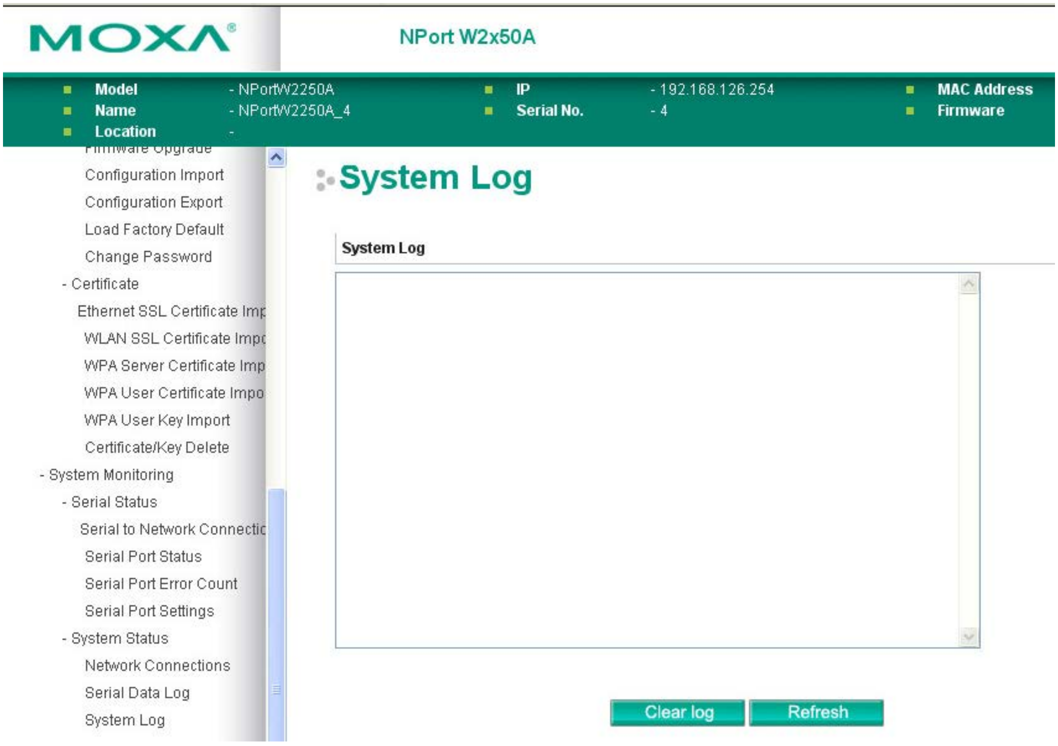
System Log



NPort W2x50A

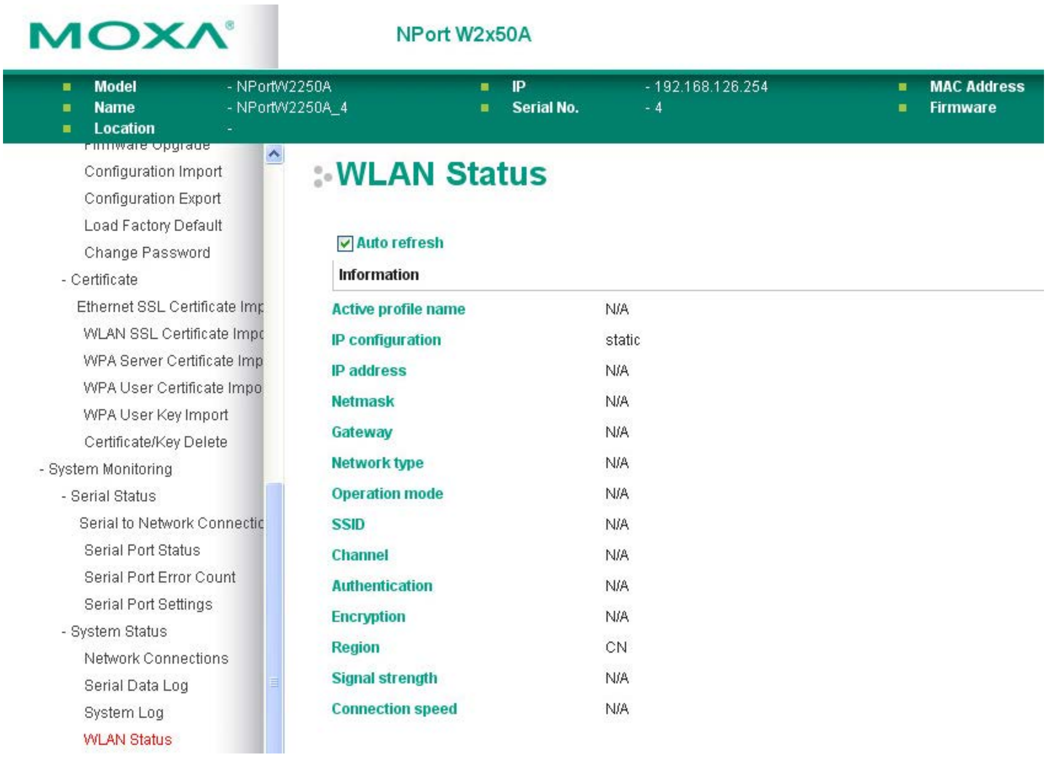
- Model - NPortW2250A
- Name - NPortW2250A_4
- Location -
- IP - 192.168.126.254
- Serial No. - 4
- MAC Address
- Firmware

System Log

System Log

The **System Log** page is located under **System Status** in the **System Monitoring** folder. This is where you can view the log of NPort system events. Click **[Clear log]** to clear the log contents. Click **[Refresh]** to refresh the log contents.

WLAN Status



NPort W2x50A

- Model - NPortW2250A
- Name - NPortW2250A_4
- Location -
- IP - 192.168.126.254
- Serial No. - 4
- MAC Address
- Firmware

WLAN Status

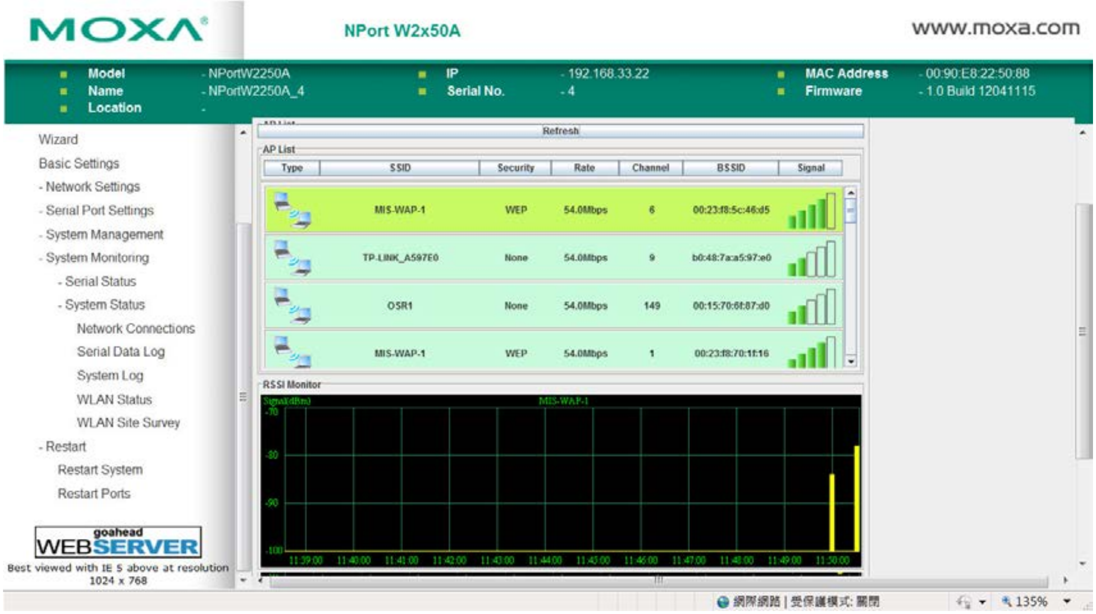
☑ Auto refresh

Information

Active profile name	N/A
IP configuration	static
IP address	N/A
Netmask	N/A
Gateway	N/A
Network type	N/A
Operation mode	N/A
SSID	N/A
Channel	N/A
Authentication	N/A
Encryption	N/A
Region	CN
Signal strength	N/A
Connection speed	N/A

The **WLAN Status** page is located under **System Status** in the **System Monitoring** folder. This is where you can view the current WLAN settings and status.

WLAN Site Survey



NPort W2x50A

- Model - NPortW2250A
- Name - NPortW2250A_4
- Location -
- IP - 192.168.33.22
- Serial No. - 4
- MAC Address - 00:90:E8:22:50:88
- Firmware - 1.0 Build 12041115

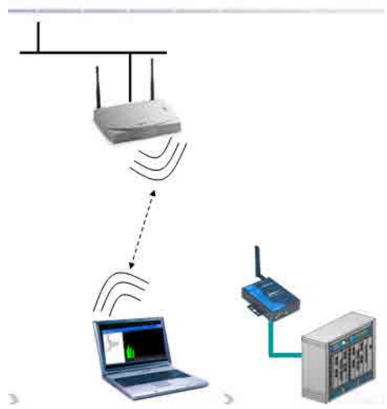
AP List

Type	SSID	Security	Rate	Channel	BSSID	Signal
	MIS-WAP-1	WEP	54.0Mbps	6	00:23:f8:5c:46:d5	
	TP-LINK_A597E0	None	54.0Mbps	9	b0:48:7a:a5:97:e0	
	OSR1	None	54.0Mbps	149	00:15:70:6f:87:d0	
	MIS-WAP-1	WEP	54.0Mbps	1	00:23:f8:70:1f:16	

The **WLAN Site Survey** page is located under **System Status** in the **System Monitoring** folder. This is where you can view live data on wireless signal strength and characteristics. It is useful tool to help you complete a wireless site survey without installing additional software.

The goal of a WLAN site survey is to determine the number and placement of access points to provide enough coverage to the facility. For most implementations, "enough coverage" means that the data rate at all locations does not fall below a certain threshold. For most wireless sites, it is necessary to perform a WLAN site survey before access point installation in order to determine the behavior of radio waves at the site.

Typical WLAN Site Survey



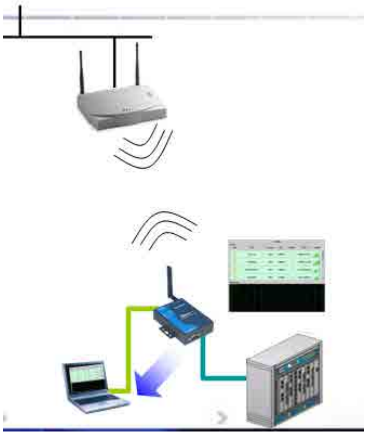
Procedure

1. Download/install site survey software.
2. Run software on laptop.
3. Measure AP signal strength using software on laptop.

Weakness

- Signal strength is read from the laptop NIC rather than from NPort

**WLAN Site Survey with
NPort W2150/W2250A Series**



Procedure

1. Open web browser
2. Measure AP signal from NPort web console.

Advantages

- Signal strength is read from NPort
- Additional software not required

Please note that Java must be enabled in your web browser for the **WLAN Site Survey** page to display properly.

10

Web Console: Restart

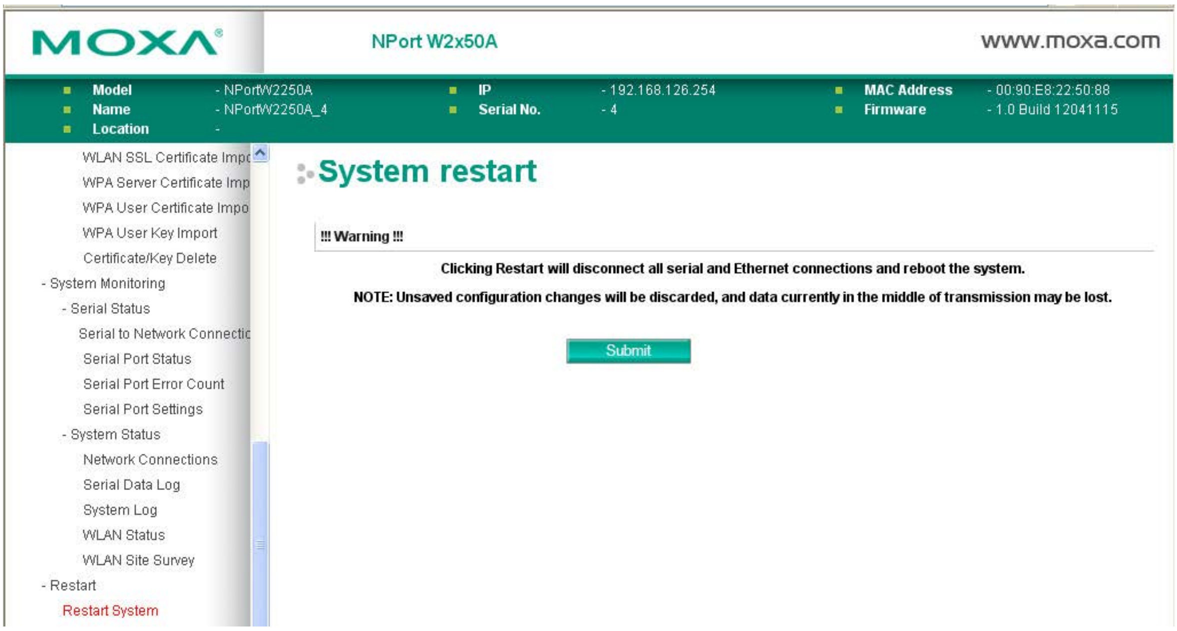
The following topics are covered in this chapter:

Overview

This chapter explains how to use save your configuration changes and restart the NPort using the NPort web console. Configuration changes will not be effective until they are saved and the NPort is rebooted.

