

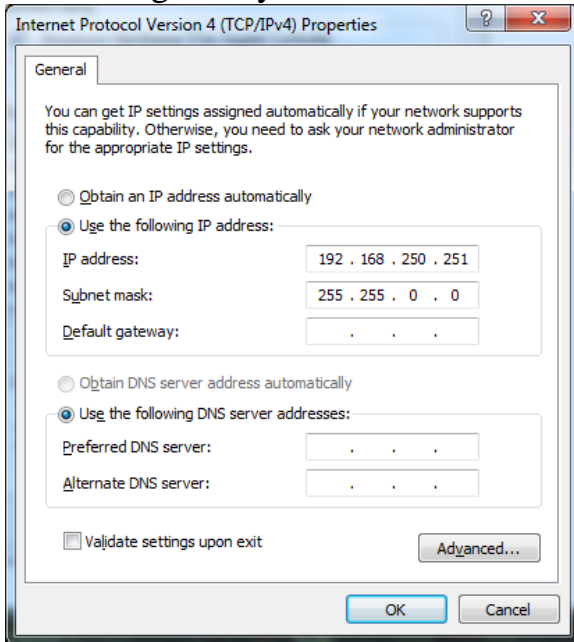
FreeWire Setup with SPR (Secure Port Redirector)

This document will show the setup, configuration and testing of a DeviceMaster FreeWire. This document will start with the FreeWire using the 'Factory Default' settings.

When the DeviceMaster FreeWire is in its default state:

(To reset a DeviceMaster FreeWire to default settings, press the "Reset" button with a paper clip for 15 seconds. The reset opening may be found next to the serial port DB9 connector.)

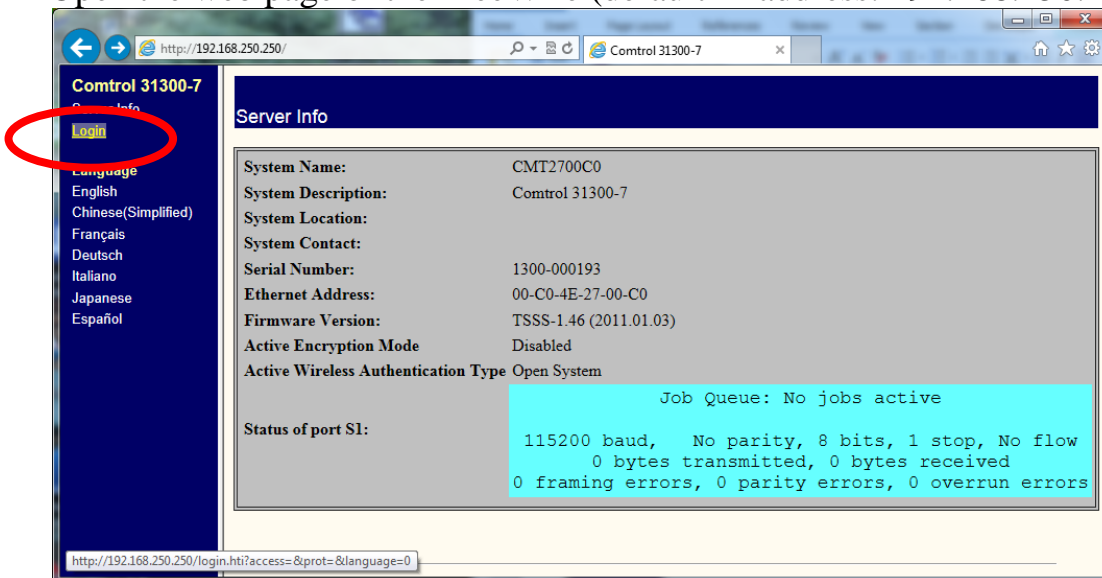
Change the IP address in your PC to be 192.168.250.251 with subnet of 255.255.0.0 as shown here. The gateway and DNS values do not need to be entered.



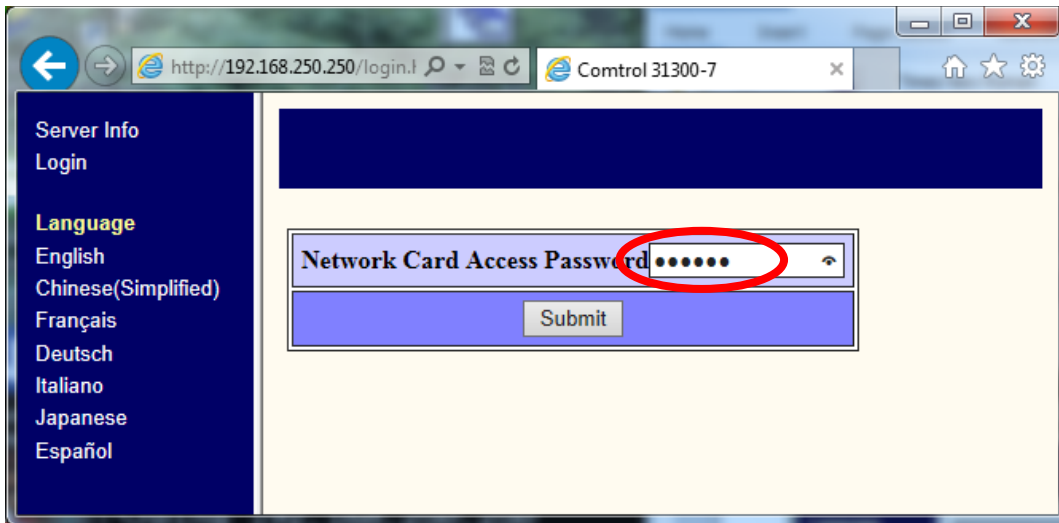
The FreeWire will be initially configured using the hardwired Ethernet port.

