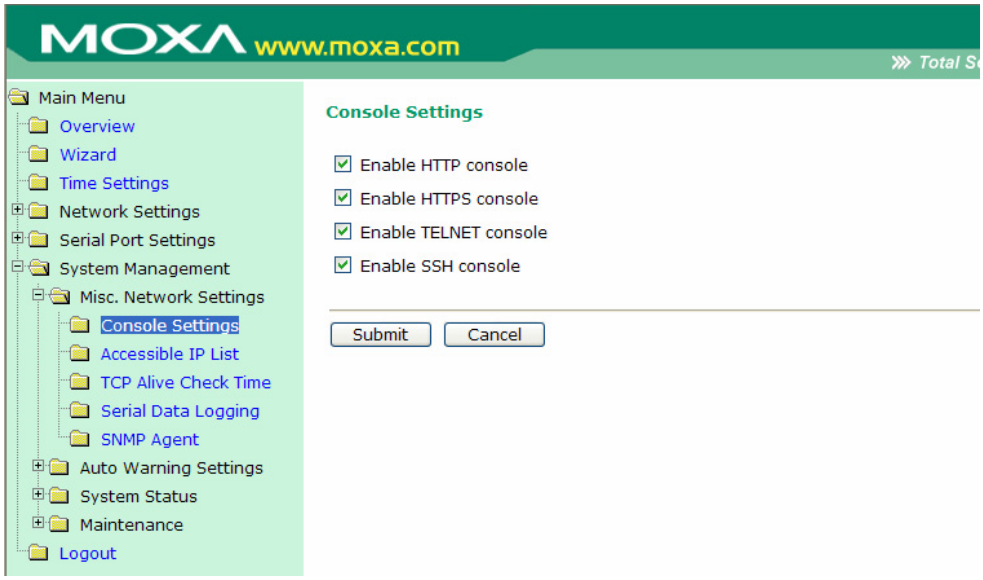
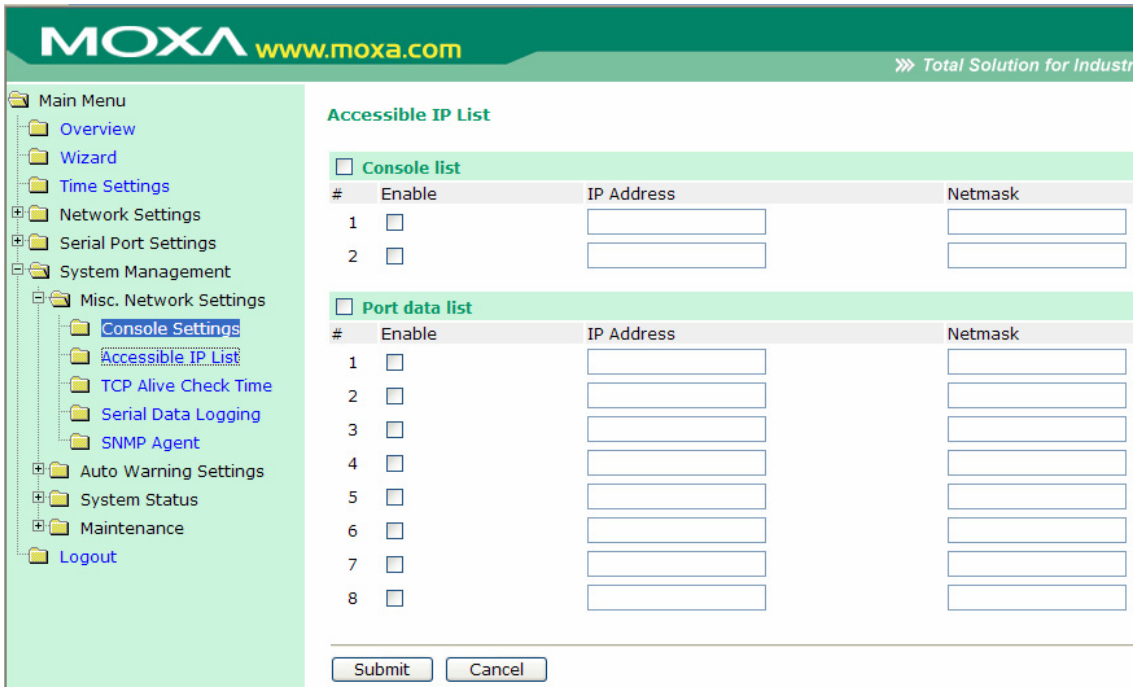


Use this screen to enable or disable **HTTP console**, **HTTPS console**, **TELNET console**, and **SSH console**.

Accessible IP List



NPort W2004 uses an IP address based filtering method to control access to itself.

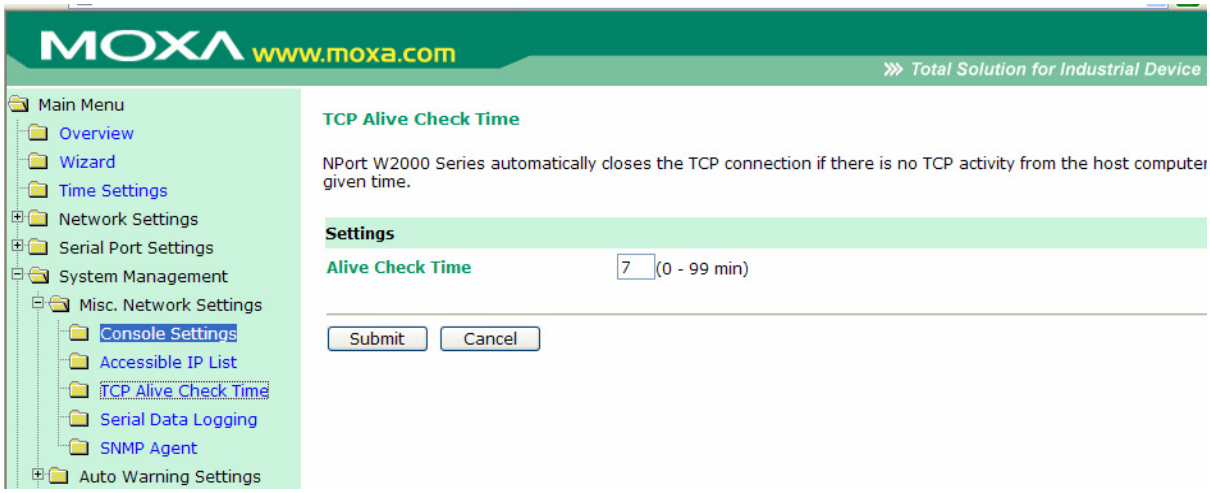
Accessible IP Settings allows you to add or block remote host IP addresses to prevent unauthorized access. Access to NPort W2004 is controlled by IP address. That is, if a host's IP address is in the accessible IP table, then the host will be allowed to access the NPort W2004. You can set up one of the following cases by setting the parameters accordingly.

- **Only one host with a specific IP Address can access the NPort W2004**
  Enter the specific IP address (e.g., 192.168.1.1), and enter 255.255.255.255 for Netmask.
- **Hosts on the specific subnet can access the NPort W2004**
  Enter an IP address (e.g., 192.168.1.0), and enter the Netmask (e.g., 255.255.255.0). Note that this type of setting will allow access to all network hosts on a particular subnet.
- **Any host can access the NE-4000T**
  Disable this function by un-checking the "Enable the accessible IP list" checkbox. Refer to the following table for more configration examples.

The following "Allowable Hosts" table gives five configuration examples.

Allowable Hosts	IP Address	Netmask
Any host	*blank*	*blank*
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0	255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128	255.255.255.128

TCP Alive Check Time



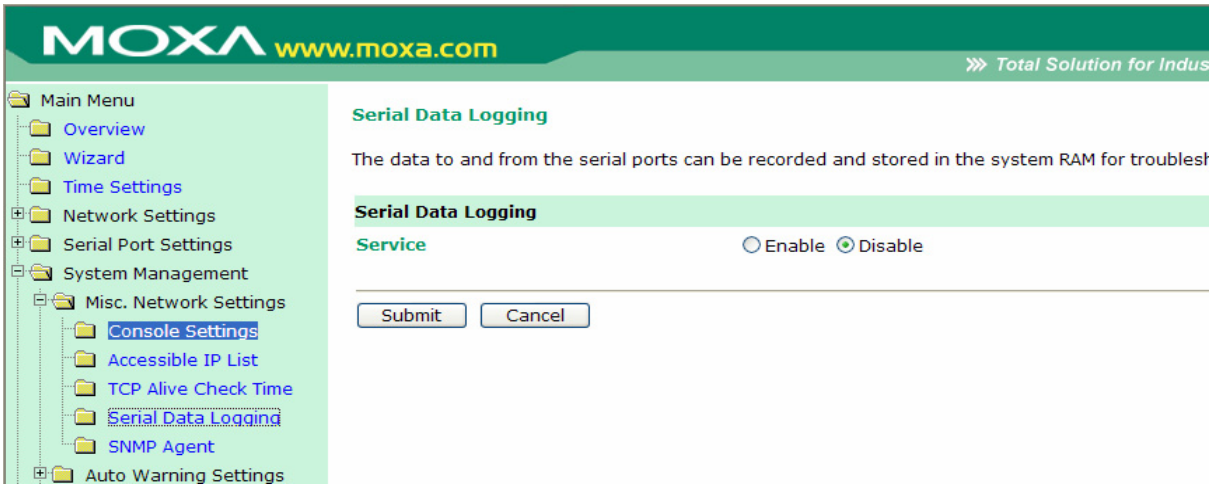
TCP alive check time

Setting	Factory Default	Necessity
0 to 99 min	7 min	Optional

0 min: TCP connection is not closed due to an idle TCP connection.

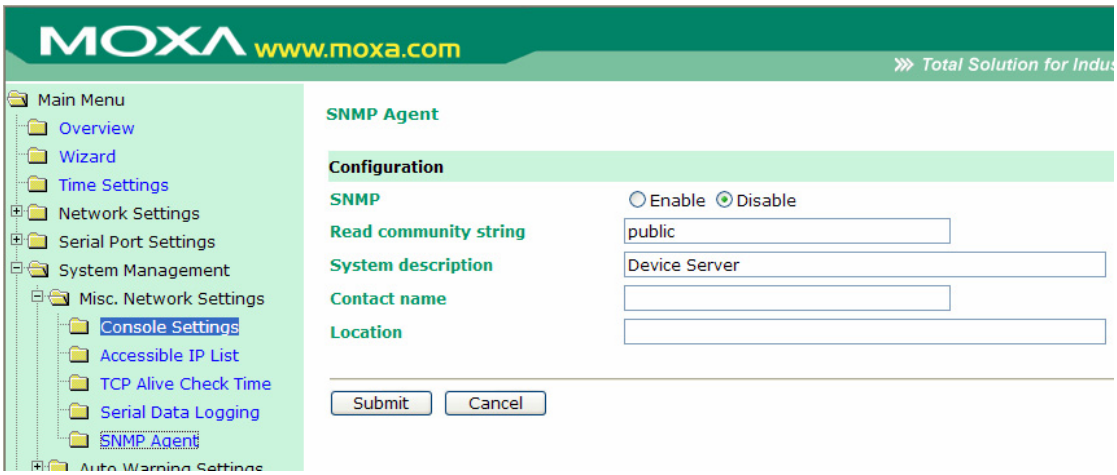
1 to 99 min: NPort W2004 automatically closes the TCP connection if there is no TCP activity for the given time. After the connection is closed, NPort W2004 starts listening for another host's TCP connection.

Serial Data Logging



NPort provides the capability to store data logs for all serial ports. The logs will be stored in the system RM. The data will be deleted when NPort is powered off. Due to the system's SDRAM limitation, the memory size of local buffers is fixed. Each serial port is allotted 64 KB to store the port's log file.

SNMP Agent



To enable the SNMP Agent function, select the enable option, and enter a Community Name (e.g., "public").

Community name

Setting	Factory Default	Necessity
1 to 39 characters (e.g., Support, 886-89191230 #300)	public	Optional

A community name is a plain-text password mechanism that is used to authenticate weakly queries to agents of managed network devices.

Contact

Setting	Factory Default	Necessity

1 to 39 characters (e.g., Support, 886-89191230 #300)	None	Optional

The SNMP contact information usually includes an emergency contact name and telephone or pager number.

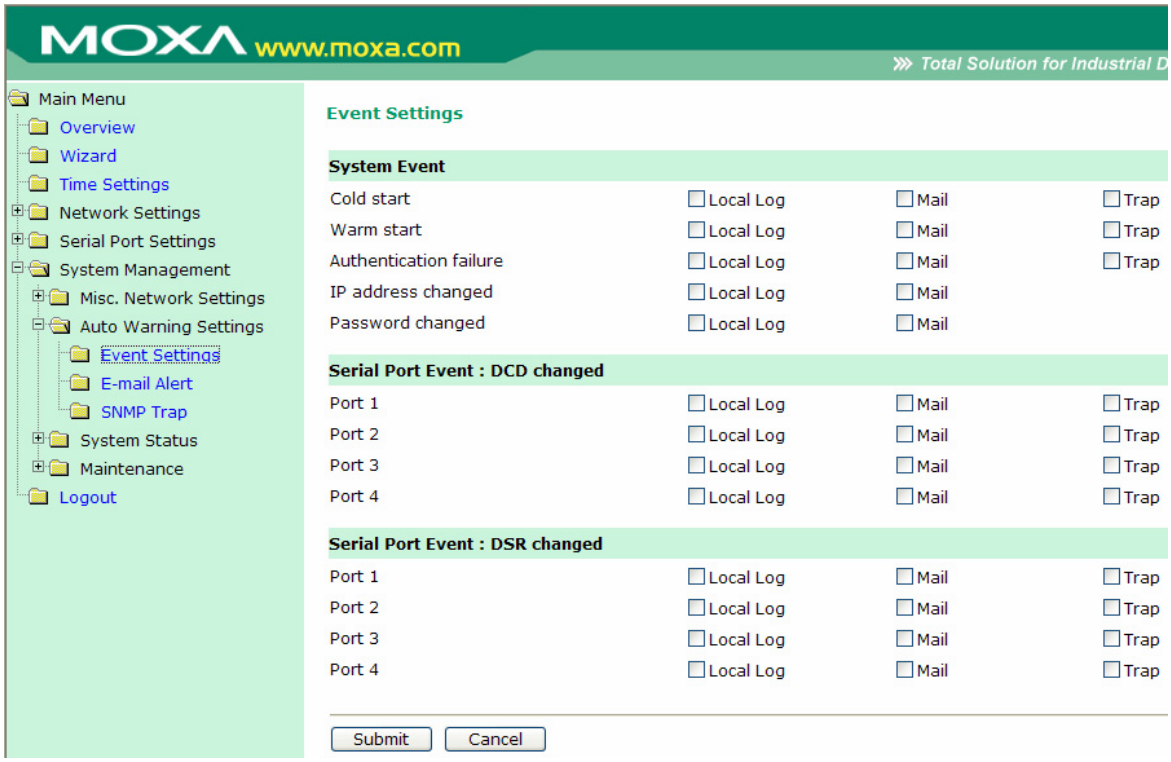
Location

Setting	Factory Default	Necessity
1 to 39 characters (e.g., Floor 1, Office No. 2)	None	Optional

Specify the location string for SNMP agents such as NPort W2004. This string is usually set to the street address where the NPort W2004 is physically located.