Restart

Restart System



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

System restart

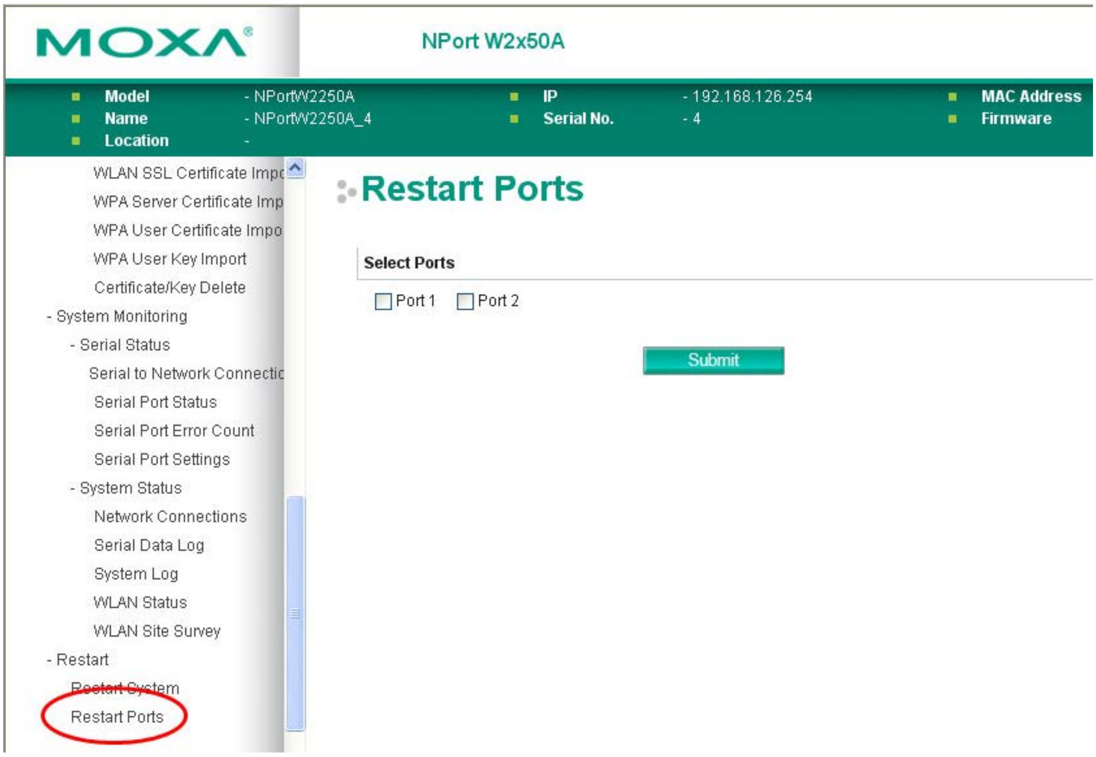
!!! Warning !!!

Clicking Restart will disconnect all serial and Ethernet connections and reboot the system.

NOTE: Unsaved configuration changes will be discarded, and data currently in the middle of transmission may be lost.

The **Restart System** page is located in the **Restart** folder. Click **[Restart]** to restart the NPort, and the new settings will take effect upon restart.

Restart Ports



NPort W2x50A

- Model - NPortW2250A
- Name - NPortW2250A_4
- Location -
- IP - 192.168.126.254
- Serial No. - 4
- MAC Address
- Firmware

Restart Ports

Select Ports

□ Port 1 □ Port 2

The **Restart Ports** page is located in the **Restart** folder. Select the desired serial and click **[Select All]** to select all serial ports. Click **[Submit]** to restart the selected serial ports.

11

Installing and Configuring the Software

The following topics are covered in this chapter:

- ❒ **Overview**
- ❒ **NPort Windows Driver Manager**
  - ➢ Installing NPort Windows Driver Manager
  - ➢ Adding Mapped Serial Ports
  - ➢ Configuring Mapped Serial Ports
- ❒ **NPort Search Utility**
  - ➢ Installing NPort Search Utility
  - ➢ Finding NPort Device Servers on Network
  - ➢ Modifying NPort IP Addresses
  - ➢ Upgrading NPort Firmware
- ❒ **Linux Real TTY Drivers**
  - ➢ Basic Steps
  - ➢ Installing Linux Real TTY Driver Files
  - ➢ Mapping TTY Ports
  - ➢ Removing Mapped TTY Ports
  - ➢ Removing Linux Driver Files
- ❒ **UNIX Fixed TTY Drivers**
  - ➢ Installing the UNIX Driver
  - ➢ Configuring the UNIX Driver

Overview

This chapter describes how to install and use NPort Windows Driver Manager, NPort Search Utility, and NPort Linux and UNIX drivers. These items are located on the Document & Software CD that is provided with the NPort W2150A/W2250A Series.

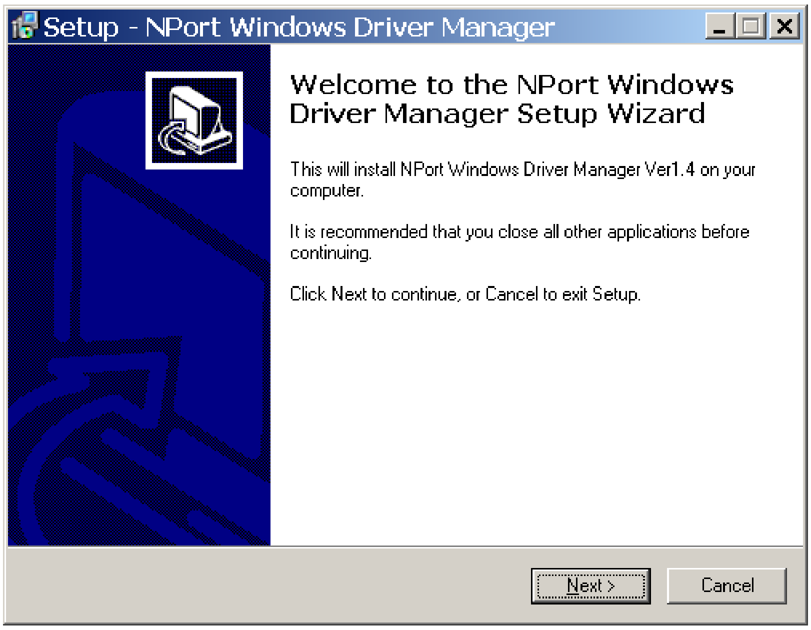
NPort Windows Driver Manager is a utility that installs and manages NPort COM drivers for COM mapping. **NPort Search Utility** is a utility for the management of NPort device servers over the network. You may also use NPort Search Utility to upgrade the firmware.

NPort Windows Driver Manager

NPort Windows Driver Manager installs remote NPort serial ports as new COM ports on your Windows PC. When the drivers are installed and configured, devices that are attached to serial ports on the NPort will be treated as if they were attached to your PC's own COM ports. The NPort serial port must be configured for RealCOM mode when being mapped to a COM port.

Installing NPort Windows Driver Manager

1. The main installation window will open when you insert the Document & Software CD. Click **[INSTALL COM Driver]** to proceed. Once the installation program starts running, click **[Yes]** to proceed.
2. The installation wizard will open. Click **[Next]** to proceed.



Setup - NPort Windows Driver Manager

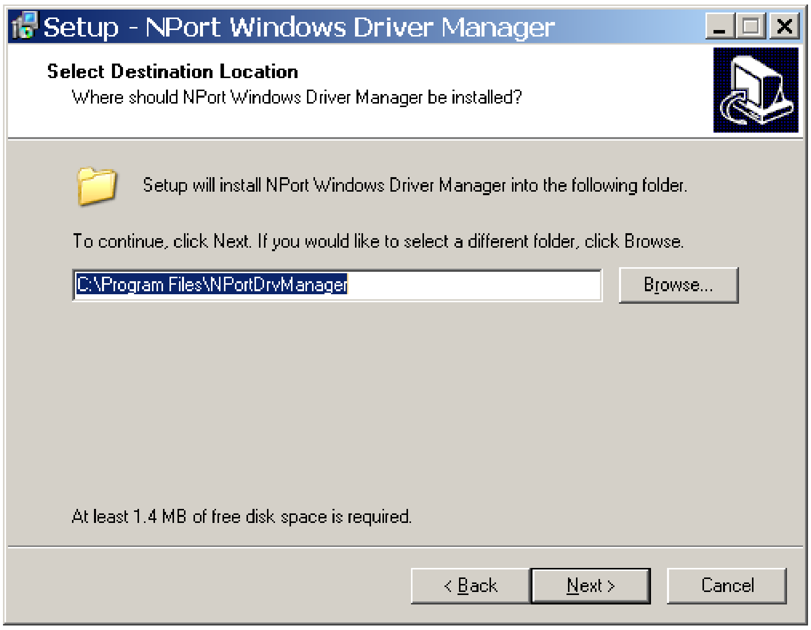
Welcome to the NPort Windows Driver Manager Setup Wizard

This will install NPort Windows Driver Manager Ver1.4 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

3. Select a destination directory and click **[Next]** to proceed.



Setup - NPort Windows Driver Manager

Select Destination Location

Where should NPort Windows Driver Manager be installed?

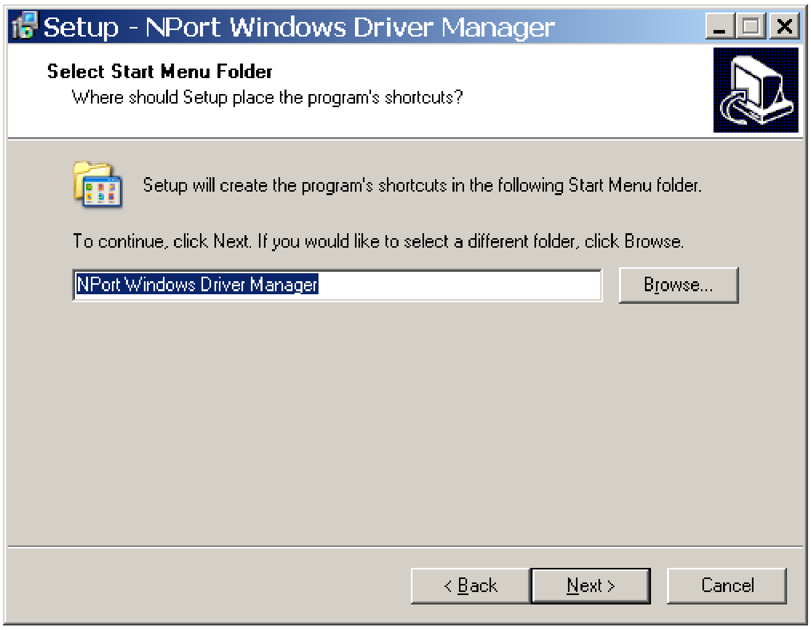
Setup will install NPort Windows Driver Manager into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\NPortDrvManager

At least 1.4 MB of free disk space is required.