Attach an Ethernet cable directly from the PC Ethernet port to the FreeWire Ethernet port.

Open the web page of the FreeWire (default IP address: 192.168.250.250) password = access

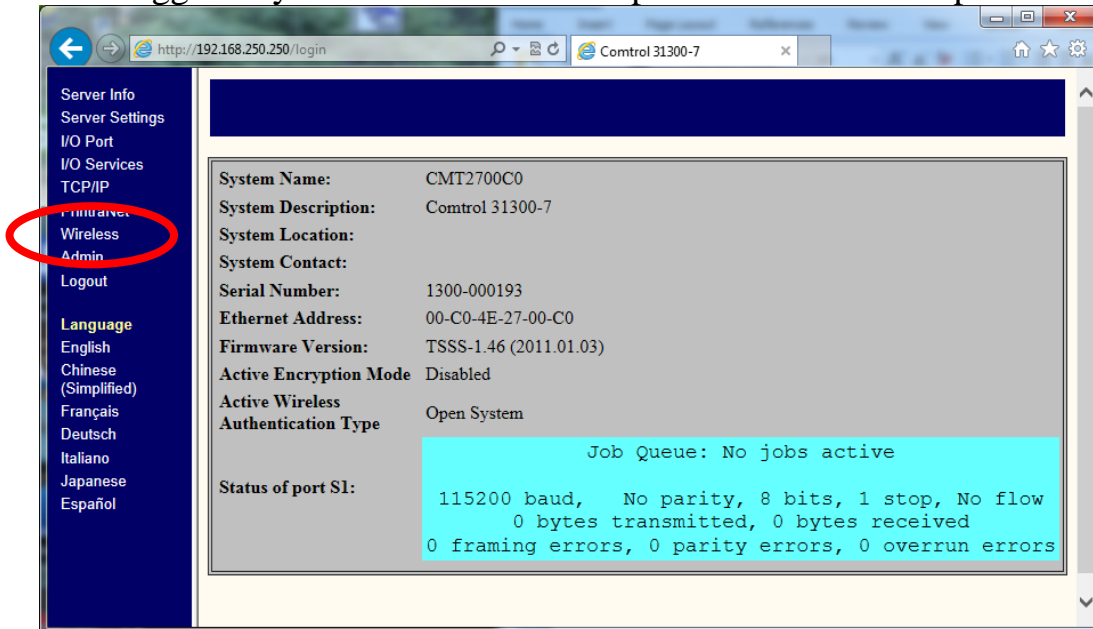


Click on Login in the left panel.



Enter "access" (without quotes, all in lower case) and press enter.

Once logged in you should have these options in the left side panel:



Click on "Wireless"

Here are the defaults:

The screenshot shows a web browser window with the URL <http://192.168.250.250/wififrm.htm?access=B62A53C0F5>. The page title is "Control 31300-7". On the left is a navigation menu with items like "Server Info", "Server Settings", "I/O Port", "I/O Services", "TCP/IP", "PrintraNet", "Wireless", "Admin", "Logout", and a "Language" section. The main content area contains a table of wireless parameters:

Mode	AD-HOC	?
Radio	802.11b-g	?
Channel Scan Mask	Configure Channel Scan Mask	
SSID	serserv	?
Network Security	Configure Network Security	
Channel	11	?
Country	United States	?
Transmit Power	100	?
Speed	0 Mbps	
Signal Quality	Disable	
<input type="button" value="Submit"/>		

Below the table is a text box: "This page allows you to modify the Wireless parameters." At the bottom left, there is a "Channel" label.

Change the Mode = Infrastructure

Change the SSID = whatever your Access Point is configured for (this demonstration uses 'FreeWire')

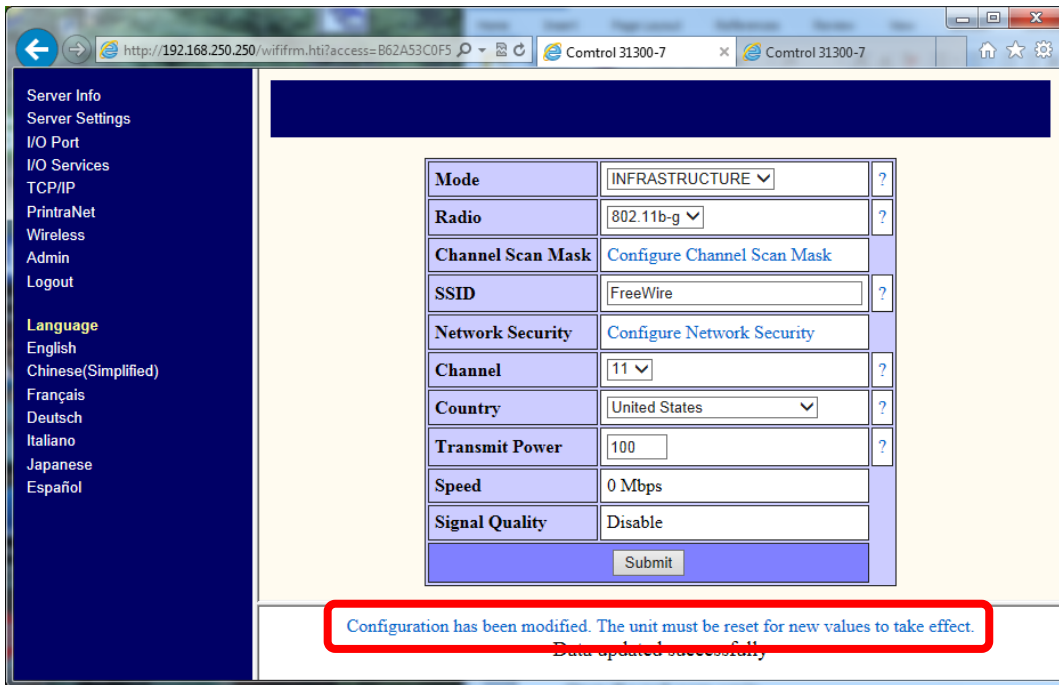
Channel = whatever your Access Point uses (this demonstration uses the default of 11)