Auto Warning Settings

Event Settings



System Event

Cold start

This refers to starting the system from power off (contrast this with warm start). When performing a cold start, NPort W2004 will automatically issue an Auto warning message by e-mail, or send an SNMP trap after booting up.

Warm start

This refers to restarting the computer without turning the power off. When performing a warm

start, NPort W2004 will automatically send an e-mail, or send an SNMP trap after rebooting.

Authentication Failure
The user inputs a wrong password from the Console or Administrator. When authentication failure occurs, NPort W2004 will immediately send an e-mail or send an SNMP trap.

IP address changed
The user has changed NPort W2004's IP address. When the IP address changes, NPort W2004 will send an e-mail with the new IP address before NPort W2004 reboots. If the NPort W2004 is unable to send an e-mail message to the mail server within 15 seconds, NPort W2004 will reboot anyway, and abort the e-mail auto warning.

Password changed
The user has changed NPort W2004's password. When the password changes, NPort W2004 will send an e-mail with the password changed notice before NPort W2004 reboots. If the NPort W2004 is unable to send an e-mail message to the mail server within 15 seconds, NPort W2004 will reboot anyway, and abort the e-mail auto warning.

Serial Port Event : DCD Changed

The DCD (Data Carrier Detect) signal has changed, also indicating that the modem connection status has changed. For example, a DCD change to high also means "Connected" between local modem and remote modem. If the DCD signal changes to low, it also means that the connection line is down.

When the DCD changes, NPort W2004 will immediately send an e-mail or send an SNMP trap.

Serial Port Event : DSR Changed

The DSR (Data Set Ready) signal has changed, also indicating that the data communication equipment's power is off. For example, a DSR change to high also means that the DCE is powered ON. If the DSR signal changes to low, it also means that the DCE is powered off.

When the DSR changes, NPort W2004 will immediately send an e-mail or send an SNMP trap.

Checkbox Items

Local Log

Setting	Factory Default	Necessity
Enable, Disable	Disable	Optional

This feature helps the administrator manage how the NPort W2004 logs system events when enabled events—such as Cold start, Warm start, Authentication failure, etc.—occur. To configure this feature, click on the Event Type **Local Log** checkbox.

Mail

Setting	Factory Default	Necessity
Enable, Disable	Disable	Optional

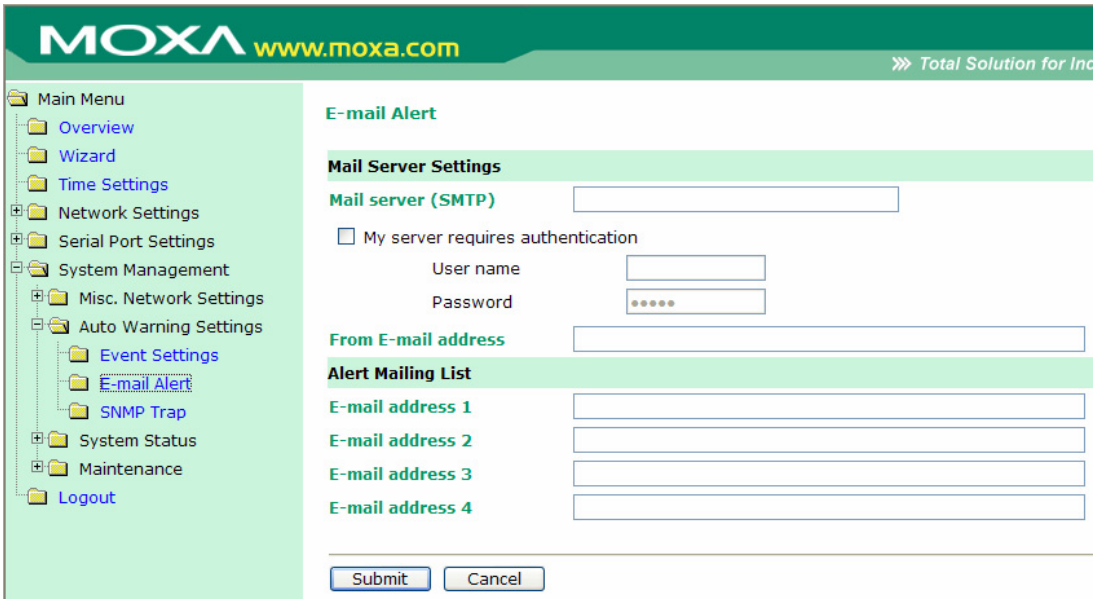
This feature helps the administrator manage how the NPort W2004 sends e-mail to pre-defined e-mail boxes when the enabled events—such as Cold start, Warm start, Authentication failure, etc.—occur. To configure this feature, click on the Event Type **Mail** checkbox.

Trap

Setting	Factory Default	Necessity
Enable, Disable	Disable	Optional

This feature helps the administrator manage how the NPort W2004 sends SNMP Trap to a pre-defined SNMP Trap server when the enabled events—such as Cold start, Warm start, Authentication failure, etc.—occur. To configure this feature, click on the Event Type **Trap** checkbox.

E-mail Alert



Mail Server Settings

Mail server (SMTP)

Setting	Factory Default	Necessity
IP Address or Domain Name	None	Optional

User name

Setting	Factory Default	Necessity
1 to 15 characters	None	Optional

Password

Setting	Factory Default	Necessity
1 to 15 characters	None	Optional

From E-mail address

Setting	Factory Default	Necessity
1 to 63 characters	None	Optional

Alert Mailing List

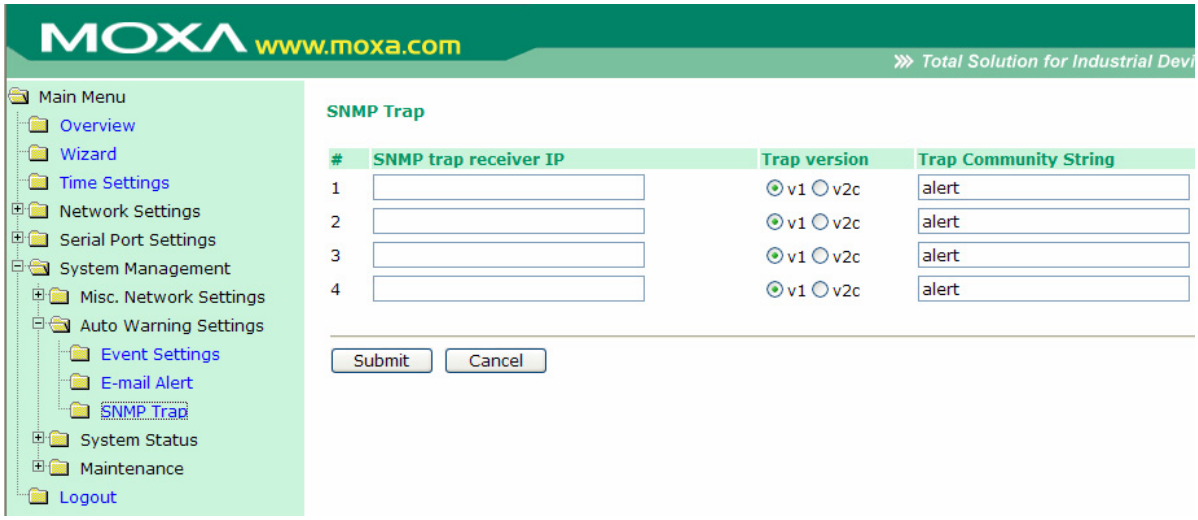
E-mail address 1/2/3/4

Setting	Factory Default	Necessity
1 to 63 characters	None	Optional

ATTENTION

Consult your Network Administrator or ISP for the proper mail server settings. The Auto warning function may not work properly if it is not configured correctly. NPort W2004 SMTP AUTH supports LOGIN, PLAIN, CRAM-MD5 (RFC 2554).

SNMP Trap



SNMP trap receiver IP (or domain name)

Setting	Factory Default	Necessity
IP address or Domain Name	None	Optional

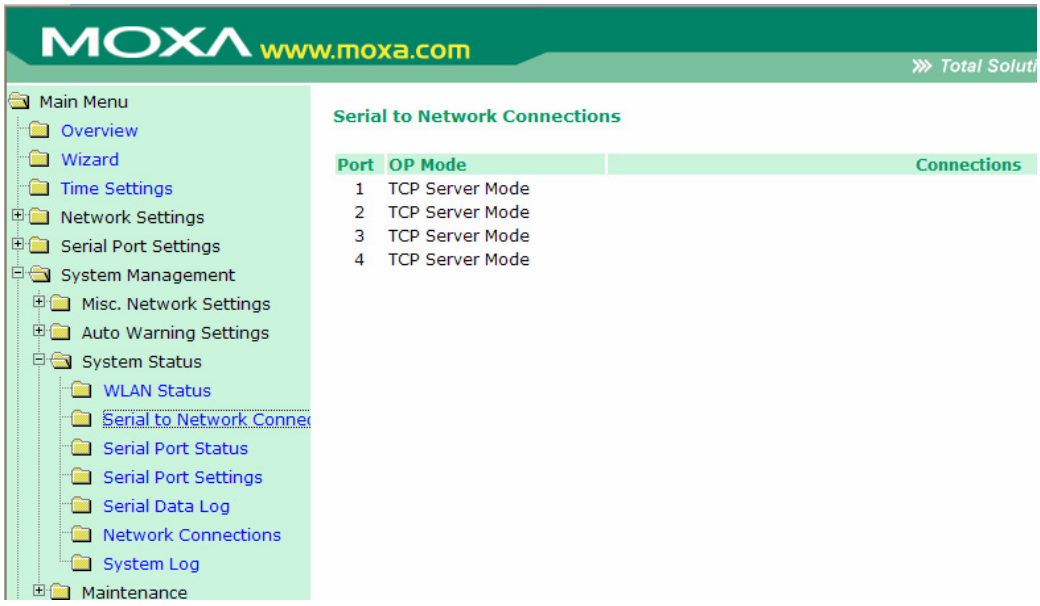
System Status

WLAN Status

The **WLAN Status** page lists **Mode**, **SSID**, **Band**, **Channel**, **Link Status**, **Signal Strength**, **Connection Speed**, **WEP Mode**, **IP Configuration**, **IP Address**, and **Netmask**, as shown in the following figure.

Serial to Network Connections

The **Serial to Network Connections** page lists the operation modes and IP addresses associated with each of the wireless device server's serial ports.



Serial Port Status

The **Serial Port Status** page lists serial transmission stats for each of the wireless device server's serial ports.

Serial Port Status

Port	TxCnt	RxCnt	TxTotalCnt	RxTotalCnt	DSR	CTS	DCD
1	0	0	0	0	Off	Off	Off
2	0	0	0	0	Off	Off	Off
3	0	0	0	0	Off	Off	Off
4	0	0	0	0	Off	Off	Off

Serial Port Settings

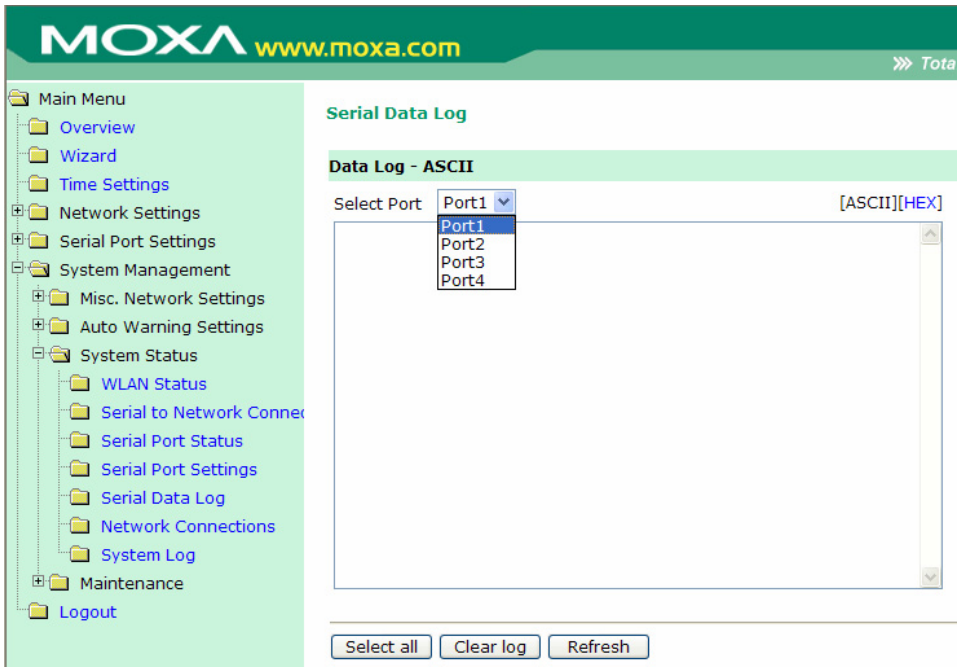
The **Serial Port Settings** page lists the serial transmission settings for each of the four ports.