4. Select a folder for the program shortcuts and click **[Next]** to proceed.



Setup - NPort Windows Driver Manager

Select Start Menu Folder

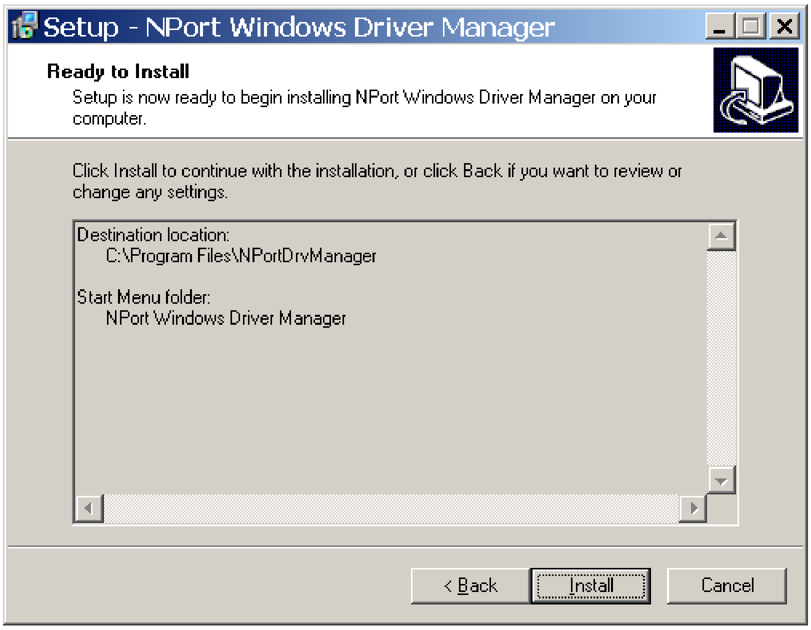
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

NPort Windows Driver Manager

5. Verify the installation parameters and click **Install** to proceed.



Setup - NPort Windows Driver Manager

Ready to Install

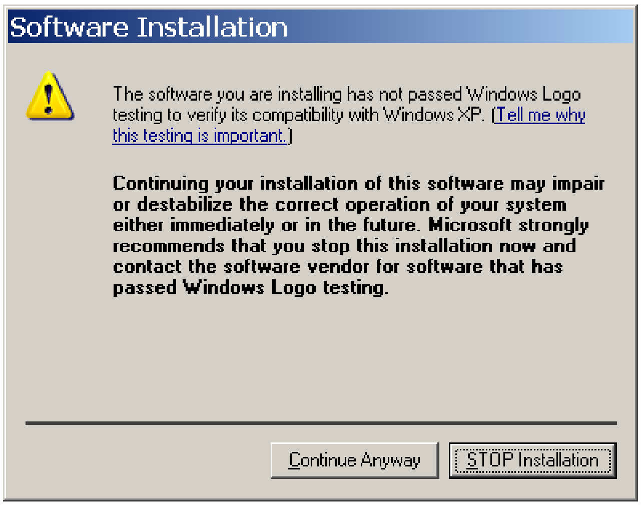
Setup is now ready to begin installing NPort Windows Driver Manager on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
      C:\Program Files\NPortDrvManager

