

# NPort W2150A/W2250A Series User's Manual

---

First Edition, April 2012

[www.moxa.com/product](http://www.moxa.com/product)

**MOXA**<sup>®</sup>

© 2012 Moxa Inc. All rights reserved.

# NPort W2150A/W2250A Series User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

## Copyright Notice

© 2012 Moxa Inc. All rights reserved.

## Trademarks

The MOXA logo is a registered trademark of Moxa Inc.  
All other trademarks or registered marks in this manual belong to their respective manufacturers.

## Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

## Technical Support Contact Information

[www.moxa.com/support](http://www.moxa.com/support)

### Moxa Americas

Toll-free: 1-888-669-2872  
Tel: +1-714-528-6777  
Fax: +1-714-528-6778

### Moxa Europe

Tel: +49-89-3 70 03 99-0  
Fax: +49-89-3 70 03 99-99

### Moxa China (Shanghai office)

Toll-free: 800-820-5036  
Tel: +86-21-5258-9955  
Fax: +86-21-5258-5505

### Moxa Asia-Pacific

Tel: +886-2-8919-1230  
Fax: +886-2-8919-1231

# Table of Contents

<b>1. Introduction</b>	<b>1-1</b>
Overview	1-2
Package Checklist	1-2
Product Features	1-2
Product Specifications	1-3
Serial Port Pin Assignments	1-4
<b>2. Getting Started</b>	<b>2-1</b>
Overview	2-2
Panel Layout	2-2
LED Indicators	2-3
Top Panel LED Indicators	2-3
End Panel LED Indicators	2-3
Pull High/Low Resistors for RS-422/485	2-4
Placement Options	2-5
Connecting the Hardware	2-5
Connecting to the Network	2-6
Connecting the Power	2-6
Connecting to a Serial Device	2-6
<b>3. Initial IP Configuration</b>	<b>3-1</b>
Overview	3-2
Factory Default IP Settings	3-2
Using ARP to Assign IP Address	3-2
Using the Telnet Console to Assign IP Address	3-3
Using the Serial Console to Assign IP Address	3-6
<b>4. Introduction to Operation Modes</b>	<b>4-1</b>
Overview	4-2
RealCOM Mode	4-2
RFC2217 Mode	4-3
TCP Server Mode	4-3
TCP Client Mode	4-3
UDP Mode	4-4
Pair Connection Modes	4-4
Ethernet Modem Mode	4-4
<b>5. Web Console: Basic Settings</b>	<b>5-1</b>
Overview	5-2
Basic Settings	5-4
<b>6. Web Console: Network Settings</b>	<b>6-1</b>
Overview	6-2
Network Settings	6-2
General Settings	6-2
Ethernet Settings	6-3
WLAN Settings	6-4
Advanced Settings	6-21
<b>7. Web Console: Serial Port Settings</b>	<b>7-1</b>
Overview	7-2
Serial Port Settings	7-2
Communication Parameters	7-22
Data Buffering/Log	7-24
<b>8. Web Console: System Management</b>	<b>8-1</b>
Overview	8-2
System Management	8-2
Misc. Network Settings	8-2
Auto Warning Settings	8-6
Maintenance	8-10
Maintenance	8-11
Certificate	8-14
<b>9. Web Console: System Monitoring</b>	<b>9-1</b>
Overview	9-2
System Monitoring	9-2
Serial Status	9-2
System Status	9-4
<b>10. Web Console: Restart</b>	<b>10-1</b>
Overview	10-2
Restart	10-2

Restart System .....	10-2
Restart Ports.....	10-3
<b>11. Installing and Configuring the Software .....</b>	<b>11-1</b>
Overview .....	11-2
NPort Windows Driver Manager .....	11-2
Installing NPort Windows Driver Manager .....	11-2
Adding Mapped Serial Ports .....	11-5
Configuring Mapped Serial Ports.....	11-8
NPort Search Utility.....	11-13
Installing NPort Search Utility .....	11-13
Finding NPort Device Servers on Network.....	11-15
Modifying NPort IP Addresses.....	11-16
Upgrading NPort Firmware.....	11-17
Linux Real TTY Drivers .....	11-18
Basic Steps.....	11-18
Installing Linux Real TTY Driver Files .....	11-18
Mapping TTY Ports.....	11-19
Removing Mapped TTY Ports.....	11-19
Removing Linux Driver Files.....	11-20
UNIX Fixed TTY Drivers .....	11-20
Installing the UNIX Driver.....	11-21
Configuring the UNIX Driver .....	11-21
<b>A. SNMP Agents with MIB II &amp; RS-232-Like Groups .....</b>	<b>A-1</b>
RFC1213 MIB-II Supported SNMP Variables .....	A-1
System MIB.....	A-1
Interfaces MIB .....	A-1
IP MIB .....	A-1
ICMP MIB .....	A-2
UDP MIB .....	A-2
Address Translation .....	A-2
TCP MIB.....	A-2
SNMP MIB .....	A-2
RFC1317: RS-232 MIB Objects .....	A-3
Generic RS-232-like Group .....	A-3
RS-232-like General Port Table .....	A-3
RS-232-like Asynchronous Port Group.....	A-3
The Input Signal Table .....	A-3
The Output Signal Table.....	A-3
<b>B. Well Known Port Numbers .....</b>	<b>B-1</b>
<b>C. Ethernet Modem Commands.....</b>	<b>C-1</b>
Dial-in Operation .....	C-1
Dial-out .....	C-1
Disconnection Request from Local Site .....	C-1
Disconnection Request from Remote Site.....	C-1
AT Commands.....	C-2
S Registers .....	C-3
<b>D. Federal Communication Commission Interference Statement .....</b>	<b>D-1</b>
<b>E. FCC Warning Statement .....</b>	<b>E-1</b>

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Product Specifications**
- **Serial Port Pin Assignments**
- **Overview**
- **Panel Layout**
- **LED Indicators**
  - Top Panel LED Indicators
  - End Panel LED Indicators
- **Pull High/Low Resistors for RS-422/485**
- **Placement Options**
- **Connecting the Hardware**
  - Connecting to the Network
  - Connecting the Power
  - Connecting to a Serial Device

# Overview

In this chapter we introduce the basic features and specifications of the NPort W2150A/W2250A and NPort W2150A/W2250A-T, referred to collectively as the NPort W2150A/W2250A Series.