At bottom of page, click on "Submit"

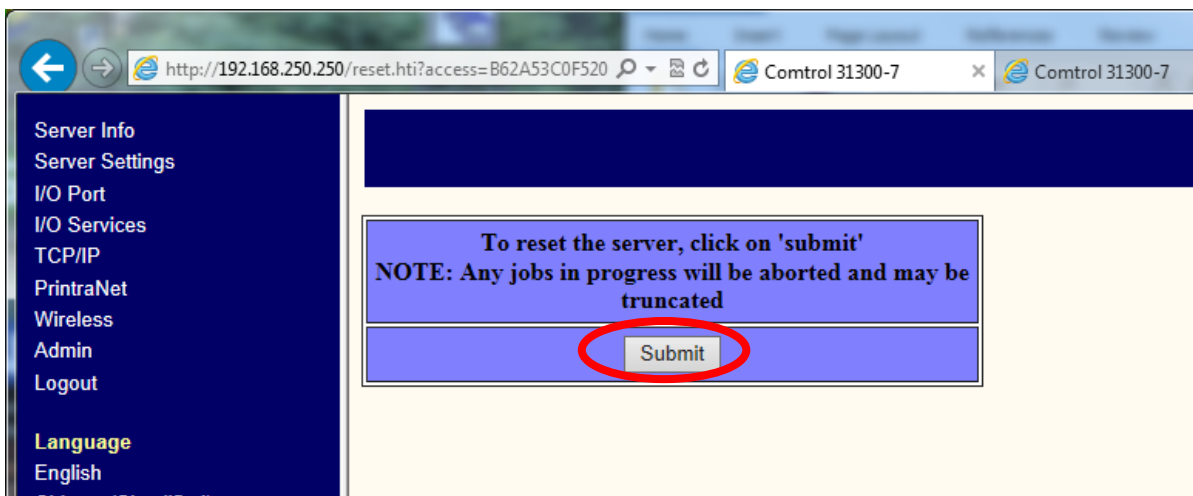
The screenshot shows the same web browser window as before, but with the following changes in the configuration table:

Mode	INFRASTRUCTURE	?
Radio	802.11b-g	?
Channel Scan Mask	Configure Channel Scan Mask	
SSID	FreeWire	?
Network Security	Configure Network Security	
Channel	11	?
Country	United States	?
Transmit Power	100	?
Speed	0 Mbps	
Signal Quality	Disable	
<input type="button" value="Submit"/>		

The text box below the table remains: "This page allows you to modify the Wireless parameters." At the bottom left, there is a "Channel" label and a small link: http://192.168.250.250/wifi_update.



Click on the notice: Configuration has been modified. The unit must be reset for new values to take effect.



Click on “Submit” to apply changes and reboot the FreeWire.

You will be presented the notice: The server will reset in 5 seconds. The HTTP connection will be unavailable while the server resets. Please wait several seconds before trying to reestablish a connection

Open the web page again using the 192.168.250.250 IP address.

Login

Return to the ‘Wireless’ page.

Click on "Configure Network Security"

The screenshot shows a web browser window with the URL `http://192.168.250.250/wififrm.hti?access=C58836C0B5`. The page title is "Control 31300-7". On the left is a navigation menu with "Language" selected. The main content area contains a table of wireless settings:

Mode	INFRASTRUCTURE	?
Radio	802.11b-g	?
Channel Scan Mask	Configure Channel Scan Mask	
SSID	FreeWire	?
Network Security	Configure Network Security	
Channel	11	?
Country	United States	?
Transmit Power	100	?
Speed	0 Mbps	
Signal Quality	Disable	

Below the table, there is a text box: "This page allows you to modify the Wireless parameters." and a section titled "Channel" with the text: "Enter the desired 802.11 channel to be used on your network. The channel number only applies to AD_HOC mode. In Infrastructure, the access point determines the channel used."

This will open a new page:

The screenshot shows the same web browser window, but now displaying the "Configure Network Security" page. The URL is `http://192.168.250.250/wifisecfrm.hti?access=C58836C0B5318F18&prot=&language=0`. The page title is "Control 31300-7". The main content area contains a table of security settings:

Active Encryption Mode	Disabled	
Encryption Mode	Disabled	?
Key Selection	1	?
WEP Key	Key #1: <input type="text"/> Key #2: <input type="text"/> Key #3: <input type="text"/> Key #4: <input type="text"/>	?
Active Wireless Authentication Type	Open System	
Wireless Authentication Type	Open System	?
Wired Authentication Type	None	?
Authentication Attempts	0	?

Below the table, there is a section titled "Encryption Mode" with the text: "Select the desired encryption mode for the wireless link."

Defaults are shown in this window.

The screenshot shows a web browser window with the URL <http://192.168.2.191/wifisecfrm.ht?access=46A>. The browser tab is titled "Control 31300-7". On the left side, there is a navigation menu with the following items: Server Info, Server Settings, I/O Port, I/O Services, TCP/IP, PrintraNet, Wireless, Admin, Logout, and a Language section with options: English, Chinese(Simplified), Français, Deutsch, Italiano, Japanese, and Español.