Start Menu folder:
      NPort Windows Driver Manager
```

6. If you see a warning that the software has not passed Windows Logo testing, click **[Continue Anyway]** to proceed.

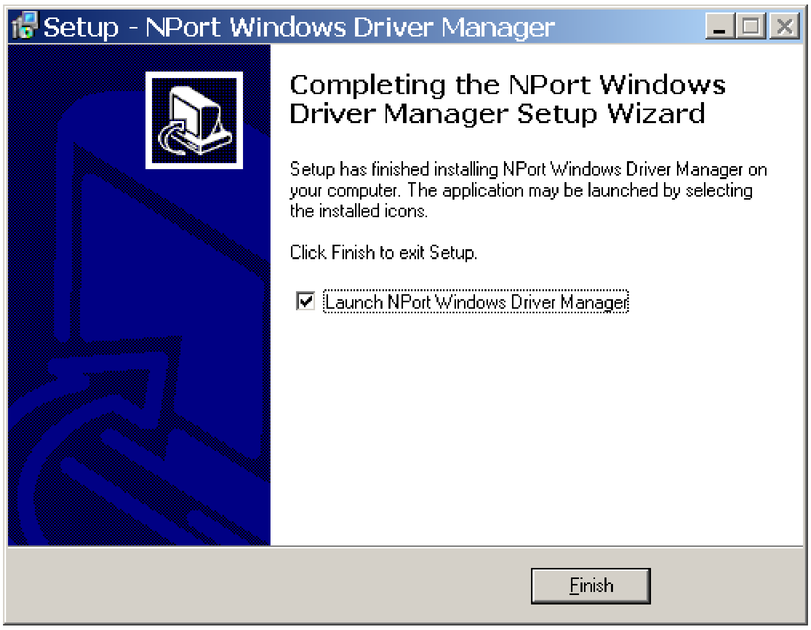


Software Installation

The software you are installing has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the software vendor for software that has passed Windows Logo testing.

7. The wizard will begin installing the files. When the files have been installed, click **[Finish]** to complete the installation.



Setup - NPort Windows Driver Manager

Completing the NPort Windows Driver Manager Setup Wizard

Setup has finished installing NPort Windows Driver Manager on your computer. The application may be launched by selecting the installed icons.

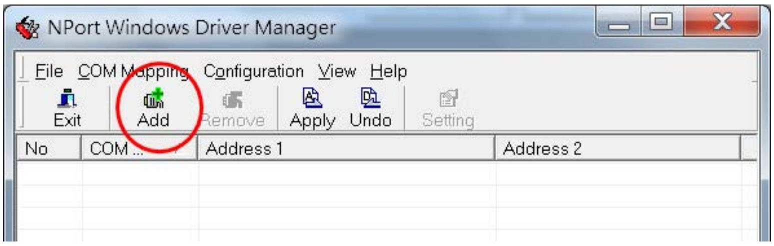
Click Finish to exit Setup.

☑ Launch NPort Windows Driver Manager

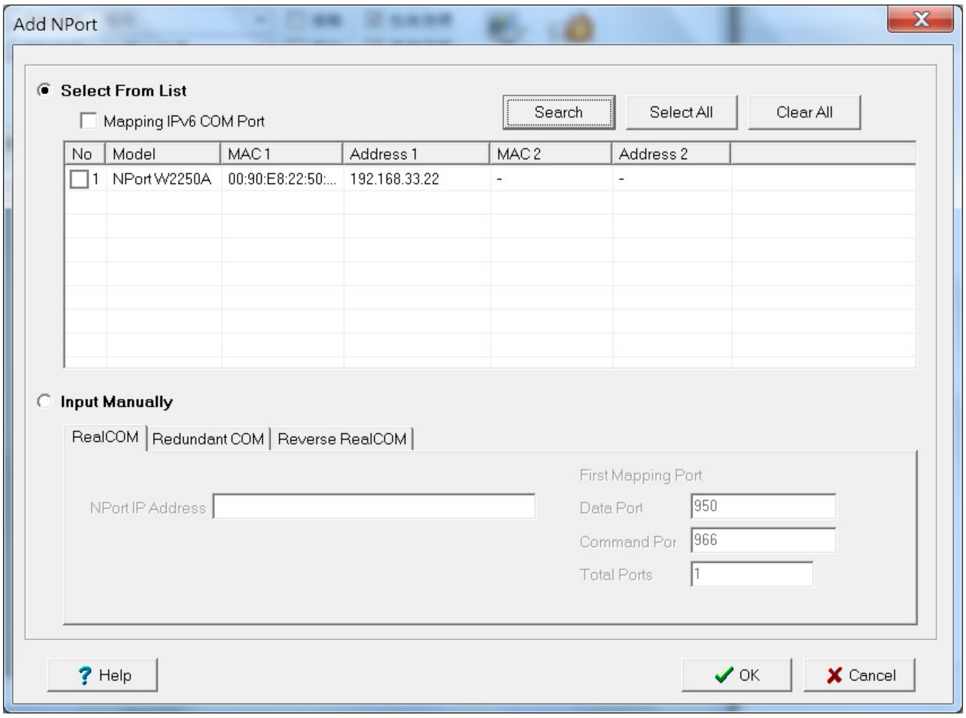
Adding Mapped Serial Ports

NPort Windows Driver Manager adds a COM port to your PC that is mapped to an NPort serial port. The destination NPort serial port must be set to RealCOM mode.

1. In **NPort Windows Driver Manager**, click **[Add]** on the main toolbar.



2. Click **[Rescan]** to search the network for NPort device servers. In the list of NPort device servers that are found, select the unit(s) that you will use for COM mapping and click **[OK]**.



Add NPort

● Select From List

□ Mapping IPv6 COM Port

No	Model	MAC 1	Address 1	MAC 2	Address 2
□ 1	NPort W2250A	00:90:E8:22:50:...	192.168.33.22	-	-

○ Input Manually

RealCOM | Redundant COM | Reverse RealCOM

NPort IP Address

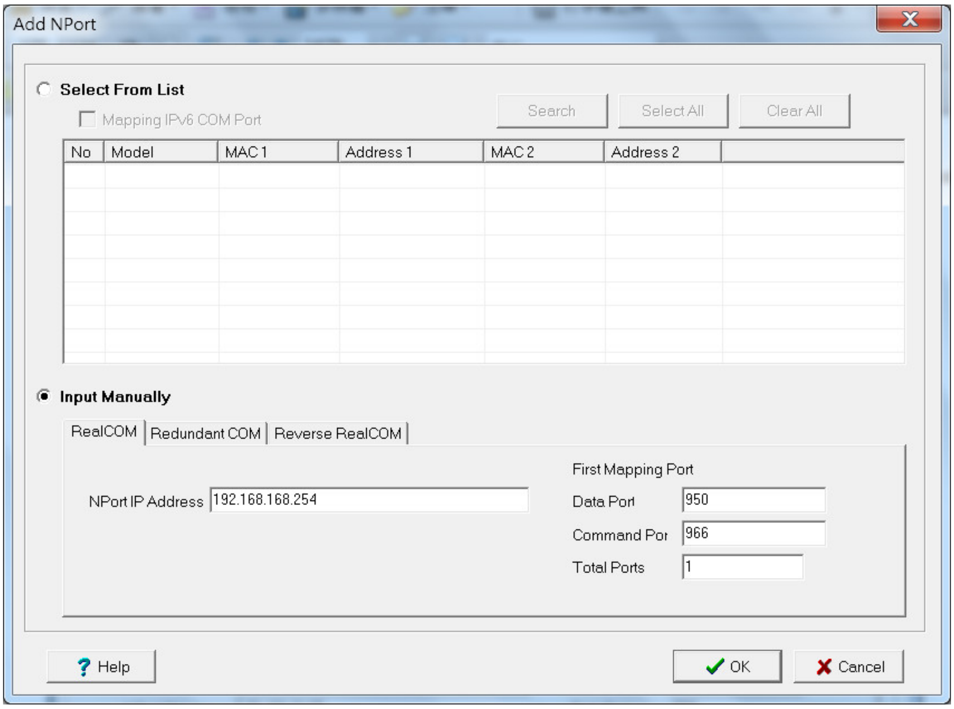
First Mapping Port

Data Port: 950

Command Por: 966

Total Ports: 1

Alternatively, you can select **Input Manually** and manually enter the **NPort IP Address**, **1st Data Port**, **1st Command Port**, and **Total Ports** for the desired NPort unit. Click **[OK]** to proceed.



Add NPort

○ Select From List

□ Mapping IPv6 COM Port

No	Model	MAC 1	Address 1	MAC 2	Address 2

● Input Manually

RealCOM | Redundant COM | Reverse RealCOM

NPort IP Address: 192.168.168.254

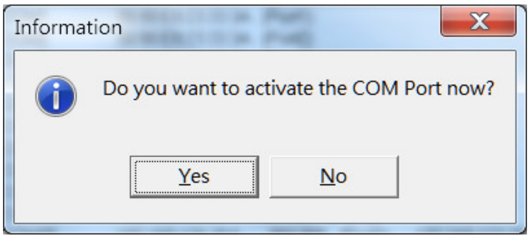
First Mapping Port

Data Port: 950

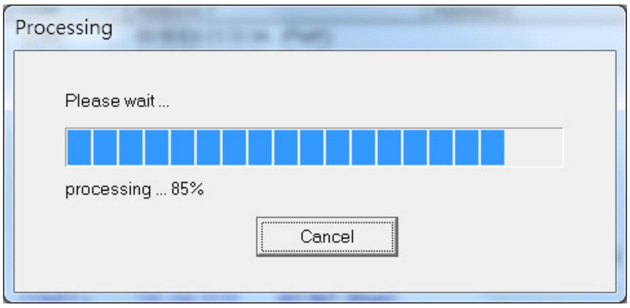
Command Por: 966

Total Ports: 1

3. NPort Windows Driver Manager will list each available serial port and will automatically assign a new COM port to each one. The new COM port will not be accessible by the host system until it has been activated in NPort Windows Driver Manager. Activating a mapped COM port saves the information in the host system registry and makes the COM port available for use. Click **[Yes]** to activate the COM port(s) at this time; click **[No]** to activate the COM port(s) later.

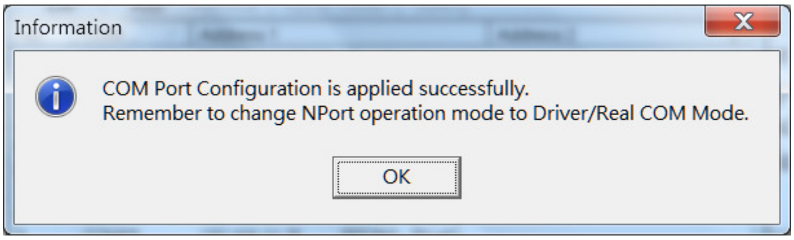

Information

Do you want to activate the COM Port now?


Processing

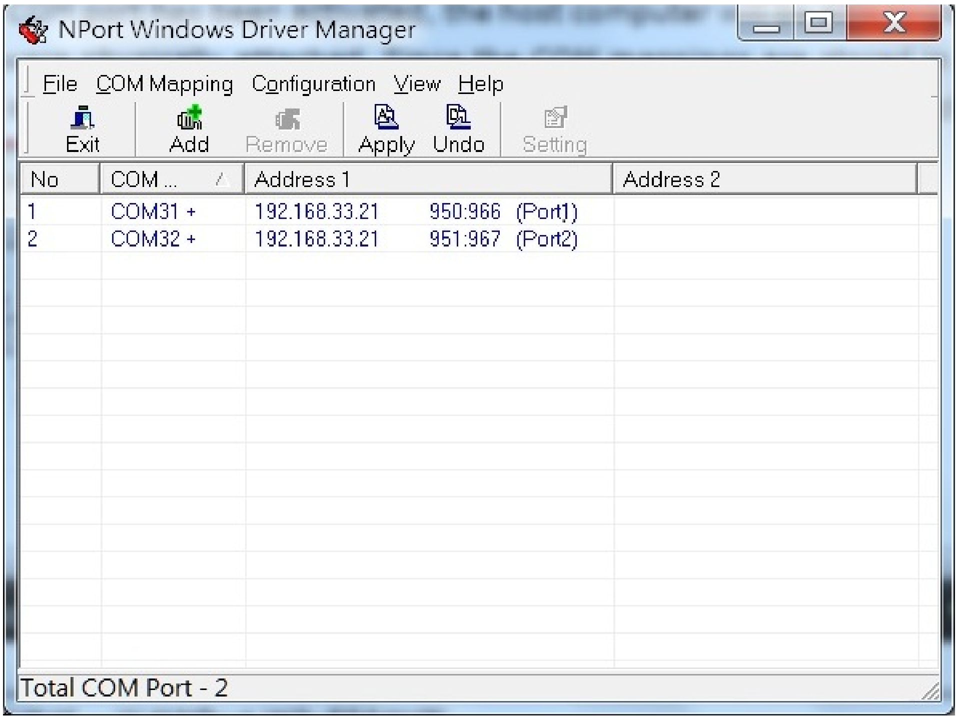
Please wait ...

processing ... 85%


Information

COM Port Configuration is applied successfully.
Remember to change NPort operation mode to Driver/Real COM Mode.

4. Activated COM ports will be listed in black; COM ports that have not been activated will be listed in blue. Once a COM port has been activated, the host computer will be able to communicate with the new COM port as if it were physically attached. Since the COM mappings are stored in the host system registry, they will still be in effect if the PC is restarted or if Windows Driver Manager is closed.

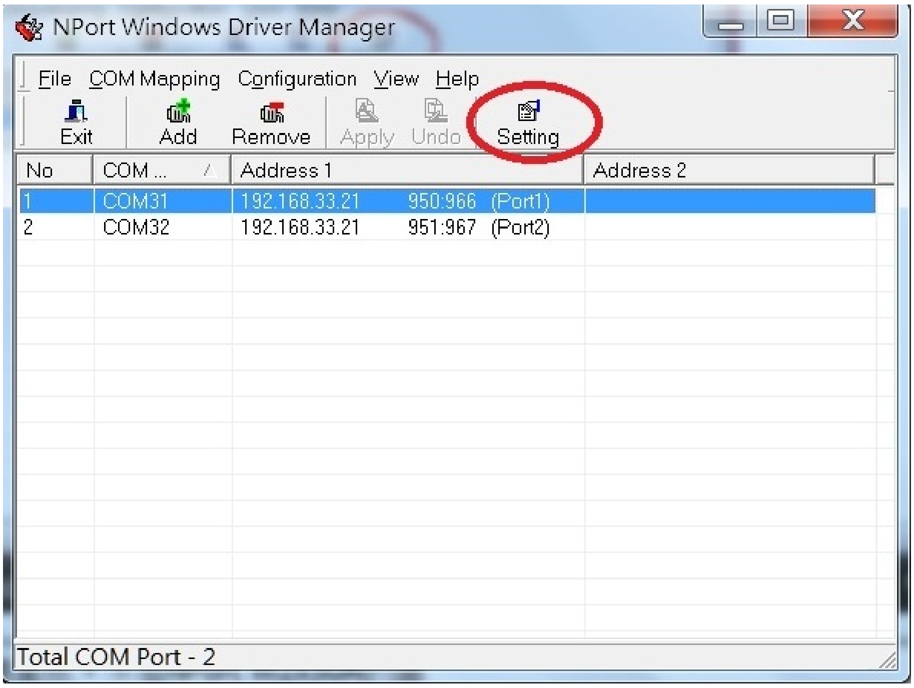

NPort Windows Driver Manager

No	COM ...	Address 1	Address 2
1	COM31 +	192.168.33.21 950:966 (Port1)	
2	COM32 +	192.168.33.21 951:967 (Port2)	

Total COM Port - 2

Configuring Mapped Serial Ports

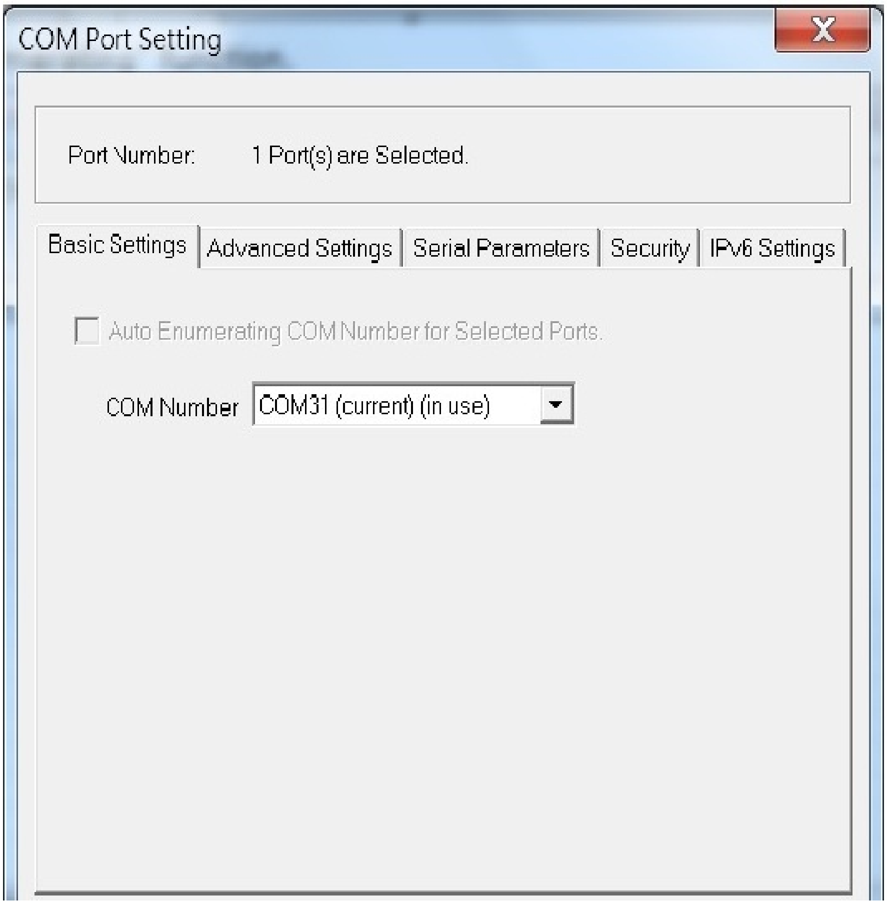
1. To modify the settings of a mapped serial port, select the desired port(s) and click **[Setting]** on the main toolbar.



No	COM ...	Address 1	Address 2
1	COM31	192.168.33.21 950:966 (Port1)	
2	COM32	192.168.33.21 951:967 (Port2)	

Total COM Port - 2

2. On the **Basic Setting** tab, select the **COM Number** that will be assigned to the serial port. If you have selected multiple ports, you can assign COM numbers automatically in sequential order by selecting the "Auto Enumerating COM Number for Selected Ports" function.

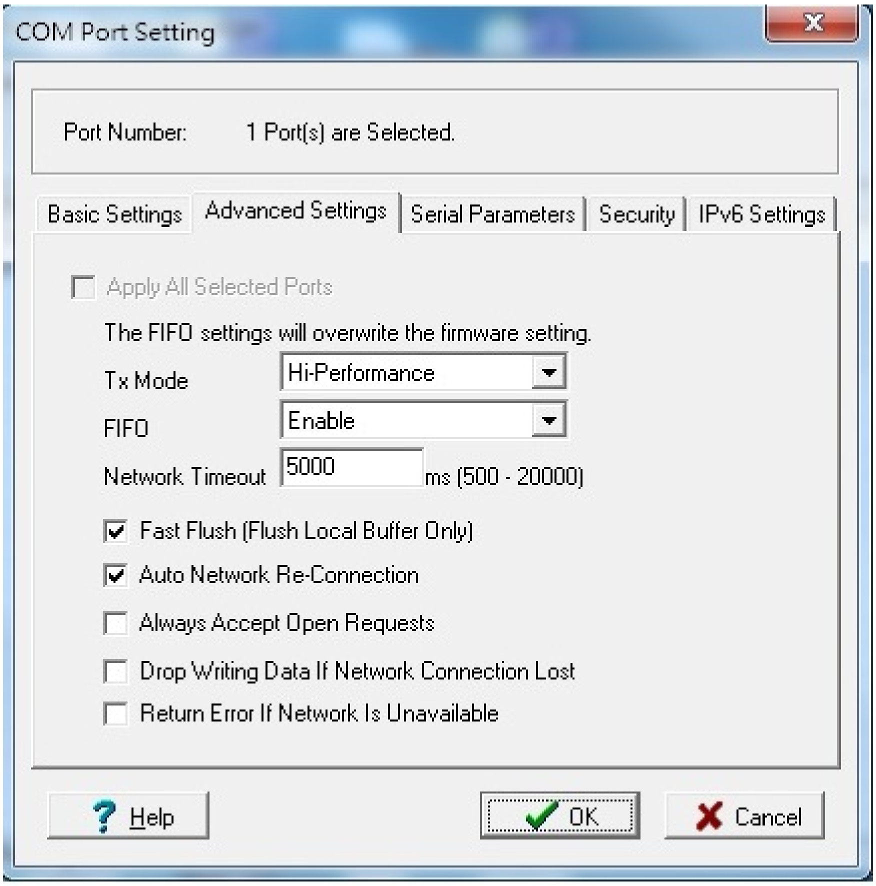


Port Number: 1 Port(s) are Selected.

☐ Auto Enumerating COM Number for Selected Ports.

COM Number: COM31 (current) (in use)

3. On the **Advanced Setting** tab, configure **Tx Mode**, **FIFO**, and **Fast Flush**.



Port Number: 1 Port(s) are Selected.

□ Apply All Selected Ports

The FIFO settings will overwrite the firmware setting.

Tx Mode: Hi-Performance

FIFO: Enable

Network Timeout: 5000 ms (500 - 20000)

☑ Fast Flush (Flush Local Buffer Only)

☑ Auto Network Re-Connection

□ Always Accept Open Requests

□ Drop Writing Data If Network Connection Lost

□ Return Error If Network Is Unavailable

Tx Mode: In Hi-Performance mode, the driver immediately issues a “Tx Empty” response to the program after sending data to the NPort. In Classical mode, the driver sends the “Tx Empty” response after confirmation is received from the NPort. Classical mode is recommended if you want to ensure that all data is sent out before further processing.

FIFO: This tells the driver whether or not to use the FIFO.

Network Timeout: You can use this option to prevent blocking if the target NPort is unavailable.

Fast Flush: When enabled, the driver flushes only the local buffer on the host for a Win32 PurgeComm() function call. When disabled, both the local and remote buffers are flushed. If your application uses PurgeComm() and performance seems sluggish, try enabling Fast Flush.

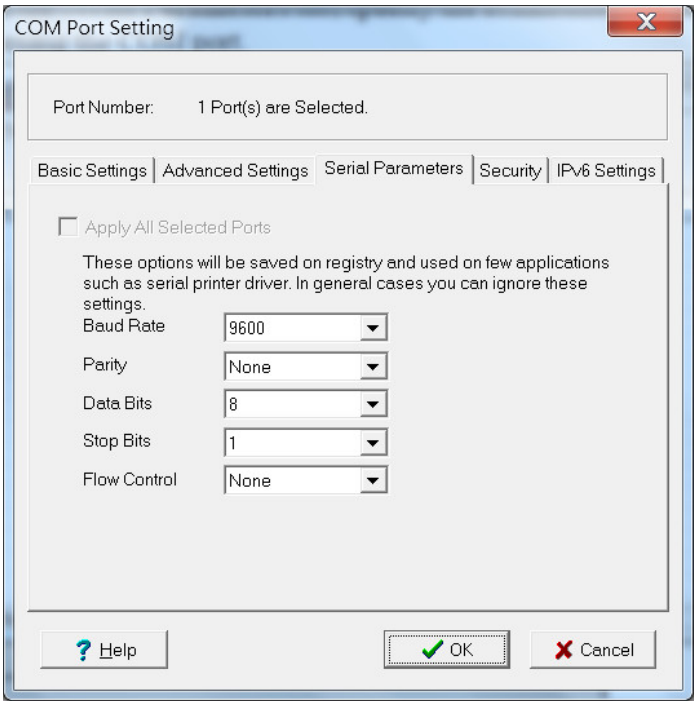
Auto Network Re-Connection: With this option enabled, the driver will repeatedly attempt to re-establish the TCP connection if the NPort does not respond to background “check alive” packets