Serial Port Settings

Port	Baud Rate	Bits	Stop	Parity	Flow Control	FIFO	Interface
1	115200	8	1	None	XON/XOFF	Enable	RS-232
2	115200	8	1	None	XON/XOFF	Enable	RS-232
3	115200	8	1	None	XON/XOFF	Enable	RS-232
4	115200	8	1	None	XON/XOFF	Enable	RS-232

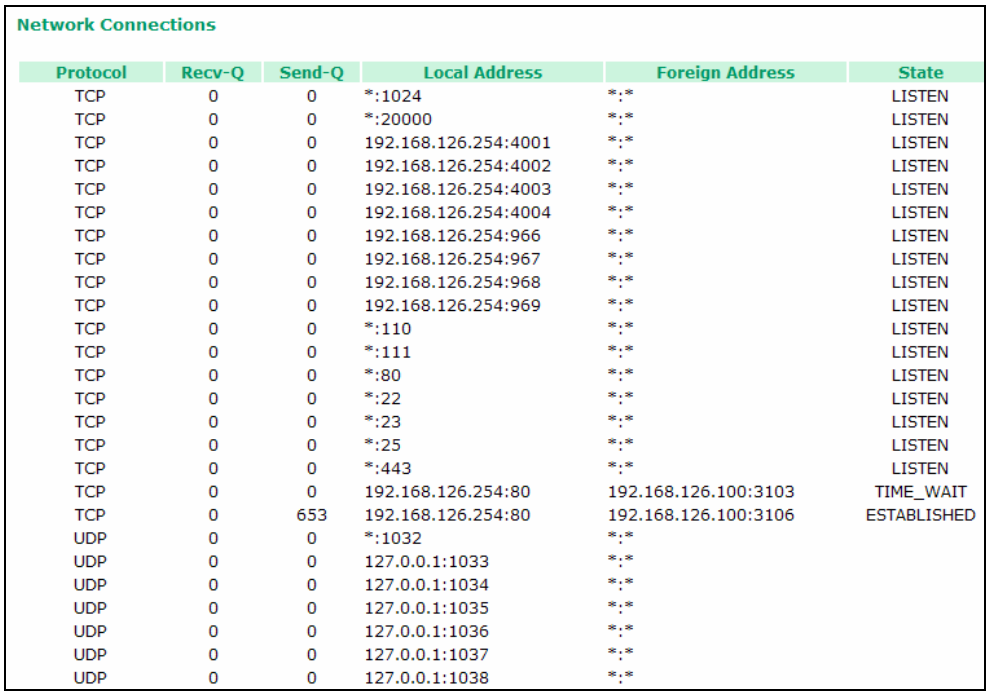
Serial Data Log

This Text box is enabled only when Data logging is enabled. The data log contents are displayed in ASCII mode or HEX mode. Use the **Select all** button to select the entire log; you can then copy and paste the contents into a text file. The **Clear log** and **Refresh** buttons are used to clear the log, and refresh the log contents, respectively.



Network Connections

The **Network Connections** page displays the current status of the network connection.



Network Connections

Protocol	Recv-Q	Send-Q	Local Address	Foreign Address	State
TCP	0	0	*:1024	*:*	LISTEN
TCP	0	0	*:20000	*:*	LISTEN
TCP	0	0	192.168.126.254:4001	*:*	LISTEN
TCP	0	0	192.168.126.254:4002	*:*	LISTEN
TCP	0	0	192.168.126.254:4003	*:*	LISTEN
TCP	0	0	192.168.126.254:4004	*:*	LISTEN
TCP	0	0	192.168.126.254:966	*:*	LISTEN
TCP	0	0	192.168.126.254:967	*:*	LISTEN
TCP	0	0	192.168.126.254:968	*:*	LISTEN
TCP	0	0	192.168.126.254:969	*:*	LISTEN
TCP	0	0	*:110	*:*	LISTEN
TCP	0	0	*:111	*:*	LISTEN
TCP	0	0	*:80	*:*	LISTEN
TCP	0	0	*:22	*:*	LISTEN
TCP	0	0	*:23	*:*	LISTEN
TCP	0	0	*:25	*:*	LISTEN
TCP	0	0	*:443	*:*	LISTEN
TCP	0	0	192.168.126.254:80	192.168.126.100:3103	TIME_WAIT
TCP	0	653	192.168.126.254:80	192.168.126.100:3106	ESTABLISHED
UDP	0	0	*:1032	*:*	
UDP	0	0	127.0.0.1:1033	*:*	
UDP	0	0	127.0.0.1:1034	*:*	
UDP	0	0	127.0.0.1:1035	*:*	
UDP	0	0	127.0.0.1:1036	*:*	
UDP	0	0	127.0.0.1:1037	*:*	
UDP	0	0	127.0.0.1:1038	*:*	

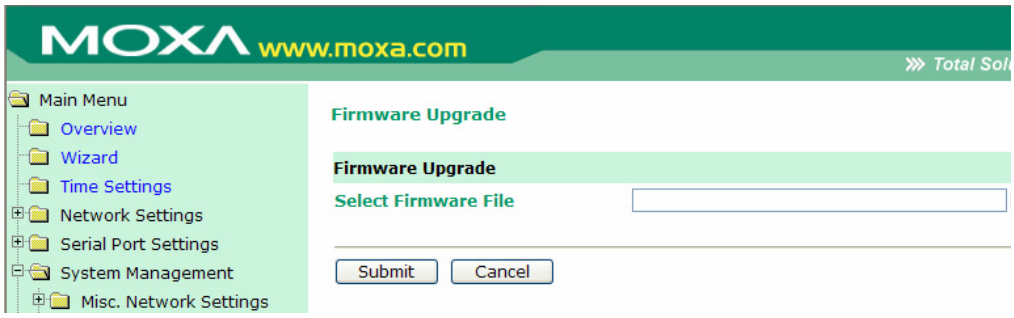
System Log

This window displays the **System Log**. Use the **Select all** button to select the entire log; you can then copy and paste the contents into a text file. The **Clear log** and **Refresh** buttons are used to clear the log, and refresh the log contents, respectively.

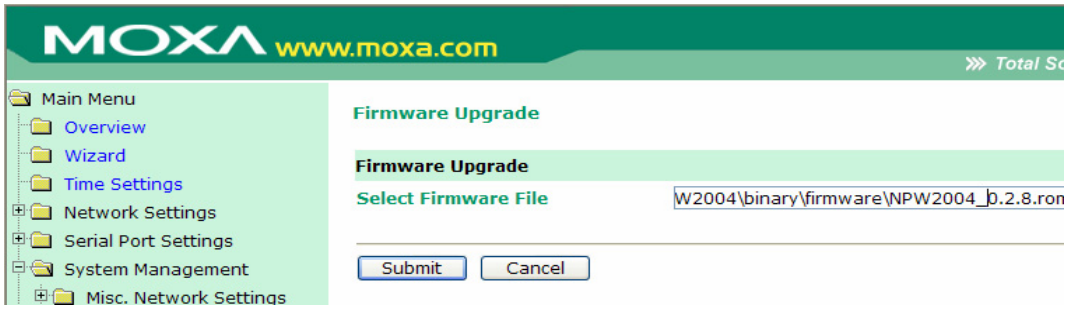
Change Password

Firmware Upgrade

Click on **Firmware Upgrade** to upgrade the firmware.

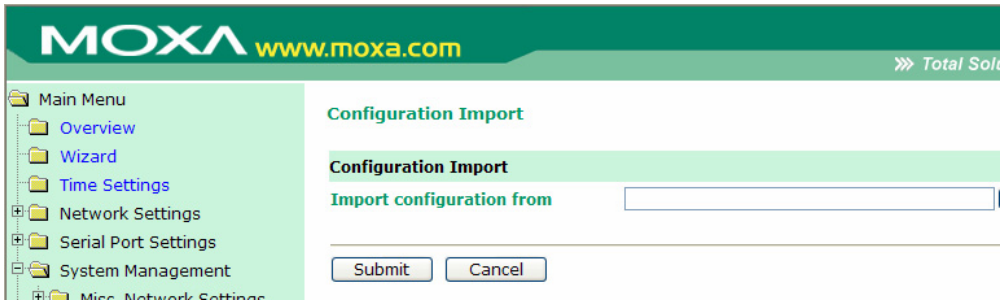


Select the correct firmware file, and then click on **Submit** to load the new firmware into the NPort W2004's memory.



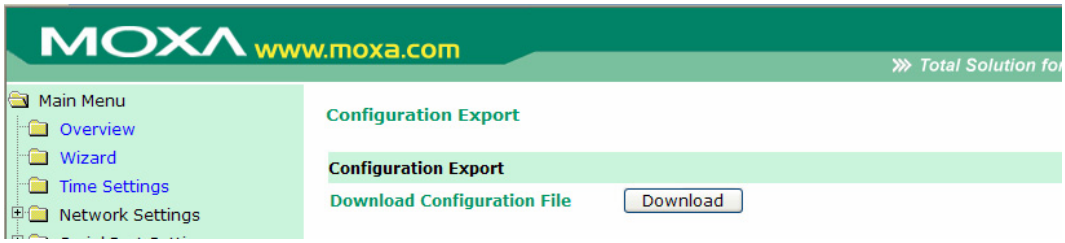
Configuration Import

Select the a configuration file, and then click on **Submit** to load the configuration settings into the NPort W2004.



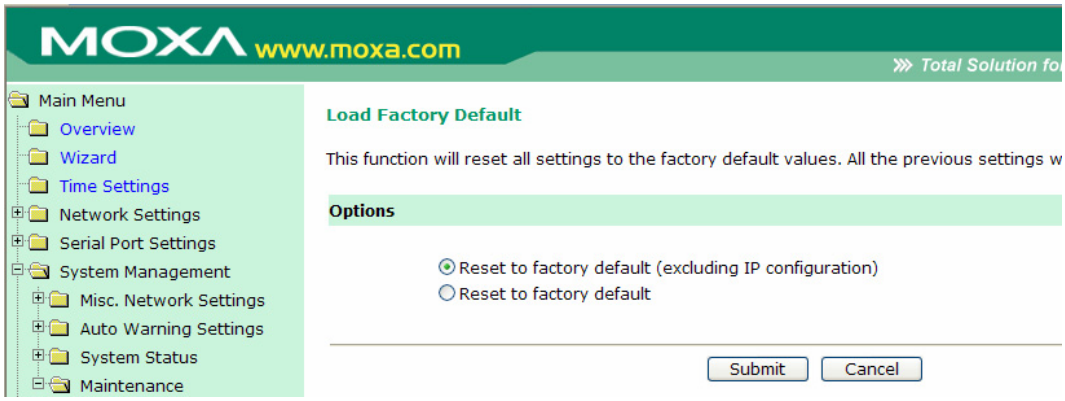
Configuration Export

Click on the **Download** button, and then select the file that you would like to export the current configuration to.



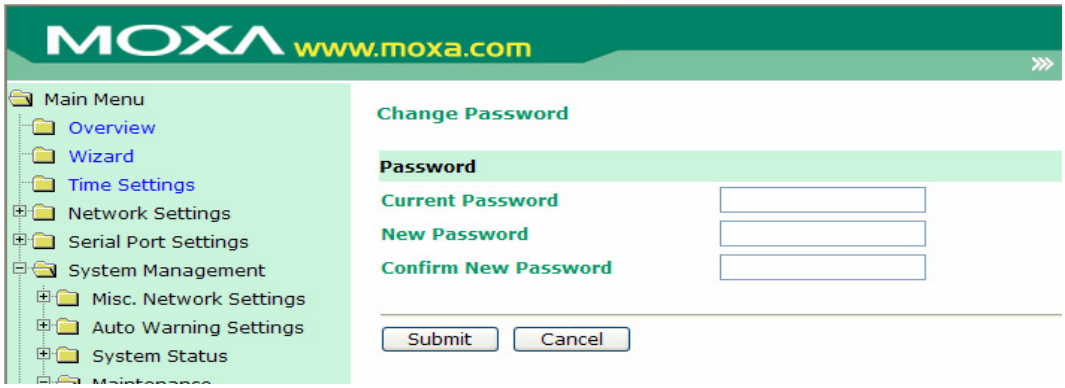
Configuration Export

Use this page to reset the NPort W2004's settings to the factory default values. Be aware that previous settings will be lost. Choose one of the two options—**Reset to factory default (excluding IP configuration)** or **Reset to factory default**—and then click on **Submit**. Choose the first option to retain the current IP address, Netmask, and Gateway address.



Change Password

To change the password for the NPort W2004, input the **Old password**, **New password**, and then retype the new password in the **Retype password** input box. To erase the password, simply leave all three text input boxes blank, and then click on **Submit**.

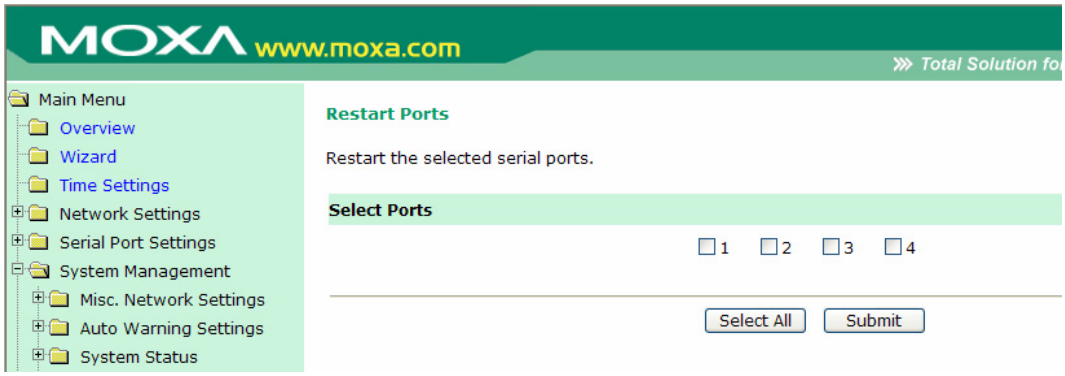


ATTENTION

If you forget the password, the ONLY way to configure NPort W2004 is by using the Reset button on NPort W2004's casing to "Load Factory Default."

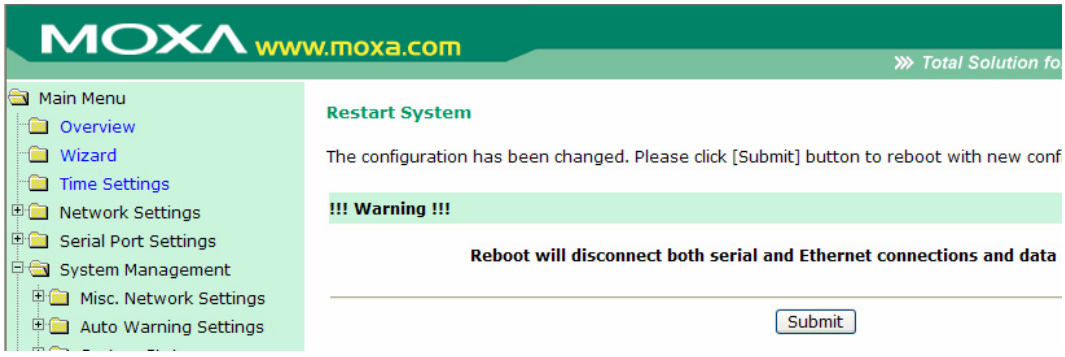
Restart Ports

Select the ports you would like to restart, and then click on the **Submit** button to restart the ports.