The main configuration area contains the following settings:

Active Encryption Mode	WPA	
Encryption Mode	WPA	?
Key Selection	1	?
WEP Key	Key #1: <input type="text"/> Key #2: <input type="text"/> Key #3: <input type="text"/> Key #4: <input type="text"/>	?
Active Wireless Authentication Type	PSK	
Wireless Authentication Type	PSK	?
Wired Authentication Type	None	?
Authentication Attempts	0	?
User ID	anonymous	?
Password	<input type="text"/>	?
Authentication Protocol	PAP	?
PSK	*****	?
Authentication Server Certificate	Configure Authentication Server Certificate	
SSL/TLS Private Key	Configure Private Key	
<input type="button" value="Submit"/>		

Encryption mode = WPA

Wireless Authentication Type = PSK

Authentication protocol = PAP

PSK = (Pre-shared key) Whatever is used with your Wireless Access Point

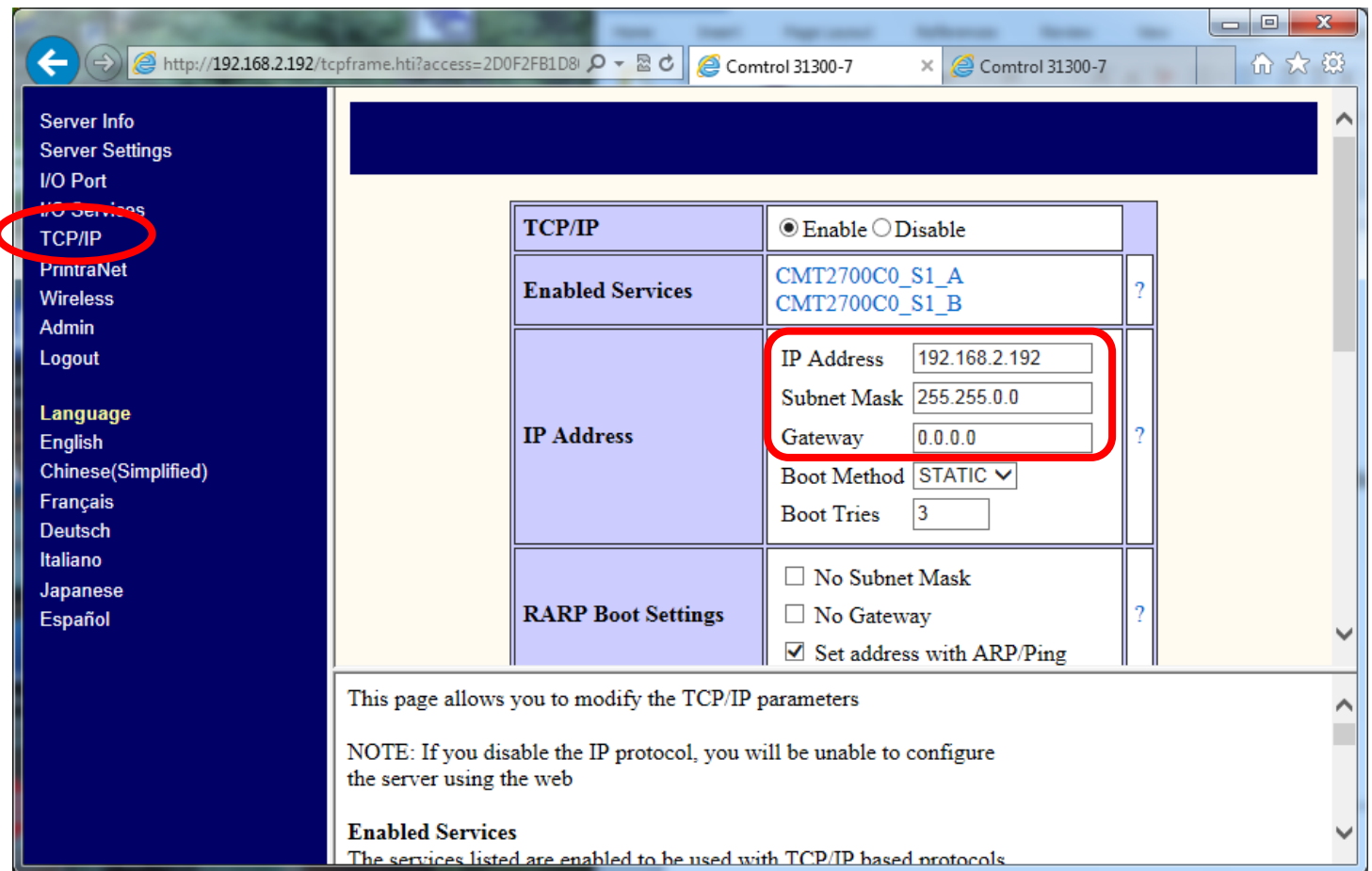
At bottom of page, click on "Submit"

New line "Configuration has been modified. The unit must be reset for new values to take effect." Click this to reboot FreeWire.

Open the web page again using the 192.168.250.250 IP address.