The NPort W2150A/W2250A Series of wireless device servers are used to connect RS-232/422/485 serial devices such as PLCs, meters, and sensors, to a wired Ethernet LAN or wireless LAN. Your communications software will be able to access the serial devices from anywhere over a local LAN, WLAN, or the Internet. Moreover, the WLAN environment offers an excellent solution for applications in which the serial devices are moved frequently from place to place.

The NPort W2150A/W2250A supports both automatic IP configuration protocols (DHCP, BOOTP) and manual configuration using a standard web browser. Both IP configuration methods ensure quick and effective installation. In addition, a utility called "NPort Windows Driver Manager" makes port mapping easy.

The external antenna can be adjusted for maximum signal strength. You can also choose to use your own antenna for additional flexibility and scalability. A signal strength indicator on the front panel makes it easier for you to troubleshoot any connection problems.

The NPort W2150A/W2250A Series offers different operation modes to ensure compatibility with standard network APIs, including TCP Server Mode, TCP Client Mode, and UDP Mode. RealCOM/TTY drivers are provided to allow legacy serial-based software to communicate over an IP network instantly. This preserves your software investment while providing all the advantages of networking your serial devices.

For easier management, the NPort W2150A/W2250A include features such as password authentication, IP filtering, 64-bit and 128-bit WEP encryption, and SNMP support.

## Package Checklist

### Standard Accessories

- NPort W2150A, NPort W2150A-T, NPort W2250A, or NPort W2250A-T.
- Document & Software CD
- RJ45 to RJ45 Ethernet cross-over cable
- Warranty statement
- Quick Installation Guide

### Optional Accessories

- DK-35A: DIN-rail mounting kit (35 mm)
- Power jack to terminal block power cable (P/N: 919900000900)

*NOTE: Please notify your sales representative if any of the above items are missing or damaged*

## Product Features

- Instant connection of any serial device to IEEE 802.11a/b/g network
- RS-232/422/485 ports supporting baudrates up to 921.6 Kbps
- Web-based configuration over Ethernet or WLAN
- Enhanced remote configuration with HTTPS, SSH
- Secure data access with WEP, WPA, WPA2
- Built-in WLAN site survey Tool
- Fast roaming when signal strength is weak
- Per-port offline port buffering and serial data log
- Dual power inputs via power jack and terminal block

# Product Specifications

## Ethernet Interface

**Number of Ports:** 1

**Speed:** 10/100 Mbps, auto MDI/MDIX

**Connector:** RJ45

**Magnetic Isolation Protection:** 1.5 KV built-in

## WLAN Interface

**Standard Compliance:** 802.11a/b/g

**Network Modes:** Infrastructure, Ad-Hoc

**Transmit Power:**

802.11a: 14 dBm (typical)

802.11b: 17 dBm (typical)

802.11g: 15 dBm (typical)

**Receive Sensitivity:** -80 dBm

**Radio Frequency Type:** DSSS/OFDM

**Transmission Rate:**

802.11a: 54 Mbps

802.11b: 11 Mbps

802.11g: 54 Mbps (max.) with auto fallback (54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps)

**Transmission Distance:** Up to 100 meters (in open areas)

**Wireless Security:**

- WEP: 64-bit/128-bit data encryption
- WPA, WPA2, 802.11i: Enterprise mode and Pre-Share Key (PSK) mode
- Encryption: 128-bit TKIP/AES-CCMP EAP-TLS, PEAP/GTC, PEAP/MD5, PEAP/MSCHAPV2, EAP-TTLS/PAP, EAP-TTLS/CHAP, EAP-TTLS/MSCHAP, EAP-TTLS/MSCHAPV2, EAP-TTLS/EAP-MSCHAPV2, EAP-TTLS/EAP-GTC, EAP-TTLS/EAP-MD5, LEAP

**Antenna Connector:** Reverse SMA

## Serial Interface

**Number of Ports:**

NPort W2150A: 1

NPort W2250A: 2

**Serial Standards:** RS-232/422/485 (DB9 male connector)

**Off-line Port Buffering:**

NPort W2150A: 20 MB

NPort W2250A: 10 MB

**Serial Line Surge Protection:** 1KV (level 2)

## Serial Communication Parameters

**Data Bits:** 5, 6, 7, 8

**Stop Bits:** 1, 1.5, 2

**Parity:** None, Even, Odd, Space, Mark

**Flow Control:** RTS/CTS, XON/XOFF

**Baudrate:** 50 bps to 921.6 Kbps

**Serial Data Log:** 64 KB

## Serial Signals

**RS-232:** TxD, RxD, RTS, CTS, DTR, DSR, DCD, GND

**RS-422:** TxD+, TxD-, RxD+, RxD-, GND

**RS-485-4w:** TxD+, TxD-, RxD+, RxD-, GND

**RS-485-2w:** Data+, Data-, GND

## Software

**Network Protocols:** ICMP, IP, TCP, UDP, DHCP, Telnet, DNS, SNMP V1/V2c/V3, HTTP, SMTP, SNTP, SSH, HTTPS

**Configuration Options:** Web Console, Serial Console, Telnet Console

**Secure Configuration Options:** HTTPS, SSH

**Windows RealCOM Drivers:** Windows 95/98/ME/NT/2000, Windows XP/2003/Vista/2008/7 x86/x64, Embedded CE 5.0/6.0, XP Embedded

**Fixed TTY Drivers:** SCO Unix, SCO OpenServer, UnixWare 7, UnixWare 2.1, SVR 4.2, QNX 4.25, QNX 6, Solaris 10, FreeBSD, AIX 5.x, HP-UX 11i

**Linux Real TTY Drivers:** 2.4.x, 2.6.x, 3.x

**Utilities:** NPort Search Utility and NPort Windows Driver manager

**Management:** SNMP MIB-II

**Physical Characteristics**

**Housing:** Aluminum sheet metal (1 mm)

**Weight:** 780 g

**Dimensions:**

Without ears or antenna: 77 x 111 x 26 mm (3.03 x 4.37 x 1.02 in)

With ears, without antenna: 100 x 111 x 26 mm (3.94 x 4.37 x 1.02 in)

Antenna Length: 109.79 mm (4.32 in)

**Environmental Limits**

**Operating Temperature:**

Standard Models: 0 to 55°C (32 to 131°F)

