# Hardware Configuration Guide

GEMINI
NavSoft Technologies Inc.

**20 Barrett Court**
**Fredericton, NB, Canada**
**E3B 6Y1**

www.gemini-navsoft.com

**Note:** This guide is meant as a supplement to the operator's manuals of hardware manufacturers to facilitate hardware integration. For complete product manuals, please visit the respective websites of the hardware manufacturers.

# 1. NovAtel GPS Receivers

**I. Novatel OEM4 and OEM5 Receiver Setup**

Novatel OEM4 and OEM5 receivers must be configured to send 2 data logs (RANGECMPB and RAWEPHEMB) through its COM port (or Ethernet port). All other data being sent through the COM port should be disabled.

Below are the commands issued in Novatel CDU software through the command line interface. Note that the commands should be issued over a different port than that which will be used to collect the data. Once the SAVECONFIG command is issued, the receiver will reboot using the saved configuration.

| Command / Data Log | Description |
|---|---|
| FRESET STANDARD | Sets receiver to factory defaults. This will set baud rates of all COM ports to 9600. |
| LOG COM1 RANGECMPB ONTIME 5 | Log range observations to COM1 every 5 seconds |
| LOG COM1 RAWEPHEMB ONCHANGED | Log ephemeris data to COM1 as it changes |
| LOG COM1 BESTXYZB ONTIME 60 (optional) | Log best position solution to COM1 every 60 seconds |
| COM COM1 57600 n 8 1 n off on | Configure COM1 at 57600 kps<br>The baud rate much match the baud rate of the serial-to-Ethernet device |
| SAVECONFIG | Save current configuration |
| LOG LOGLIST | Check current configuration to see that logs are in receiver memory. The RANGECMPB, RAWEPHEMB and BESTXYZB (optional) logs should be listed on COM1 |
| LOG COMCONFIG | Check current COM port configuration to verify that the desired setting are in place. |

⚠ If COM1 is being configured for data collection, when possible, it is recommended to use COM2 to issue the above commands. Otherwise, once the COM command is issued, you may lose connection to the receiver.

⚠ If using NovAtel's CDU configuration software, make sure to close all viewing windows while issuing logging commands. Each viewing window requests a different data log from the receiver, which will interfere with desired data logs.

# 2. Javad GPS Receivers

## I. Javad Receiver Setup (Delta G2)

The following commands should be copied and paste into a txt file.

a) For mmVu™ operation:

```
%  BINEX  %
%1%set,/par/rover/mode/,off
%2%set,/par/base/mode/,off
%3%set,/par/raw/time/sync,steady
%4%set,/par/pos/mode/cur,sp
%5%remove,/msg/def/
%6%set,/par/raw/msint,50
%7%em,/dev/ser/a,/msg/binex/01_01:{1,0,0,0x2}
%8%em,/dev/ser/a,/msg/binex/7F_03:{5,0,0,0x0}
```

b) For AutoVu™ operation:

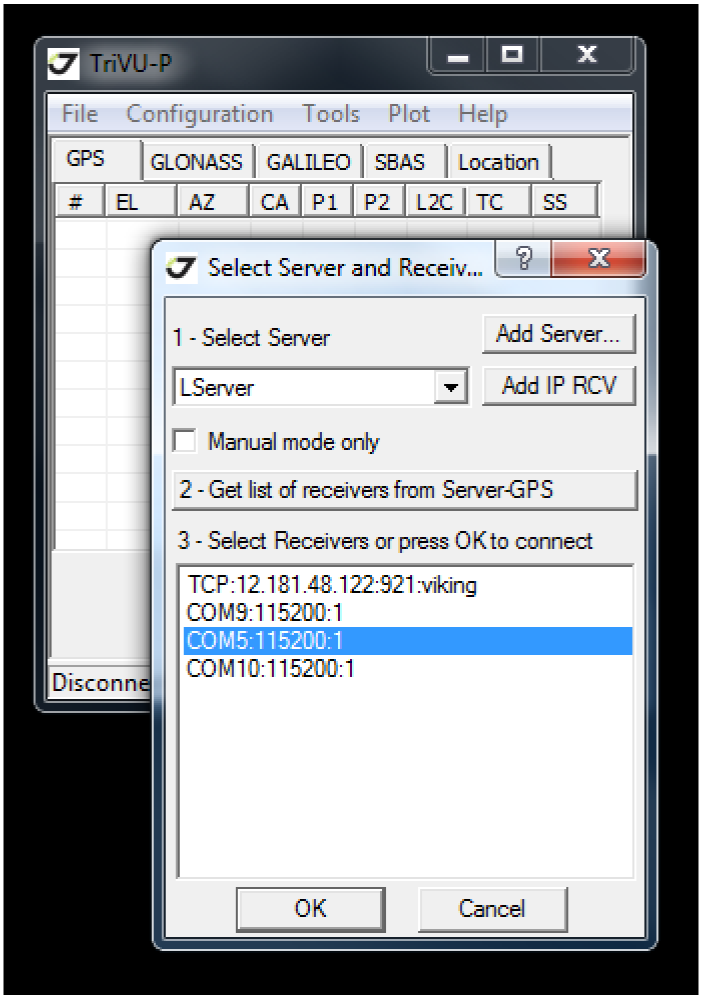
```
%  BASE STATION %
%1%set,/par/rover/mode/,off
%2%set,/par/base/mode/,off
%3%set,/par/pos/mode/cur,sp
%%remove,/msg/def/
%6%set,/par/ref/ant/id,JAV_TRIUMPH-1
%7%dm,dev/udp/a
%7%set,/par/dev/udp/a/addr,100.1.110.1
%8%set,/par/dev/udp/a/port,8000
%9%em,dev/udp/a,/msg/rtcm3/1004:1

%  ROVER1  %
%1%set,/par/rover/mode/,off
%2%set,/par/base/mode/,off
%%set,/par/raw/time/sync,steady
%3%set,/par/pos/mode/cur,sp
%6%set,/par/raw/msint,50
%7%set,/par/pos/msint,50
%8%dm,/dev/udp/a
%9%set,/par/dev/udp/a/addr,100.1.210.1
%10%set,/par/dev/udp/a/port,8001
%11%em,/dev/udp/a,/msg/jps/{RT,GT,SI,rc,cp,DC,CE,2r,2p,D2,2E,ET}:{0.1,0.00,0,0x0}

%  ROVER2  %
%1%set,/par/rover/mode/,off
```

```
%2%set,/par/base/mode/,off
%%set,/par/raw/time/sync,steady
%3%set,/par/pos/mode/cur,sp
%6%set,/par/raw/msint,50
%7%set,/par/pos/msint,50
%8%dm,/dev/udp/a
%9%set,/par/dev/udp/a/addr,100.1.210.1
%10%set,/par/dev/udp/a/port,8002
%11%em,/dev/udp/a,/msg/jps/{RT,GT,SI,rc,cp,DC,CE,2r,2p,D2,2E,ET}:{0.1,0.00,0,0x0}
```

Use JAVAD's TriVu software to connect to the receiver (Figure 1). Select Manual Mode from the File menu. Select Load Script and locate your text file (Figure 2). Click Send Command. Make SURE to **Disconnect** before Exiting. Otherwise, additional TriVu messages will be sent by your receiver while it is logging data, which will prevent GNT software from functioning properly.



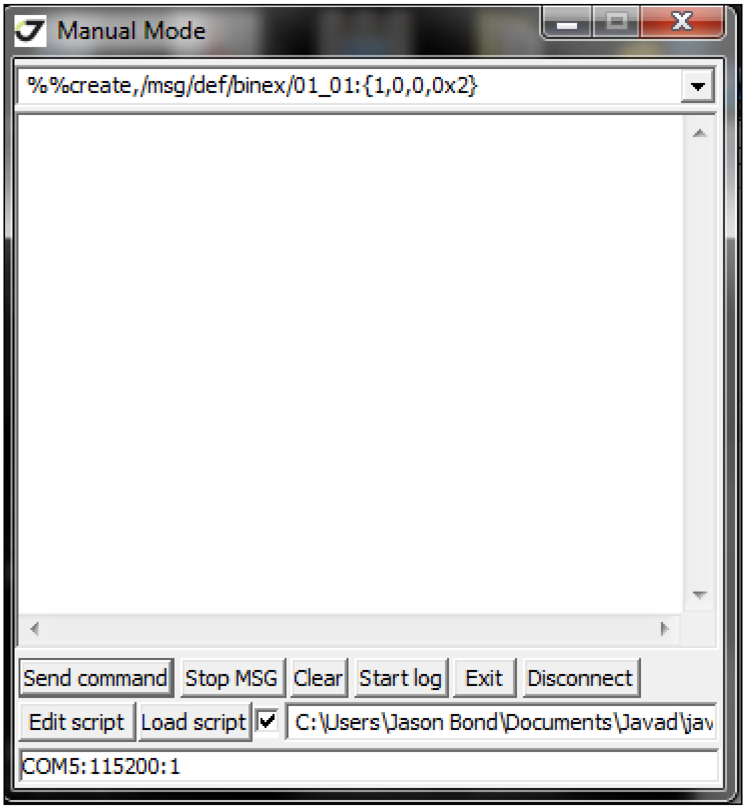
1 - Select Server: LServer

□ Manual mode only

3 - Select Receivers or press OK to connect

TCP:12.181.48.122:921:viking
COM9:115200:1
COM5:115200:1
COM10:115200:1

**Figure 1: JAVAD TriVu Software**



```
%%create,/msg/def/binex/01_01:{1,0,0,0x2}
C:\Users\Jason Bond\Documents\Javad\jav
COM5:115200:1
```

**Figure 2: Loading a Javad Script File**

# 3. PC Setup

**I. General**

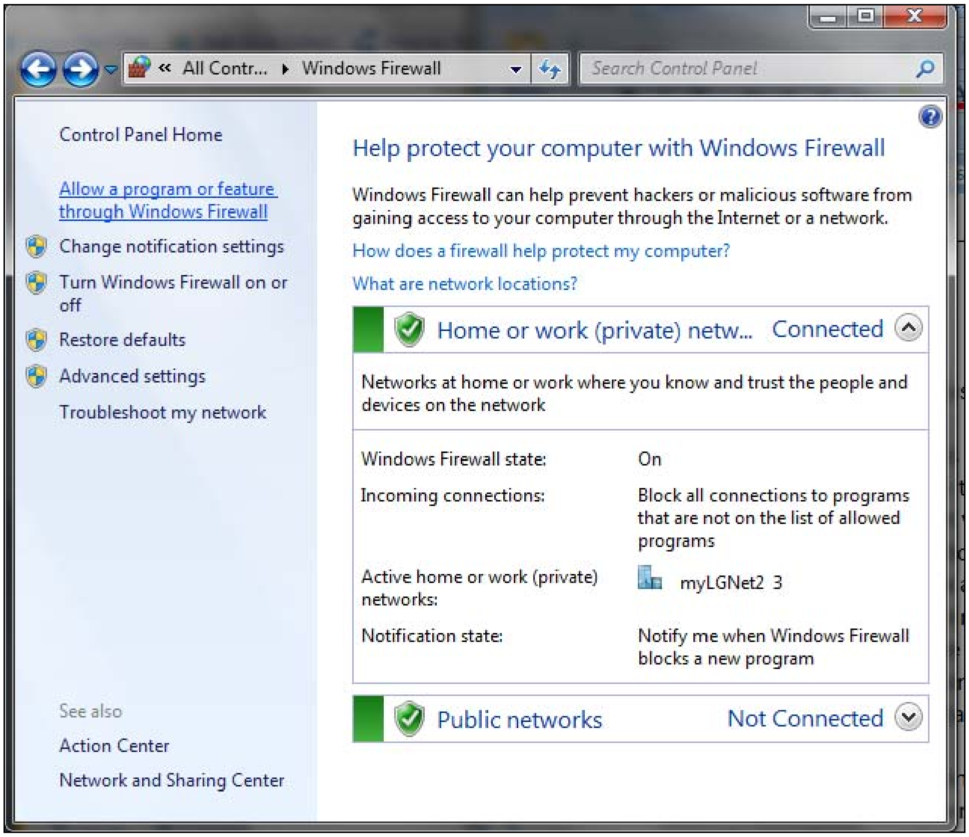
The following settings should be adjusted on the PC used to run GNT software:

1. If a wireless connection is being used, make sure that the PC is configured to automatically reconnect to the wireless network if connection is lost. It is strongly advised to remove any other wireless networks from the list of preferred networks.

2. The PCs power saving options should be configured such that it will not go into hibernation or standby mode after a certain period of time of inactivity. This will prevent the software from functioning. It is okay to turn the monitor off after a period of inactivity. Make sure that the hard disk does not get turned off.

3. Windows Firewall and Antivirus software should be configured to allow any serial-to-Ethernet devices to send data to the PC

   For Windows 7: From the Control Panel, Navigate to Windows Firewall. Select “Allow a program or feature through Windows Firewall” from the left hand panel (Figure 3). From the window, select “Allow another program…” (Figure 4). Select “Browse” and navigate to C:\Gemini\mmVu\PPMS_RT_GUIs.exe or C:\Program Files\Gemini Navsoft Technologies\RoverVU.exe (Figure 5).



Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Action Center

Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

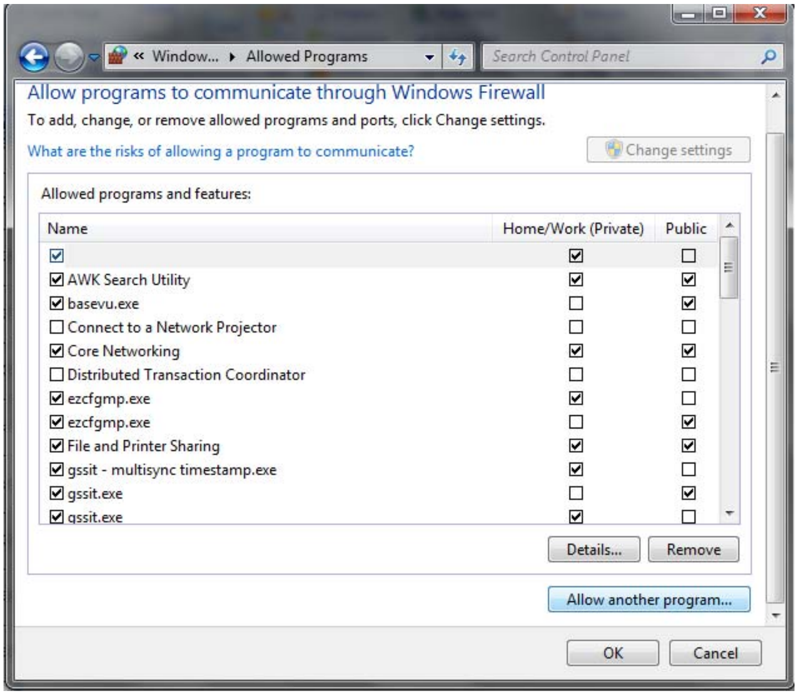
Home or work (private) netw... Connected

Networks at home or work where you know and trust the people and devices on the network

| | |
|---|---|
| Windows Firewall state: | On |
| Incoming connections: | Block all connections to programs that are not on the list of allowed programs |
| Active home or work (private) networks: | myLGNet2 3 |
| Notification state: | Notify me when Windows Firewall blocks a new program |

Public networks Not Connected

**Figure 3: Allowing mmVu to Communicate through Windows Firewall**



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

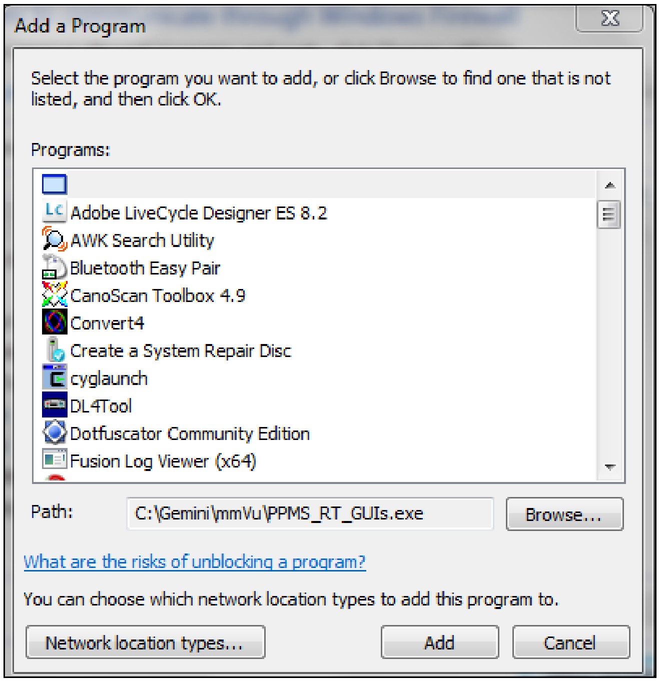
What are the risks of allowing a program to communicate?