Login

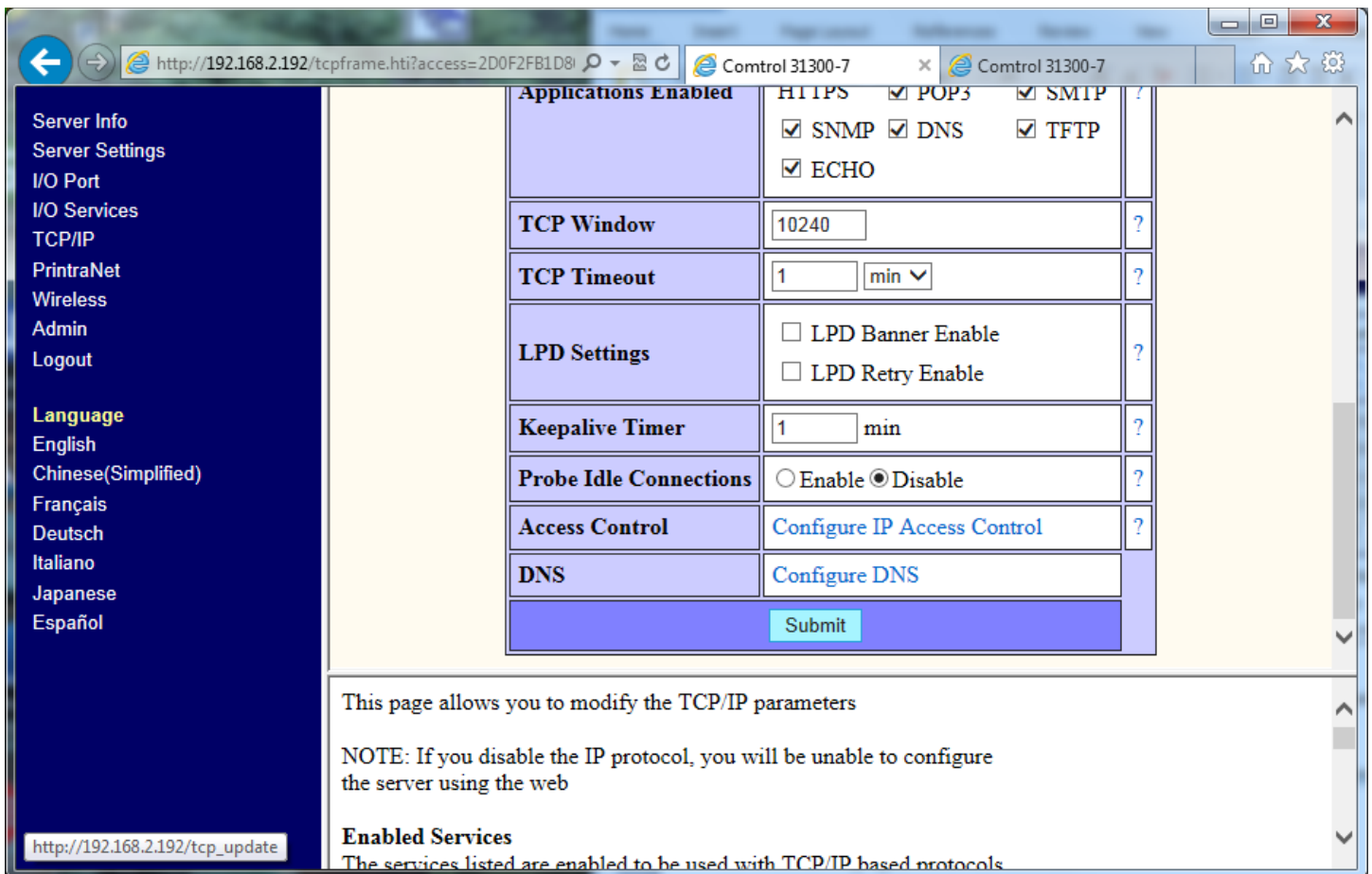
In right hand panel click on TCP/IP



Set IP address and Subnet Mask

Optionally set the Gateway

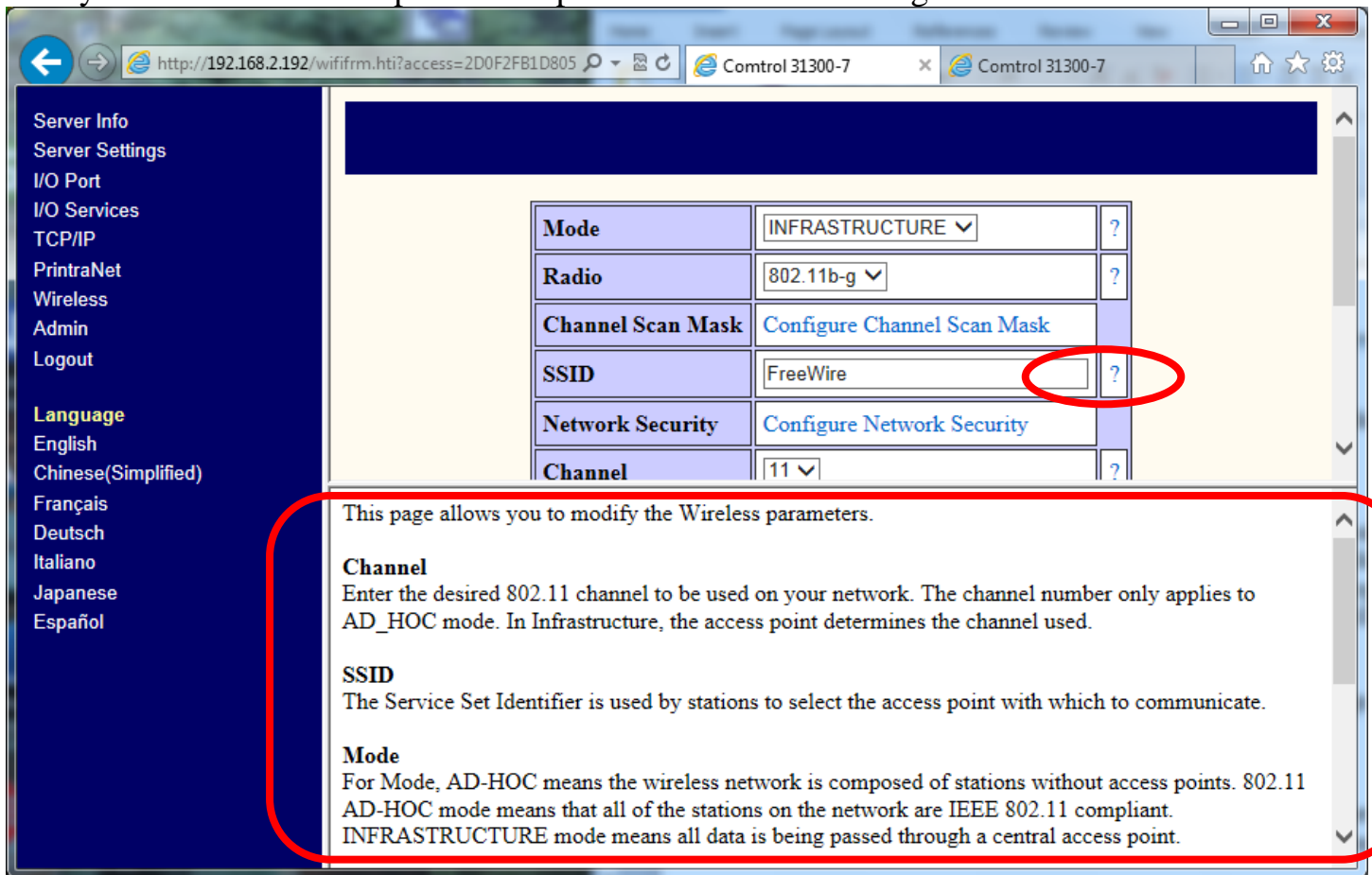
At bottom of page, click on "Submit"