Wide Temp. Models: -40 to 75°C (-40 to 167°F)

**Storage Temperature:** -40 to 85°C (-40 to 185°F)

**Ambient Relative Humidity:** 5 to 95% (non-condensing)

**Power Requirements**

**Input Voltage:** 12 to 48 VDC

**Power Consumption:**

237 mA @ 12 V, 125 mA @ 24 V, 50 mA @ 48 V

**Standards and Certifications**

**Safety:** UL 60950-1, EN 60950-1

**EMC:** CE, FCC

**EMI:** FCC Part 15 Subpart B Class A, FCC Subpart C/E, VCCI

**EMS:** EN 55022 Class A

**Radio:** CE (ETSI EN 301 893, ETSI EN 300 328), ARIB RCR STD-33, ARIB STD-66

**Power Line Surge Protection:** 2 KV (level 3)

**Reliability**

**Alert Tool:** RTC (real-time clock)

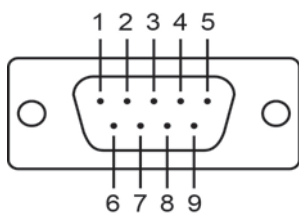
**Automatic Reboot Trigger:** Built-in WDT (watchdog timer)

**Warranty**

**Warranty Period:** 5 years

**Details:** See [www.moxa.com/warranty](http://www.moxa.com/warranty)

## Serial Port Pin Assignments



Pin	RS-232	RS-422/ RS-485 (4W)	RS-485 (2W)
1	DCD	TxD-(A)	---
2	RXD	TxD+(B)	---
3	TXD	RxD+(B)	Data+(B)
4	DTR	RxD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	---	---
7	RTS	---	---
8	CTS	---	---
9	---	---	---



# 2

## Getting Started

---

The following topics are covered in this chapter:

- **Overview**
- **Panel Layout**
- **LED Indicators**
  - Top Panel LED Indicators
  - End Panel LED Indicators
- **Pull High/Low Resistors for RS-422/485**
- **Placement Options**
- **Connecting the Hardware**
  - Connecting to the Network
  - Connecting the Power
  - Connecting to a Serial Device

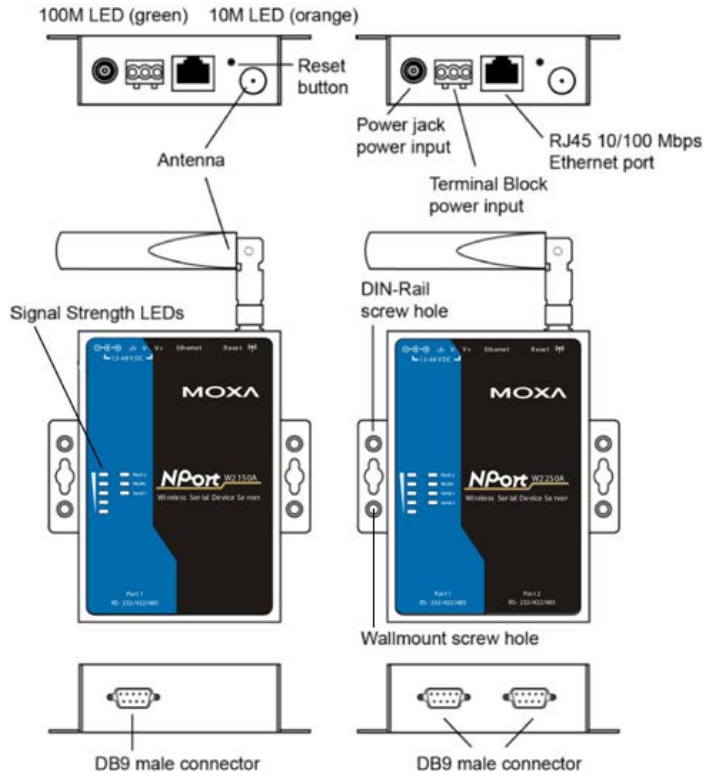
# Overview

This chapter presents the hardware features of the NPort W2150/W2250A Series and explains how to connect the hardware.

## Panel Layout

NPort W2150A/W2150A-T

NPort W2250A/W2250A-T



# LED Indicators

## Top Panel LED Indicators

Name	Color	Function
Ready	Red	Steady on: Power is on and NPort is booting up. Blinking: IP conflict or DHCP/ BOOTP server did not respond properly.
	Green	Steady on: NPort is functioning normally. Blinking: Unit is responding to Locate function.
	Off	Power is off or a power error condition exists.
WLAN	Green	Steady on: Wireless enabled Blinking: NPort can't establish WLAN connection with AP (Infrastructure) or station (Ad-Hoc)
	Off	Wireless not enabled.
Serial 1 Serial 2	Orange	Serial port is receiving data.
	Green	Serial port is transmitting data.
	Off	No data is flowing to or from the serial port.
Signal Strength (5 LEDS)	Red	1 Red - the signal strength is between 0% and 20% 2 Red - the signal strength is between 21% and 40%
	Green	3 Green - the signal strength is between 41% and 60% 4 Green - the signal strength is between 61% and 80% 5 Green - the signal strength is between 81% and 100%

## End Panel LED Indicators

Name	Color	Function
Ethernet	Orange	10 Mbps Ethernet connection
	Green	100 Mbps Ethernet connection
	Off	Ethernet cable is disconnected

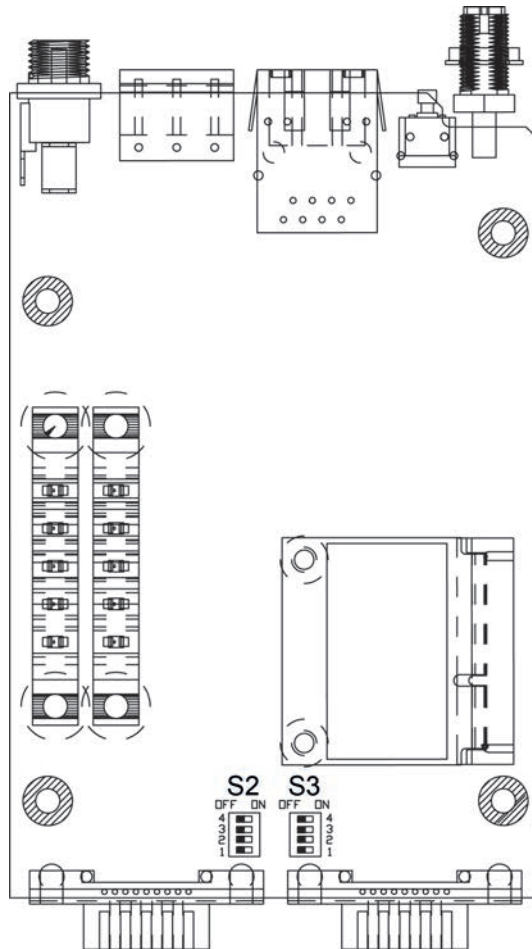
# Pull High/Low Resistors for RS-422/485

You may need to set the pull high/low resistors when termination resistors are used for certain RS-422 or RS-485 environments.