Always Accept Open Requests: When enabled, the NPort driver will always accept requests to open a virtual COM port, even if communications with the device can not be established. With this option, the NPort driver will agree to open a virtual COM port on the system even if the port is blocked or the Ethernet connection is disabled. If this is the case, the connected device will not receive and transmit data even though the system has opened a virtual COM port.

Drop Writing Data if Network Connection is Lost: This function will assure the data to be kept in the buffer or dropped when network connection is lost. The buffer size is 4 KBytes.

Return error if network is unavailable: If this option is disabled, the driver will not return any error even when a connection cannot be established to the NPort. With this option enabled, calling the Win32 Comm function will result in the error return code “STATUS_NETWORK_UNREACHABLE” when a connection cannot be established to the NPort. This usually means that your host’s network connection is down, perhaps due to a cable being disconnected. However, if you can reach other network devices, it may be that the NPort is not powered on or is disconnected. Not that **Auto Network Re-Connection** must be enabled in order to use this function.

4. On the **Serial Parameters** tab, specify the communication settings that the host will use when opening the COM port.



COM Port Setting

Port Number: 1 Port(s) are Selected.

□ Apply All Selected Ports

These options will be saved on registry and used on few applications such as serial printer driver. In general cases you can ignore these settings.

Baud Rate 9600

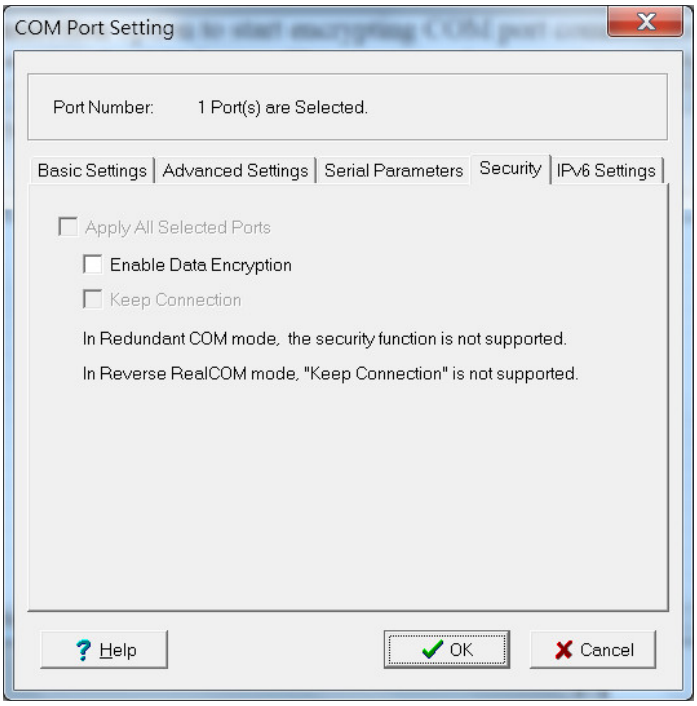
Parity None

Data Bits 8

Stop Bits 1

Flow Control None

5. On the **Security** tab, select the **Enable Data Encryption** option to enable data to be encrypted when transmitted over the COM ports. After selecting the encryption option, select the **Keep connection** option to start encrypting COM port communications immediately without restarting the COM ports. This may speed up opening and closing of the COM port for your host, but it also causes your host to tie up the NPort serial port so other hosts cannot use it.



COM Port Setting

Port Number: 1 Port(s) are Selected.

□ Apply All Selected Ports

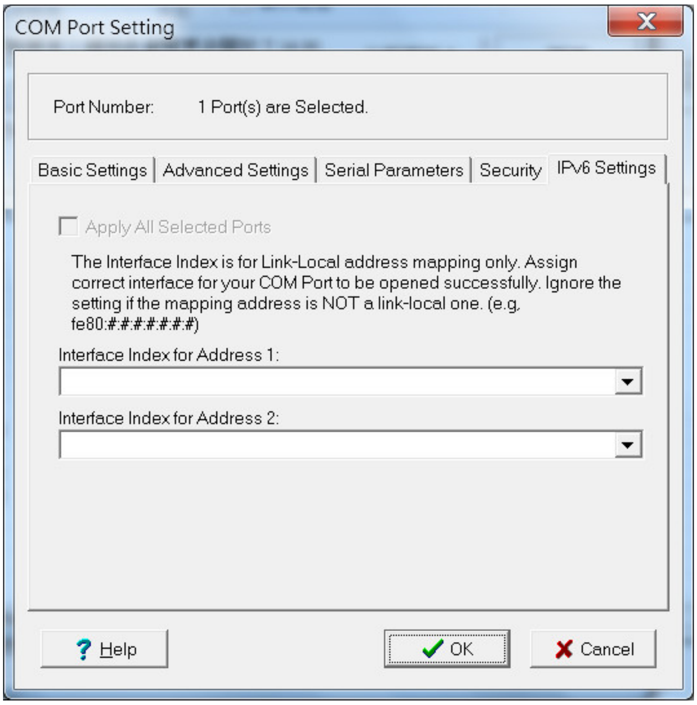
□ Enable Data Encryption

□ Keep Connection

In Redundant COM mode, the security function is not supported.

In Reverse RealCOM mode, "Keep Connection" is not supported.

6. On the IPv6 Setting tab, interface 1 and 2 are able to change.



COM Port Setting

Port Number: 1 Port(s) are Selected.

□ Apply All Selected Ports

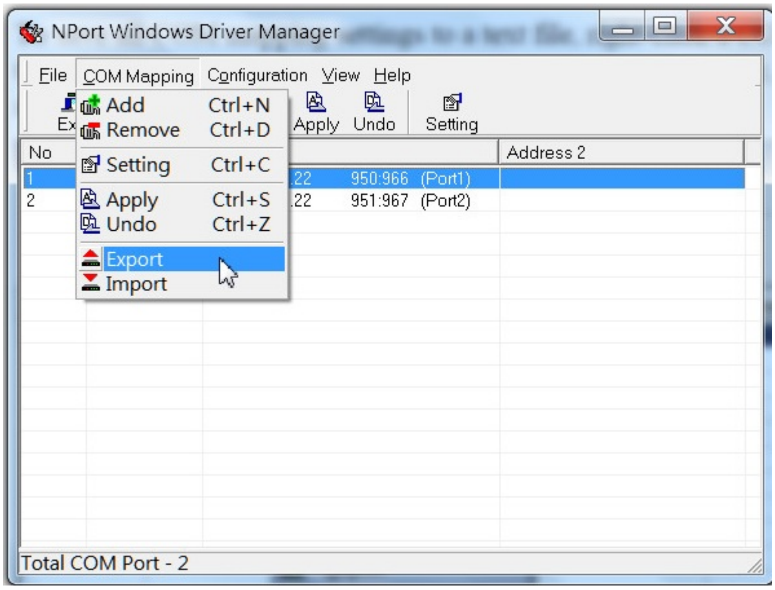
The Interface Index is for Link-Local address mapping only. Assign correct interface for your COM Port to be opened successfully. Ignore the setting if the mapping address is NOT a link-local one. (e.g, fe80:#:#:#:#:#:#:#)

Interface Index for Address 1:

Interface Index for Address 2:

7. Click **[OK]** when you have finished configuring the COM port

8. To save all COM mapping settings to a text file, right-click a COM port and select **Export** in the context menu. After the settings have been exported to a file, they can be imported on another host.



NPort Windows Driver Manager

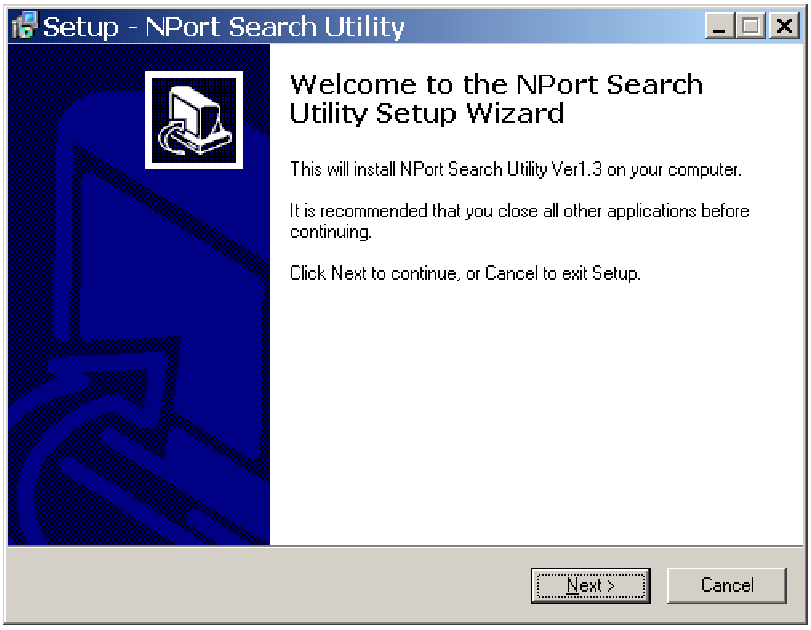
No		Address 2
1	22 950:966 (Port1)	
2	22 951:967 (Port2)	

Total COM Port - 2

NPort Search Utility

Installing NPort Search Utility

1. The main installation window will open when you insert the Document & Software CD. Click **[INSTALL UTILITY]** to proceed. Once the program starts running, click **[Yes]** to proceed.
2. The installation wizard will open. Click **[Next]** to proceed.



Setup - NPort Search Utility

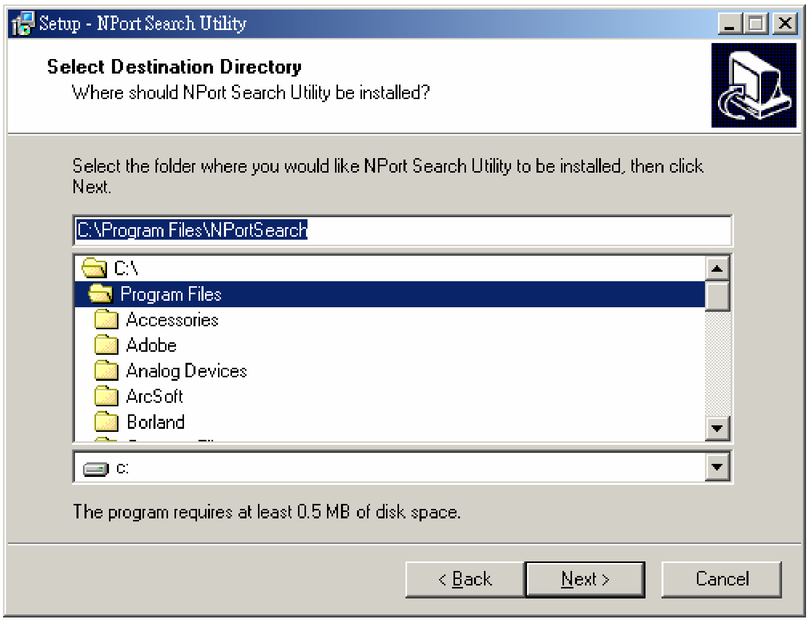
Welcome to the NPort Search Utility Setup Wizard

This will install NPort Search Utility Ver1.3 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

3. Select a destination directory and click **[Next]** to proceed.



Setup - NPort Search Utility

Select Destination Directory

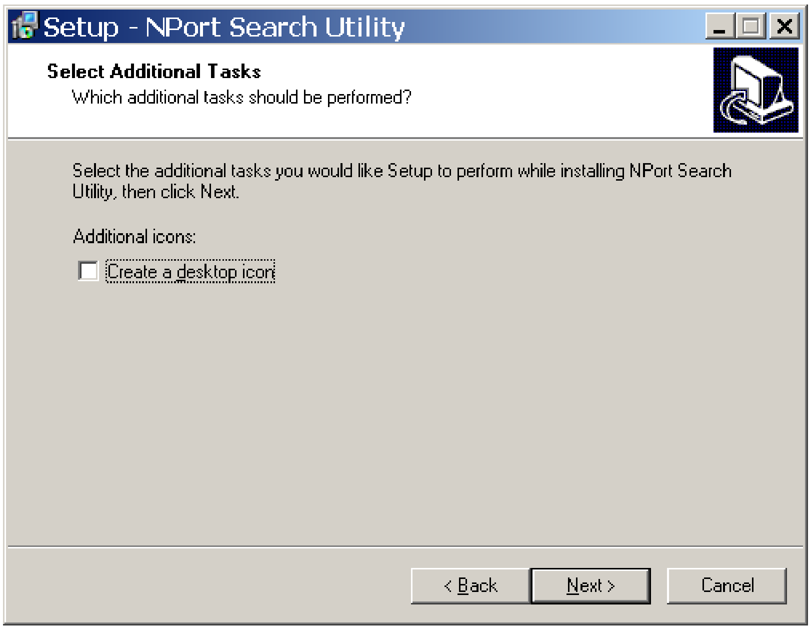
Where should NPort Search Utility be installed?

Select the folder where you would like NPort Search Utility to be installed, then click Next.

C:\Program Files\NPortSearch

The program requires at least 0.5 MB of disk space.

4. Indicate if you wish to create a desktop icon and click **[Next]** to proceed.



Select Additional Tasks

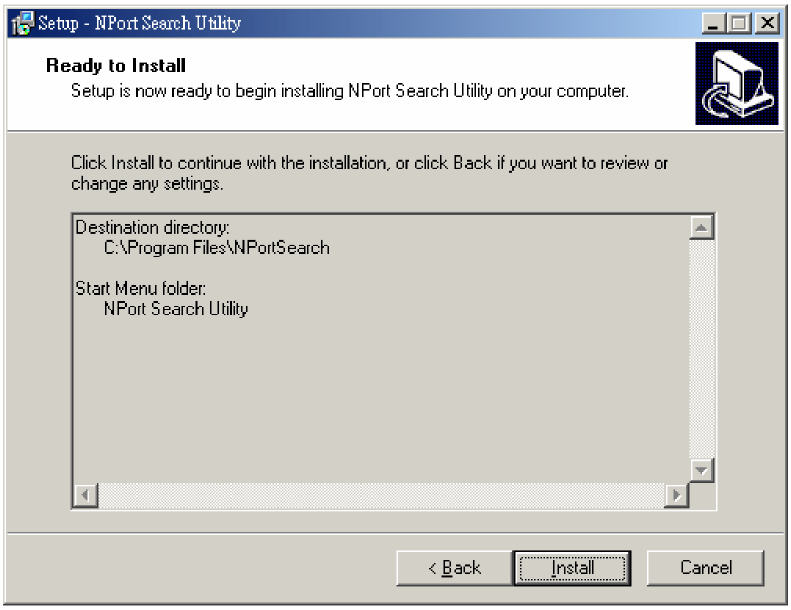
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing NPort Search Utility, then click Next.

Additional icons:

□ Create a desktop icon

5. Verify the installation parameters and click **Install** to proceed.



Ready to Install

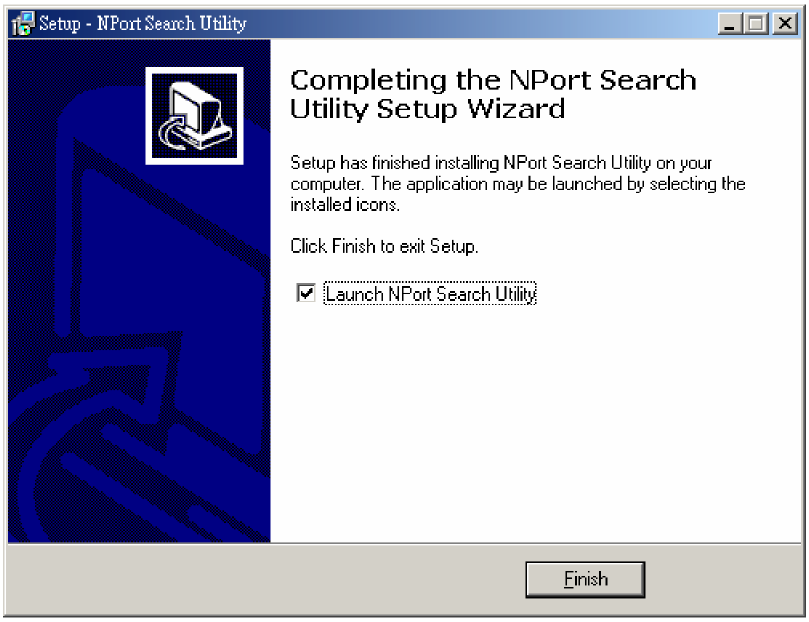
Setup is now ready to begin installing NPort Search Utility on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination directory:
C:\Program Files\NPortSearch

Start Menu folder:
NPort Search Utility

6. The wizard will begin installing the files. After the files have been installed, click **[Finish]** to complete the installation.



Completing the NPort Search Utility Setup Wizard

Setup has finished installing NPort Search Utility on your computer. The application may be launched by selecting the installed icons.

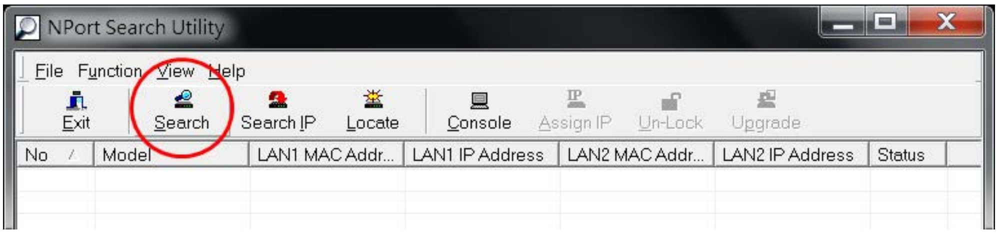
Click Finish to exit Setup.

☑ Launch NPort Search Utility

Finding NPort Device Servers on Network

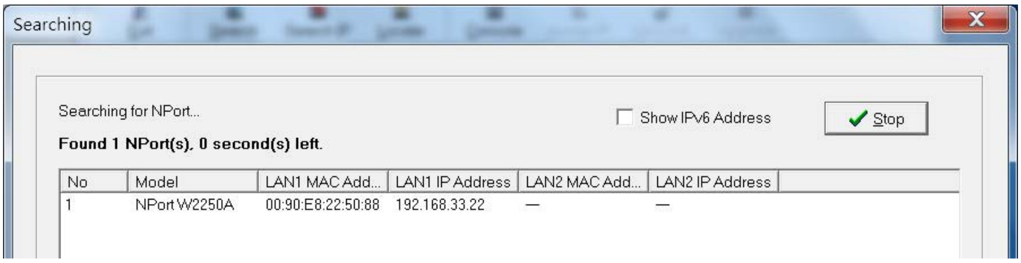
You can use **NPort Search Utility** to look up or change the IP address of any NPort device servers on the network. Since the utility searches by MAC address rather than IP address, all NPort units that are connect to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

1. In **NPort Search Utility**, click **[Search]** on the main toolbar.