New line "Configuration has been modified. The unit must be reset for new values to take effect." Click this to reboot FreeWire.

These are all of the changes that **MUST** be completed. Other tweaks may be necessary depending on your environment. This is to show a basic and quick setup. This document will not cover other configuration options. To find definitions of the options, you will notice the window is broken into two horizontal panels. The lower panel will provide help for the configuration options.

Here you can see the lower panel example for the wireless settings:



Mode	INFRASTRUCTURE	?
Radio	802.11b-g	?
Channel Scan Mask	Configure Channel Scan Mask	
SSID	FreeWire	?
Network Security	Configure Network Security	
Channel	11	?

This page allows you to modify the Wireless parameters.

Channel
Enter the desired 802.11 channel to be used on your network. The channel number only applies to AD_HOC mode. In Infrastructure, the access point determines the channel used.

SSID
The Service Set Identifier is used by stations to select the access point with which to communicate.

Mode
For Mode, AD-HOC means the wireless network is composed of stations without access points. 802.11 AD-HOC mode means that all of the stations on the network are IEEE 802.11 compliant. INFRASTRUCTURE mode means all data is being passed through a central access point.

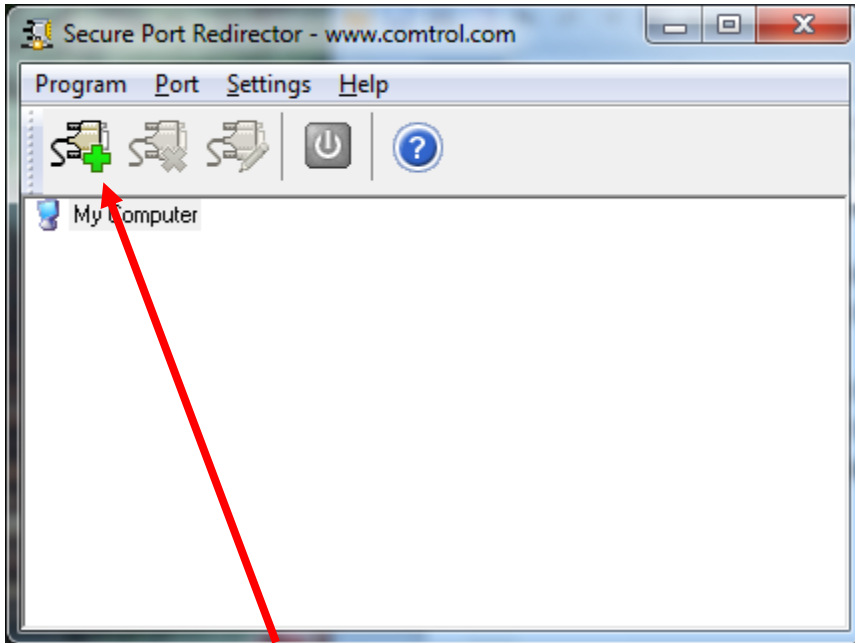
You may also click on the “?” on the right side of the configuration value in order to have the specific help displayed in the lower panel.

Set the IP address of your PC back to what it should be.

Disconnect the Ethernet cable and see if you can open the web server in the FreeWire by opening a web browser and entering the IP address you programmed.

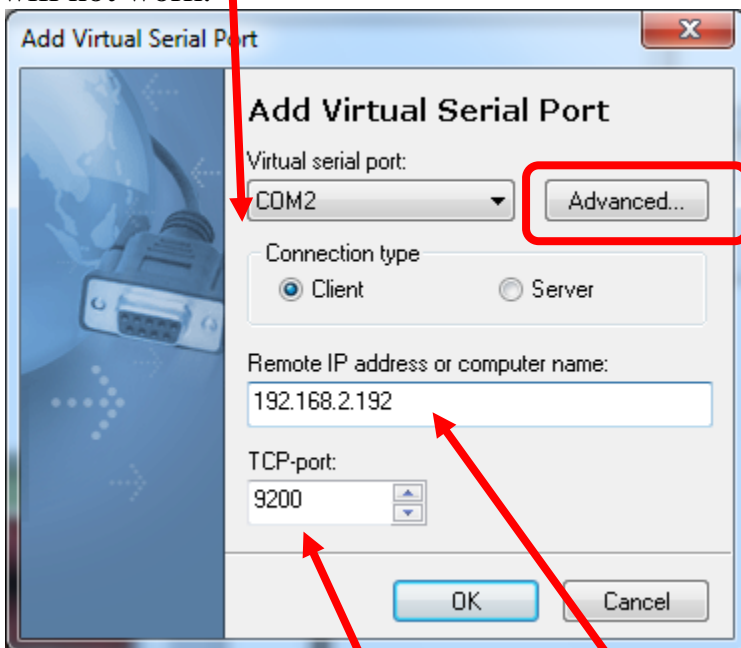
Now that the wireless side has been configured we will setup SPR to use the serial port.