S2 (Serial 1) S3 (Serial 2)	DIP 1	DIP 2	DIP 3	DIP 4
ON	Pull high resistor 1 KΩ	Pull low resistor 1 KΩ	Terminal resistor 120 Ω	Reserved -----
OFF	*150 KΩ	*150 KΩ	*N/A	-----

\*Default

S3 is for NPort W2250A only

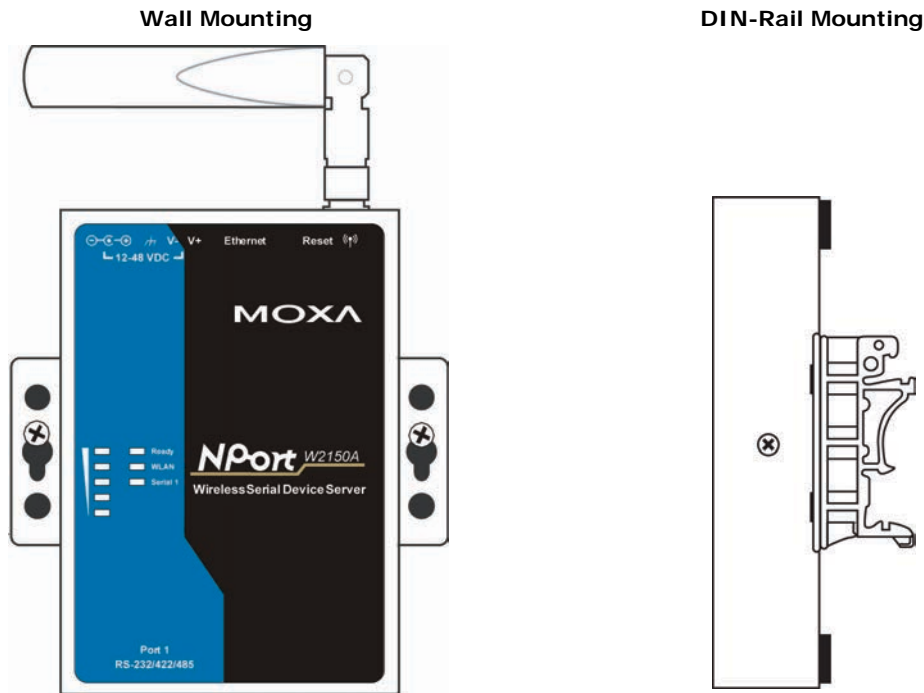


## ATTENTION

Do not use the 1 KΩ setting while in RS-232 mode. Doing so will degrade the RS-232 signals and reduce the effective communication distance.

# Placement Options

The NPort can be placed on a desktop or other horizontal surface. You can also install the NPort on a DIN-rail or on the wall.



# Connecting the Hardware



**ATTENTION**

Before connecting the hardware, follow these important wiring safety precautions:

**Disconnect power source**

Do not install or wire this unit or any attached devices with the power connected. Disconnect the power before installation by removing the power cord before installing and/or wiring your unit.

**Follow maximum current ratings**

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.

If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

**Use caution - unit may get hot**

The unit will generate heat during operation, and the casing may feel hot to the touch. Take care when handling unit. Be sure to leave adequate space for ventilation.

The following guidelines will help ensure trouble-free signal communication with the NPort.

- Use separate paths to route wiring for power and devices to avoid interference. Do not run signal or communication wiring and power wiring in the same wire conduit. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
- Keep input wiring and output wiring separate.
- Label all wiring to each device in the system for easier testing and troubleshooting

## Connecting to the Network

Use the supplied Ethernet cable to connect the NPort to your Ethernet network. If the cable is properly connected, the NPort will indicate a valid connection to the Ethernet as follows:

- A green Ethernet LED indicates a valid connection to a 100 Mbps Ethernet network.
- An orange Ethernet LED indicates a valid connection to a 10 Mbps Ethernet network.
- A flashing Ethernet LED indicates that Ethernet packets are being transmitted or received.

## Connecting the Power

Connect the VDC power line (12 to 48 V) to the NPort's power jack or terminal block. If power is properly connected, the "Ready" LED will initially glow red. When the system is ready, the "Ready" LED will turn green.

## Connecting to a Serial Device

Use a serial cable to connect your serial device to a serial port on the NPort.

## Initial IP Configuration

---

The following topics are covered in this chapter:

- ❑ **Overview**
- ❑ **Factory Default IP Settings**
- ❑ **Using ARP to Assign IP Address**
- ❑ **Using the Telnet Console to Assign IP Address**
- ❑ **Using the Serial Console to Assign IP Address**

## Overview

This chapter presents several ways to assign the NPort's IP address for the first time. Please refer to Chapter 2 for instructions on connecting to the network.

The web console is the recommended method for configuring the NPort. Please refer to Chapter 5 and 6 for details on using the web console for configuration.



### ATTENTION

The LAN and WLAN interfaces cannot be used at the same time. If the Ethernet link is active, then WLAN connections will be disabled. If the WLAN connection is active, then the Ethernet link will be disabled.



### ATTENTION

Make sure that the Ethernet cable is connected before powering up the NPort.

## Factory Default IP Settings

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

If your NPort is configured to obtain its IP settings from a DHCP or BOOTP server but is unable to get a response, it will use the factory default IP address and netmask.



### ATTENTION

If you forget the IP address of your NPort, you can look it up using the NPort Search Utility. After NPort Search Utility has found all NPorts on the network, each unit will be listed with its IP address. Please refer to Chapter 11 for additional information on using NPort Search Utility.