Change settings

Allowed programs and features:

| Name | Home/Work (Private) | Public |
|---|---|---|
| ☑ | ☑ | □ |
| ☑ AWK Search Utility | ☑ | ☑ |
| ☑ basevu.exe | □ | ☑ |
| □ Connect to a Network Projector | □ | □ |
| ☑ Core Networking | ☑ | ☑ |
| □ Distributed Transaction Coordinator | □ | □ |
| ☑ ezcfgmp.exe | ☑ | □ |
| ☑ ezcfgmp.exe | □ | ☑ |
| ☑ File and Printer Sharing | ☑ | ☑ |
| ☑ gssit - multisync timestamp.exe | ☑ | □ |
| ☑ gssit.exe | □ | ☑ |
| ☑ gssit.exe | ☑ | □ |

**Figure 4: Select "Allow another program..."**



Add a Program

Select the program you want to add, or click Browse to find one that is not listed, and then click OK.

Path: C:\Gemini\mmVu\PPMS_RT_GUIs.exe

You can choose which network location types to add this program to.

Programs:
Adobe LiveCycle Designer ES 8.2
AWK Search Utility
Bluetooth Easy Pair
CanoScan Toolbox 4.9
Convert4
Create a System Repair Disc
cyglaunch
DL4Tool
Dotfuscator Community Edition
Fusion Log Viewer (x64)
Browse...
What are the risks of unblocking a program?
Network location types...
Add
Cancel

**Figure 5: Adding GNT Software to the Firewall Exception List**

Make sure the “Network location types” matches your network setup. Click “Add”.

4. IP addresses of serial-to-Ethernet devices and of the PC should be fixed so that Ethernet connections will resume if there is a power failure or other interruption of the router.

5. Install the latest Windows Updates.

6. Configure the PC for remote access.

## II. Automatic Login and Automatic Application Starting

To enable automatic starting of the application, Automatic Login must be enabled. Setting Automatic Login can only be done while logged on to an account with administrator privileges.

### Automatic Login:

To enable automatic login of the application when the computer boots up:

a. Type netplwiz in the search line of the Start Menu (Figure 6).
b. Check “Users must enter a user name and password to use this computer.” (Figure 7)
c. Select the user account name that you want to have automatically start up when the computer boots.
d. Uncheck the “Users must enter a user name and password to use this computer,” check box.
e. Click “OK”

f. Confirm Automatic Login by typing in your Username and Password (Figure 8).

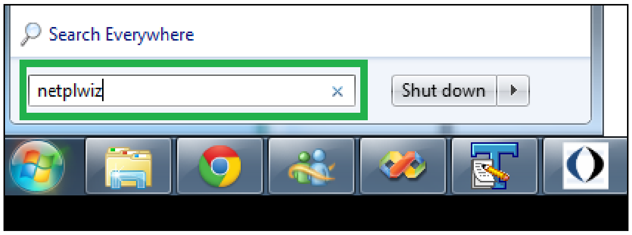
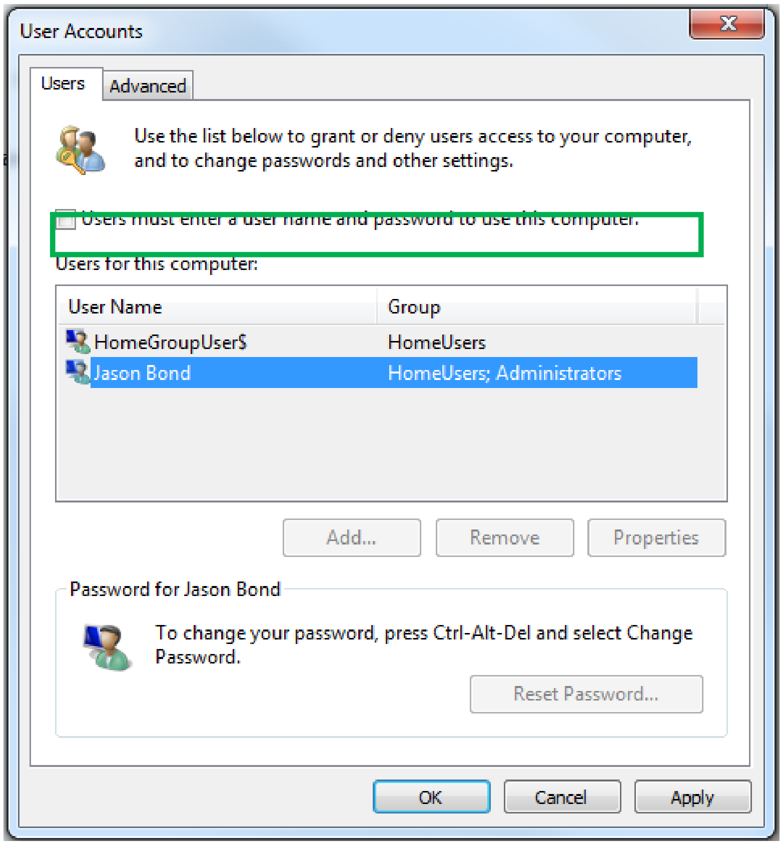


**Figure 6: Accessing User Account Settings**


User Accounts

Users | Advanced

Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

□ Users must enter a user name and password to use this computer.

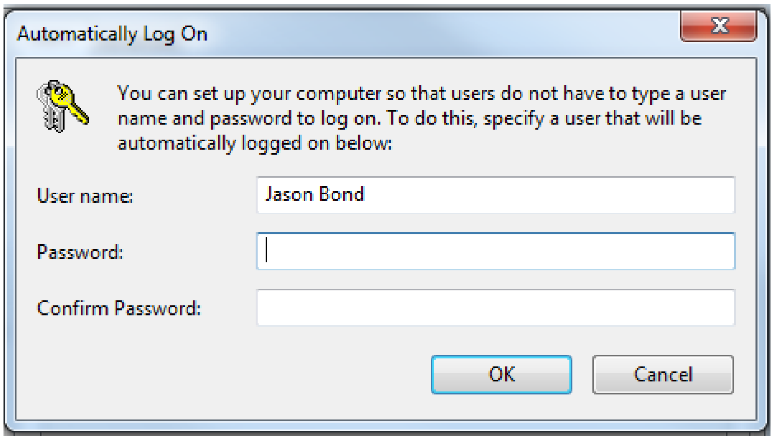
Users for this computer:

| User Name | Group |
|---|---|
| HomeGroupUser$ | HomeUsers |
| Jason Bond | HomeUsers; Administrators |

Password for Jason Bond

To change your password, press Ctrl-Alt-Del and select Change Password.

**Figure 7: Enabling Automatic Login**



Automatically Log On

You can set up your computer so that users do not have to type a user name and password to log on. To do this, specify a user that will be automatically logged on below:

User name: Jason Bond

Password:

Confirm Password:

**Figure 8: Confirming Automatic Login**

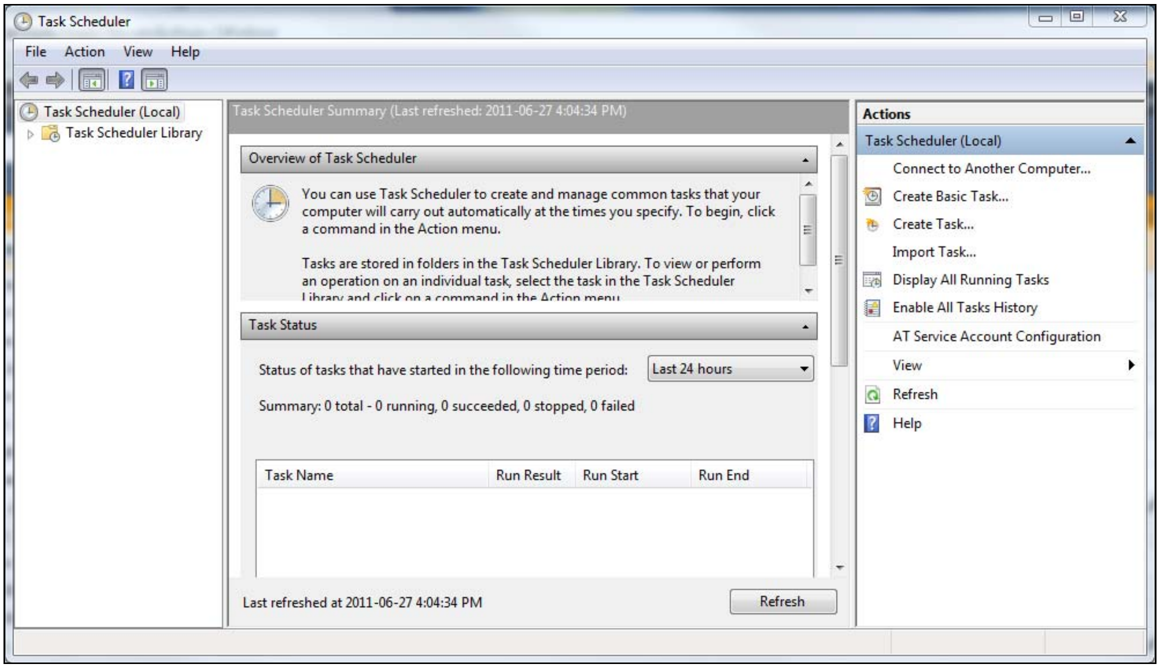
Enabling automatic login could pose a security risk if other people have access to the computer. If your computer logs in automatically, others may have access to that account.

**Automatic Application Starting:**

To enable the application to automatically start at boot up, a new task must be added to the task scheduler in Windows.

a. Select “Administrative Tools” from the Control Panel and select “Task Scheduler” (or simply type in “Task” in the Search Box of the Start Menu and select “Task Scheduler”.

b. Select “Create Task” from the Actions list (Figure 9).



Task Scheduler

Task Scheduler Summary (Last refreshed: 2011-06-27 4:04:34 PM)

Overview of Task Scheduler

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Tasks are stored in folders in the Task Scheduler Library. To view or perform an operation on an individual task, select the task in the Task Scheduler Library and click on a command in the Action menu.

Task Status

Status of tasks that have started in the following time period: Last 24 hours

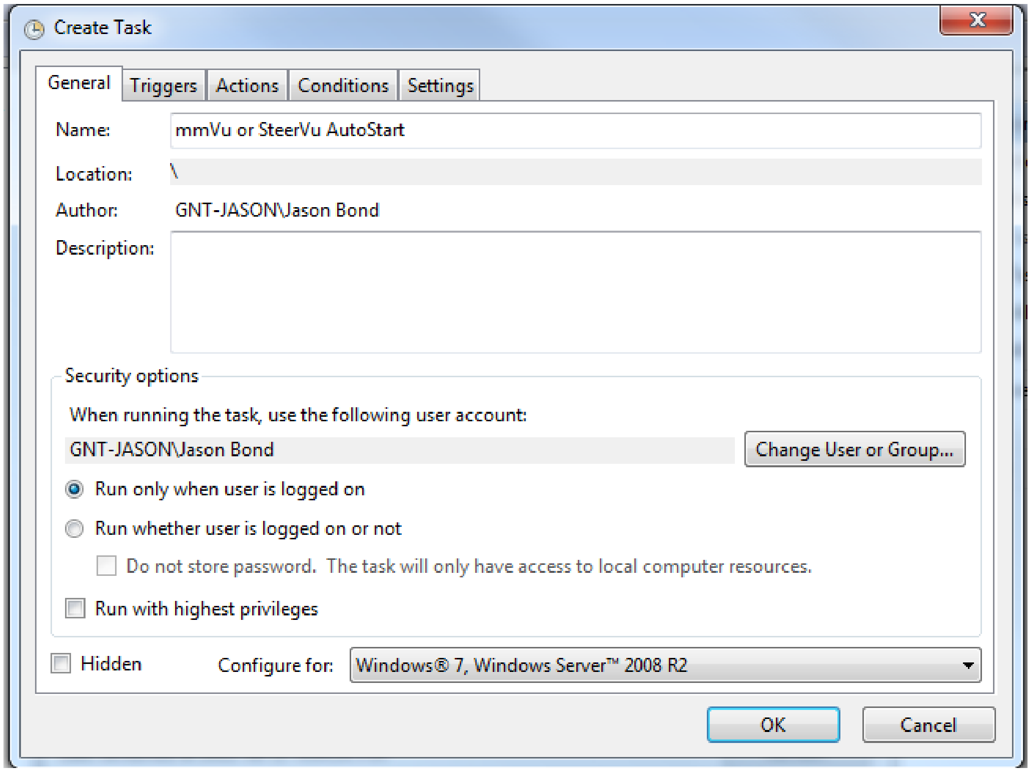
Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed

| Task Name | Run Result | Run Start | Run End |
|---|---|---|---|

Last refreshed at 2011-06-27 4:04:34 PM

**Figure 9: Windows Task Scheduler**

c. Under the "General" tab, type a name for the Task. Select the operation system being used (Figure 10).



Name: mmVu or SteerVu AutoStart

Location: \

Author: GNT-JASON\Jason Bond

Description:

Security options

When running the task, use the following user account:

GNT-JASON\Jason Bond

● Run only when user is logged on

○ Run whether user is logged on or not

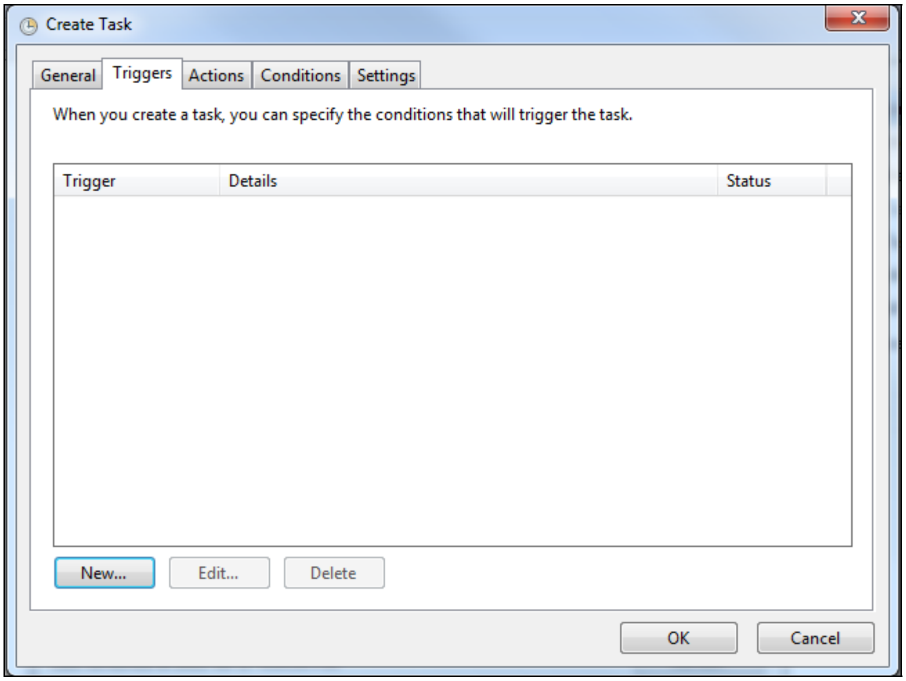
□ Do not store password. The task will only have access to local computer resources.