Restart System

Click on **Submit** to reboot the NPort W2004..



6

Installing and Configuring the Software

This following topics are covered in this chapter:

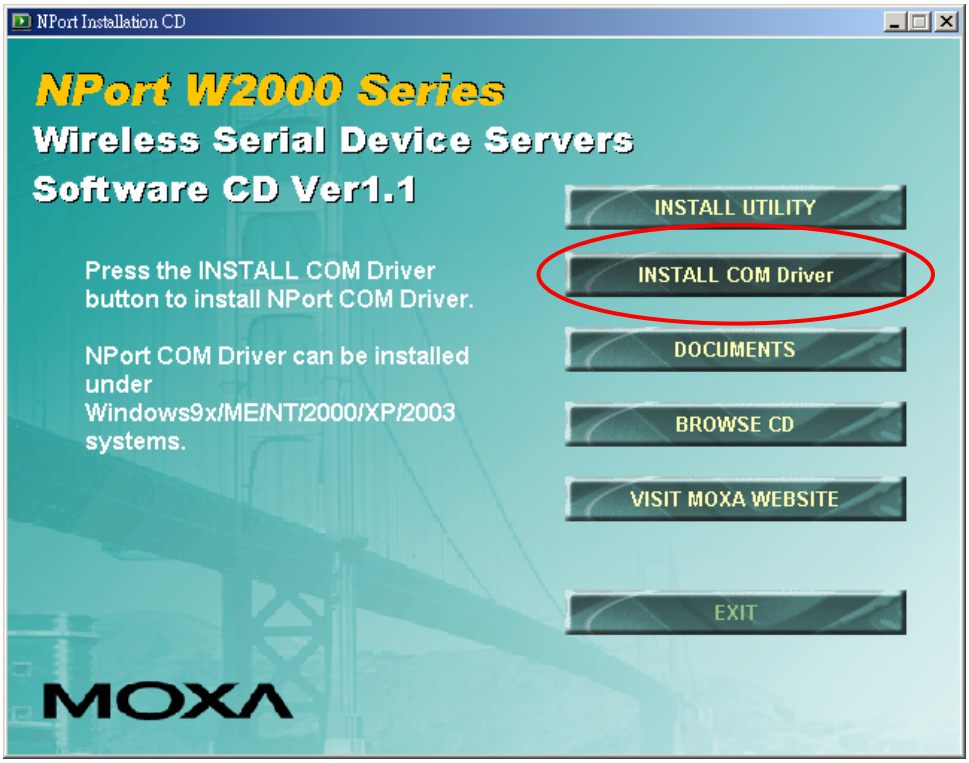
- **Overview**
- **Installing NPort COM Driver**
- **Intalling NPort Search Utility**
- **Configuring NPort COM Driver**
- **Configuring NPort Search Utility**
- **Real TTY and Fixed TTY Installation**
- **Upgrading the Firmware**

Overview

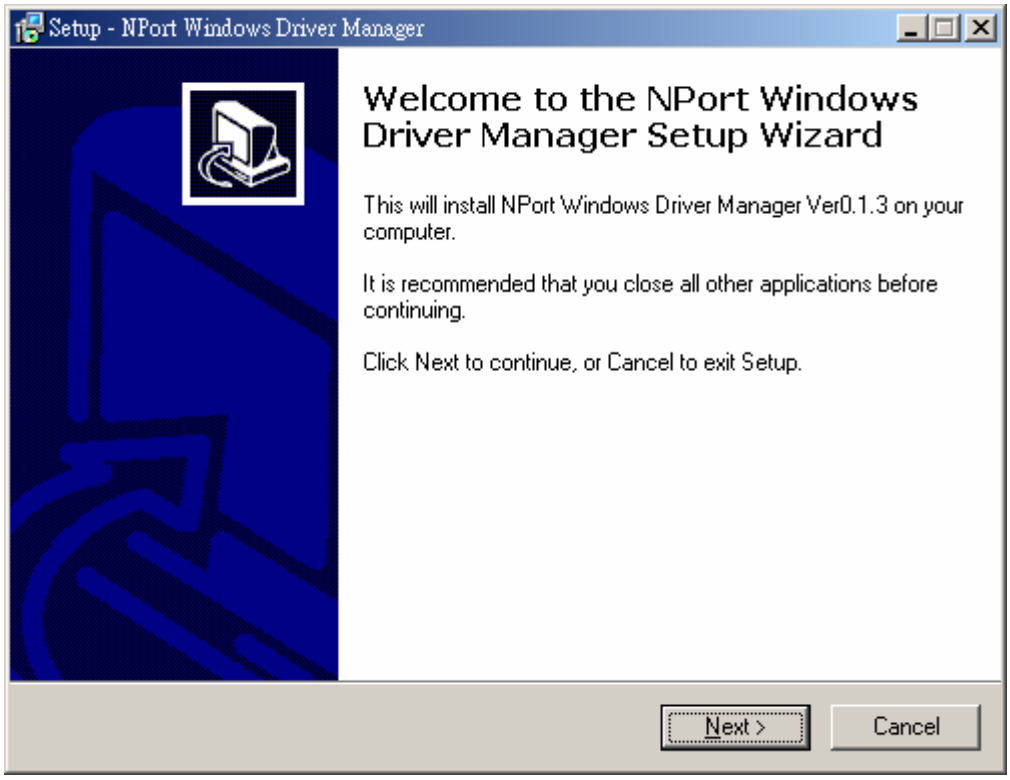
The Documentation & Software CD included with your NPort W2004 is designed to make the installation and configuration procedure easy and straightforward. This auto-run CD includes the NPort COM Driver (for COM mapping), NPort Search Utility (to broadcast search for all NPort W2004 accessible over the network), User's Manual, and firmware upgrade utility.

Installing NPort COM Driver

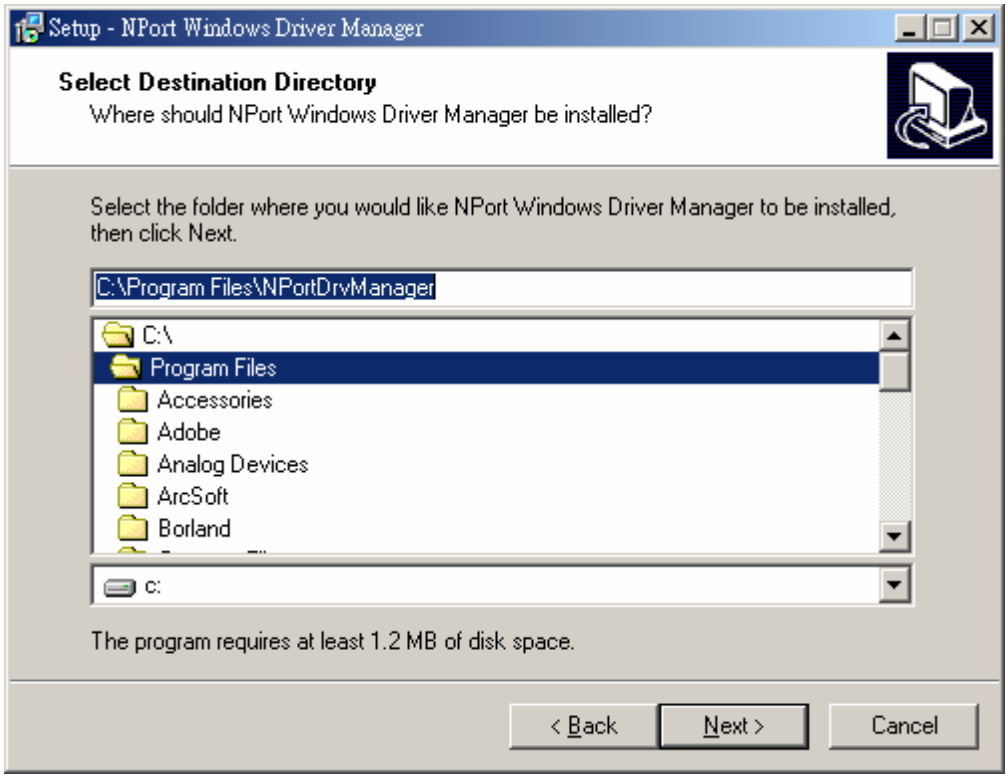
1. Click on the **INSTALL COM Driver** button in the NPort Installation CD auto-run window to install the NPort W2000 Series COM Driver.



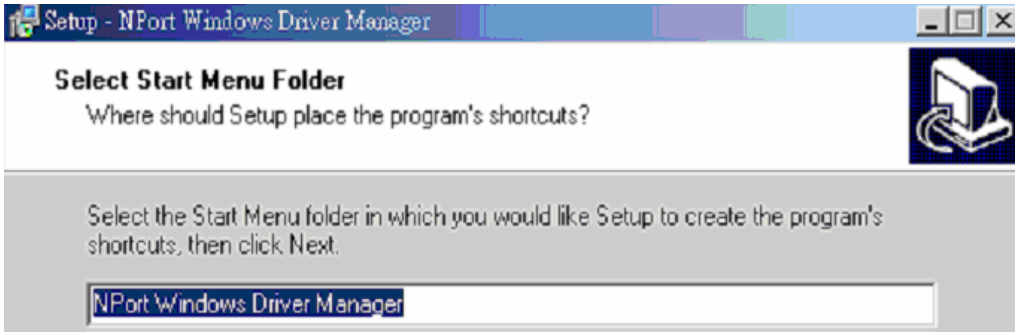
2. Once the installation program starts running, click on **Yes** to proceed.
3. Click on **Next** when the Welcome window opens to proceed with the installation.



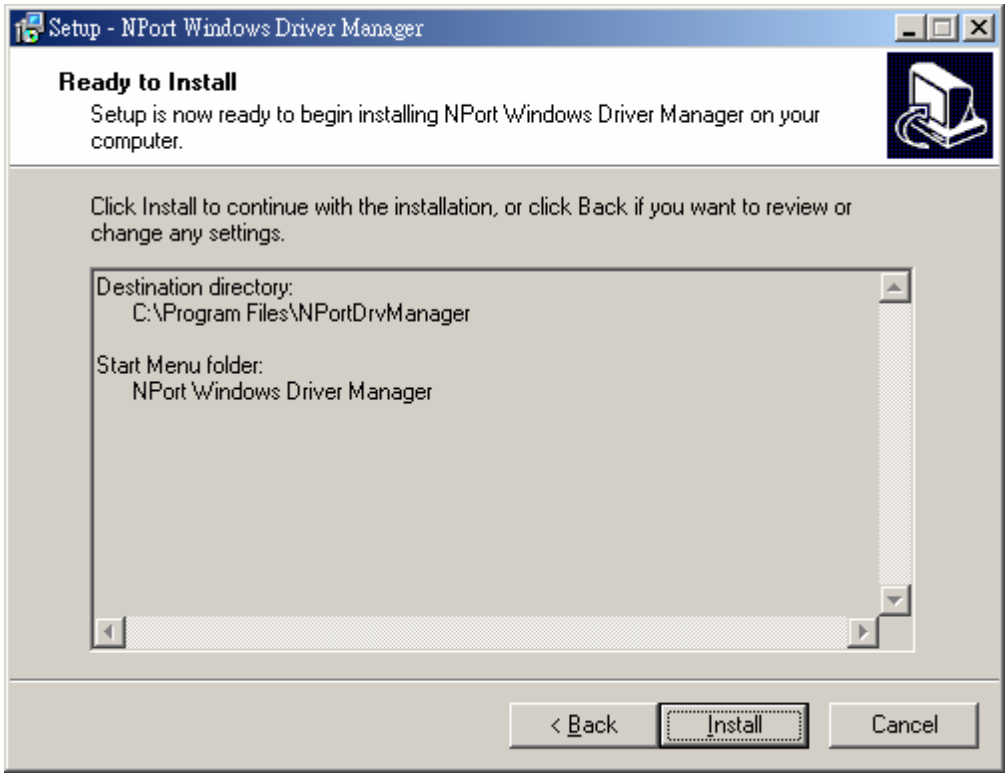
4. Click on **Next** to install program files in the default directory, or use the folder menu to select an alternative location.



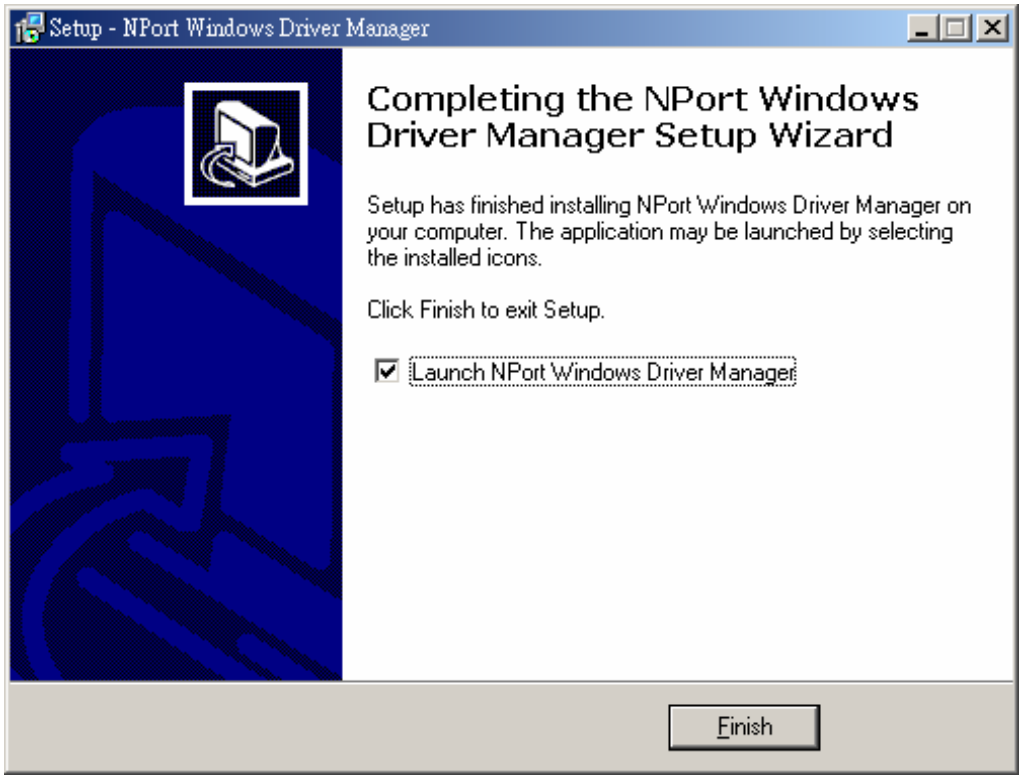
5. Click on **Next** to install the program's shortcuts in the **NPort Windows Driver Manager** Start Menu folder.