## Using ARP to Assign IP Address

The ARP (Address Resolution Protocol) command can be used to assign an IP address to the NPort. The ARP command tells your computer to associate the NPort's MAC address with the specified IP address. You must then use Telnet to access the NPort, at which point the device server's IP address will be reconfigured. This method only works when the NPort is configured with default IP settings.

1. Select a valid IP address for your NPort. Consult with your network administrator if necessary.
2. Obtain the NPort's MAC address from the label on its bottom panel.
3. From the DOS prompt, execute the **arp -s** command with the desired IP address and the NPort's MAC address, as in the following example:

```
arp -s 192.168.200.100 00-90-E8-xx-xx-xx
```

In this example 192.168.200.100 is the new IP address that will be assigned to the NPort, and 00-90-E8-xx-xx-xx is the NPort's MAC address.

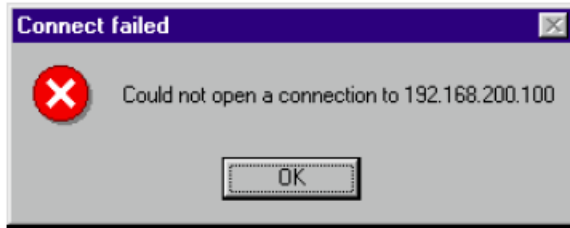
4. From the DOS prompt, execute a special Telnet command using port 6000, as in the following example:

```
telnet 192.168.200.100 6000
```

In this example, 192.168.200.100 is the new IP address that will be assigned to the NPort.



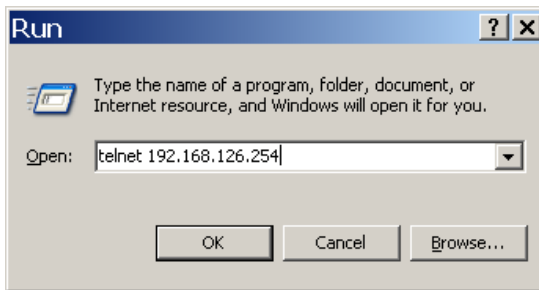
5. You will see a message indicating that the connection failed.



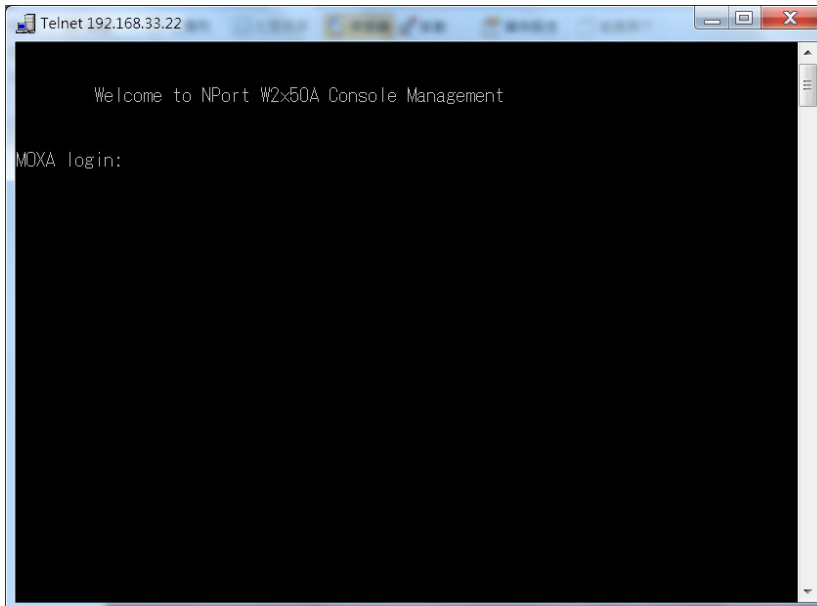
The NPort will automatically reboot with the new IP address. You can verify that the configuration was successful by connecting to the new IP address with Telnet, ping, the web console, or NPort Search Utility.

## Using the Telnet Console to Assign IP Address

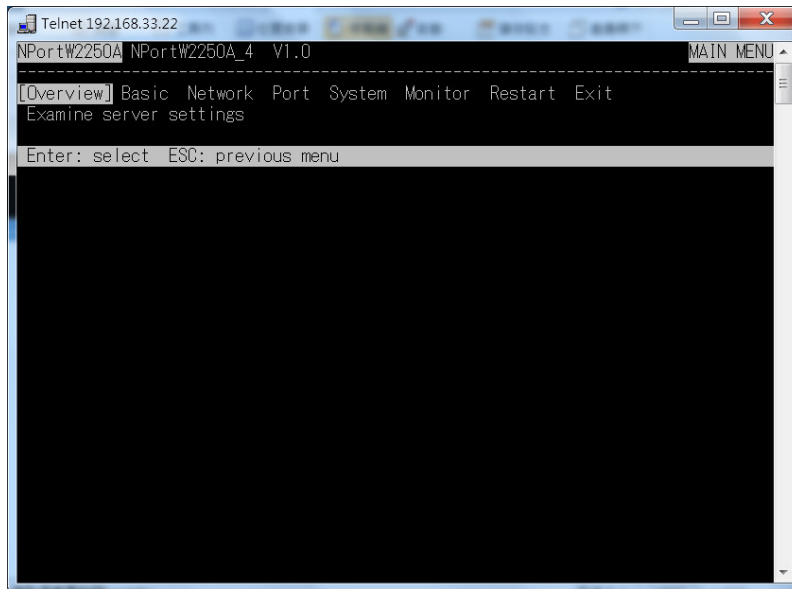
1. Select **Run...** from the Windows Start menu.
2. Enter **telnet 192.168.126.254** (the NPort's default IP address) and click **[OK]**.