□ Run with highest privileges

□ Hidden Configure for: Windows® 7, Windows Server™ 2008 R2

**Figure 10: Creating a Task – General**

d. Under the "Triggers" tab, select "New" (Figure 11).

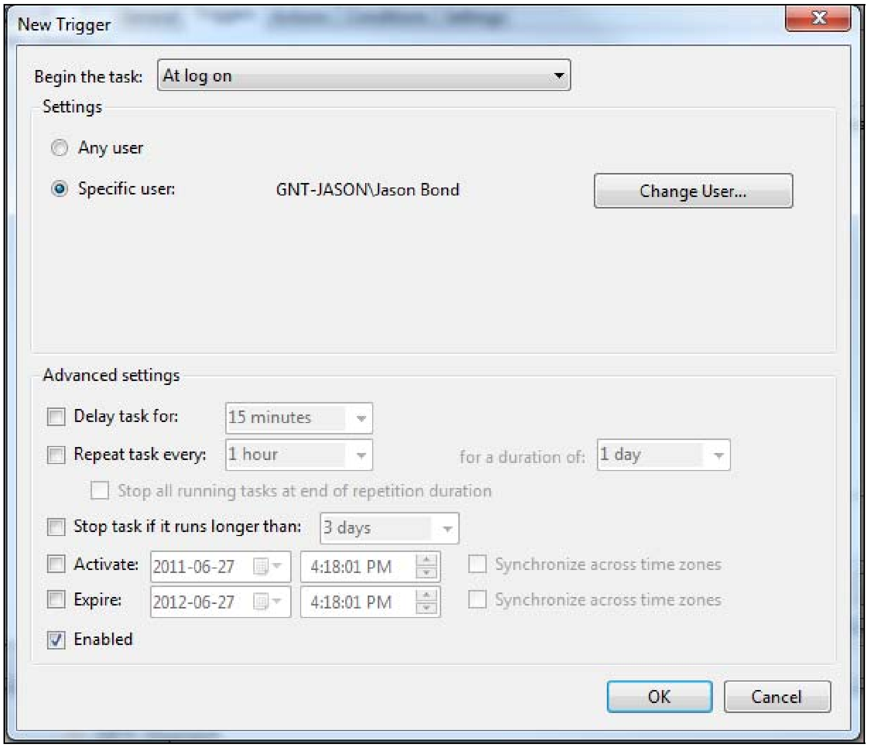


When you create a task, you can specify the conditions that will trigger the task.

| Trigger | Details | Status |
|---|---|---|

**Figure 11: Configuring a Task – Triggers**

e. Select Begin the task: “At log on”. Specify the user account (Figure 12).



Begin the task: At log on

Settings

○ Any user

● Specific user: GNT-JASON\Jason Bond

Advanced settings

□ Delay task for: 15 minutes

□ Repeat task every: 1 hour    for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

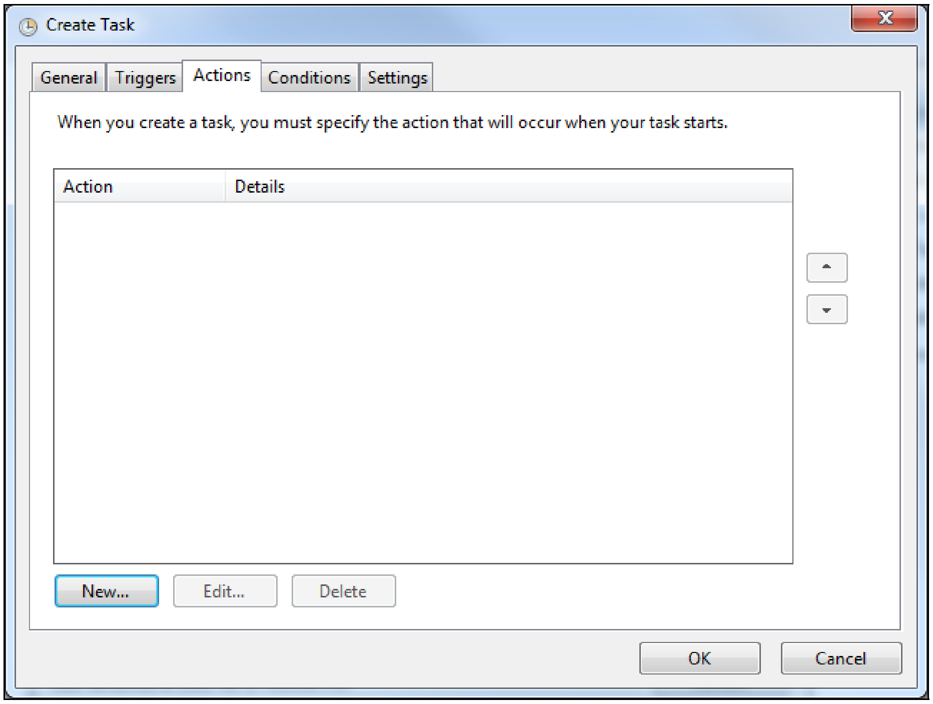
□ Activate: 2011-06-27 4:18:01 PM □ Synchronize across time zones

□ Expire: 2012-06-27 4:18:01 PM □ Synchronize across time zones

☑ Enabled

**Figure 12: Configuring a Task - New Trigger**

f. Under the “Actions” tab, select “New” (Figure 13).



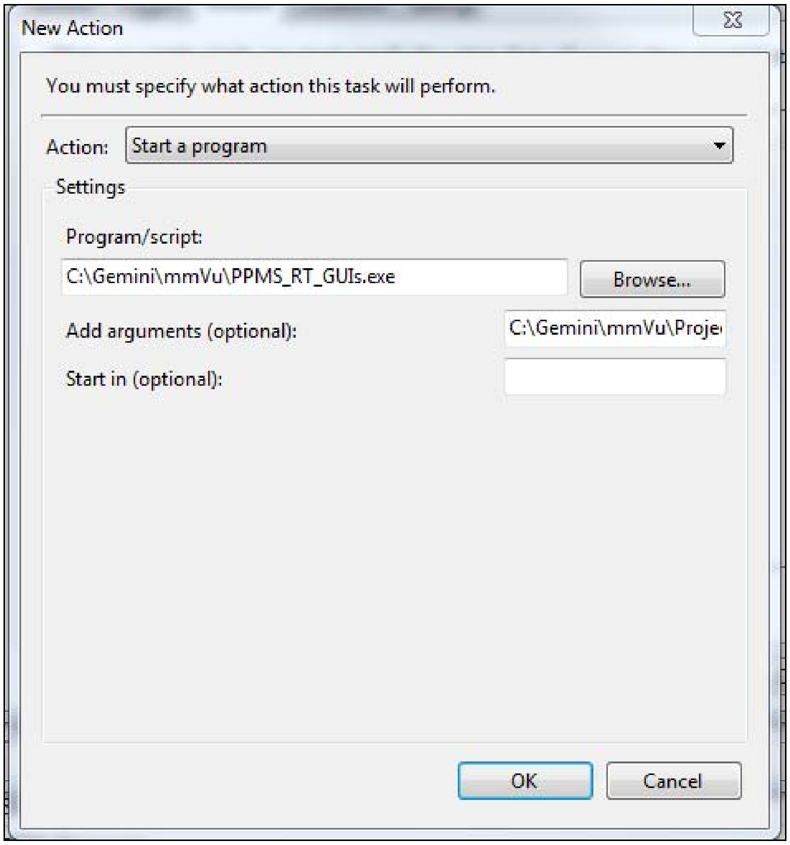
Create Task

When you create a task, you must specify the action that will occur when your task starts.

| Action | Details |
|---|---|

**Figure 13: Configuring a Task - Actions**

g. Select “Start a program” as the Action. Specify “C:\Gemini\mmVu\PPMS_RT_GUIs.exe” for mmVu as the Program (Figure 14). Specify the full path of the project that you wish to start as an argument. Enclose the path in quotation marks (E.g., "C:\Gemini\mmVu\Projects\Test.mVu")



You must specify what action this task will perform.

Action: Start a program

Settings

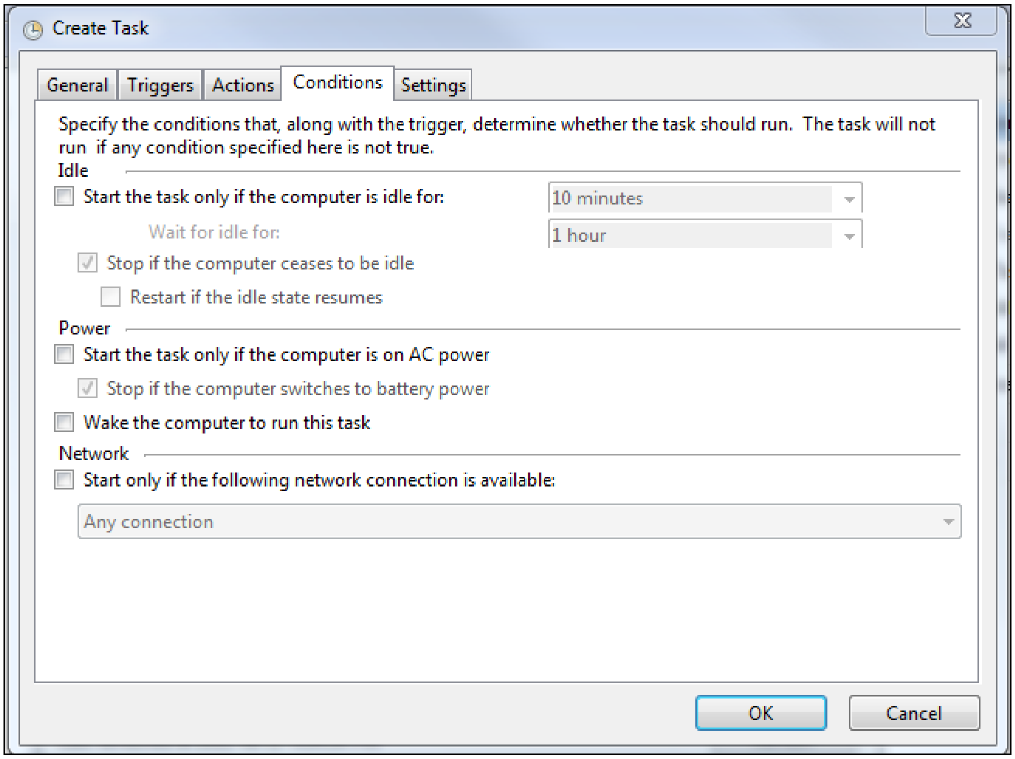
Program/script: C:\Gemini\mmVu\PPMS_RT_GUIs.exe

Add arguments (optional): C:\Gemini\mmVu\Proje

Start in (optional):

**Figure 14: Configuring a Task - New Action**

h. Under the “Conditions” tab, deselect “Start the task only if the computer is on AC power” (Figure 15).



Create Task

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

☐ Start the task only if the computer is idle for: 10 minutes

Wait for idle for: 1 hour

☑ Stop if the computer ceases to be idle

☐ Restart if the idle state resumes

Power

☐ Start the task only if the computer is on AC power

☑ Stop if the computer switches to battery power

☐ Wake the computer to run this task

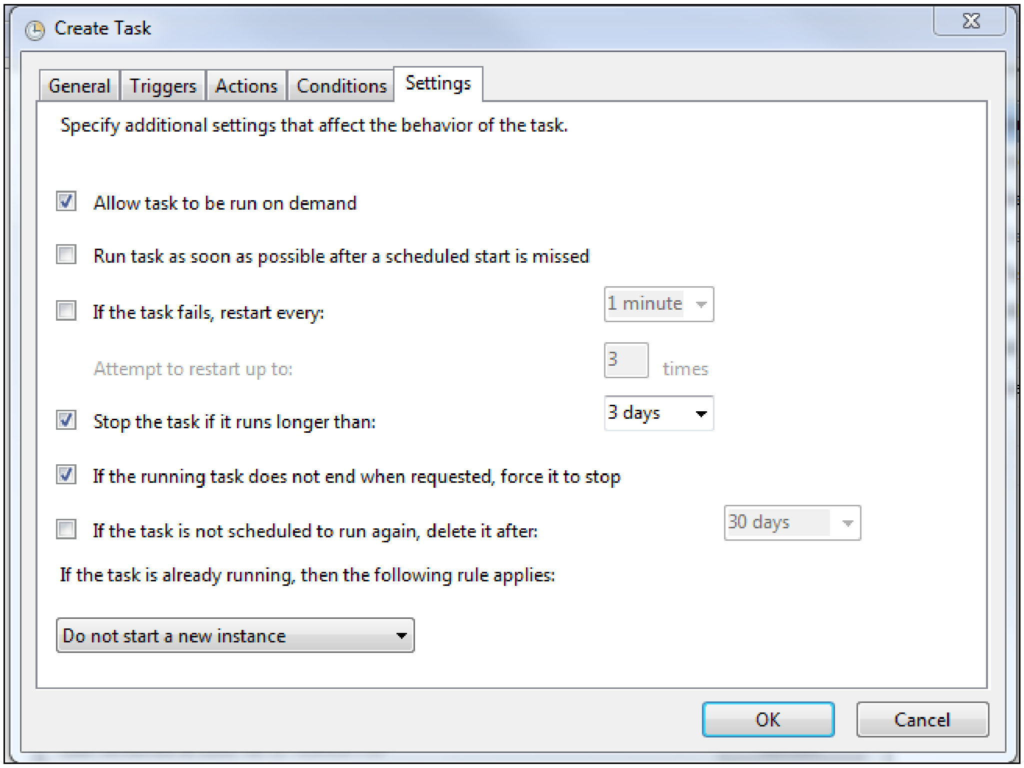
Network

☐ Start only if the following network connection is available:

Any connection

**Figure 15: Configuring a Task – Conditions**

i. Under the "Settings" tab, deselect "Stop the task if it runs longer than 3 days" (Figure 16).



Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

□ Run task as soon as possible after a scheduled start is missed

□ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

□ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

**Figure 16: Creating a Task - Settings**

j. Click “OK” and test.

### III. Configuring the PC Boot Sequence

In some cases having peripheral devices (such as USB keys) attached to your PC at boot up may prevent automatic application starting. Any potential conflict should be avoided. For example, the boot sequence for Lenovo computers is often set to:

a. FDD
b. USB FDD
c. USB Key
d. HDD
e. CD/DVD
f. Network

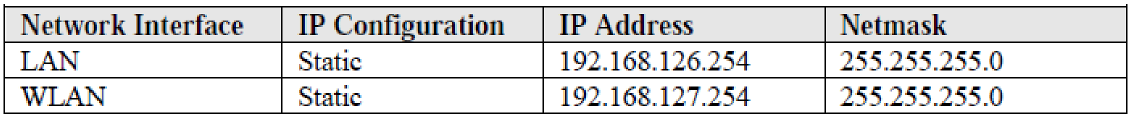
The computer will not automatically start the application in this case with a USB key connected. For such situations remove b) and c) from the list. Make sure that the boot sequence on your PC won’t cause unexpected results. The BIOS of the PC will need to be entered to alter the boot sequence. Contact your PC manufacturer to determine how to enter the system BIOS.