Install and launch SPR (Secure Port Redirector)



Click on the 'Green Plus'

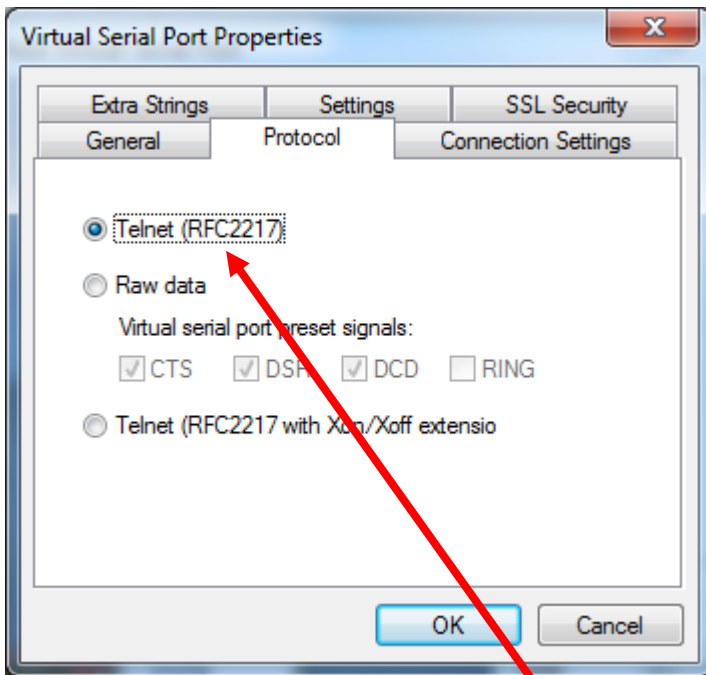
Start by adding the port to the SPR (Secure Port Redirector). Be sure that you do not select an existing com number as SPR (Secure Port Redirector) will allow doing so, but that com number will not work.



Enter the IP address of the DeviceMaster.

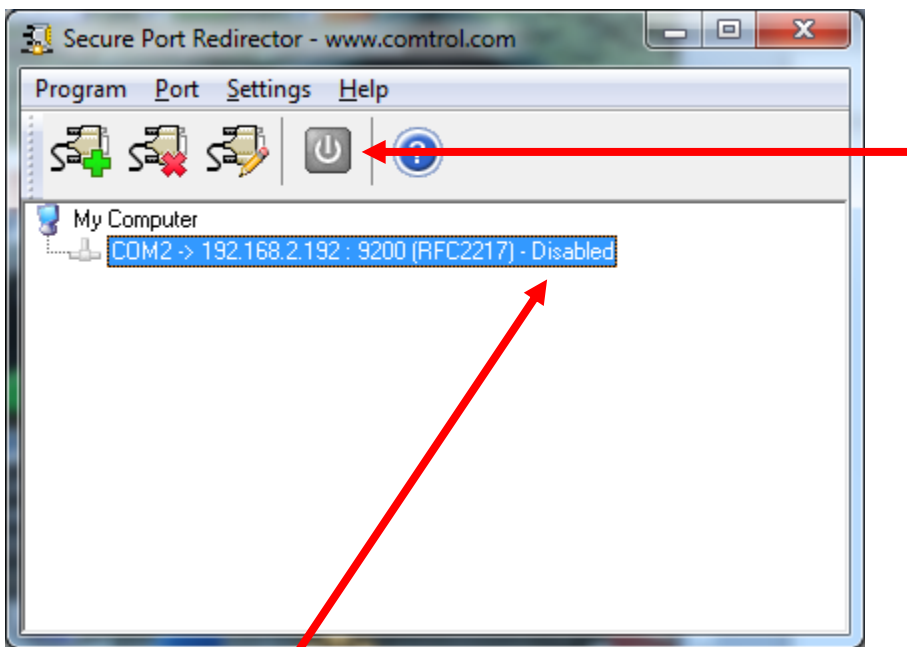
Set the TCP-port to 9200

Click the Advanced button:



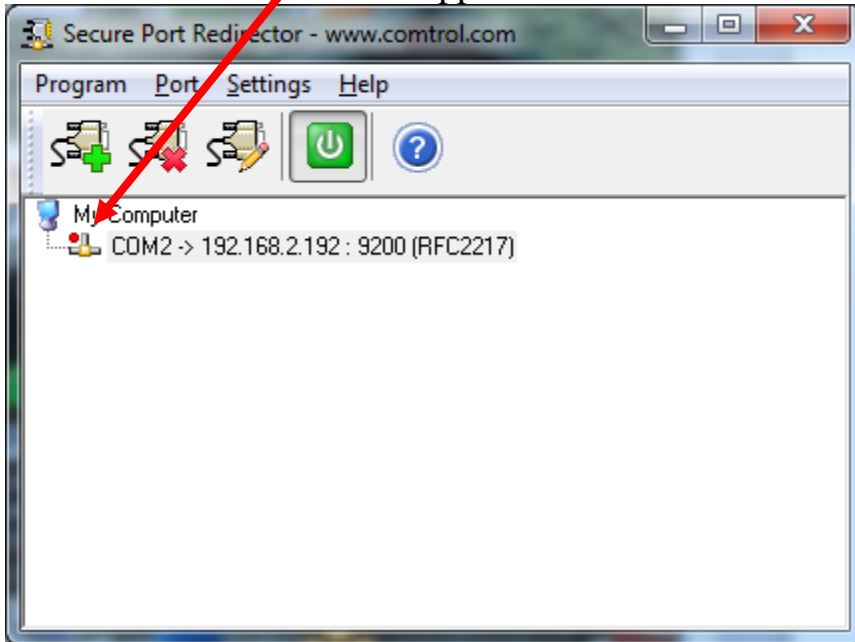
Select the Telnet (RFC2217) option

Click OK here to exit the Advanced options and click OK again to close the 'Add Virtual SP' dialog