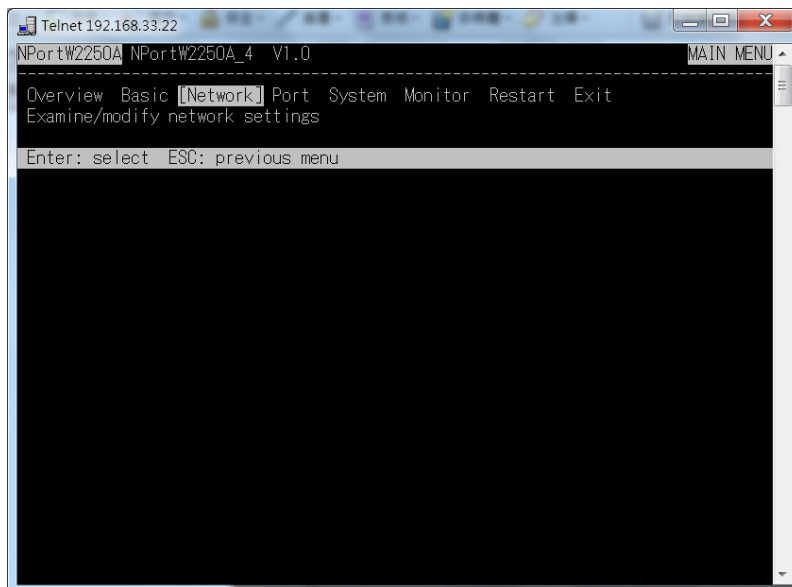
3. Enter your login account and password, then press **ENTER**.



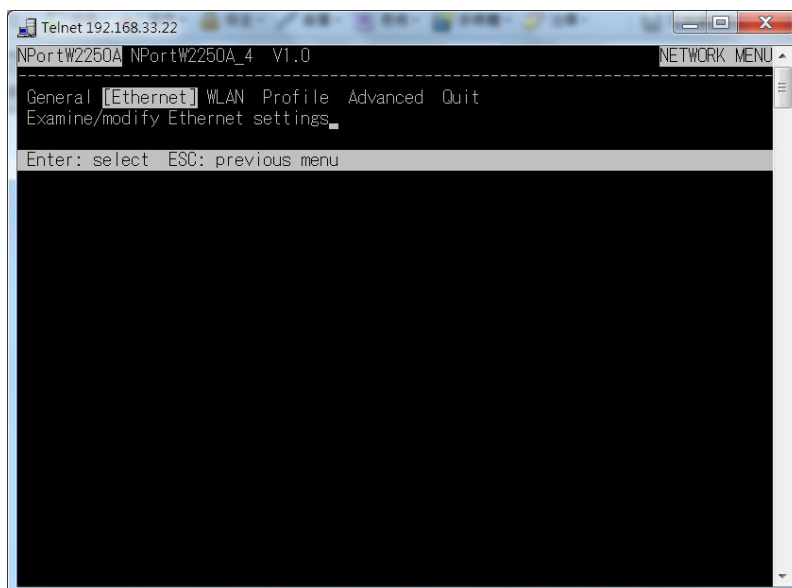
4. You will login to the **Overview** page.



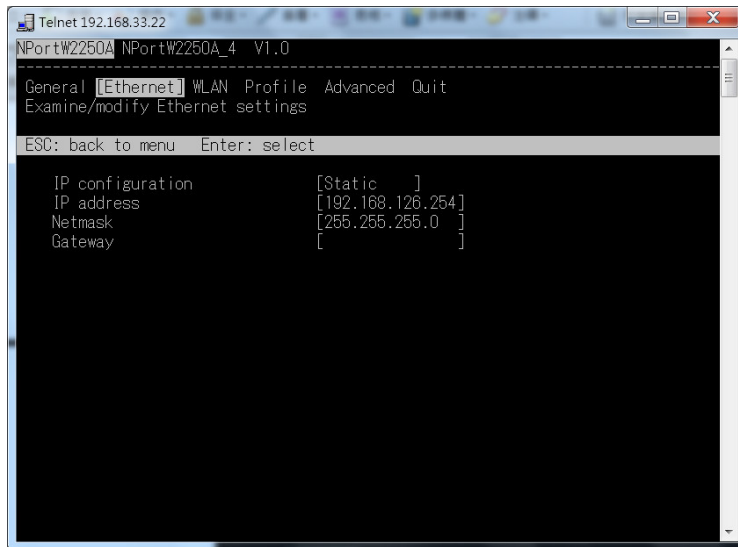
5. Press **N** or use the cursor keys to select **Network** and press **ENTER**.



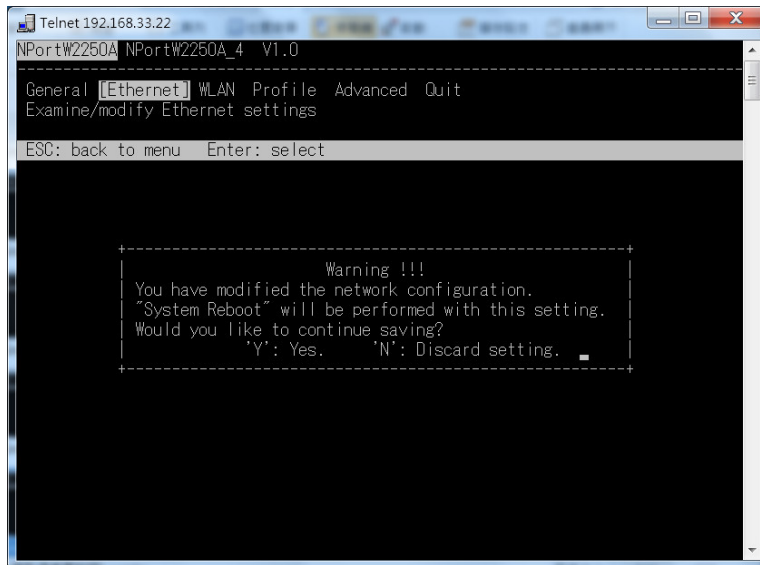
6. Press **E** or use the cursor keys to select **Ethernet** and press **ENTER**.