# 4. Moxa Communications Hardware

### I. Moxa NPortW2150 Serial-to-Ethernet Device Setup

The following procedure should be used when setting up an NPortW2150 device:

1. Setup your PC WLAN or LAN Ethernet adapter so that it is on the same subnet as the NPort. The Windows Network Properties form should be closed to commit the new IP information to memory. The factory default IP settings are:



| Network Interface | IP Configuration | IP Address | Netmask |
|---|---|---|---|
| LAN | Static | 192.168.126.254 | 255.255.255.0 |
| WLAN | Static | 192.168.127.254 | 255.255.255.0 |

   The IP address can be set for you PC by navigating to Network Connections in the Control Panel, right clicking on the Local Area Connection and clicking on Properties. Select Protocol Version 4 and click Properties (Figure 28). The Windows Network Properties form should be closed to commit the new IP information to memory.

| ⚠ | If you are unable to bring up the Web Console for the NPort:<br>a) verify that your IP address is what you think it is by typing in ipconfig/all at the command prompt in MS-DOS (type cmd in the box at the bottom of the Start menu to bring up the command prompt). You will see the current IP address of your PC's network interfaces b) verify the IP address of the NPort buy using the MOXA NPort search utility. |
|---|---|

2. If using LAN, plug the Ethernet cable in before applying power. WLAN/LAN mode cannot be changed once the device is powered on.

3. Using your web browser, type in the address of the NPort to bring up the Web Console. Load the latest firmware for your device. Contact Moxa to ensure the latest firmware is available from their website.

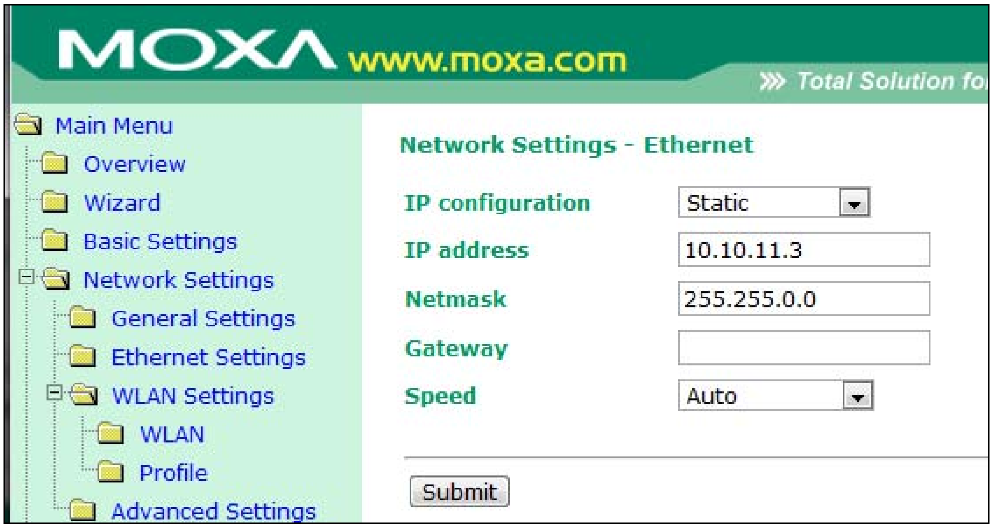
4. Assign critical settings:

   a. **IP Address**: If an existing network will be used, contact you network administrator to obtain an IP address for your device. When creating your own local network, the suggested IP naming system is: 10.10.0ND.### where:

      N = Network connection type (1 = LAN, 2 = WLAN)
      D = Device type (1 = GPS receiver or directly connected device, 2 = PC, 3 = Access Point)
      # = Unique identifying number (range is from 0 – 255)

The Net Mask should be 255.255.0.0. IP Addresses should be static. Both LAN and WLAN address should be assigned.

⚠ When using the Web Console, all changes must be submitted before moving on to the next page. Once all changes have been submitted, the device must be restarted to commit them.



Network Settings - Ethernet

IP configuration: Static
IP address: 10.10.11.3
Netmask: 255.255.0.0
Gateway:
Speed: Auto

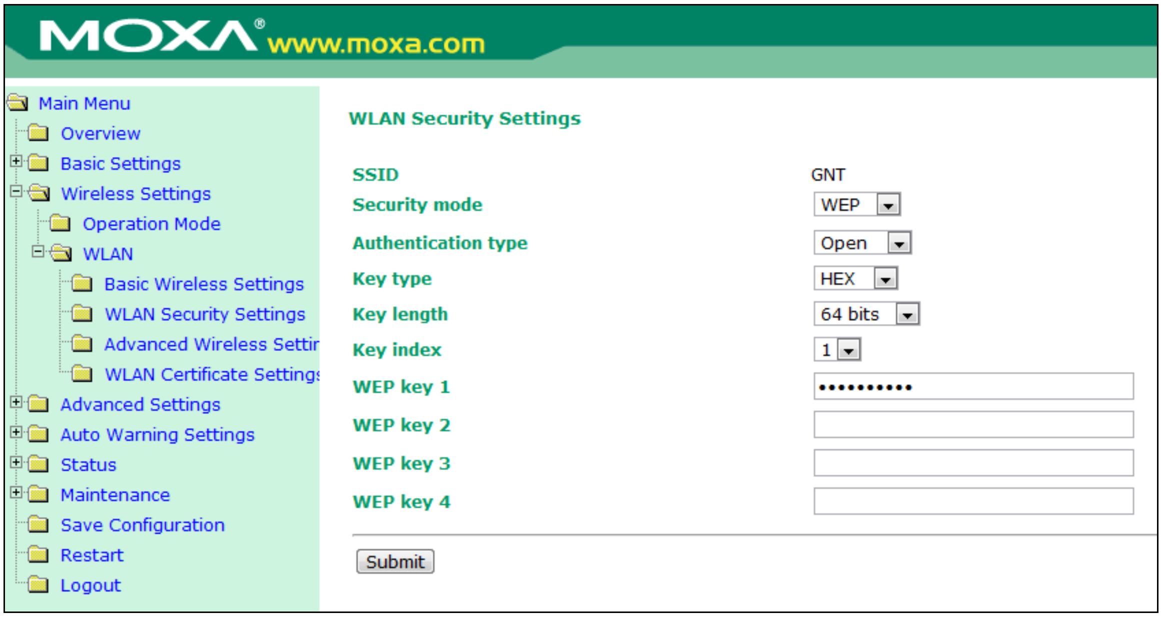
**Figure 17: Configuring NPort IP Address**

b. **Wireless LAN Profile**:

   i. Set **Network Type** to Infrastructure Mode or Ad-hoc Mode. Devices that are configured for Ad-hoc Mode automatically detect and communicate directly with each other and do not require a wireless access point (AP) or gateway. Wireless devices that are configured for Infrastructure Mode do not communicate directly with each other, but through a wireless access point (AP).

   ii. Set Profile1's **SSID** to the SSID of your network.

   iii. Set Profile1's **Security Properties** (Figure 18). If Moxa AWK-4121 access points are used and WDS mode is employed, only WEP shared keys are permitted.

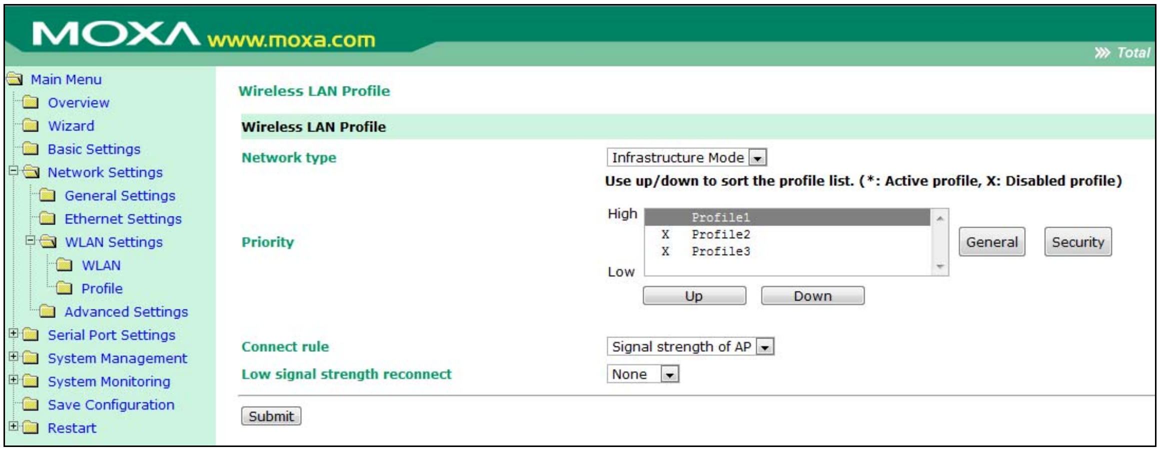


WLAN Security Settings

| | |
|---|---|
| SSID | GNT |
| Security mode | WEP |
| Authentication type | Open |
| Key type | HEX |
| Key length | 64 bits |
| Key index | 1 |
| WEP key 1 | •••••••••• |
| WEP key 2 | |
| WEP key 3 | |
| WEP key 4 | |

**Figure 18: NPort W2150 Plus Security Properties**

iv. Make sure Profile2 and Profile3 are **disabled**.
v. Set the **Connect Rule** to Signal Strength of AP
vi. Set the **Low Signal Strength Reconnect** to None.



Wireless LAN Profile

**Wireless LAN Profile**

Network type: Infrastructure Mode

Use up/down to sort the profile list. (*: Active profile, X: Disabled profile)

Priority:

High
```
  Profile1
X Profile2
X Profile3
```
Low

General | Security

Up | Down

Connect rule: Signal strength of AP

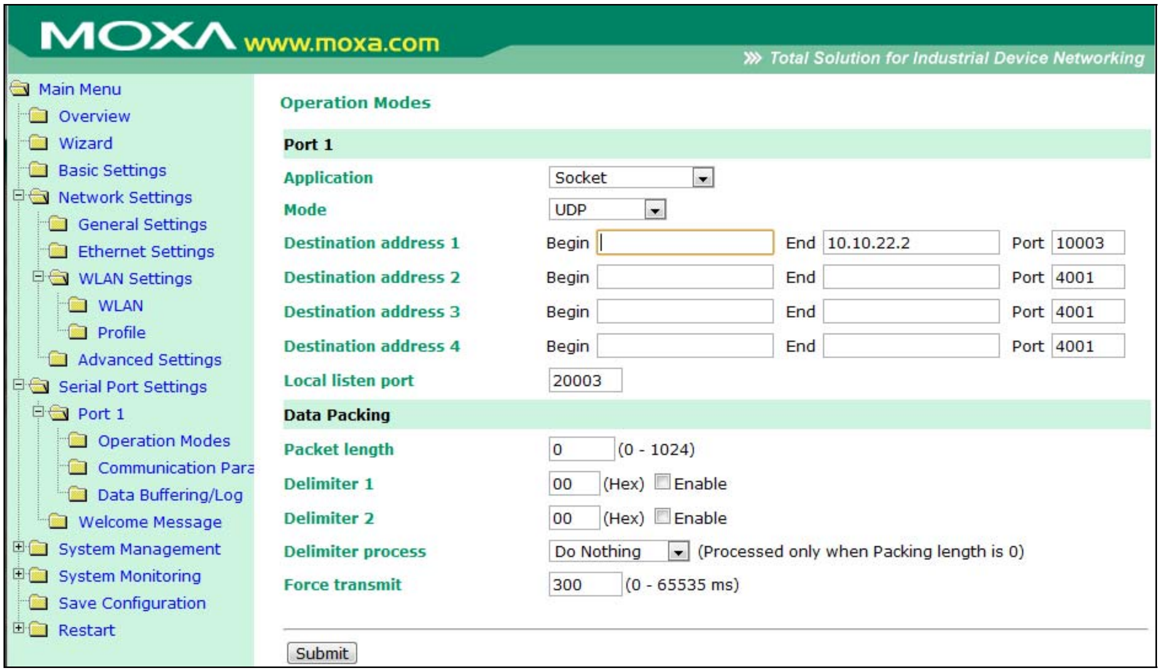
Low signal strength reconnect: None

Submit

**Figure 19: Configuring NPort W2150 Plus Wireless LAN Profile**

c. **Serial Port:** For each serial port:

i. Set **Application** to Socket (Figure 20)



Operation Modes

**Port 1**

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Socket | | | | | |
| Mode | UDP | | | | | |
| Destination address 1 | Begin | | End | 10.10.22.2 | Port | 10003 |
| Destination address 2 | Begin | | End | | Port | 4001 |
| Destination address 3 | Begin | | End | | Port | 4001 |
| Destination address 4 | Begin | | End | | Port | 4001 |
| Local listen port | 20003 | | | | | |

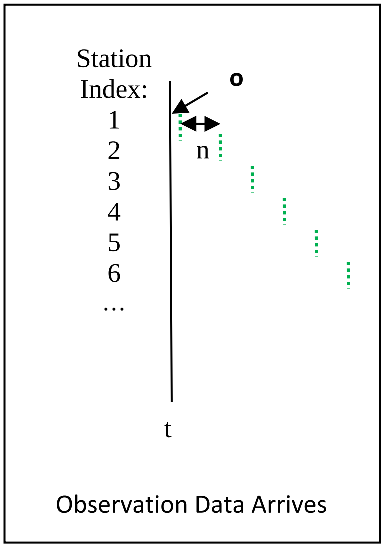
**Data Packing**

| | | |
|---|---|---|
| Packet length | 0 | (0 - 1024) |
| Delimiter 1 | 00 | (Hex) □ Enable |
| Delimiter 2 | 00 | (Hex) □ Enable |
| Delimiter process | Do Nothing | (Processed only when Packing length is 0) |
| Force transmit | 300 | (0 - 65535 ms) |

Submit

**Figure 20: Configuring NPort W2150 Plus Serial Port Settings**

ii. Set **Mode** to UDP or TCP, depending on application. If UDP, specify the IP address of destination PC and the port number of the PC. Specify the local listening port number (to simply, keep the same for all NPort devices. E.g., 50000). **Data Packing** parameters are very important in determining how data gets transmitted from the receiver. Ideally, data from the receiver will get sent in complete packets and the data will arrive at the PC at different moments from each NPort (because all receivers are synchronized to GPS Time, if there is no offset then all data could arrive at the PC simultaneously. In UDP mode, there is no second chance to recover data that was not received after the first transmission. The Data Packing strategy should be based upon Forced Transmit time. The forced transmit time for each station should be calculated based upon baud rate settings, and the maximum packet size (in bytes) for the data logs. An initial offset must be calculated that allows a delay of at least as long as it takes one character to arrive. An offset between stations must also be calculated to stagger the arrival of data packets at the PC. Figure 21 illustrates the concept. The maximum offset permitted is 65535. The maximum station offset should never exceed the sample rate of the receiver. This would be a concern if a station offset of 60000 ms or greater was used and the sample rate of the receiver was 1s or higher. The station offset for any station can be calculate as: o + (station index -1) x n