6. Click on **Install** to proceed with the installation.

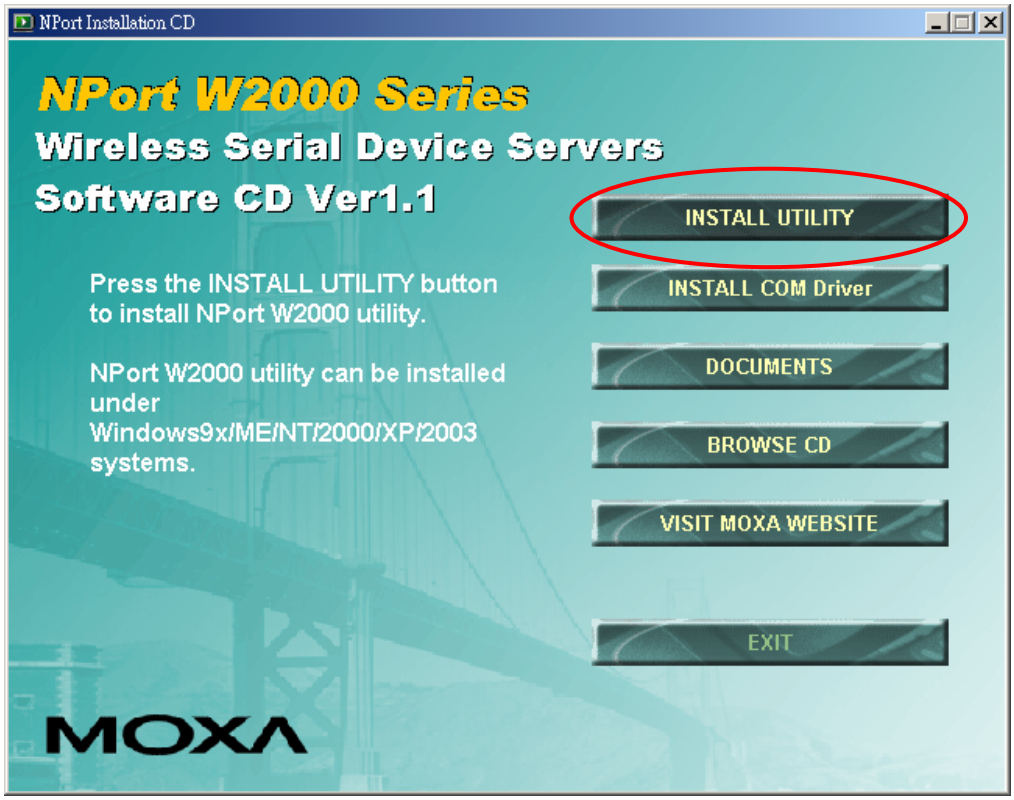


7. The Installing window will report the progress of the installation.
8. Click on **Finish** to complete the installation of the NPort W2004 COM Mapping Utility.

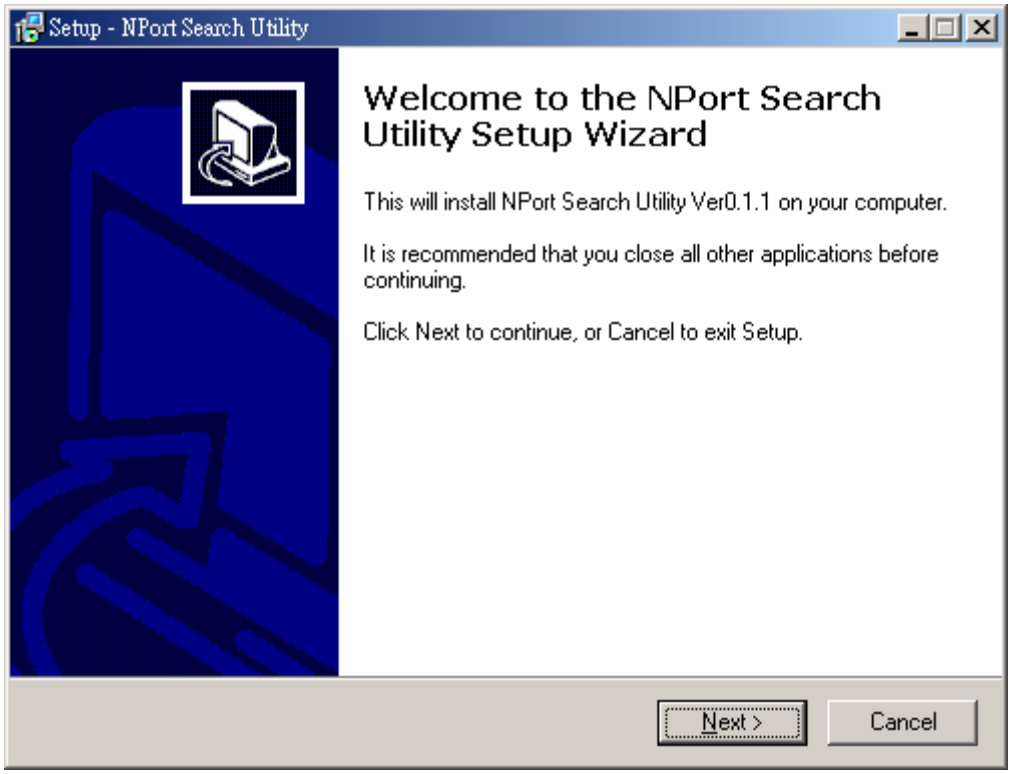


Installing NPort Search Utility

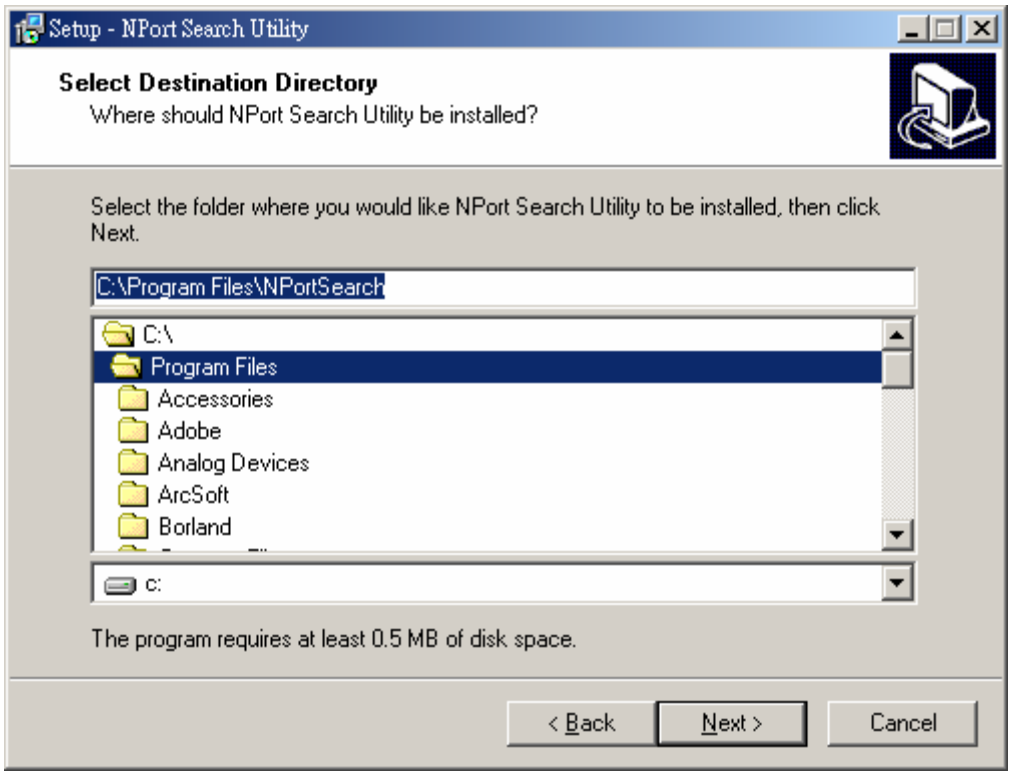
1. Click on the **INSTALL UTILITY** button in the NPort Installation CD auto-run window to install the NPort Search Utility.



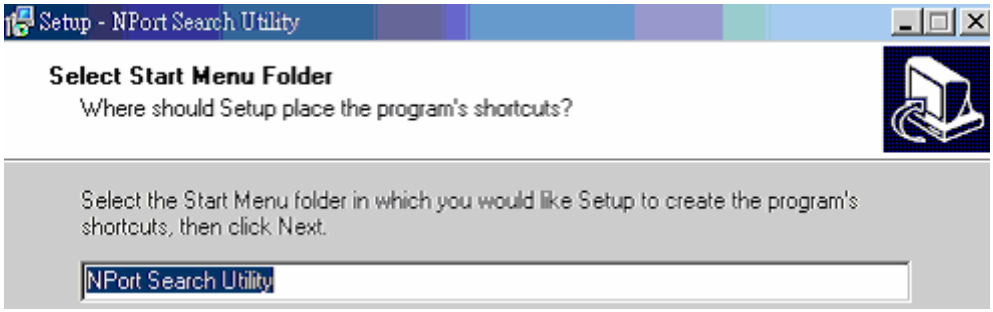
2. Once the program starts running, click on **Yes** to proceed.
3. Click on **Next** when the Welcome window opens to proceed with the installation.



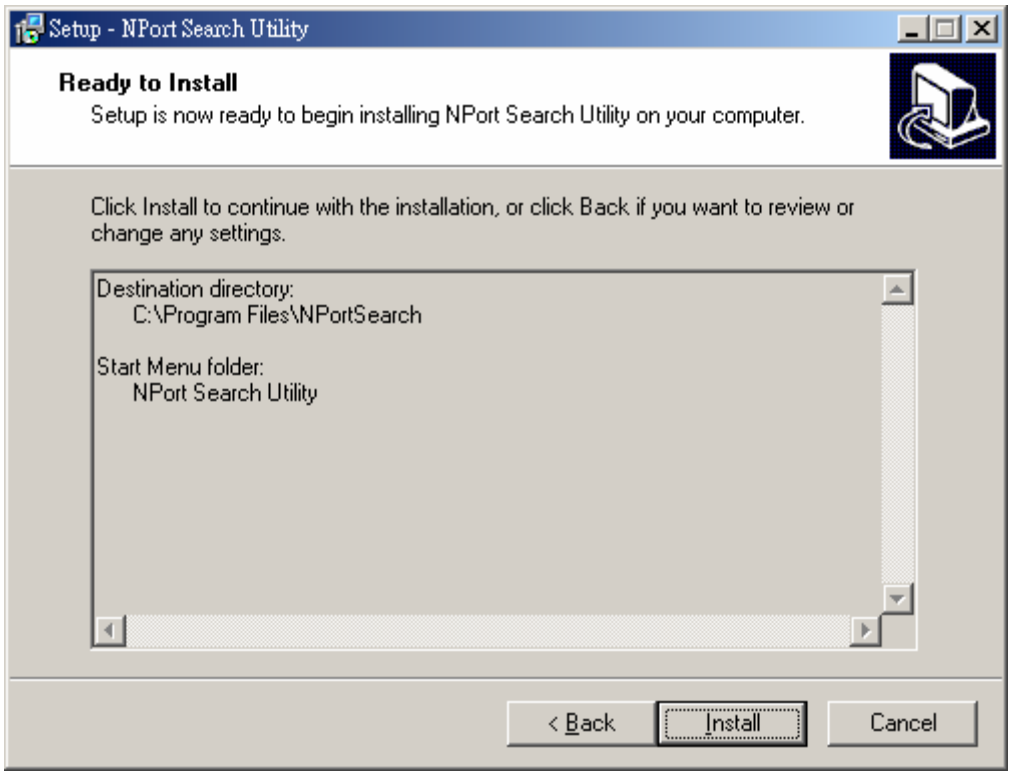
4. Click on **Next** to install program files in the default directory, or use the folder menu to select an alternative location.



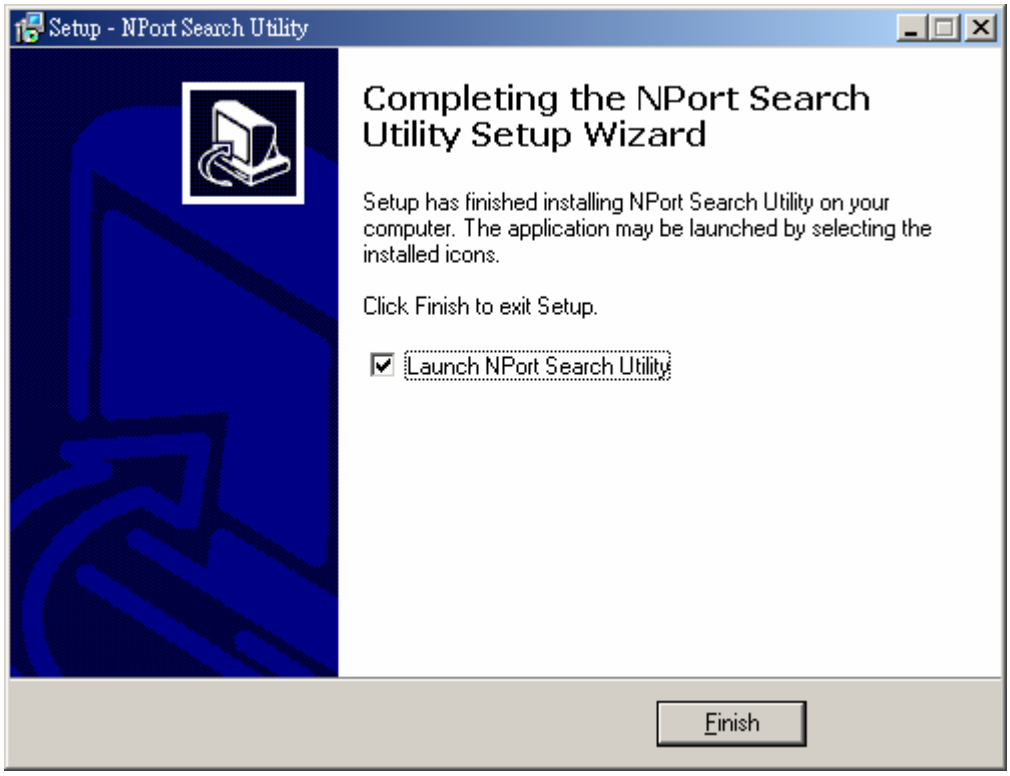
5. Click on **Next** to install the program's shortcuts in the **NPort Search Utility** Start Menu folder.