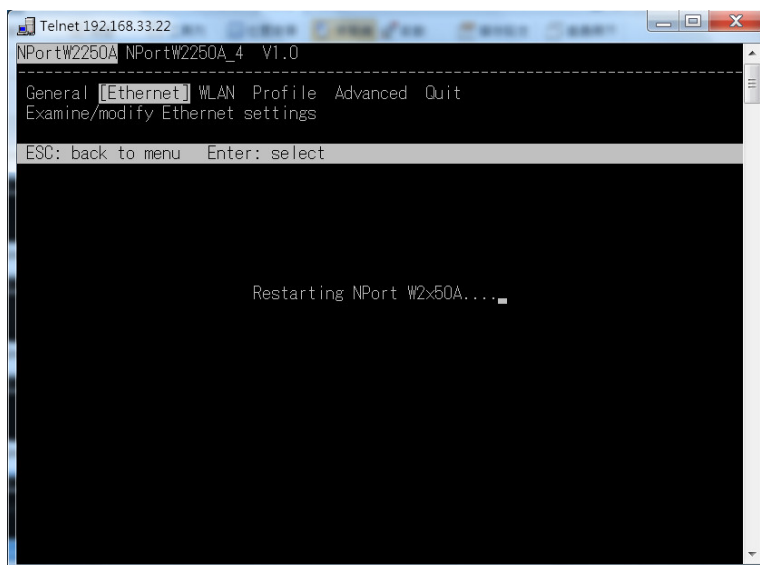
- Use the cursor keys to navigate between the different fields. For **IP address**, **Netmask**, and **Gateway**, enter the desired values directly. For **IP configuration** and **LAN speed**, press **ENTER** to open a submenu and select between the available options.



- Press **ESC** to return to the menu. When prompted, press **Y** to save the configuration changes.



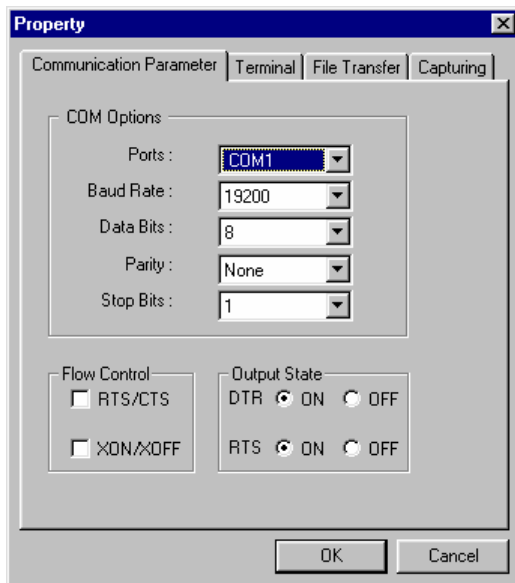
The NPort will reboot with the new IP settings. You can telnet to the new IP to login again.



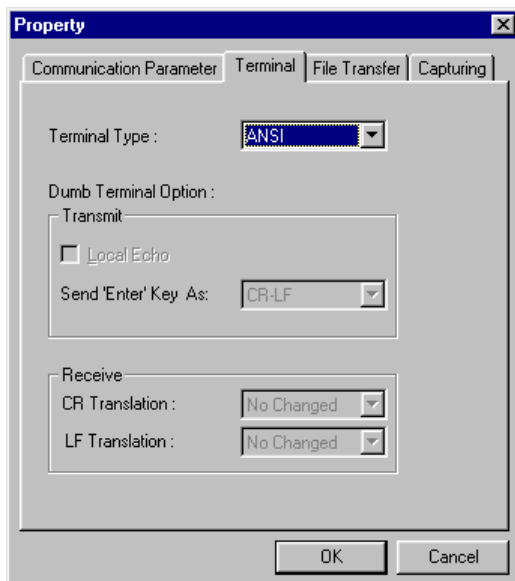
## Using the Serial Console to Assign IP Address

Before using the NPort's serial console, turn off the power and use a serial cable to connect the NPort console port to your computer's serial port. Port 1 on the NPort serves as the console port. Use Port 1 connecting to the console port with a serial-based terminal or terminal emulator program, such as Windows HyperTerminal. You may also download PComm Lite at [www.moxa.com](http://www.moxa.com). The terminal type should be set as ANSI or VT100, and the serial communication parameters should be set as 19200, 8, N, 1 (19200 for baud rate, 8 for data bits, None for parity, and 1 for stop bits). As soon as the connection is open, you will be presented with a text menu displaying the NPort W2150A/W2250A Series general settings. Please refer to Chapter 4 for a description of the available settings. The following instructions, we recommend using PComm Terminal Emulator, which can be downloaded free of charge from [www.moxa.com](http://www.moxa.com), to carry out the configuration procedure.

1. Connect your PC's serial port to the NPort's console port.
2. Open your terminal emulator program, such as Windows HyperTerminal. We recommend using PComm Terminal Emulator, which can be downloaded for free at [www.moxa.com](http://www.moxa.com).
3. In your terminal emulator program, configure the communication parameters for the serial port on the PC. The parameters should be set to **19200** for baud rate, **8** for data bits, **None** for parity, and **1** for stop bits.



4. In your terminal emulator program, set the terminal type to **ANSI** or **VT100**. If you select **Dumb Terminal** as the terminal type, some of the console functions—especially the “Monitor” function—may not work properly.



5. Hold the **grave accent** key ( ` ) down and power up the NPort.



The continuous string of grave accent characters triggers the NPort to switch from data mode to console mode.

6. The serial console will open and will be functionally identical to the Telnet console. Please refer to the Telnet console section for instructions on how to navigate the console and configure the IP settings.

# Introduction to Operation Modes

---

The following topics are covered in this chapter:

- **Overview**
- **RealCOM Mode**
- **RFC2217 Mode**
- **TCP Server Mode**
- **TCP Client Mode**
- **UDP Mode**
- **Pair Master and Pair Connection Modes**
- **Ethernet Modem Mode**

## Overview

This chapter introduces the different serial port operation modes that are available on the NPort W2150A/W2250A Series. Each serial port on the NPort is configured independently of the other ports, with its own serial communication parameters and operation mode. The serial port's operation mode determines how it interacts with the network, and different modes are available to encompass a wide variety of applications and devices.

**RealCOM** and **RFC2217** modes allow serial-based software to access the NPort serial port as if it were a local serial port on a PC. These modes are appropriate when your application relies on Windows or Linux software that was originally designed for locally attached COM or TTY devices. With these modes, you can access your devices from the network using your existing COM/TTY-based software, without investing in additional software.