**o** = initial offset from t, giving enough time to detect a delay between received messages

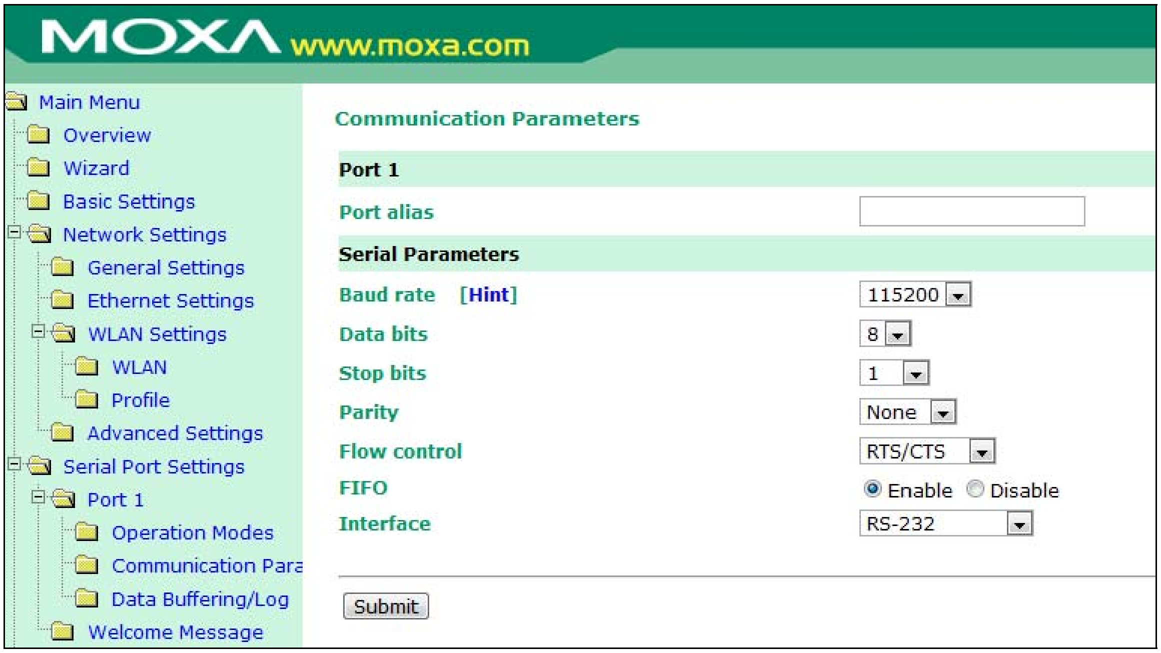
o = 10 [bits/byte] / baud rate [bits per second]
(E.g., o = 0.087 ms at 115,200 bps, so round up to 1 or 2 ms)

**n** = station offset in ms between each station’s transmission

n = (max packet size [bytes] x # bits per byte) / baud rate [bits per second]
(E.g., n = 87 ms when 1000 byte packet, 10 bit/byte, 115,200bps, round up to 100 ms)

**Figure 21: Calculating NPort Force Transmit Times**

iii. Set Communication Parameters to match that of the GPS receiver, as illustrated in Figure 20.



Communication Parameters

Port 1

Port alias

Serial Parameters

Baud rate [Hint]: 115200

Data bits: 8

Stop bits: 1

Parity: None

Flow control: RTS/CTS

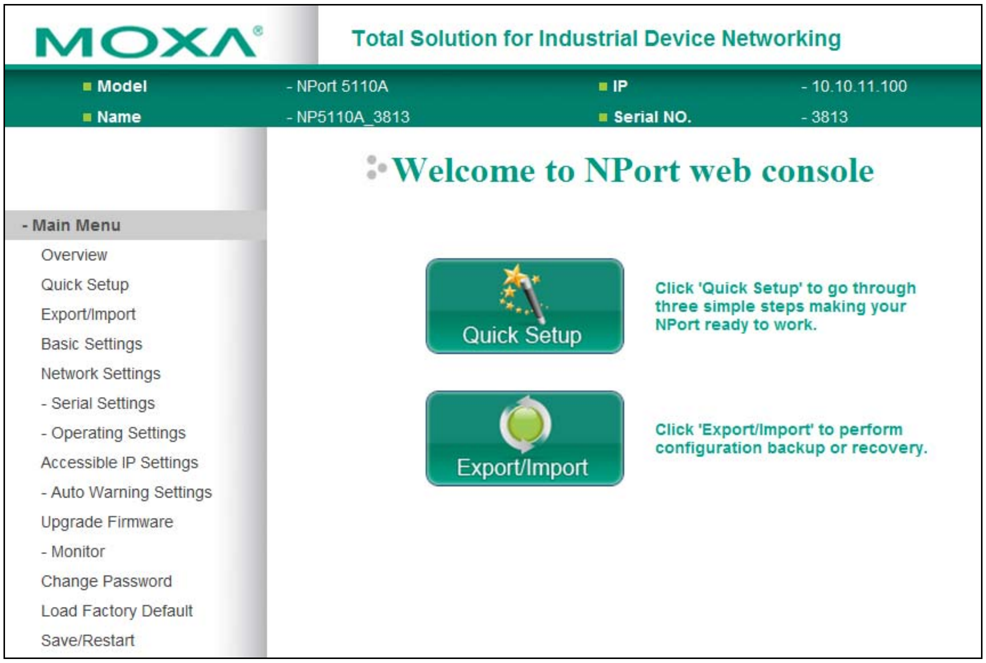
FIFO: ● Enable ○ Disable

Interface: RS-232

**Figure 22: Setting NPort W2150 Plus Communication Parameters**

## II. Moxa NPort 5110A Serial-to-Ethernet Device Setup

The NPort 5110A should be configured similarly to the NPort 2150W described above. The web console is slightly different as it employs a 3 step approach for ease of configuration (Figure 23). Unfortunately, all critical parameters cannot be set using the 3 step wizard. The wizard can be utilized to set general settings and then remaining parameters must be set. Alternatively, you can manually go through each setting to mimic the procedure described for the NPort W2150 Plus. Described is a setup approach which uses the Quick Setup procedure plus one additional step.



Total Solution for Industrial Device Networking

| | | | |
|---|---|---|---|
| Model | - NPort 5110A | IP | - 10.10.11.100 |
| Name | - NP5110A_3813 | Serial NO. | - 3813 |

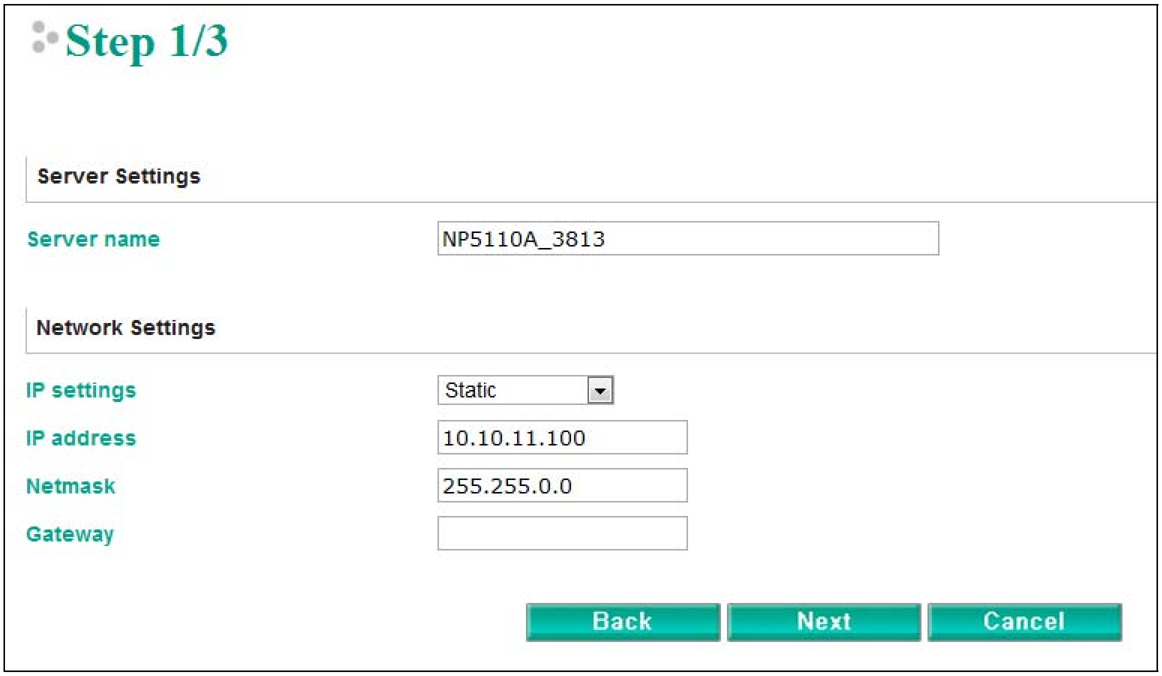
Welcome to NPort web console

Click 'Quick Setup' to go through three simple steps making your NPort ready to work.

Click 'Export/Import' to perform configuration backup or recovery.

**Figure 23: NPort 5110A Web Console**

Using the Quick Setup wizard, input the IP address and network mask for your device at Step 1 (Figure 24).



Step 1/3

Server Settings

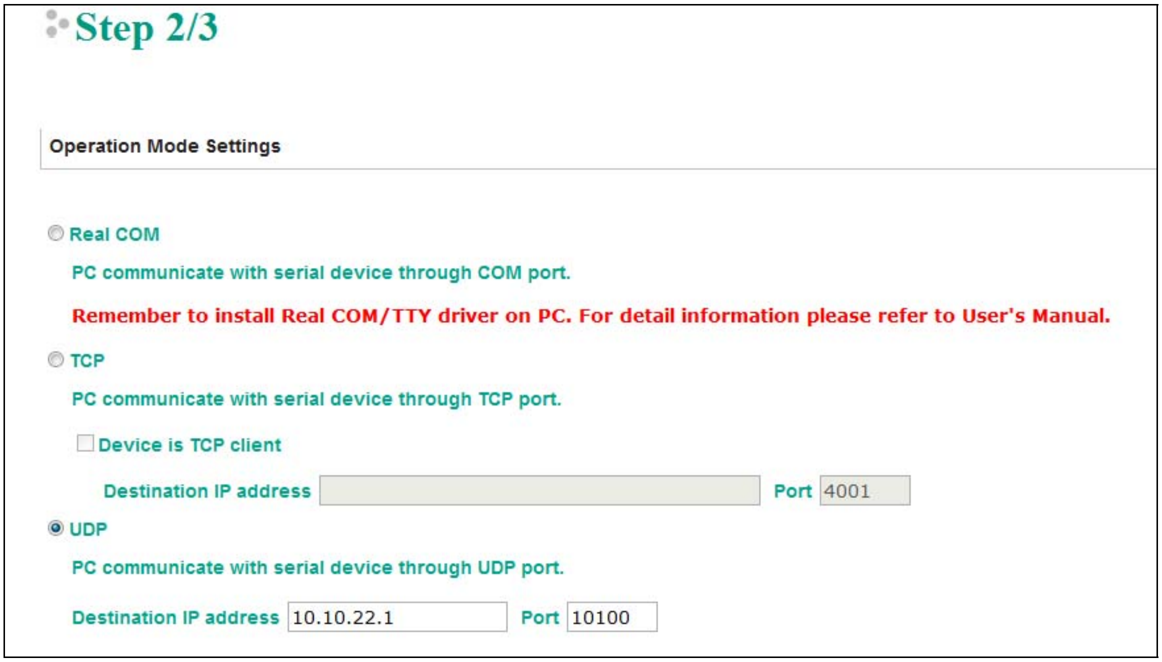
| | |
|---|---|
| Server name | NP5110A_3813 |

Network Settings

| | |
|---|---|
| IP settings | Static |
| IP address | 10.10.11.100 |
| Netmask | 255.255.0.0 |
| Gateway | |

**Figure 24: Step 1/3 of NPort 5110A Setup**

At Step 2, select UDP and enter the destination IP Address and Port number (Figure 25).



Step 2/3

Operation Mode Settings

○ Real COM

PC communicate with serial device through COM port.

Remember to install Real COM/TTY driver on PC. For detail information please refer to User's Manual.

○ TCP

PC communicate with serial device through TCP port.

□ Device is TCP client

Destination IP address: | Port: 4001

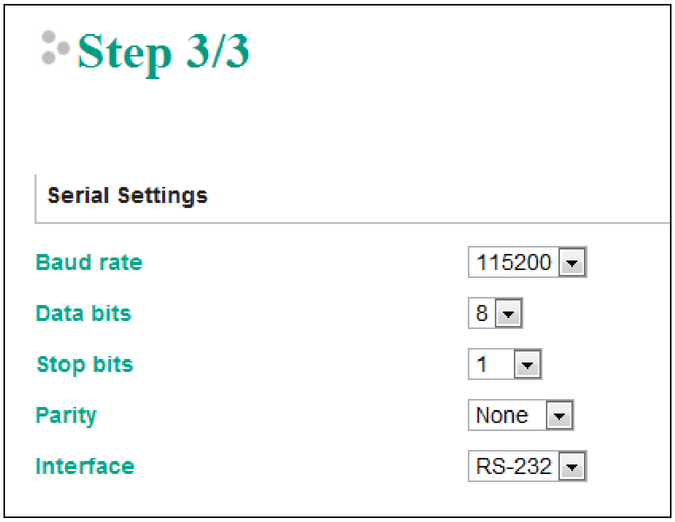
● UDP

PC communicate with serial device through UDP port.

Destination IP address: 10.10.22.1 | Port: 10100

**Figure 25: Step 2/3 of NPort 5110A Setup**

At Step 3, configure the serial port settings (Figure 26)



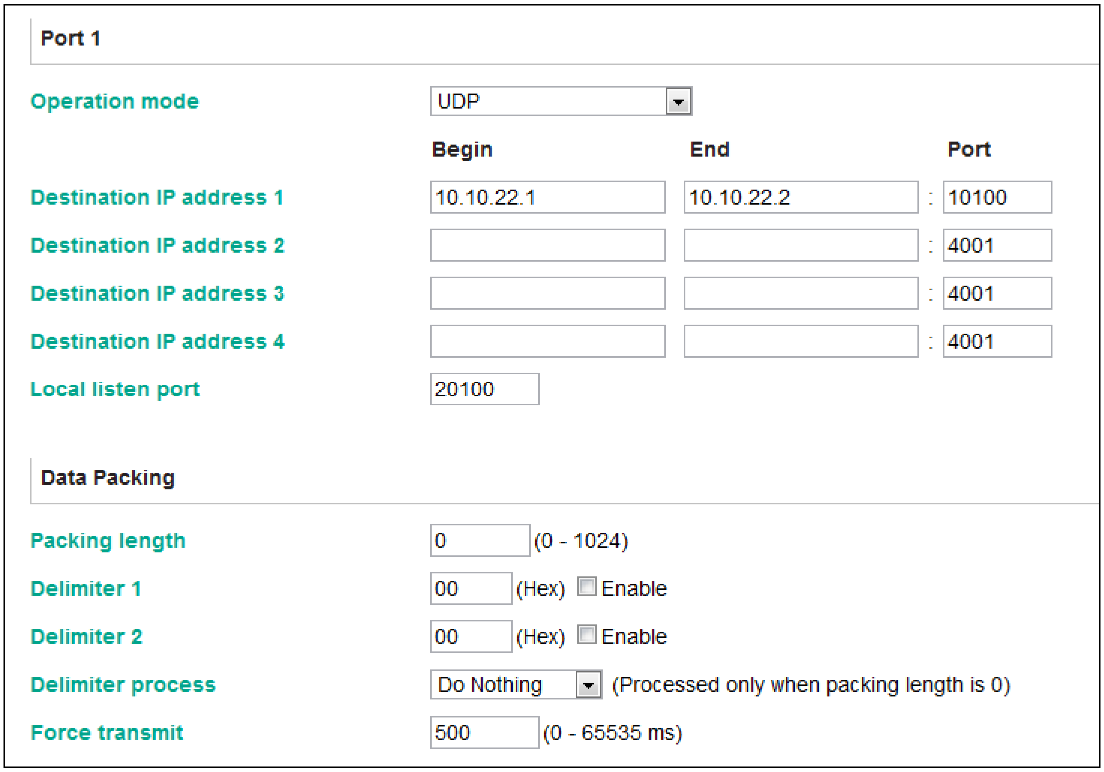
Step 3/3

Serial Settings

| | |
|---|---|
| Baud rate | 115200 |
| Data bits | 8 |
| Stop bits | 1 |
| Parity | None |
| Interface | RS-232 |

**Figure 26: Step 3/3 of NPort 5110A Setup**

At this point, parameters have not been specified for transmitting data in UDP mode. You must click on Operating Settings – Port 1 to input this information (Figure 27). Input a transmit time based upon the discussion found in the NPort W2150 Plus setup procedure.