No	Model	LAN1 MAC Addr...	LAN1 IP Address	LAN2 MAC Addr...	LAN2 IP Address	Status

2. The utility will being searching for NPort device servers.



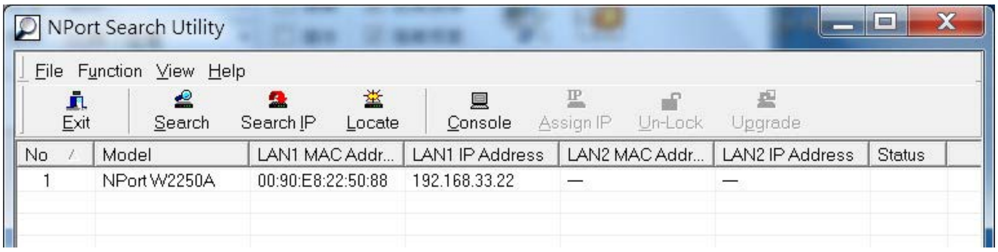
Searching for NPort...

Found 1 NPort(s), 0 second(s) left.

☐ Show IPv6 Address

No	Model	LAN1 MAC Add...	LAN1 IP Address	LAN2 MAC Add...	LAN2 IP Address
1	NPort W2250A	00:90:E8:22:50:88	192.168.33.22	—	—

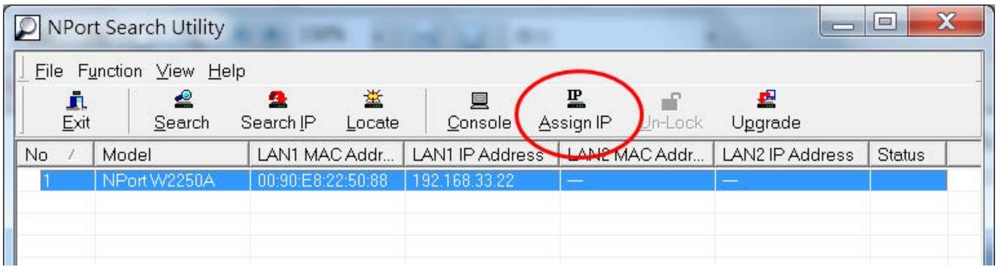
When the search is complete, NPort units that were found will be listed in the main window.



No	Model	LAN1 MAC Addr...	LAN1 IP Address	LAN2 MAC Addr...	LAN2 IP Address	Status
1	NPort W2250A	00:90:E8:22:50:88	192.168.33.22	—	—	

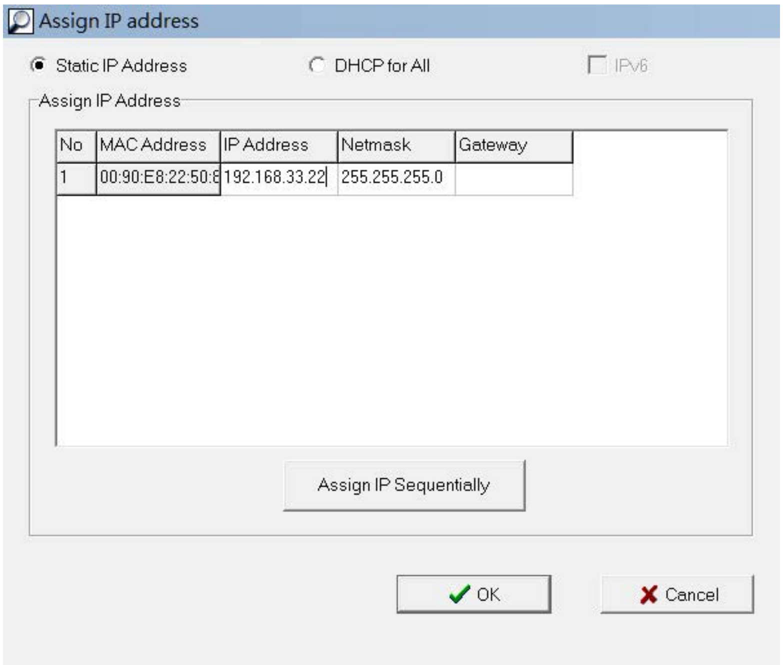
Modifying NPort IP Addresses

1. Once NPort Search Utility has found NPort device servers on the LAN, you can modify any unit’s IP address. Select the desired NPort in the main window and click **[Assign IP]** on the main toolbar. This will modify the IP address for the active network connection (LAN or WLAN).



No	Model	LAN1 MAC Addr...	LAN1 IP Address	LAN2 MAC Addr...	LAN2 IP Address	Status
1	NPort W2250A	00:90:E8:22:50:88	192.168.33.22	—	—	

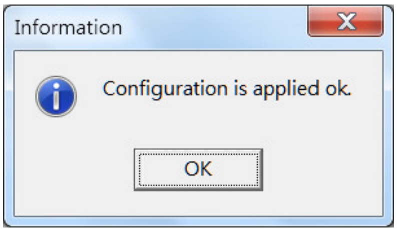
2. Enter the new IP address and netmask. If multiple units were selected, you may assign addresses sequentially by clicking **[Assign IP Sequentially]**. Click **[OK]** to proceed.



● Static IP Address ○ DHCP for All □ IPv6

No	MAC Address	IP Address	Netmask	Gateway
1	00:90:E8:22:50:8	192.168.33.22	255.255.255.0	

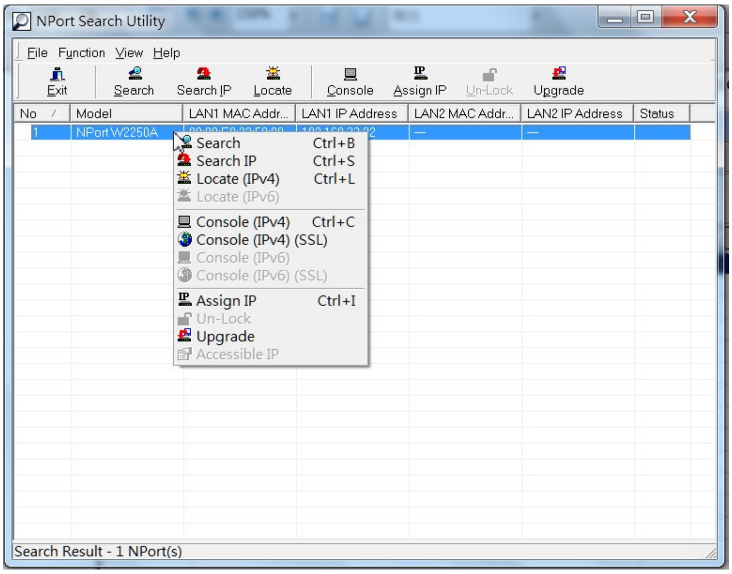
3. The selected NPort will be restarted by NPort Search Utility with the new IP address.



Configuration is applied ok.

Upgrading NPort Firmware

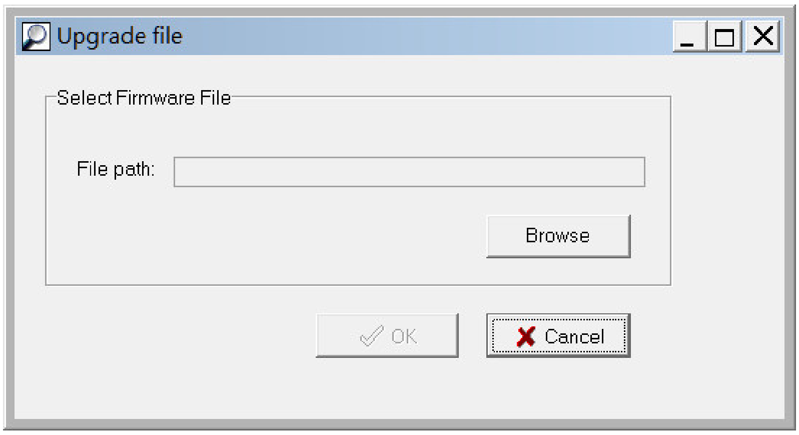
1. Once NPort Search Utility has found NPort device servers on the LAN, you can upgrade any unit's firmware. Right-click the desired NPort in the main window and select **Upgrade**.



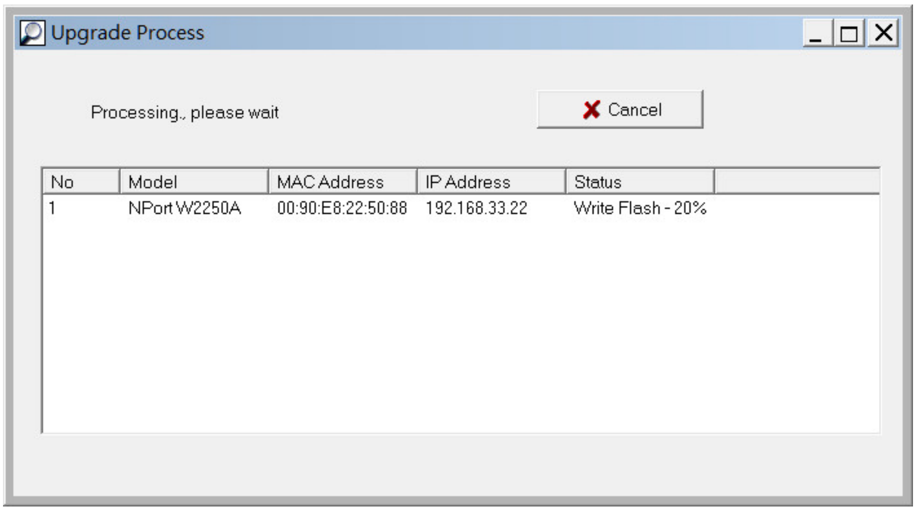
No	Model	LAN1 MAC Addr...	LAN1 IP Address	LAN2 MAC Addr...	LAN2 IP Address	Status
1	NPort W2250A	00:90:E8:22:50:88	192.168.33.22	—	—	

Search Result - 1 NPort(s)

2. Select the new firmware file and click **[OK]** to proceed. To obtain the latest firmware for the NPort W2150A/W2250A, visit www.moxa.com.



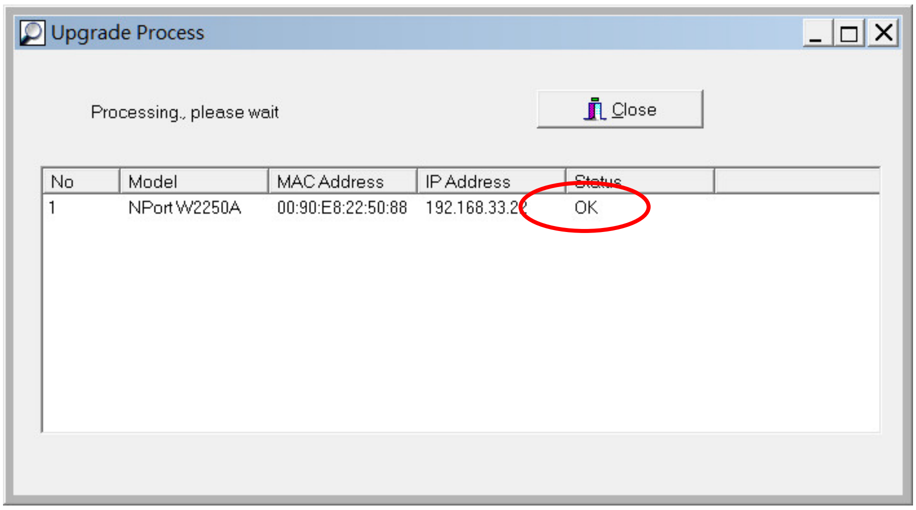
3. The utility will begin upgrading the firmware for the selected unit. Do not disconnect or power off the unit while the firmware is being upgraded.



Processing, please wait

No	Model	MAC Address	IP Address	Status
1	NPort W2250A	00:90:E8:22:50:88	192.168.33.22	Write Flash - 20%

4. When the displayed status is "**OK**", click **[Close]** to complete the process.



Processing., please wait

No	Model	MAC Address	IP Address	Status
1	NPort W2250A	00:90:E8:22:50:88	192.168.33.2	OK

ATTENTION

NPort Search Utility supports upgrading the firmware of multiple units simultaneously, if each unit is the same model. Hold down the CTRL to add additional units to your selection; hold down the SHIFT key to select a block of units.

Linux Real TTY Drivers

Real TTY driver are provided that will map Linux host TTY ports to NPort serial ports. Once the mapping has been set up, Linux users and applications can connect to a serial port as if it were a local TTY port. These drivers have been designed and tested for the majority of Linux distributions, including Linux kernel version 2.4.x, 2.6.x, and 3.x. Please check http://www.moxa.com for the latest Linux kernel supported.

Basic Steps

Follow these instructions to map a TTY port to a NPort serial port:

1. Install the NPort device server and set the target device port to RealCOM mode.
2. Install the Real TTY driver files on the Linux host.
3. Map the host's TTY port to the target device port on the NPort.

Installing Linux Real TTY Driver Files

Before proceeding with the software installation, make sure you have completed the NPort device server has been installed and configured correctly. Note that the default LAN IP address for the NPort is **192.168.126.254**, whereas the default WLAN IP address is **192.168.127.254**.

ATTENTION

The target serial port must be operating in RealCOM mode in order to map TTY ports.

1. Obtain the driver file from the Document and Software CD, or from http://www.moxa.com.
2. Log in to the console as a super user (root).
3. Execute **cd /** to go to the root directory.
4. Copy the driver file **npreal2xx.tgz** to the / directory.

5. Execute **tar xvfz npreal2xx.tgz** to extract all files into the system.
6. Execute **/tmp/moxa/mxinst**. (For RedHat AS/ES/WS and Fedora Core1, execute "**# /tmp/moxa/mxinst SP1**".) The shell script will install the driver files automatically.
7. After installing the driver, you will be able to see several files in the **/usr/lib/npreal2/driver** folder:

   mxaddsvr (add server, map TTY port)
   mxdelsvr (delete server, undo TTY port mapping)
   mxloadsvr (reload server)
   mxmknod (create device node/TTY port)
   mxrmnod (remove device node/TTY port)
   mxuninst (remove TTYport and driver files)

   At this point, you may map the TTY port to the NPort serial port.

Mapping TTY Ports

Make sure that you set the operation mode of the desired NPort serial port to RealCOM mode. After logging in as a super user, enter the directory **/usr/lib/npreal2/driver** and then execute **mxaddsvr** to map the target NPort serial port to the host TTY ports. The syntax of **mxaddsvr** is as follows:

mxaddsvr [*NPort IP Address*] [*Total Ports*] ([*Data port*] [*Cmd port*])

The **mxaddsvr** command performs the following actions:

1. Modify npreal2d.cf.
2. Create TTY ports in directory /dev with major and minor number configured in npreal2d.cf.
3. Restart the driver.

Mapping TTY ports automatically

To map TTY ports automatically, you may execute **mxaddsvr** with just the IP address and number of ports, as in the following example:

```
# cd /usr/lib/npreal2/driver
# ./mxaddsvr 192.168.3.4 16
```

In this example, 16 TTY ports will be added, all with IP 192.168.3.4, with data ports from 950 to 965 and command ports from 966 to 981.

Mapping TTY ports manually

To map TTY ports manually, you may execute **mxaddsvr** and manually specify the data and command ports, as in the following example:

```
# cd /usr/lib/npreal2/driver
# ./mxaddsvr 192.168.3.4 16 4001 966
```

In this example, 16 TTY ports will be added, all with IP 192.168.3.4, with data ports from 4001 to 4016 and command ports from 966 to 981.

Removing Mapped TTY Ports

After logging in as root, enter the directory **/usr/lib/npreal2/driver** and then execute **mxdelsvr** to delete a server. The syntax of mxdelsvr is:

mxdelsvr [*IP Address*]

Example:

```
# cd /usr/lib/npreal2/driver
# ./mxdelsvr 192.168.3.4
```

The following actions are performed when executing **mxdelsvr**:

1. Modify npreal2d.cf.
2. Remove the relevant TTY ports in directory /dev.
3. Restart the driver.

If the IP address is not provided in the command line, the program will list the installed servers and total ports on the screen. You will need to choose a server from the list for deletion.

Removing Linux Driver Files

A utility is included that will remove all driver files, mapped TTY ports, and unload the driver. Enter the directory **/usr/lib/npreal2/driver** and execute **mxuninst** to uninstall the driver. This program will perform the following actions:

1. Unload the driver.
2. Delete all files and directories in /usr/lib/npreal2.
3. Delete directory /usr/lib/npreal2.
4. Modify the system initializing script file.

UNIX Fixed TTY Drivers

A fixed TTY driver is provided that will map UNIX host TTY ports to NPort serial ports. Once the mapping has been set up, UNIX users and applications can connect to an NPort serial port as if it were a local TTY port. This driver has been designed and tested for the majority of UNIX systems. Please check http://www.moxa.com for the latest UNIX systems support.

Installing the UNIX Driver

1. Log in to UNIX and create a directory for the MOXA TTY. To create a directory named **/usr/etc**, execute the command:

   ```
   # mkdir –p /usr/etc
   ```

2. Copy **moxattyd.tar** to the directory you created. For the **/usr/etc** directory, you would execute the following commands:

   ```
   # cp moxattyd.tar /usr/etc
   # cd /usr/etc
   ```

3. Extract the source files from the tar file by executing the command:

   ```
   # tar xvf moxattyd.tar
   ```

   The following files will be extracted:

   README.TXT
   moxattyd.c --- source code
   moxattyd.cf --- an empty configuration file
   Makefile --- makefile
   VERSION.TXT --- fixed TTY driver version
   FAQ.TXT

4. Compile and link.

   For SCO UNIX:

   ```
   # make sco
   ```

   For UnixWare 7:

   ```
   # make svr5
   ```

   For UnixWare 2.1.x, SVR4.2:

   ```
   # make svr42
   ```

Configuring the UNIX Driver

Modify the configuration:

The configuration used by **moxattyd** is defined in the text file **moxattyd.cf**, which is in the same directory. You may use vi or any text editor to modify the file, as follows:

```
ttyp1 192.168.1.1 950
```

You can refer to **moxattyd.cf** for detailed descriptions of the various configuration parameters. Please note that “Device Name” depends on the OS. See the Device Naming Rule section in README.TXT for more information.

To start the moxattyd daemon after system bootup, add an entry into **/etc/inittab** using the TTY name you defined in **moxattyd.cf**, as in the following example:

```
ts:2:respawn:/usr/etc/moxattyd/moxattyd –t 1
```

Device naming rule

For UnixWare 7, UnixWare 2.1.x, and SVR4.2, use:
pts/[*n*]

For all other UNIX operating systems, use:
ttyp[*n*]

The value of [n] should be equal or larger than 11 in order to prevent conflicts with the device names of functional keys in some UNIX systems.

Starting moxattyd

Execute the command **init q** or reboot your UNIX operating system.

Adding an additional server

Modify the text file **moxattyd.cf** to add an additional server. User may use vi or any text editor to modify the file. For more configuration information, refer to **moxattyd.cf**, which contains detailed descriptions of the various configuration parameters.

Find the process ID (PID) of the **moxattyd**.
# ps -ef | grep moxattyd

Update the configuration of **moxattyd**.
# kill -USR1 [*PID*]
(e.g., if moxattyd PID = 404, **kill -USR1 404**)

This completes the process of adding an additional server.

A

SNMP Agents with MIB II & RS-232-Like Groups

The NPort has built-in SNMP (Simple Network Management Protocol) agent software that supports SNMP Trap, RFC1317 RS-232 like groups and RFC 1213 MIB-II. The following table lists the standard MIB-II groups, as well as the variable implementation for the NPort.

RFC1213 MIB-II Supported SNMP Variables

System MIB

SysDescr
SysObjectID
SysUpTime
SysContact
SysName
SysLocation
SysServices

Interfaces MIB

itNumber
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
ifOperStatus
ifLastChange
ifInOctets
ifInUcastPkts
ifInNUcastPkts
ifInDiscards
ifInErrors
ifInUnknownProtos
ifOutOctets
ifOutUcastPkts
ifOutNUcastPkts
ifOutDiscards
ifOutErrors
ifOutQLen
ifSpecific

IP MIB

ipForwarding
ipDefaultTTL
ipInreceives
ipInHdrErrors
ipInAddrErrors
ipForwDatagrams
ipInUnknownProtos
ipInDiscards
ipInDelivers
ipOutRequests
ipOutDiscards
ipOutNoRoutes
ipReasmTimeout
ipReasmReqds
ipReasmOKs
ipReasmFails
ipFragOKs
ipFragFails
ipFragCreates
ipAdEntAddr
ipAdEntIfIndex
ipAdEntNetMask
ipAdEntBcastAddr
ipAdEntReasmMaxSize
IpNetToMediaIfIndex
IpNetToMediaPhysAddress
IpNetToMediaNetAddress
IpNetToMediaType
IpRoutingDiscards

ICMP MIB

IcmpInMsgs
IcmpInErrors
IcmpInDestUnreachs
IcmpInTimeExcds
IcmpInParmProbs
IcmpInSrcQuenchs
IcmpInRedirects
IcmpInEchos
IcmpInEchoReps
IcmpInTimestamps
IcmpTimest ampReps
IcmpInAddrMasks
IcmpOutMsgs
IcmpOutErrors
IcmpOutDestUnreachs
IcmpOutTimeExcds
IcmpOutParmProbs
IcmpOutSrcQuenchs
IcmpOutRedirects
IcmpOutEchos
IcmpOutEchoReps
IcmpOutTimestamps
IcmpOutTimestampReps
IcmpOutAddrMasks
IcmpOutAddrMaskReps

UDP MIB

UdpInDatagrams
UdpNoPorts
UdpInErrors
UdpOutDatagrams
UdpLocalAddress
UdpLocalPort

Address Translation

AtIfIndex
AtPhysAddress
AtNetAddress

TCP MIB

tcpRtoAlgorithm
tcpRtoMin
tcpRtoMax
tcpMaxConn
tcpActiveOpens
tcpPassiveOpens
tcpAttempFails
tcpEstabResets
tcpCurrEstab
tcpInSegs
tcpOutSegs
tcpRetransSegs
tcpConnState
tcpConnLocalAddress
tcpConnLocalPort
tcpConnRemAddress
tcpConnRemPort
tcpInErrs
tcpOutRsts

SNMP MIB

snmpInPkts
snmpOutPkts
snmpInBadVersions
snmpInBadCommunityNames
snmpInASNParseErrs
snmpInTooBigs
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnlys
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetRequests
snmpInGetNexts
snmpInSetRequests
snmpInGetResponses
snmpInTraps
snmpOutTooBigs
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEnableAuthenTraps

RFC1317: RS-232 MIB Objects

Generic RS-232-like Group

rs232Number

RS-232-like General Port Table

rs232PortTable
rs232PortEntry
rs232PortIndex
rs232PortType
rs232PortInSigNumber
rs232PortOutSigNumber
rs232PortInSpeed
rs232PortOutSpeed

RS-232-like Asynchronous Port Group

rs232AsyncPortTable
rs232AsyncPortEntry
rs232AsyncPortIndex
rs232AsyncPortBits
rs232AsyncPortStopBits
rs232AsyncPortParity

The Input Signal Table

rs232InSigTable
rs232InSigEntry
rs232InSigPortIndex
rs232InSigName
rs232InSigState

The Output Signal Table

rs232OutSigTable
rs232OutSigEntry
rs232OutSigPortIndex
rs232OutSigName
rs232OutSigState

B

Well Known Port Numbers

Listed below are Well Known Port Numbers that may cause network problems if they are assigned to an NPort serial port. Refer to RFC 1700 for Well Known Port Numbers or refer to the following introduction from IANA.

The port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports.

- **Well Known Ports** range from 0 through 1023.
- **Registered Ports** range from 1024 through 49151.
- **Dynamic and/or Private Ports** range from 49152 through 65535.

The Well Known Ports are assigned by IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. The following table shows famous port numbers among the well-known port numbers. For more details, please visit the IANA website at http://www.iana.org/assignments/port-numbers.

TCP Socket	Application Service
0	reserved
1	TCP Port Service Multiplexor
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
13	Daytime
15	Netstat
20	FTP data port
21	FTP CONTROL port
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
37	Time (Time Server)
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (Login)
53	Domain Name Server (domain)
79	Finger protocol (Finger)
80	World Wide Web HTTP
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol
213	IPX
160 to 223	Reserved for future use

UDP Socket	Application Service
0	reserved
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
13	Daytime
35	Any private printer server
39	Resource Location Protocol
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (Login)
53	Domain Name Server (domain)
69	Trivial Transfer Protocol (TETP)
70	Gopher Protocol
79	Finger Protocol
80	World Wide Web HTTP
107	Remote Telnet Service
111	Sun Remote Procedure Call (Sunrpc)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
161	(Simple Network Mail Protocol (SNMP)
162	SNMP Traps
213	IPX (Used for IP Tunneling)

C

Ethernet Modem Commands

A serial port on the NPort can be set to Ethernet Modem mode, allowing a PC or device to connect to the NPort as if it was an Ethernet modem. This section provides additional detail about how the NPort operates in Ethernet Modem mode.

Dial-in Operation

The NPort can listen for a TCP/IP connection request from a remote Ethernet modem or host. The NPort's response depends on the ATS0 value, as follows.

ATS0=0: The NPort will temporarily accept the TCP connection and then send the "**RING**" signal out through the serial port. The serial controller must reply with "**ATA**" within 2.5 seconds to accept the connection request, after which the NPort enters data mode. If no "**ATA**" command is received, the NPort will disconnect after sending three "**RING**" signals.

ATS0≧1: The NPort will accept the TCP connection immediately. It will send the "**CONNECT** {*baudrate*}" command to the serial port and will immediately enter data mode.

Dial-out

The NPort accepts ATD commands such as "**ATD 192.168.1.1:4001**" from the serial port. It will then request a TCP connection from the specified remote Ethernet modem or PC. Once the remote unit accepts this TCP connection, the NPort will send the "**CONNECT** {*baudrate*}" command to the serial port and will immediately enter data mode.

Disconnection Request from Local Site

When the NPort is in data mode, you can initiate disconnection by sending "**+++**". Some applications allow you to directly set the DTR signal to off, which will also initiate disconnection. The NPort will enter command mode, and you can then enter "**ATH**" to close the TCP connection "**NO CARRIER**" will be returned to the serial port.

⚠ **ATTENTION**

When entering "+++" to disconnect, the three "+" characters must be sent in quick succession, and the sequence must be prefaced and followed by a guard time to protect the raw data. You can change the disconnect character using register S2. You can set the guard time using register S12.

Disconnection Request from Remote Site

After the TCP connection has been closed by the remote Ethernet modem or PC, the NPort will send "**NO CARRIER**" to the serial port and will return to command mode.

AT Commands

Ethernet Modem mode supports the following common AT commands, as used with a typical modem:

No.	Command	Description	Remarks
1	ATA	Answer manually	
2	ATD	Dial up specified IP address and port number ATD 192.168.1.1:950 (example)	

3	ATE	ATE0=Echo OFF
		ATE1=Echo ON (default)	

4	ATH	ATH0=On-hook (default)
		ATH1=Off-hook	

5	ATI, ATI0, ATI1, ATI2	Modem version	reply “OK” only
6	ATL	Speaker volume option	reply “OK” only
7	ATM	Speaker control option	reply “OK” only
8	ATO	On line command	
9	ATP, ATT	Set Pulse/Tone Dialing mode	reply “OK” only
10	ATQ0, ATQ1	Quiet command (default=ATQ0)	
11	ATSr=n	Change the contents of S register	see “S registers”
12	ATSr?	Read the contents of S register	see “S registers”
13	ATV	Result code type ATV0 for digit code, ATV1 for text code (default) 0=OK 1=connect 2=ring 3=No carrier 4=error	
14	ATZ	Reset (disconnect, enter command mode and restore the flash settings)	
15	AT&C	Serial port DCD control AT&C0=DCD always on AT&C1=DTE detects connection by DCD on/off (default)	
16	AT&F	Restore manufacturer’s settings	
17	AT&G	Select guard time	reply “OK” only
18	AT&R	Serial port RTS option command	reply “OK” only
19	AT&S	Serial port DSR control	reply “OK” only
20	AT&V	View settings	
21	AT&W	Write current settings to flash for next boot up	

S Registers

No.	Register	Description	Remarks
1	S0	Ring to auto-answer (default=0)	
2	S1	Ring counter (always=0)	no action applied
3	S2	Escape code character (default=43 ASCII "+")	
4	S3	Return character (default=13 ASCII)	
5	S4	Line feed character (default=10 ASCII)	
6	S5	Backspace character (default= 8 ASCII)	
7	S6	Wait time for dial tone (always=2, unit=sec)	no action applied
8	S7	Wait time for carrier (default=3, unit=sec)	
9	S8	Pause time for dial delay (always=2, unit=sec)	no action applied
10	S9	Carrier detect response time (always=6, unit 1/10 sec)	no action applied
11	S10	Delay for hang up after carrier (always=14, unit 1/10 sec)	no action applied
12	S11	DTMF duration and spacing (always=100 ms)	no action applied
13	S12	Escape code guard time (default=50, unit 1/50 sec) to control the idle time for "+++"	

D

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference and
2. This device must accept any interference received, including interference that may cause undesired operation.

Labeling requirements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: "Contains FCC ID: SLE-W2X50A "

Information for the OEMs and Integrators

The following statement must be included with all versions of this document supplied to an

OEM or integrator, but should not be distributed to the end user.

1. This device is intended for OEM integrators only.
2. Please see the full Grant of Equipment document for other restrictions.

This radio transmitter FCCID: SLE-W2X50A has been approved by FCC to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna List

No.	Manufacturer	Model No.	Antenna Type	Peak Gain
1	KINSUN	ANT-WDB-ARM-02	Dipole Antenna	1.21 dBi for 2.4GHz 1.73 dBi for 5GHz

Note: The antenna connector is Reverse SMA type.

E

FCC Warning Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. The operation frequency of the device is in the 5150-5250 MHz band and is for indoor use only.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety Information

To maintain compliance with FCC's RF exposure guidelines, when installing and/or operating this equipment, you should maintain a minimum distance of 20 cm between the transmitter and your body. Use only the supplied antenna. Unauthorized antennae, modifications, or attachments could damage the transmitter and may violate FCC regulations.