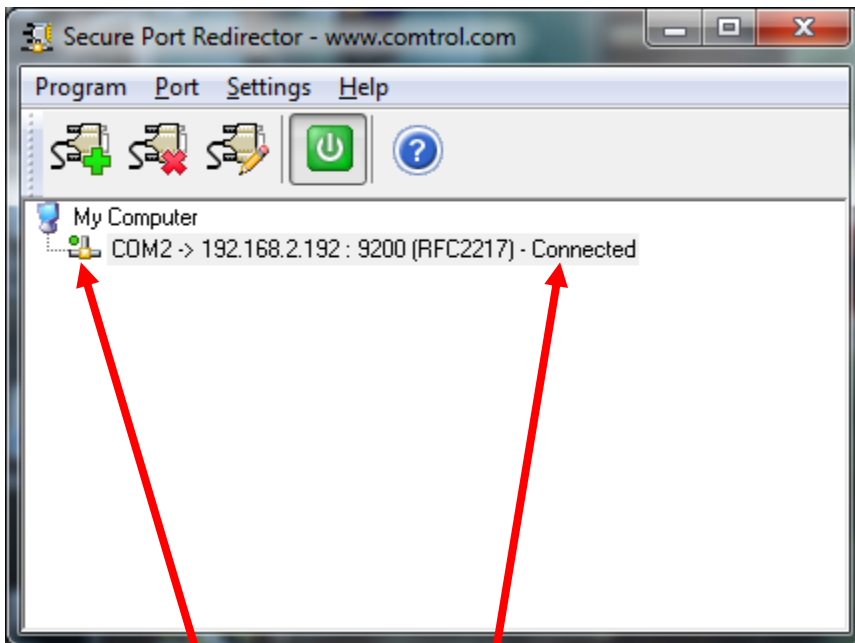


Change it from "Disabled" to "Enabled" by clicking the 'Power' icon on the launch bar

Once enabled a red dot will appear next to the icon.



This indicates that the serial port is not currently in use.



Once the serial port is opened, the line will look like what is seen in this graphic. This shows an active connection from the Test Terminal application. Note the "Green Dot" and "Connected"

Now the serial port is ready to be tested.

DeviceMaster Serial Port Testing

Test the serial ports using the Test Terminal app in the PortVision Program and the Loopback plug provided with the hardware. If the testing does not complete successfully, then I recommend that you give our tech support group a call at 763-957-6000.

If you need to create a loopback plug you can download the instructions at ftp://ftp.comtrol.com/RPort/HW_doc/Loopback/2000042_A.pdf

Control's utilities for Ethernet connected products are included with the PortVision application from the 'Tools' menu.

Stop all applications that may be accessing the ports such as RAS, RRAS or any faxing or production software. See the appropriate manuals for instructions on stopping these services or applications. If another application is controlling the port, then Test Terminal will be unable to open the port and an error message will be shown.

Remember to restart the application once testing of the ports has been completed.

Testing The Control ports.

- 1a.) From the 'Tools>Applications' drop-down menu in PortVision, select Test Terminal (WCOM2))
- 2a.) Port>openport>ComX (where X is the com port number to test)
- 3a.) Attach the Control supplied loopback plug onto the serial port of the controller
- 4a.) Port>openport>send test data
- 5a.) You should see the alphabet scrolling across the port. If so, then the port installed properly and is operational.
- 6a.) Port>openport>send test data (data should stop)
- 7a.) Port>openport>loopback test (This is a pass fail test and will take a second or two to complete)
- 8a.) Repeat for each port that needs testing.
- 9a.) Close test terminal

If both of these tests successfully complete, then the port is operational as expected. Close Test Terminal and start the application that will be using the serial ports.

There are, as you have seen, two tests in the Test Terminal and I will describe both.

Send Test Data: This is simply sending data out the transmit line to the 'Loopback' plug which has the transmit and receive pins connected thus sending the data back through the Receive line to the Test Terminal app which then displays the received data in the terminal window for that port. The send test data test is only testing the transmit and receive signal lines and nothing else. This test will work in either RS232 or RS422 modes as both modes have transmit and receive capability. A failure in this test will essentially prevent the port from working in any manner.

Loopback Test: This test using the Control supplied loopback is testing all of the modem control signals, RTS, DTR, CTS, DSR and CD. When a signal is made HI in one line the corresponding signal line will indicate this. The Loopback test changes the state of the lines and looks for the corresponding state change. It will then send certain commands and confirm the transmission and receipt of these commands. If it successfully recognizes all of these changes, the port passes. A failure on this test is not necessarily critical, as it will depend on what is connected and how many signal lines are in use. For example, if you are using RS232 in 3-wire mode (Transmit, Receive and Ground) a failure will cause no discernable issue since the other signals are not being used. If the port is configured in some products for use as either RS422 (or RS485) this test will fail and is expected to fail since RS422 (and RS485) do not have the modem control signals that are present in RS232 that this test is designed for.