**Port 1**

| | | | |
|---|---|---|---|
| Operation mode | UDP ▾ | | |
| | Begin | End | Port |
| Destination IP address 1 | 10.10.22.1 | 10.10.22.2 | : 10100 |
| Destination IP address 2 | | | : 4001 |
| Destination IP address 3 | | | : 4001 |
| Destination IP address 4 | | | : 4001 |
| Local listen port | 20100 | | |

**Data Packing**

| | |
|---|---|
| Packing length | 0 (0 - 1024) |
| Delimiter 1 | 00 (Hex) □ Enable |
| Delimiter 2 | 00 (Hex) □ Enable |
| Delimiter process | Do Nothing ▾ (Processed only when packing length is 0) |
| Force transmit | 500 (0 - 65535 ms) |

**Figure 27: Additional Step of NPort 5110A Setup**

Setup is complete.

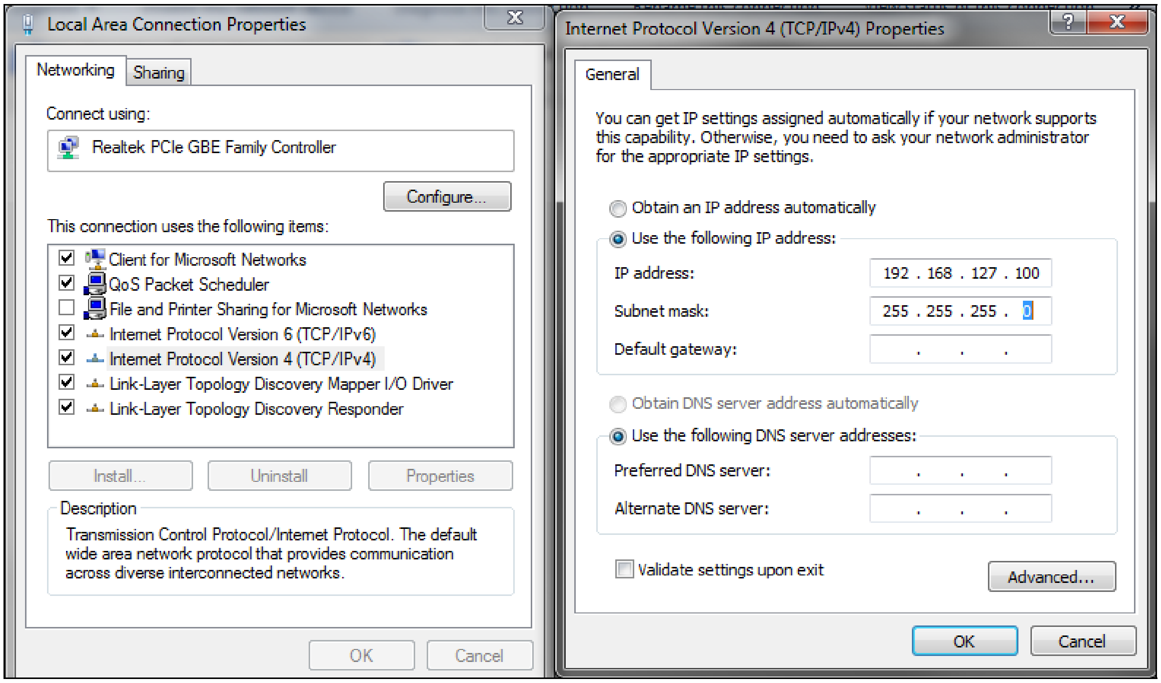
Since the NPort 5110A is a wired device, wireless security parameters do not need to be entered like the NPort W2150 Plus.

### III. Moxa AWK-4121 (and AWK-3121) Access Point Setup

The following procedure should be used when setting up an NPortW2150 device:

1. Setup your PC WLAN or LAN Ethernet adapter so that it is on the same subnet as the NPort. The factory default IP address is 192.168.127.253 and the subnet mask is 255.255.255.0. Your PC IP address should be set to 192.168.127.xxx (not 253). The IP address can be set for you PC by navigating to Network Connections in the Control Panel, right clicking on the Local Area Connection and clicking on Properties. Select Protocol Version 4 and click Properties (Figure 28). The Windows Network Properties form should be closed to commit the new IP information to memory.

If you are unable to bring up the Web Console for the AWK-4121:
a) verify that your IP address is what you think it is by typing in ipconfig/all at the command prompt in MS-DOS (type cmd in the box at the bottom of the Start menu to bring up the command prompt). You will see the current IP address of your PC's network interfaces b) verify the IP address of the AWK-4121, buy using the MOXA AWK-4121 search utility.



Connect using:

Realtek PCIe GBE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☐ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 127 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

**Figure 28: Setting Your PC's IP Address**

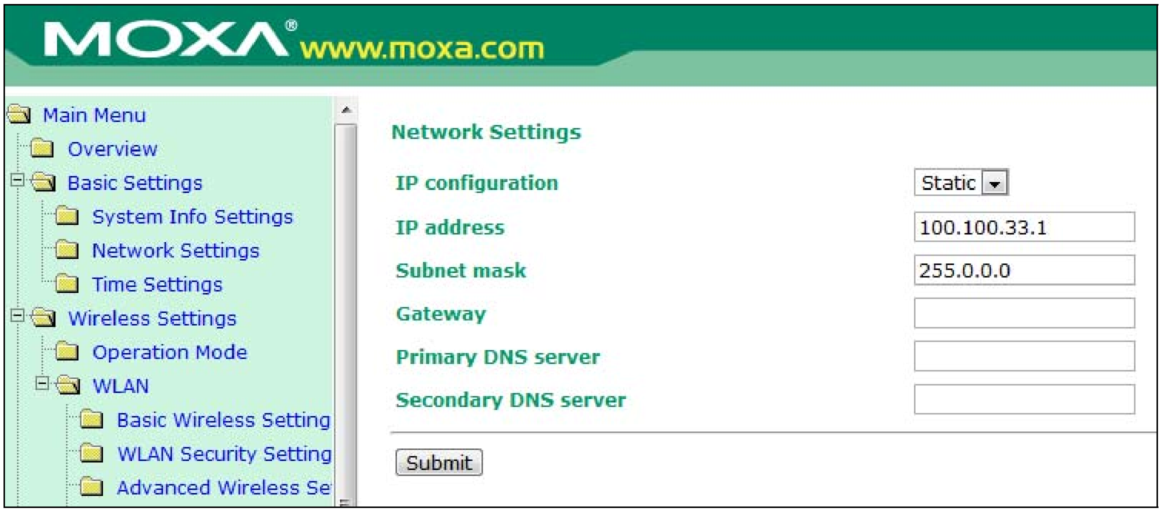
2. Using your web browser, type in the address of the AWK-4121 to bring up the Web Console. Load the latest firmware for your device. Contact Moxa to ensure the latest firmware is available from their website.

3. Assign critical settings:
   a. **Basic Settings|Network Settings**: If an existing network will be used, contact you network administrator to obtain an IP address for your device. When creating your own local network, the suggested IP naming system is: 10.10.0ND.### where:

      N = Network connection type (1 = LAN, 2 = WLAN, 3 = Both)
      D = Device type (1 = GPS receiver or directly connected device, 2 = PC, 3 = Access Point)
      # = Unique identifying number (range is from 0 – 255)

      The Netmask should be 255.255.0.0. IP Addresses should be static. Both LAN and WLAN address should be assigned. Figure 29 illustrates setting the IP address of the AWK-4121

When using the Web Console, all changes must be submitted before moving on to the next page. Once all changes have been submitted, the device must be restarted to commit them.

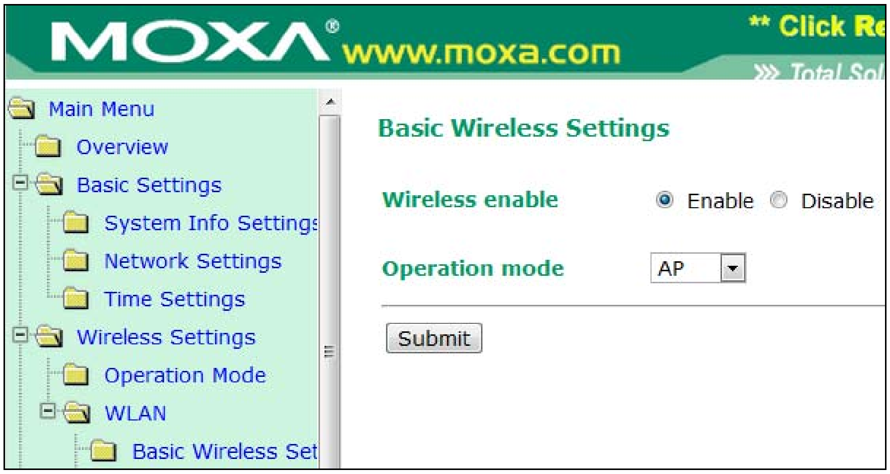


Network Settings

| | |
|---|---|
| IP configuration | Static |
| IP address | 100.100.33.1 |
| Subnet mask | 255.0.0.0 |
| Gateway | |
| Primary DNS server | |
| Secondary DNS server | |

**Figure 29: Setting AWK-4121 IP Address**

b. **Wireless Settings|Operation Mode**: Wireless enable selected and Operation mode = AP



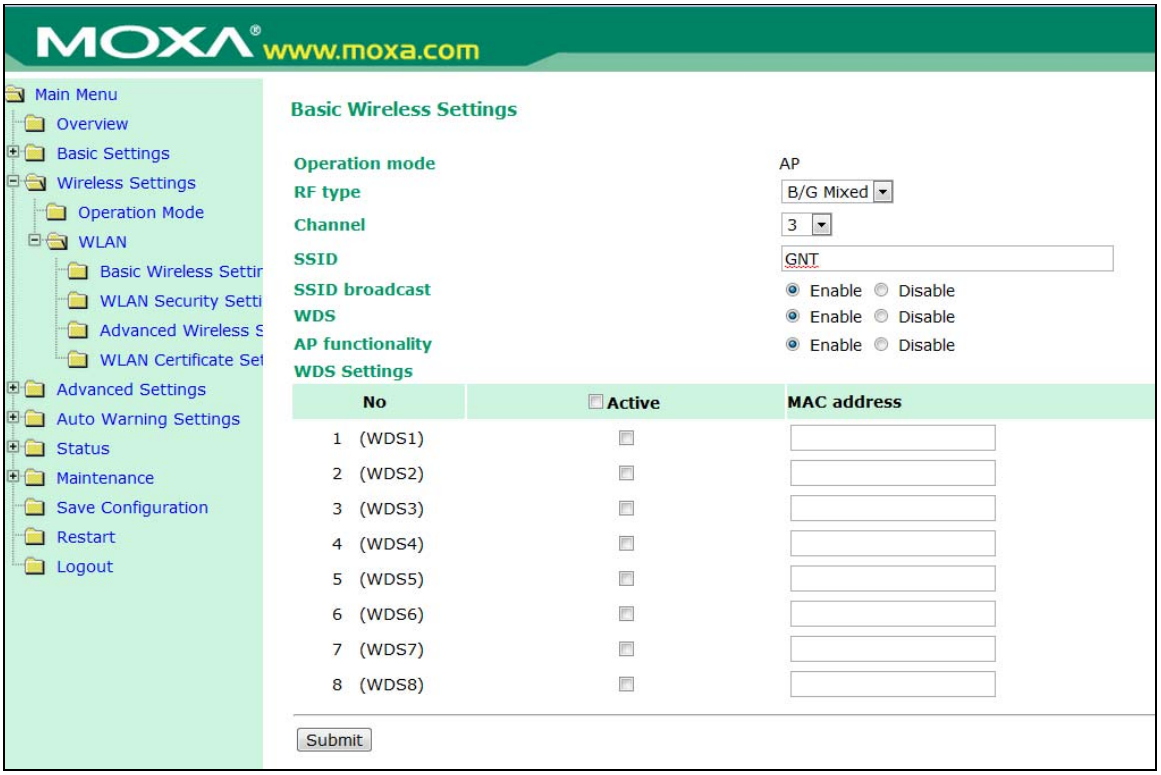
Basic Wireless Settings

Wireless enable ● Enable ○ Disable

Operation mode AP

**Figure 30: Setting Basic Wireless Settings**

c. **WLAN|Basic Wireless Settings**: Click "Edit". Set the Channel to a value not in use in the application area (6 is commonly used). Set the SSID for your network. If using multiple AWK-4121s, enable WDS mode and specify the MAC addresses of the other AWK-4121s.



Basic Wireless Settings

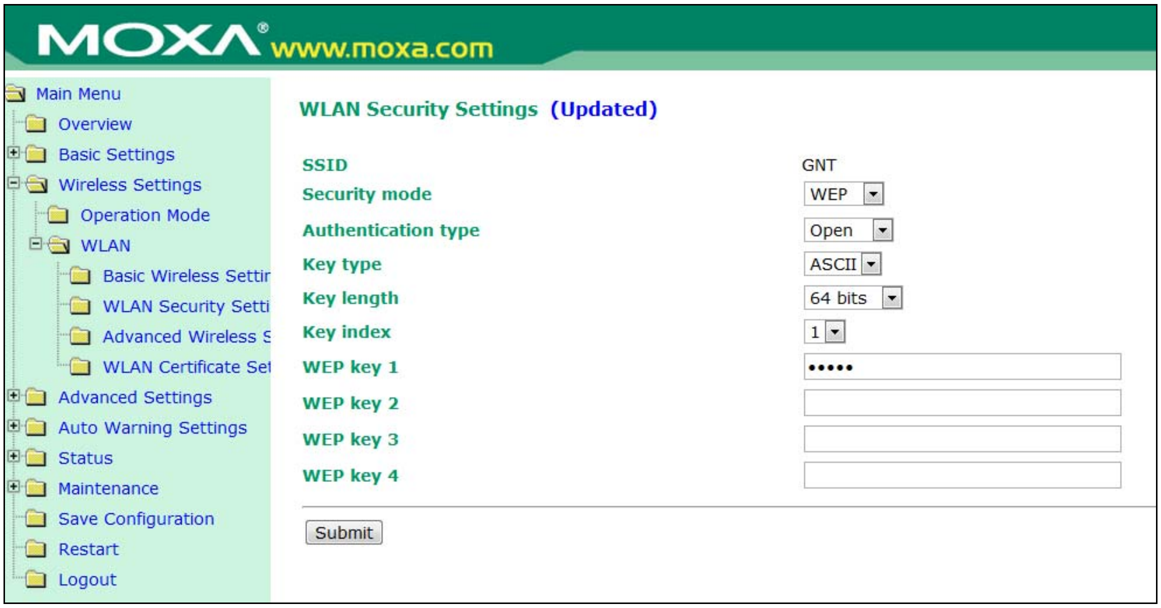
| | |
|---|---|
| Operation mode | AP |
| RF type | B/G Mixed |
| Channel | 3 |
| SSID | GNT |
| SSID broadcast | ● Enable ○ Disable |
| WDS | ● Enable ○ Disable |
| AP functionality | ● Enable ○ Disable |

WDS Settings

| No | □ Active | MAC address |
|---|---|---|
| 1 (WDS1) | □ | |
| 2 (WDS2) | □ | |
| 3 (WDS3) | □ | |
| 4 (WDS4) | □ | |
| 5 (WDS5) | □ | |
| 6 (WDS6) | □ | |
| 7 (WDS7) | □ | |
| 8 (WDS8) | □ | |

**Figure 31: Basic Wireless Settings**

d. **WLAN|WLAN Security Settings**: If using WDS mode, WEP security is the only security mode option available. Enter WEP key(s) and the key index (Figure 32).