6. Click on **Install** to proceed with the installation.



7. The Installing window will report the progress of the installation.
8. Click on **Finish** to complete the installation of the NPort W2004 Search Utility.



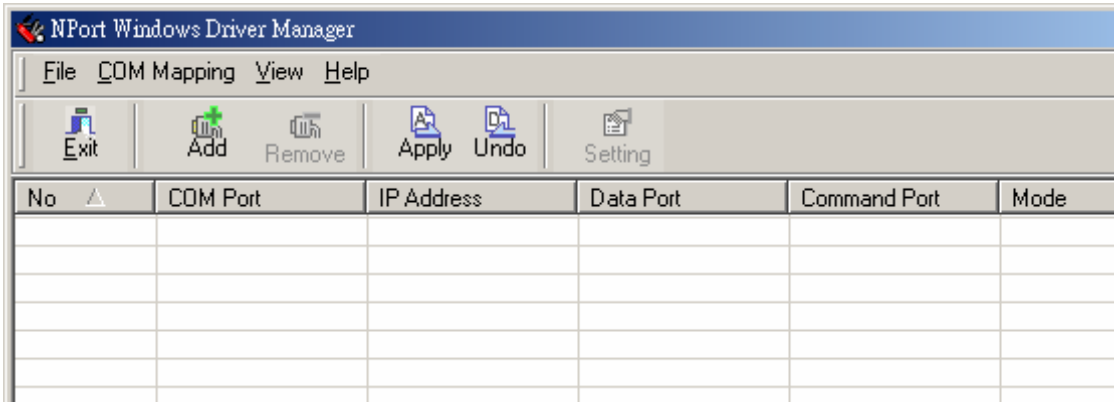
Configuring NPort COM Driver

The **NPort COM Driver** utility installs Real COM drivers that work under Windows 98/ME/2000/XP/2003. After you install NPort COM Driver, you can set up the NPort W2004's serial ports as remote COM ports for your PC host.

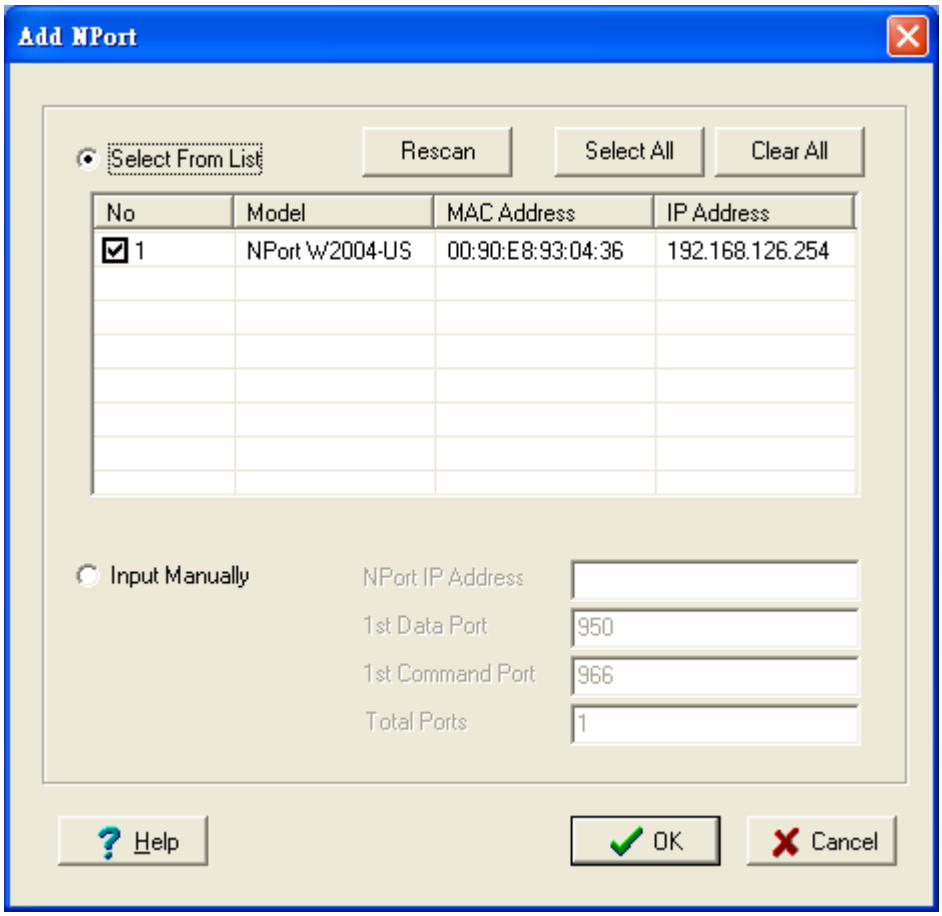
Use the following steps to map the COM ports:

1. Click on **Start → Nport Windows Driver Manager → NPort COM Mapping Utility** to start the COM mapping utility.

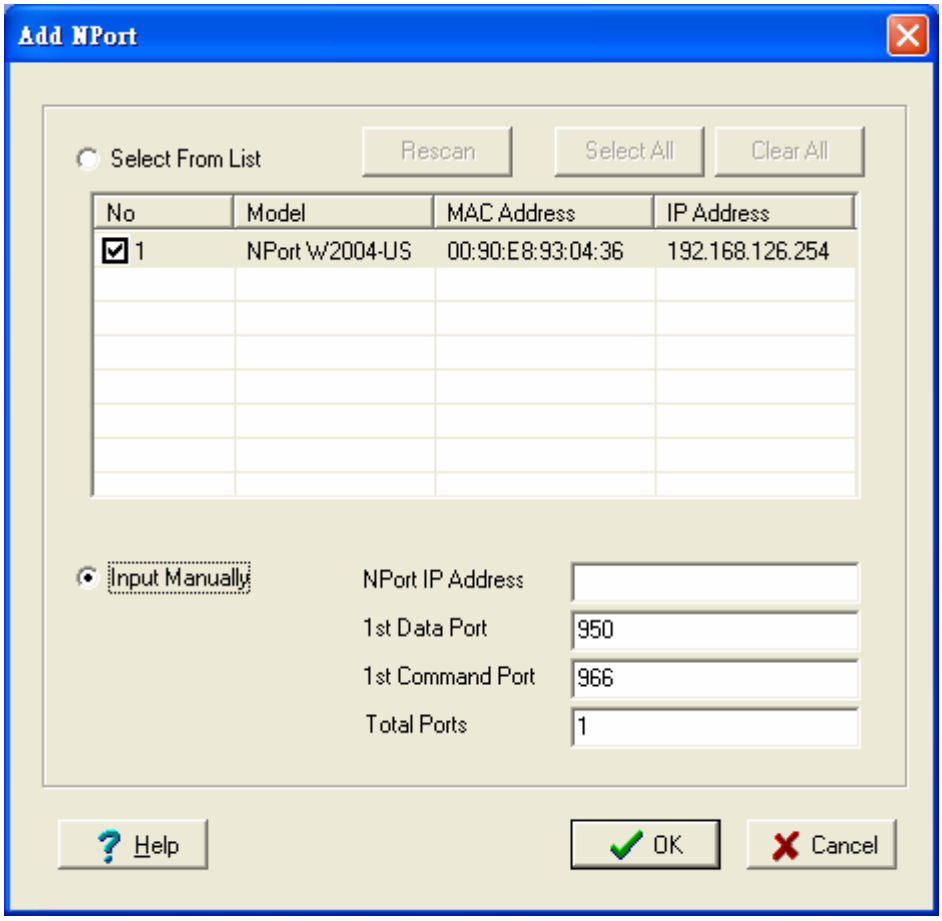
2. Click on the **Add** icon.



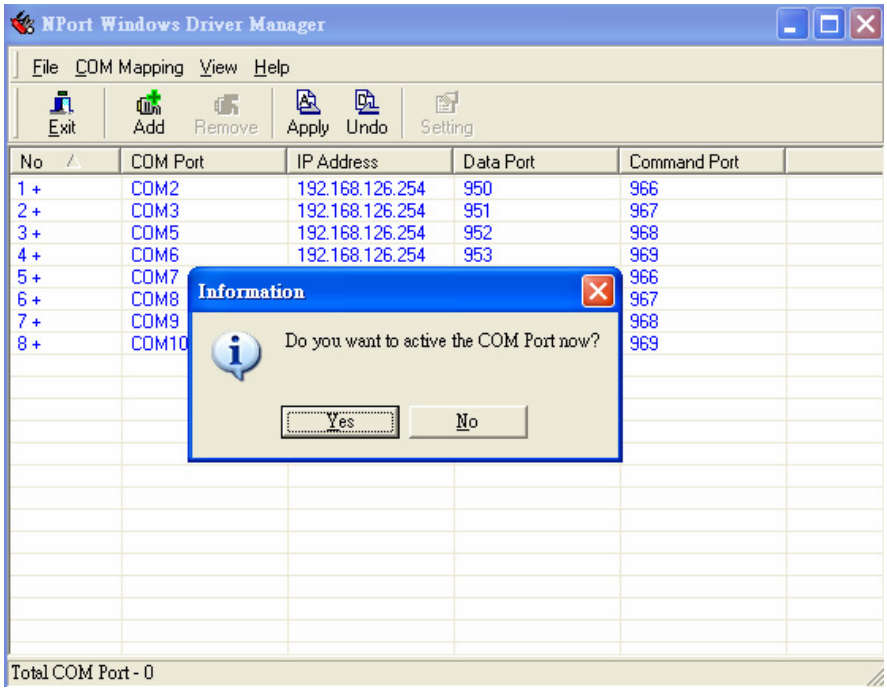
3. Click on **Rescan** to search for NPort device servers, select the server you would like to map COM ports to, and then click on **OK**.



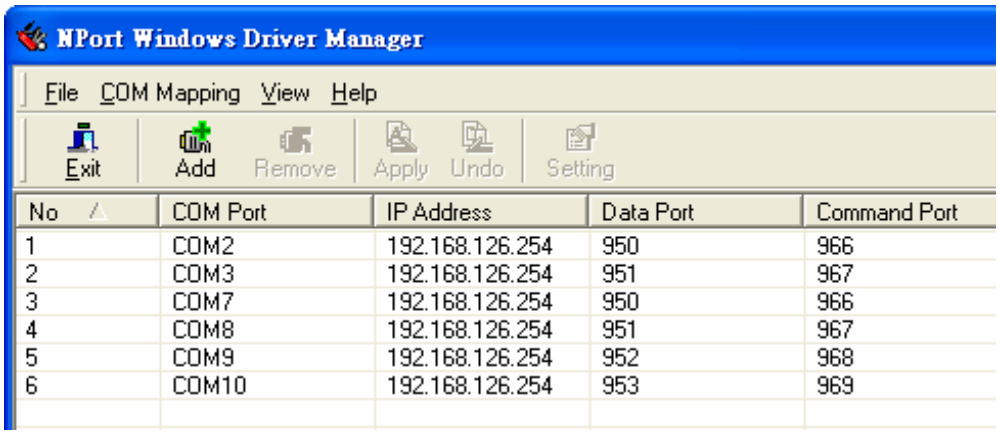
4. Alternatively, you can select **Input Manually** and then input the **NPort IP Address**, **1st Data Port**, **1st Command Port**, and **Total Ports** for the NPort W2004 that you would like to map COM ports to. Click on **OK** to proceed to the next step.



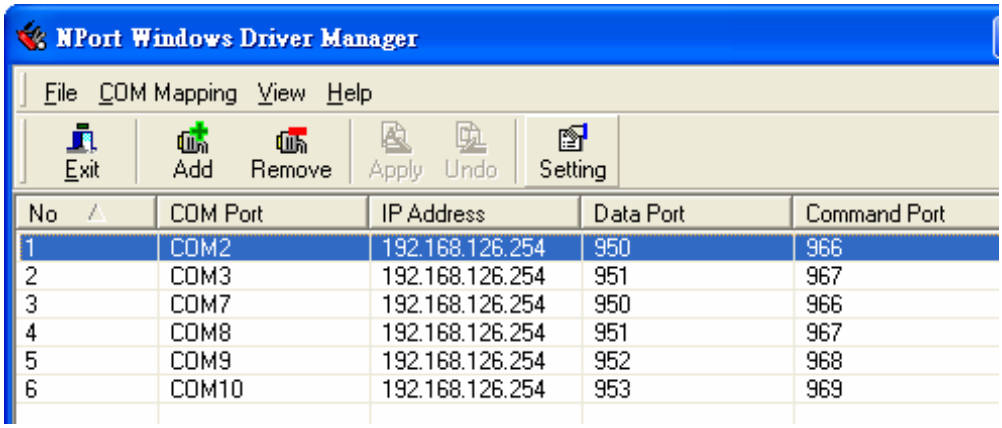
5. Click on **Yes** to activate the COM ports at this time, or click on **No** to activate the COM ports later. Activating the COM ports saves the information in the host system registry. The host computer will not have the ability to use the COM port until you click on the **Apply** icon.



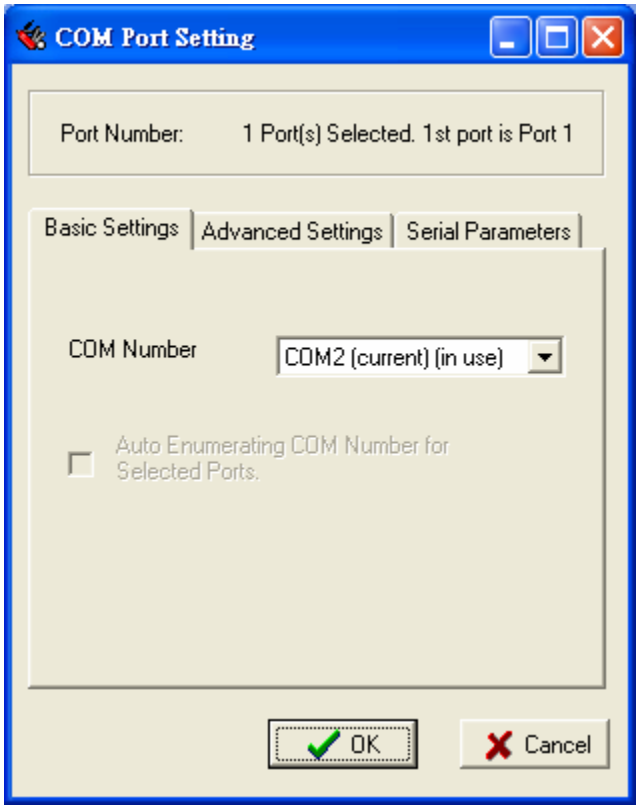
6. The display text corresponding to NPorts whose ports are activated will change from blue to black.



