers are set up and verify that all is correct.

Here you will also see that the simulator comes into play once the data is ready and the registers have been set up correctly. This code, which will not be discussed here, basically tries to behave as the EMAC transmitter does by interpreting the register set up and transmitting the data buffer contents to your local network.

10. Off-Line Simulation

Normally the simulator, or the target, will have responded to the ping request very quickly and the ping test would have been successful. We, being human beings, are rather slow and we probably took several minutes to work our way through the code before your ping reply was finally sent back. This was of course much too late as the ping test has already terminated, informing that the test failed.

This is not only a problem with the ping test but with many protocols since they use timers and expect replies within quite a short time, otherwise an error is assumed and links break down. Debugging of such protocols can become quite hard work due to this fact.

This is where the µTasker can save the day again since it supports operation in OFF LINE mode. This means simply that it can interpret Wireshark recordings as if they were real data from the network. Since we previously made a recording we can try this out right now!

A. Prepare a break point

I suggest that you set a break point in the ICMP routine itself since we have already seen how the message arrives there and this will avoid false triggers due to broadcast frames in the mean time. Let the project run again by hitting F5.

B. Open the Wireshark recording

In the menu Wireshark select `Load Wireshark/Ethereal file to play back`. Then select the `ping.eth` file which was previously recorded. If this is repeated, the command `Replay last File` can be used instead – this is also valid after the simulator is terminated normally.

Perform this action and the Wireshark file will be interpreted. The times that frames arrived will be respected – if there is a gap or 1s between two frames then these two frames will also arrive with a 1s gap. You will see that the recorded ping will be received via the receive Ethernet interrupt routine and be passed up through the software until the breakpoint in the ICMP routine is encountered. The difference is that the break point and stepping in code can not disturb the protocol since also the recording is stopped.

This can be a great advantage when debugging protocols!

Before I finish with this discussion there are a few points which should be noted, so here is a list of all relevant details which could be of use or interest.

1. When an Wireshark recording is played back, the internal NIC is closed so that there is no disturbance from the network.
2. The Wireshark recording can be repeated after it has terminated. There is no limit as to the number of times it can be repeated. Useful for incremental testing of a new piece of code...
3. After an Ethernet playback it is necessary to restart the simulator to use the simulator with the network again.
4. If you find a software error when stepping through the code, there is nothing to stop you making a correction without terminating the simulation session. Often VisualStudio can

recompile the new code and continue with the debugging session, thus allowing the correction to be immediately used – this is a major advantage of the VisualStudio environment! Try it and you will learn to love it...

5. Wireshark recordings do not have to originate from the simulator, they can be recordings from targets or from foreign devices. This means that recordings of a good known sequence can also be used as input to developments (for example the recording of an email being collected by your PC).

It is necessary that the simulator is set up to have the same IP and MAC addresses of the device in the recording and it will then receive all recorded frames to that device. Using this recording it is then possible to develop new code, verifying that it reacts as the original device did at each step.

Using this method, it is even possible to develop quite complicated protocols or services using a known good case as a reference. It can be basically tested before being switched onto the network so that there is a good chance that it will even work first go!

11. Conclusion

This tutorial first introduced the μTasker simulator's capabilities to execute the demo project software on a simulated M5225X. It showed the basics of working with the simulator and its Ethernet capabilities before turning attention to running the same project on a target board.

By working with Wireshark and the μTasker simulator's ability to play back Wireshark recordings through its complete software code, interesting methods for increasing development, debugging and test efficiency have been demonstrated.

The M5225X project supports various other features including USB. All features can be simulated using similar built-in techniques, thus enabling all aspects of real-world embedded projects to be performed with increased efficiency in comparison with convention development and debug techniques. Combining the μTasker simulator with the features of the μTasker demo project it represents the fastest method of starting and completing embedded projects with the supported devices.

Modifications:

- V0.0 22.01.2009 First provisional draft. This version is not complete but the basic tutorial for the Ethernet work is ready.
- V0.1 16.02.2009 First Release.