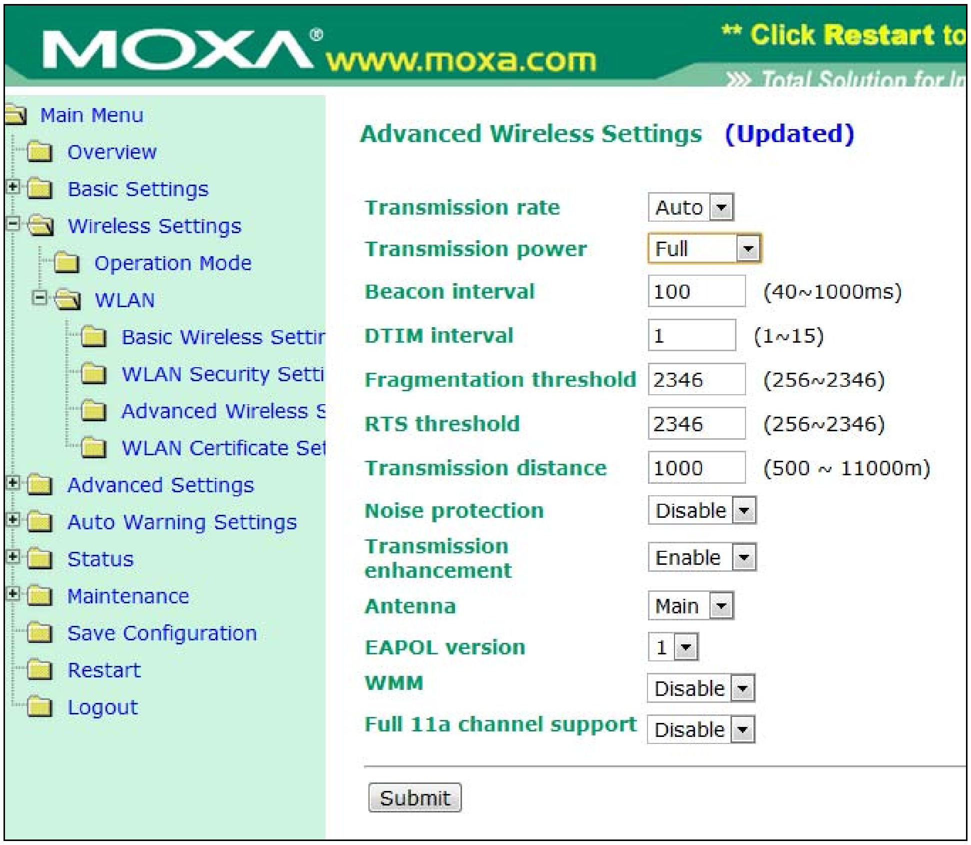
WLAN Security Settings (Updated)

| | |
|---|---|
| SSID | GNT |
| Security mode | WEP |
| Authentication type | Open |
| Key type | ASCII |
| Key length | 64 bits |
| Key index | 1 |
| WEP key 1 | ••••• |
| WEP key 2 | |
| WEP key 3 | |
| WEP key 4 | |

**Figure 32: AWK4121 Security Settings**

e. **WLAN|Advanced Wireless Settings:** Set Transmission distance to the maximum expected range between the AWK-4121 and other wireless devices. Set the corresponding transmission power. For long range communications, set Noise

Protection to Disabled, Enable Transmission Enhancement, and Select the Main or Aux port to which the antenna will be connected.



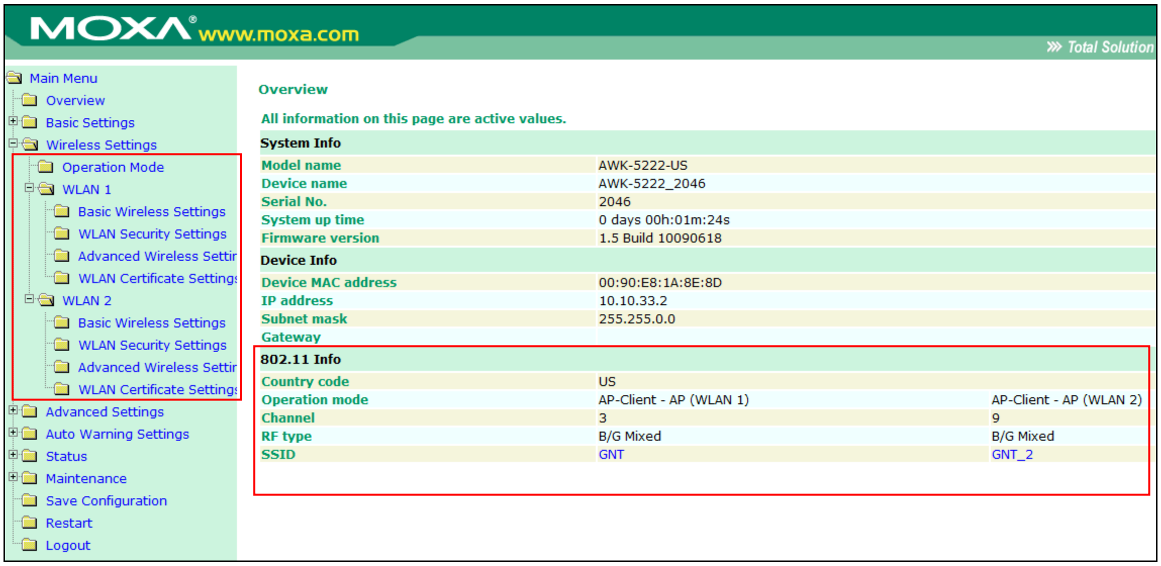
Advanced Wireless Settings (Updated)

| | | |
|---|---|---|
| Transmission rate | Auto | |
| Transmission power | Full | |
| Beacon interval | 100 | (40~1000ms) |
| DTIM interval | 1 | (1~15) |
| Fragmentation threshold | 2346 | (256~2346) |
| RTS threshold | 2346 | (256~2346) |
| Transmission distance | 1000 | (500 ~ 11000m) |
| Noise protection | Disable | |
| Transmission enhancement | Enable | |
| Antenna | Main | |
| EAPOL version | 1 | |
| WMM | Disable | |
| Full 11a channel support | Disable | |

**Figure 33: AWK-4121 Advanced Wireless Setttings**

**IV. Moxa AWK-5222 Access Point Setup**

The Moxa AWK-5222 is very similar to the AWK-4121. It offers dual RF, whereas the AWK-4121 has a single RF. The second RF is useful when it is necessary to link devices outside the range of the main network due to geographic or other restrictions. The web console configuration process for the AWK-5222 is similar to that described above for the AWK-4121.  The main difference is that additional input is required for the second RF (Figure 34).



Overview

All information on this page are active values.

| System Info | | |
|---|---|---|
| Model name | AWK-5222-US | |
| Device name | AWK-5222_2046 | |
| Serial No. | 2046 | |
| System up time | 0 days 00h:01m:24s | |
| Firmware version | 1.5 Build 10090618 | |
| **Device Info** | | |
| Device MAC address | 00:90:E8:1A:8E:8D | |
| IP address | 10.10.33.2 | |
| Subnet mask | 255.255.0.0 | |
| Gateway | | |
| **802.11 Info** | | |
| Country code | US | |
| Operation mode | AP-Client - AP (WLAN 1) | AP-Client - AP (WLAN 2) |
| Channel | 3 | 9 |
| RF type | B/G Mixed | B/G Mixed |
| SSID | GNT | GNT_2 |

**Figure 34: AWK-5222 Web Console**

When using the AWK-5222, separate channels should be used for each RF. Additionally, it is important that the Operation Mode is properly specified in the Wireless Settings. In most cases, AP-Client mode will be used and each WLAN will be set to AP mode.

## V. Creating an Extended Range, Access Point Using Multiple AWK-3121/4121s and Directional Antennas

For some applications, when the AWK-3121/4121 is used with a standard 12 dB omni-directional antenna, the range capabilities may not be sufficient to cover the project area. In such cases, a high powered access point can be simulated by using multiple AWK-3121/4121 devices with a switch (Moxa EDS-205) and high gain directional antennas (Figure 35).

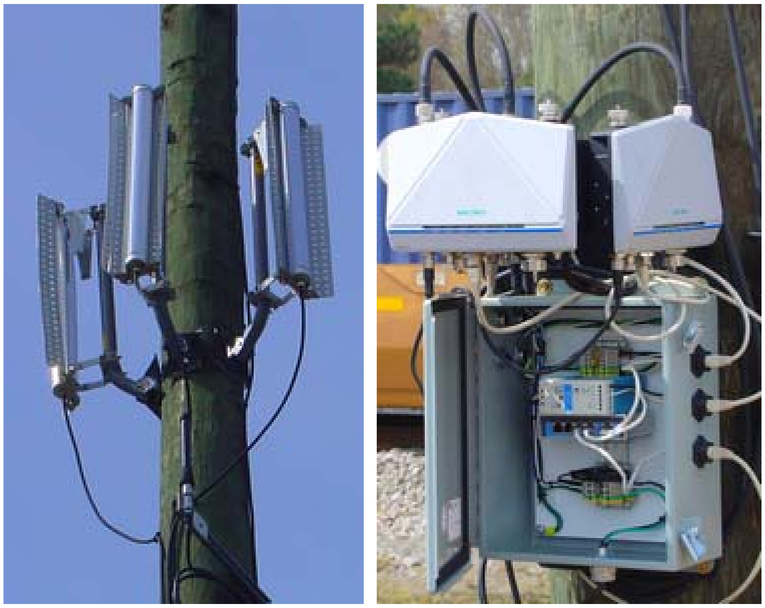


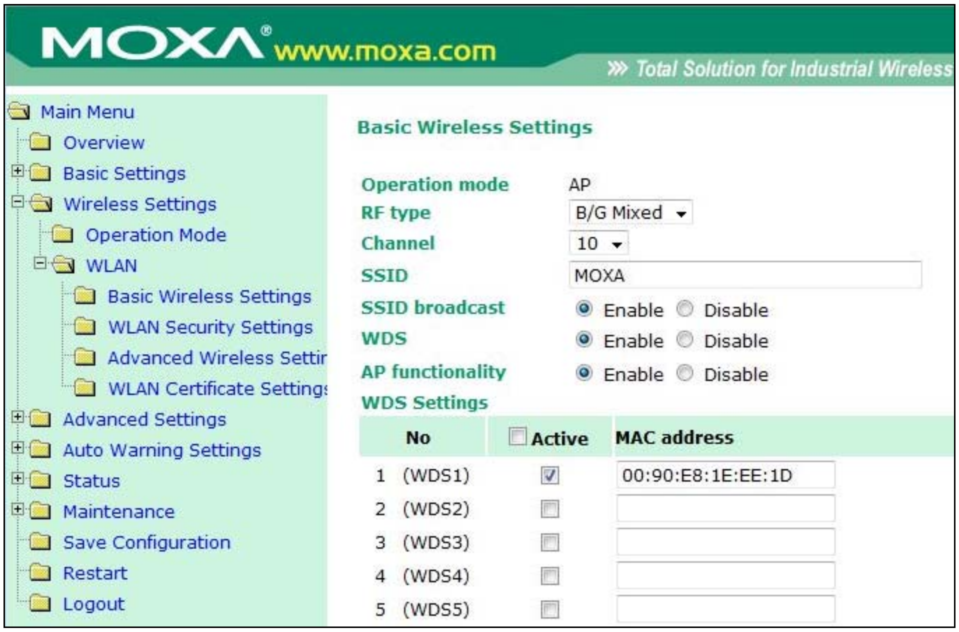
**Figure 35: Extened Range Access Point**

The procedure for creating an Extended Range Access Point is:

i. Choose one AWK-3121/4121 as the communications gateway to the local network. Enable WDS mode and exchange MAC addresses with this device (Figure 36) and the other existing AWK-3121/4121 in the local network (Figure 37) to which it will be connected.

ii. Using an Ethernet cable, connect the switch to the LAN port on the AWK-3121/4121 identified as the communications gateway. Connect additional AWK-3121/4121s to the switch. WDS mode should NOT need to be enabled on the additional AWK-3121/4121s that are not communicating with the local network (Figure 38).

iii. Use high gain, directional antennas to extend WiFi coverage in the desired direction.



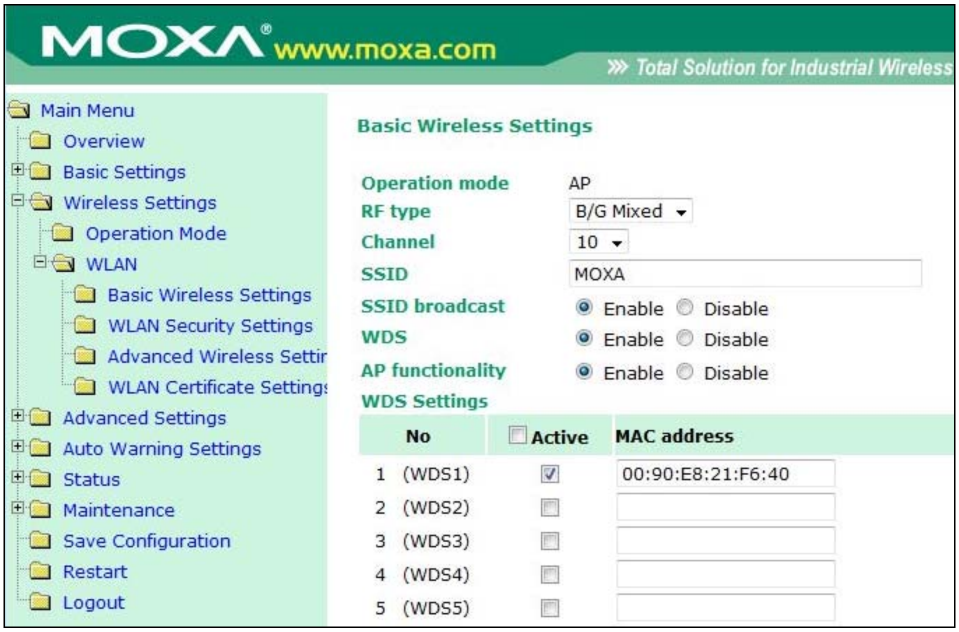
**Basic Wireless Settings**

| | |
|---|---|
| Operation mode | AP |
| RF type | B/G Mixed ▾ |
| Channel | 10 ▾ |
| SSID | MOXA |
| SSID broadcast | ● Enable ○ Disable |
| WDS | ● Enable ○ Disable |
| AP functionality | ● Enable ○ Disable |

**WDS Settings**

| No | □ Active | MAC address |
|---|---|---|
| 1 (WDS1) | ☑ | 00:90:E8:1E:EE:1D |
| 2 (WDS2) | □ | |
| 3 (WDS3) | □ | |
| 4 (WDS4) | □ | |
| 5 (WDS5) | □ | |