7. To re-configure the settings for a particular NPort, click on the row corresponding to that NPort to highlight it, and then click on the **Setting** icon.



8. In the **Basic Setting** panel, use the **COM Number** drop-down list to select a COM number for the NPort's first serial port. Check mark the **Auto Enumerating COM Number for Selected Ports** checkbox to automatically assign the next available COM number to the second serial port. Note that ports that are "in use" will be labeled accordingly.



Click on the **Advanced Setting** tab to modify **Tx Mode**, **FIFO**, and **Flash Flush**.

Tx Mode

Hi-performance mode is the default for Tx mode. When the driver finishes sending data to the NPort W2004, the driver will issue a "Tx Empty" response to the program.

Under **classical mode**, the driver will not notify the user's program that Tx transmission is finished until all Tx data has been sent out from the NPort W2004. This ODE will cause

lower throughput. Classical mode is recommended if you want to ensure that all data is sent out before further processing.

FIFO
If the FIFO is **Disabled**, NPort W2004 will transmit one byte each time the Tx FIFO becomes empty, and an Rx interrupt will be generated for each incoming byte. This will result in a faster response and lower throughput. If you want to use XON/XOFF flow control, we recommend setting the FIFO to Disable.

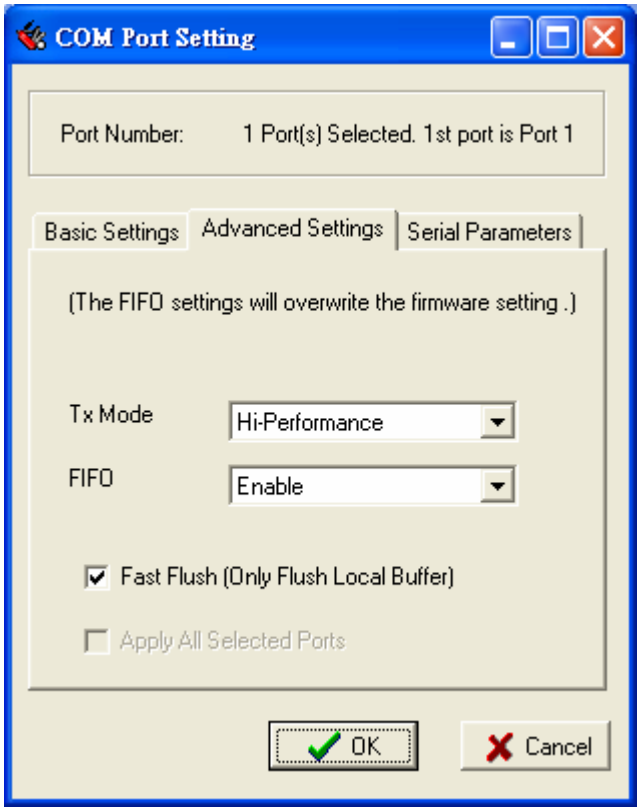
Fast Flush (only flushes the local buffer)

a. We have added one optional Fast Flush function to Moxa's new NPort Real COM driver.

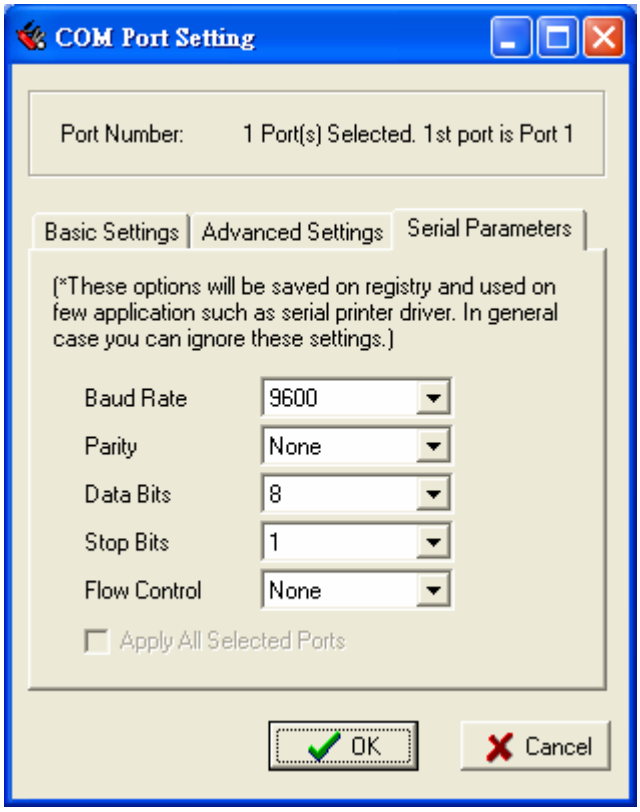
b. For some applications, the user's program will use the Win32 "PurgeComm()" function before it reads or writes data. With our design, after the program uses this Purge Comm() function, the NPort driver will keep querying NPort's firmware several times to make sure no data is queued in the NPort firmware buffer, rather than just flushing the local buffer. This kind of design is used to satisfy some special considerations. However, it might take more time (about several hundred milliseconds) than a native COM1, because it needs to work via Ethernet. That's why the native COM ports on the motherboard can work fast with this function call, but NPort requires much more time. In order to accommodate other applications that require a faster response time, the new NPort driver implements a new "Fast Flush" option. Note that by default, this function is disabled.

c. To begin with, make sure there are some "PurgeComm()" functions being used in your application program. In this kind of situation, you might find that your NPort exhibits a much poorer operation performance than when using the native COM1 port. Once you have enabled the "Fast Flush" function, you can check to see if there has been an improvement in performance.

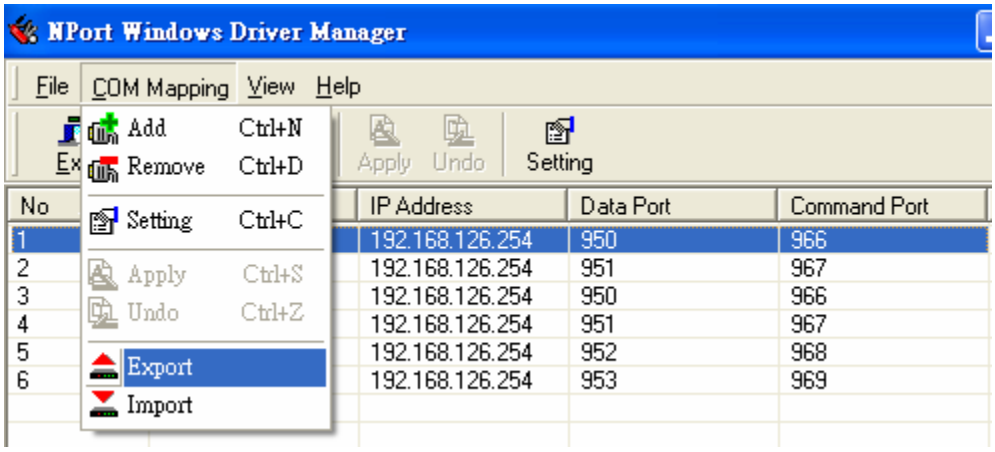
d. By default, the optional "Fast Flush" function is disabled. If you would like to enable this function, double click on the COM ports that are mapped to the NPort, and then select the "Fast Flush" checkbox. You should find that when "Fast Flush" is enabled, the NPort driver will work faster with "PurgeComm()."



9. The Serial Parameter settings shown in the following figure are the default settings when the NPort W2004 is powered on. However, the program can redefine the serial parameters to different values after the program opens the port via Win 32 API.



10. To save the configuration to a text file, select Export COM Mapping. You will then be able to import this configuration file to another host and use the same COM Mapping settings in the other host.

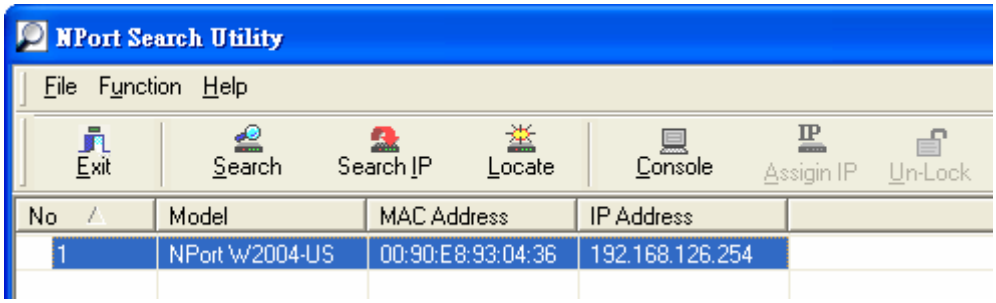


Configuring NPort Search Utility

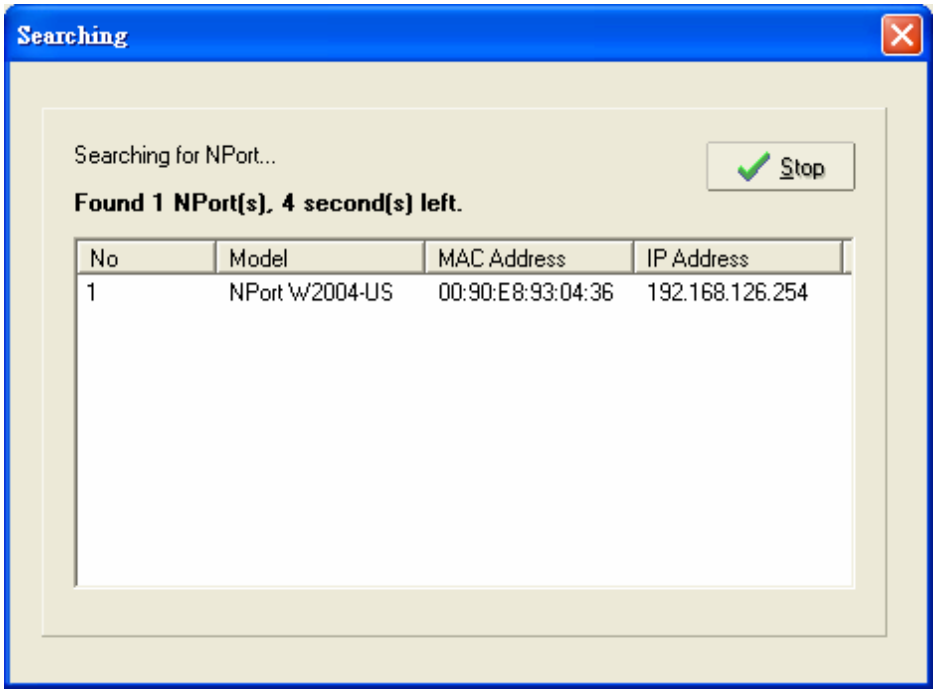
The Broadcast Search function is used to locate all NPort W2004s that are connected to the same LAN as your computer. After locating an NPort W2004, you will be able to change the IP address.

Since the Broadcast Search function searches by MAC address and not IP address, all NPort W2004s connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

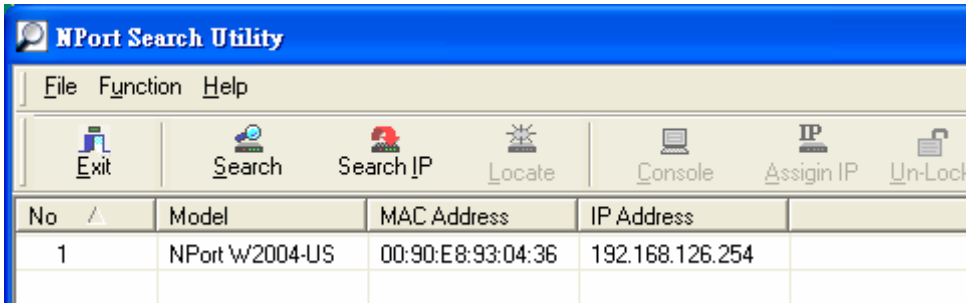
1. Open the **NPort Search Utility** and then click on the **Search** icon.



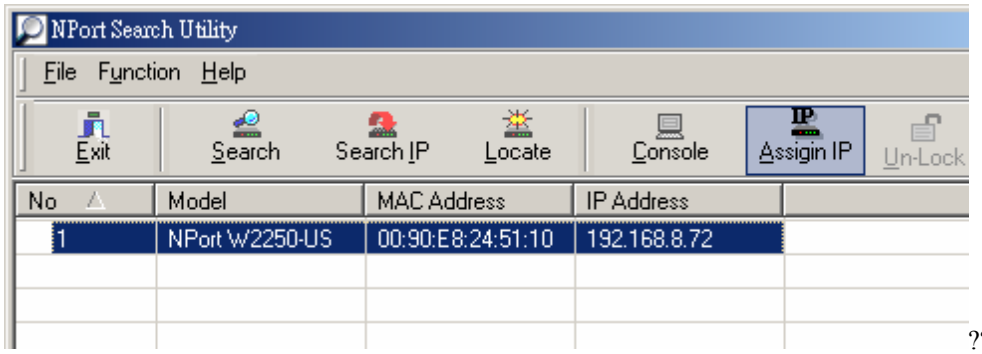
2. The **Searching** window indicates the progress of the search.