**Figure 36: WDS Mode Enabled (Communications Gateway AP)**



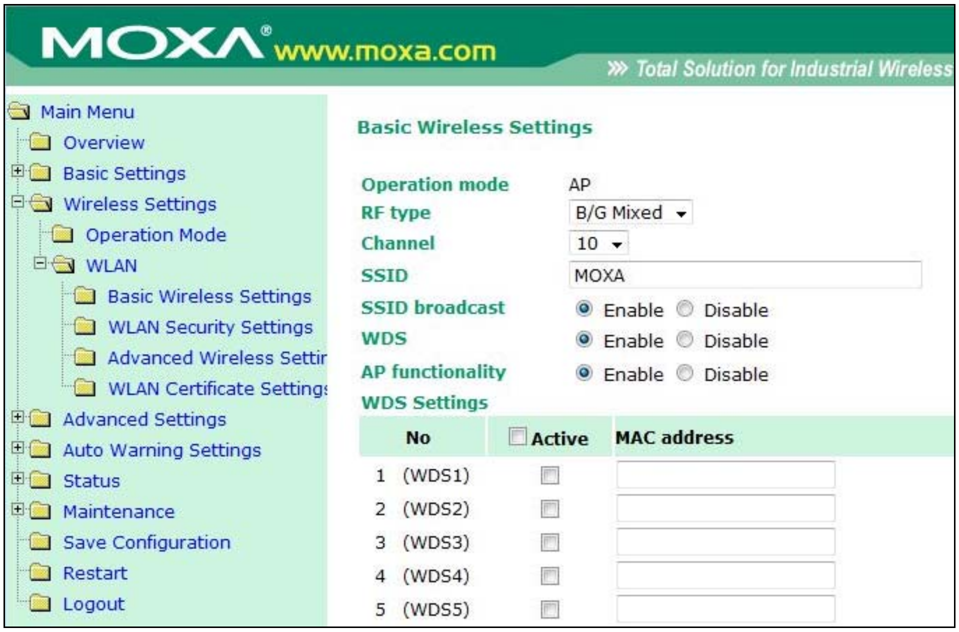
**Basic Wireless Settings**

| | |
|---|---|
| Operation mode | AP |
| RF type | B/G Mixed ▾ |
| Channel | 10 ▾ |
| SSID | MOXA |
| SSID broadcast | ● Enable ○ Disable |
| WDS | ● Enable ○ Disable |
| AP functionality | ● Enable ○ Disable |

**WDS Settings**

| No | □ Active | MAC address |
|---|---|---|
| 1 (WDS1) | ☑ | 00:90:E8:21:F6:40 |
| 2 (WDS2) | □ | |
| 3 (WDS3) | □ | |
| 4 (WDS4) | □ | |
| 5 (WDS5) | □ | |

**Figure 37: WDS Mode Enabled (Local Network AP)**



Basic Wireless Settings

| | |
|---|---|
| Operation mode | AP |
| RF type | B/G Mixed |
| Channel | 10 |
| SSID | MOXA |
| SSID broadcast | ● Enable ○ Disable |
| WDS | ● Enable ○ Disable |
| AP functionality | ● Enable ○ Disable |

WDS Settings

| No | □ Active | MAC address |
|---|---|---|
| 1 (WDS1) | □ | |
| 2 (WDS2) | □ | |
| 3 (WDS3) | □ | |
| 4 (WDS4) | □ | |
| 5 (WDS5) | □ | |

**Figure 38: WDS Mode Disabled**

## VI. Transferring Between Elevations Using Multiple AWK-3121/4121s

For some applications, when the AWK-3121/4121 is used with a standard 12 dB omni-directional antenna, large changes in elevation cannot be tolerated due to the narrow vertical beam width . In such cases, a change in elevation can be accommodated by using 2, AWK-3121/4121 devices at one location.

The procedure for transferring communications over large elevations is:

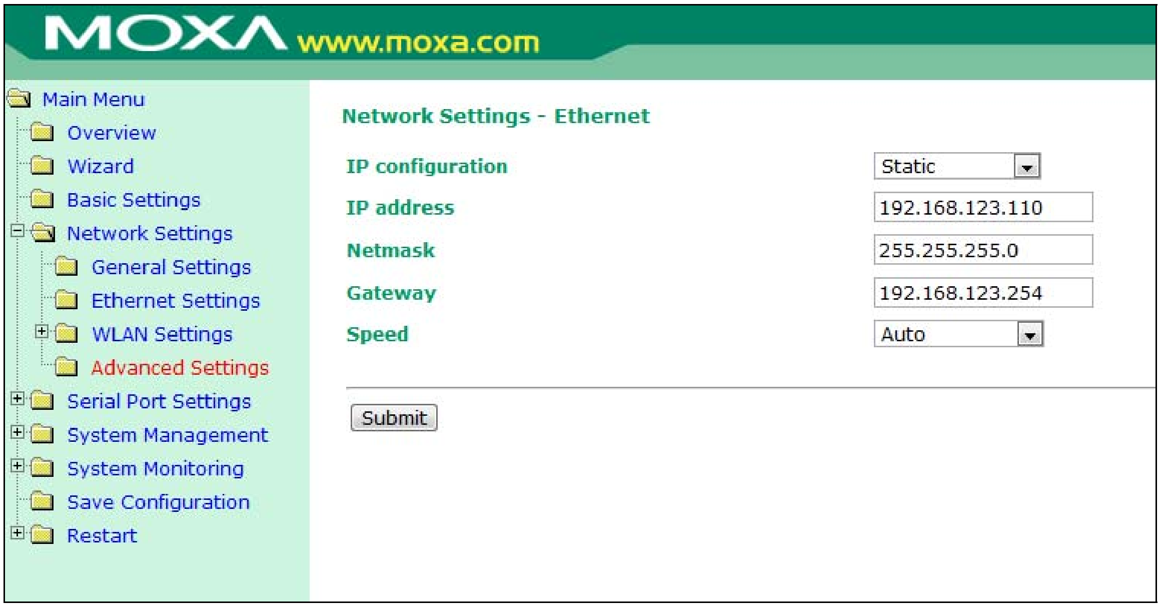
i. Choose one AWK-3121/4121 as the communications gateway to the local network. Enable WDS mode and exchange MAC addresses with this device (Figure 36) and the other existing AWK-3121/4121 in the local network to which it will be connected.

ii. Using an Ethernet cable, connect the LAN port on the AWK-3121/4121 identified as the communications gateway (above) to the LAN port on a second AWK-3121/4121. WDS mode should not be set between these two devices (Figure 38), since they are connected over the Ethernet cable.

iii. Use a directional antenna to communicate with a mirror setup on the other end. WDS mode should be enabled on the AWK-3121/4121s communicating via directional antennas (Figure 37).

## VII. Setup of NPort Devices Behind a Router

For some applications, it is necessary to deploy the NPort Serial-to-Ethernet wireless device on a local network behind a router, while still having it accessible over Internet. In such cases, the router must be configured for port forwarding, as subsequently described. The NPort's IP address should comply with the local network settings (your network administrator can provide you with a valid IP address). Additionally, the Gateway IP address should match the local IP address of the router (Figure 39).



Network Settings - Ethernet

| | |
|---|---|
| IP configuration | Static |
| IP address | 192.168.123.110 |
| Netmask | 255.255.255.0 |
| Gateway | 192.168.123.254 |
| Speed | Auto |

**Figure 39: NPort Setup for Behind-a-Router Access**

If you want the NPort to use a private IP address behind your NAT/firewall, you will need to use the NAPT protocol in your NAT router to map the router's public IP address to the NPort's private IP address. Most routers/firewalls support this function. The examples below show how TCP/UDP port numbers are mapped using a private IP address of 192.168.1.1 for the NPort and a public IP address of 61.x.x.x for the NAT router.

**For DE-311/211/30x/33x**

| Protocol | Public IP | Port No. | NPort Private IP | Port No. |
|---|---|---|---|---|
| TCP | 61.x.x.x | 23 | 192.168.1.1 | 23 |
| TCP | 61.x.x.x | 4000 | 192.168.1.1 | 4000 |
| TCP | 61.x.x.x | 950(~965) | 192.168.1.1 | 950(~965) |
| TCP | 61.x.x.x | 966(~981) | 192.168.1.1 | 966(~981) |
| UDP | 61.x.x.x | 1029 | 192.168.1.1 | 1029 |

**For NPort 5110/5200/5400/5600 and NE-4100 series**

| Protocol | Public IP | Port No. | NPort Private IP | Port No. |
|---|---|---|---|---|
| TCP | 61.x.x.x | 23 | 192.168.1.1 | 23 |
| TCP | 61.x.x.x | 80 | 192.168.1.1 | 80 |

| | | | | |
|---|---|---|---|---|
| TCP | 61.x.x.x | 4900 | 192.168.1.1 | 4900 |
| TCP | 61.x.x.x | 950(~965) | 192.168.1.1 | 950(~965) |
| TDP | 61.x.x.x | 966(~981) | 192.168.1.1 | 966(~981) |
| UDP | 61.x.x.x | 4800 | 192.168.1.1 | 4800 |

**For NPort Wireless W2150/W2250/W2004**

| Protocol | Public IP | Port No. | NPort Private IP | Port No. |
|---|---|---|---|---|
| TCP | 61.x.x.x | 23 | 192.168.1.1 | 23 |
| TCP | 61.x.x.x | 80 | 192.168.1.1 | 80 |
| TCP | 61.x.x.x | 950(~953) | 192.168.1.1 | 950(~953) |
| TDP | 61.x.x.x | 966(~969) | 192.168.1.1 | 966(~969) |
| UDP | 61.x.x.x | 4800 | 192.168.1.1 | 4800 |
| TCP | 61.x.x.x | 4900 | 192.168.1.1 | 4900 |

**For NPort 6000 series**

| Protocol | Public IP | Port No. | NPort Private IP | Port No. |
|---|---|---|---|---|
| TCP | 61.x.x.x | 22 | 192.168.1.1 | 22 |
| TCP | 61.x.x.x | 23 | 192.168.1.1 | 23 |
| TCP | 61.x.x.x | 80 | 192.168.1.1 | 80 |
| TCP | 61.x.x.x | 81 | 192.168.1.1 | 81 |
| TCP | 61.x.x.x | 950(~953) | 192.168.1.1 | 950(~953) |
| TDP | 61.x.x.x | 966(~969) | 192.168.1.1 | 966(~969) |
| UDP | 61.x.x.x | 4800 | 192.168.1.1 | 4800 |
| TCP | 61.x.x.x | 4900 | 192.168.1.1 | 4900 |

If you want to allow NPort use behind firewall, you should open the below UDP/TCP port number in your firewall rules setting.

**For DE-311/211/30x/33x**

| Protocol | Port No. | Propose |
|---|---|---|
| TCP | 23 | Telnet |
| TCP | 4000 | 1.Save Settings<br>2.Firmware upgrade |
| TCP | 950(~965) | Data port |
| TCP | 966(~981) | Command port |
| UDP | 1029 | 1.Broadcast Search<br>2.Get Current Settings<br>3.Real COM Installer mapping |

**For NPort 5110/5200/5400/5600 and NE-4100 series**

| Protocol | Port No. | Propose |
|---|---|---|
| TCP | 23 | Telnet |
| TCP | 80 | Web Console |
| TCP | 4900 | 1.Save Settings<br>2.Firmware upgrade |
| TCP | 950(~965) | Data Port |
| TCP | 966(~981) | Command Port |
| UDP | 4800 | 1.Broadcast Search/Rescan<br>2.Administrator Monitor<br>3.Get Current Settings |

**NPort Wireless W2150/W2250**

| Protocol | Port No. | Propose |
|---|---|---|
| TCP | 23 | Telnet |
| TCP | 80 | Web Console |
| TCP | 4900 | 1.Save Settings<br>2.Firmware upgrade |
| TCP | 950(~965) | Data Port |
| TCP | 966(~981) | Command Port |
| UDP | 4800 | 1.Broadcast Search/Rescan<br>2.Get Current Settings |

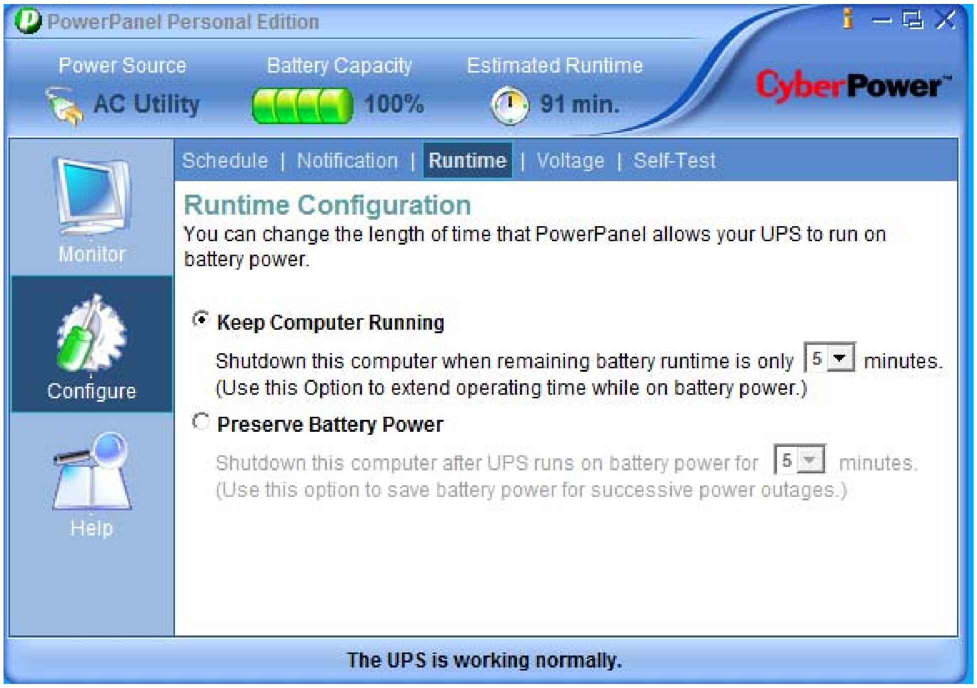
**For NPort6000 series and NPort Wireless W2004**

| Protocol | Port No. | Propose |
|---|---|---|
| TCP | 22 | Secure Telnet(SSH) |
| TCP | 23 | Telnet |
| TCP | 80 | Web Console |
| TCP | 443 | Secure Web Console(SSL) |
| TCP | 4900 | 1.Save Settings<br>2.Firmware upgrade |
| TCP | 950(~965) | Data Port |
| TCP | 966(~981) | Command Port |
| UDP | 4800 | 1.Broadcast Search/Rescan<br>2.Get Current Setting |

# 5. CyberPower UPS

**I. Setting up the CyberPower UPS:**

Install the PowerPanel software that comes with your UPS. Connect the UPS to your PC with the USB cable. Click on the “Configure” button in the left hand menu (Figure 40). Under “Runtime”, select “Keep Computer Running”. Specify 5 minutes as the time remaining in battery life before shutting down the computer. Alarms can be disabled under the “Notification” tab of the “Configure” page. The PC should be the only device plugged into the Battery and Surge Protection outlets. Monitors and peripheral devices should be plugged into the Surge only outlets.


PowerPanel Personal Edition
CyberPower
Schedule | Notification | Runtime | Voltage | Self-Test
Monitor
Configure
Help

Power Source: AC Utility
Battery Capacity: 100%
Estimated Runtime: 91 min.

Runtime Configuration

You can change the length of time that PowerPanel allows your UPS to run on battery power.

● Keep Computer Running

Shutdown this computer when remaining battery runtime is only 5 minutes.
(Use this Option to extend operating time while on battery power.)

○ Preserve Battery Power

Shutdown this computer after UPS runs on battery power for 5 minutes.
(Use this option to save battery power for successive power outages.)

The UPS is working normally.

**Figure 40: Configuring the CyberPower UPS**