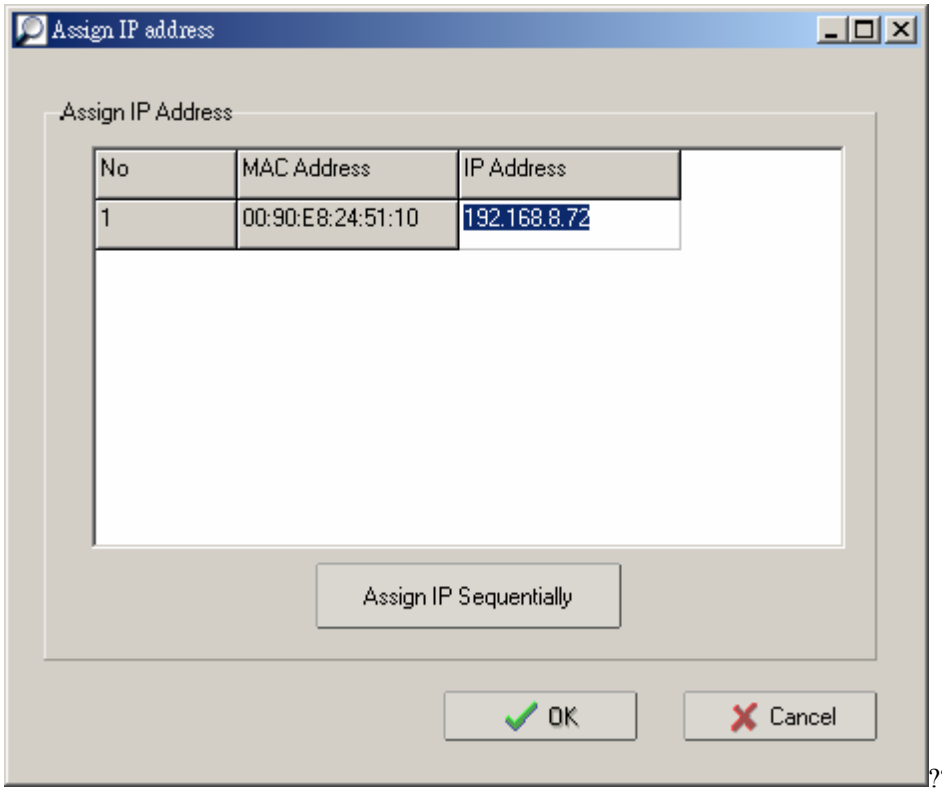
3. When the search is complete, the NPort W2004 units that were located will be displayed in the NPort Search Utility window.



4. Click on the **Assign IP** icon to change the IP address.



???



???

Real TTY and Fixed TTY Installation

Installing the Real TTY driver

Procedure

To map an NPort serial port to the host's tty port, you need to:

1. *Set up NPort*
   Make sure the IP configuration is ok and you can access the NPort (ping, telnet...) successfully, and then configure the NPort serial port to **Real COM Mode**.
2. *Install driver files on the host*
   Refer to "Driver Files Installation" below for details.
3. *Map the NPort serial port to the host's tty port*
   Refer to "Mapping TTY Ports" below for details.

Hardware Installation

Before proceeding with the software installation, make sure you have completed the hardware installation, as illustrated in the user's manual.

The default IP address for NPort Server is 192.168.127.254.

NOTE After installing the hardware, you MUST configure the NPort operating mode to **Real COM Mode**.

Driver Files Installation

a. Get the driver file from the product CD-ROM or Moxa website.

b. Log in to the console as a super user (root).

c. Execute **cd /** to go to the root directory.

d. Copy the driver file **npreal2xx.tgz** to the " / " directory.

e. Execute **tar xvfz npreal2xx.tgz** to copy all files into the system.

f. Execute **/tmp/moxa/mxinst**.

NOTE For RedHat AS/ES/WS and Fedora Core1, extra argument is needed: # /tmp/moxa/mxinst SP1

g. The shell script will install the driver files automatically.

After installing the driver, you will be able to see several files in the **/usr/lib/npreal2/driver** folder, including"

> mxaddsvr (Add Server, mapping tty port)

> mxdelsvr (Delete Server, un-mapping tty port)

> mxloadsvr (Reload Server)

> mxmknod (Create device node/tty port)

> mxrmnod (Remove device node/tty port)

> mxuninst (Remove tty port and driver files)

At this point, you will be ready to map the NPort serial port to the system tty port. See "Mapping TTY Ports" below for detailed instructions.

Mapping TTY Ports

Before mapping tty ports, you must set the operation mode of your NPort to **Real Com Mode**. We provide two ways to map tty ports.

Mapping tty ports automatically

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:

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

Example 1:

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

Example2:

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

In Example 1, 16 tty ports will be added, all with IP **192.168.3.4**, but with data ports equal to (950, 951, …, 965), and command ports equal to (966, 967, 968, …, 981).

In example2, 16 tty ports will be added, all with IP **192.168.3.4**, but with data ports equal to (4001, 4002, …, 4016), and command ports equal to (966, 967, 968, …, 981).

The following actions will be performed:

> Modify the "npreal2d.cf"

> Create tty ports in directory "/dev" with major & minor number configured in **npreal2d.cf**.

> Stop and then restart the driver.

Remove Mapped TTY ports

As with the "Mapping TTY Ports" task, we provide two ways to remove mapped tty ports:

Remove the mapped tty ports automatically

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]

Example:

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

If you don't provide the IP address in the command line, the program will list the installed servers and total ports on screen, so that you can only choose the index of the installed server list to delete. The following actions will be performed:

> Modify the **npreal2d.cf**

> Remove the relevant tty ports in directory **/dev**

> Stop and then restart the driver.

Driver Files Removal

Driver Removal will remove all driver files, mapped tty ports, and unload the driver. To do this, you only need to enter the directory **/usr/lib/npreal2/driver**, and then execute **mxuninst** to uninstall the driver. This program will perform the following actions:

> Unload the driver.

> Delete all files and directories in "/usr/lib/npreal2"

> Delete directory "/usr/lib/npreal2".

> Modify the system initializing script file.

Installing the fixed TTY driver

Installation and Configuration

step 1: login to UNIX and create a directory for MOXA TTY,
for instance, /usr/etc.
mkdir /usr/etc
cd /usr/etc

step 2: Extract source code from tar-file :
Type "tar xvf moxattyd.tar".

After extract, you can find the following files :
README --> this file
moxattyd.c --> source program
moxattyd.cf --> empty configuration file
Makefile --> makefile

step 3: Compile and Link :
For SCO UNIX:
make sco
For Linux:
make linux
For UnixWare 7:
make svr5
For UnixWare 2.1.x, SVR4.2:
make svr42
For IBM AIX:
make aix
For HP-UNIX:
make hpunix
For SunOS 5.8:
make sun
For QNX6:
make qnx6

step 4: Modify configuration :
The configuration of moxattyd program is defined on
"moxattyd.cf" file at the same directory where contains

program moxattyd.
User can use vi or any edit to modify it. It's a text file.
For more configuration information, please take a look at moxattyd.cf file. We put detail decription on it.

!!
Please note that the "Device Name" is depended on OS.
See "E. Device Naming Rule" for more information.
!!

step 5: Add program moxattyd into /etc/inittab and any tty name you configued at moxattyd.cf.
eg. for Linux:
ts:2:respawn:/usr/etc/moxattyd
p1:345:respawn:/etc/mingetty ttyp1
p2:345:respawn:/etc/mingetty ttyp2

finish: You have finished the installation and configuration of MOXA TTY.

Start moxattyd program

Run "init q" or reboot your UNIX.

Add additional server

Step 1 : Modify "moxattyd.cf" file to add additional server.
User can use vi or any edit to modify it. It's a text file.
For more configuration information, please take a look at moxattyd.cf file. We put detail decription on it.

Step 2 : Find the proccess id (PID) of program "moxattyd".
ps -ef | grep moxattyd

Step 3 : Update configuration of moxattyd program.
kill -USR1 PID
(ex. if "moxattyd" PID = 404, "kill -USR1 404")

finish: You have finished to add additional server.

A

SNMP Agents with MIB II & RS-232 Like Groups

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 NPort .

RFC1213 MIB-II supported SNMP variables:

System MIB	Interfaces MIB	IP MIB	ICMP MIB
SysDescr	itNumber	ipForwarding	IcmpInMsgs
SysObjectID	ifIndex	ipDefaultTTL	IcmpInErrors
SysUpTime	ifDescr	ipInreceives	IcmpInDestUnreachs
SysContact	ifType	ipInHdrErrors	IcmpInTimeExcds
SysName	ifMtu	ipInAddrErrors	IcmpInParmProbs
SysLocation	ifSpeed	ipForwDatagrams	IcmpInSrcQuenchs
SysServices	ifPhysAddress	ipInUnknownProtos	IcmpInRedirects
	ifAdminStatus	ipInDiscards	IcmpInEchos
	ifOperStatus	ipInDelivers	IcmpInEchoReps
	ifLastChange	ipOutRequests	IcmpInTimestamps
	ifInOctets	ipOutDiscards	IcmpTimestampReps
	ifInUcastPkts	ipOutNoRoutes	IcmpInAddrMasks
	ifInNUcastPkts	ipReasmTimeout	IcmpOutMsgs
	ifInDiscards	ipReasmReqds	IcmpOutErrors
	ifInErrors	ipReasmOKs	IcmpOutDestUnreachs

System MIB	Interfaces MIB	IP MIB	ICMP MIB
SysServices	ifInUnknownProtos	ipReasmFails	IcmpOutTimeExcds
	ifOutOctets	ipFragOKs	IcmpOutParmProbs
	ifOutUcastPkts	ipFragFails	IcmpOutSrcQuenchs
	ifOutNUcastPkts	ipFragCreates	IcmpOutRedirects
	ifOutDiscards	ipAdEntAddr	IcmpOutEchos
	ifOutErrors	ipAdEntIfIndex	IcmpOutEchoReps
	ifOutQLen	ipAdEntNetMask	IcmpOutTimestamps
	ifSpecific	ipAdEntBcastAddr	IcmpOutTimestampReps
		ipAdEntReasmMaxSize	IcmpOutAddrMasks
		IpNetToMediaIfIndex	IcmpOutAddrMaskReps
		IpNetToMediaPhysAddress	
		IpNetToMediaNetAddress	
		IpNetToMediaType	
		IpRoutingDiscards	

UDP MIB	TCP MIB	SNMP MIB
UdpInDatagrams	tcpRtoAlgorithm	snmpInPkts
UdpNoPorts	tcpRtoMin	snmpOutPkts
UdpInErrors	tcpRtoMax	snmpInBadVersions
UdpOutDatagrams	tcpMaxConn	snmpInBadCommunityNames
UdpLocalAddress	tcpActiveOpens	snmpInASNParseErrs
UdpLocalPort	tcpPassiveOpens	snmpInTooBigs
	tcpAttempFails	snmpInNoSuchNames
Address Translation MIB	tcpEstabResets	snmpInBadValues
AtIfIndex	tcpCurrEstab	snmpInReadOnlys
AtPhysAddress	tcpInSegs	snmpInGenErrs
AtNetAddress	tcpOutSegs	snmpInTotalReqVars

Address Translation MIB	TCP MIB	SNMP MIB
AtNetAddress	tcpRetransSegs	snmpInTotalSetVars
	tcpConnState	snmpInGetRequests
	tcpConnLocalAddress	snmpInGetNexts
	tcpConnLocalPort	snmpInSetRequests
	tcpConnRemAddress	snmpInGetResponses
	tcpConnRemPort	snmpInTraps
	tcpInErrs	snmpOutTooBigs
	tcpOutRsts	snmpOutNoSuchNames
		snmpOutBadValues
		snmpOutGenErrs
		snmpOutGetRequests
		snmpOutGetNexts
		snmpOutSetRequests
		snmpOutGetResponses
		snmpOutTraps
		snmpEnableAuthenTraps

RFC1317: RS-232 MIB objects

Generic RS-232-like Group	RS-232-like General Port Table	RS-232-like Asynchronous Port Group
rs232Number	rs232PortTable	rs232AsyncPortTable
	rs232PortEntry	rs232AsyncPortEntry
	rs232PortIndex	rs232AsyncPortIndex
	rs232PortType	rs232AsyncPortBits
	rs232PortInSigNumber	rs232AsyncPortStopBits
	rs232PortOutSigNumber	rs232AsyncPortParity
	rs232PortInSpeed	
	rs232PortOutSpeed	

The Input Signal Table	The Output Signal Table
rs232InSigTable	rs232OutSigTable
rs232InSigEntry	rs232OutSigEntry
rs232InSigPortIndex	rs232OutSigPortIndex
rs232InSigName	rs232OutSigName
rs232InSigState	rs232OutSigState

B

Well Known Port Numbers

This appendix is for your reference. Listed below are Well Known Port Numbers that may cause network problems if you configure NE-4000T for the same 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: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.

- The Well Known Ports range from 0 through 1023.
- The Registered Ports range from 1024 through 49151.
- The 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	SMTP (Simple Mail Transfer Protocol)
37	Time (Time Server)
42	Host name server (names server)

TCP Socket	Application Service
43	Whois (nickname)
49	(Login Host Protocol) (Login)
53	Domain Name Server (domain)
79	Finger protocol (Finger)
80	World Wibe Web HTTP
119	Netword news Transfer Protocol (NNTP)
123	Network Time Protocol
213	IPX
160 – 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	Gopler Protocol
79	Finger Protocol
80	World Wide Web HTTP
107	Remote Telnet Service
111	Sun Remote Procedure Call (Sunrpc)
119	Network news Tcanster Protocol (NNTP)
123	Network Time protocol (nnp)
161	SNMP (Simple Network Mail Protocol)
162	SNMP Traps
213	IPX (Used for IP Tunneling)

C

Service Information

This appendix shows you how to contact Moxa for information about this and other products, and how to report problems.

In this appendix, we cover the following topics.

- **MOXA Internet Services**
- **Problem Report Form**
- **Product Return Procedure**

MOXA Internet Services

Customer satisfaction is our number one concern, and to ensure that customers receive the full benefit of our products, Moxa Internet Services has been set up to provide technical support, driver updates, product information, and user's manual updates.

The following services are provided

E-mail for technical support.....support@moxa.com.tw

Moxa Group website for product information, driver downloads, documentation, and more:

.....http://www.moxa.com

Problem Report Form

MOXA NPort W2004

Customer name:	
Company:	
Tel:	**Fax:**
Email:	**Date:**

1. **Moxa Product:** ☐ NPort W2004
2. **Serial Number:** _____

Problem Description: Please describe the symptoms of the problem as clearly as possible, including any error messages you see. A clearly written description of the problem will allow us to reproduce the symptoms, and expedite the repair of your product.

Product Return Procedure

For product repair, exchange, or refund, the customer must:

- Provide evidence of original purchase.
- Obtain a Product Return Agreement (PRA) from the sales representative or dealer.
- Fill out the Problem Report Form (PRF). Include as much detail as possible for a shorter product repair time.
- Carefully pack the product in an anti-static package, and send it, pre-paid, to the dealer. The PRA should be visible on the outside of the package, and include a description of the problem, along with the return address and telephone number of a technical contact.

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 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.

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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

"Moxa declares that NPort W2004 is limited to CH1-CH11 by specified firmware when controlled in the USA."

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

INFORMATION TO USER:

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.