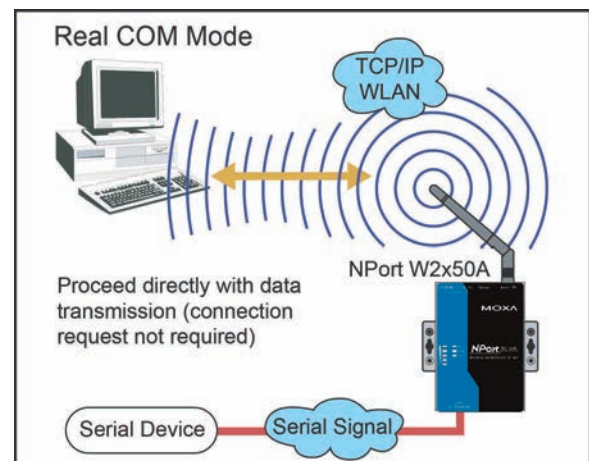
Three different socket modes are available for user-developed socket programs: **TCP Server**, **TCP Client**, and **UDP Server/Client**. For TCP applications, the appropriate mode depends on whether the connection will be hosted or initiated from the NPort serial port or from the network. The main difference between the TCP and UDP protocols is that TCP guarantees delivery of data by requiring the recipient to send an acknowledgement to the sender. UDP does not require this type of verification, making it possible to offer speedier delivery. UDP also allows multicasting of data to groups of IP addresses and would be suitable for streaming media or non-critical messaging applications such as LED message boards.

**Pair Connection Slave** and **Master** modes are designed for serial-to-serial communication over Ethernet, in order to overcome traditional limitations with serial transmission distance.

In **Ethernet Modem** mode, the NPort acts as an Ethernet modem, providing a network connection to a host through the serial port.

## RealCOM Mode

RealCOM mode is designed to work with NPort drivers that are installed on a network host. COM drivers are provided for Windows systems, and TTY drivers are provided for Linux and UNIX systems. The driver establishes a transparent connection to the attached serial device by mapping a local serial port to the NPort serial port. RealCOM mode supports up to four simultaneous connections, so multiple hosts can collect data from the attached device at the same time.



### ATTENTION

RealCOM drivers are installed and configured through NPort Windows Driver Manager.

RealCOM mode allows you to continue using your serial communications software to access devices that are now attached to your NPort device server. On the host, the NPort RealCOM driver automatically intercepts data sent to the COM port, packs it into a TCP/IP packet, and redirects it to the network. At the other end of the connection, the NPort device server accepts the Ethernet frame, unpacks the TCP/IP packet, and sends the serial data to the appropriate device.



**ATTENTION**

In RealCOM mode, several hosts can have simultaneous access control over the NPort serial port. If necessary, you can limit access by using the NPort’s Accessible IP settings. Please refer to Chapter 8 for additional information on Accessible IP settings.

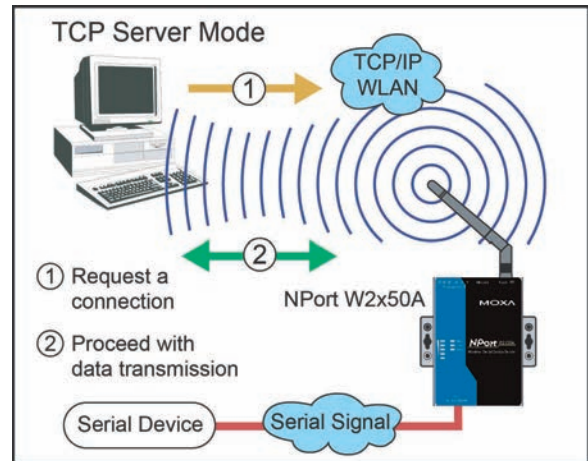
## RFC2217 Mode

RFC-2217 mode is similar to RealCOM mode, since it relies on a driver to transparently map a virtual COM port on a host computer to a serial port on the NPort. The RFC2217 standard defines general COM port control options based on the Telnet protocol and supports one connection at a time. Third party drivers supporting RFC-2217 are widely available on the Internet and can be used to implement virtual COM mapping.

## TCP Server Mode

In TCP Server mode, the NPort serial port is assigned an IP:port address that is unique on your TCP/IP network. It waits for the host computer to establish a connection to the attached serial device. This operation mode also supports up to eight simultaneous connections, so multiple hosts can collect data from the attached device at the same time.

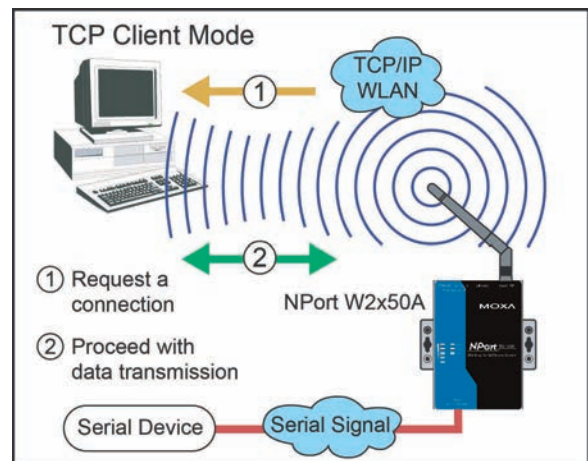
Data transmission proceeds as follows:  
 A host requests a connection to the NPort serial port. Once the connection is established, data can be transmitted in both directions—from the host to the device, and from the device to the host.



## TCP Client Mode

In TCP Client mode, the NPort actively establishes a TCP connection to a specific network host when data is received from the attached serial device. After the data has been transferred, the NPort can automatically disconnect from the host computer through the Inactivity time settings. Please refer to Chapter 7 for details on these parameters.

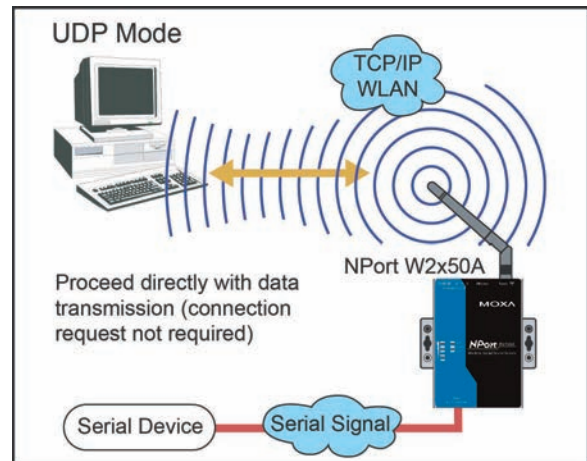
Data transmission proceeds as follows:  
 The NPort requests a connection from the host. The connection is established and data can be transmitted in both directions between the host and device.





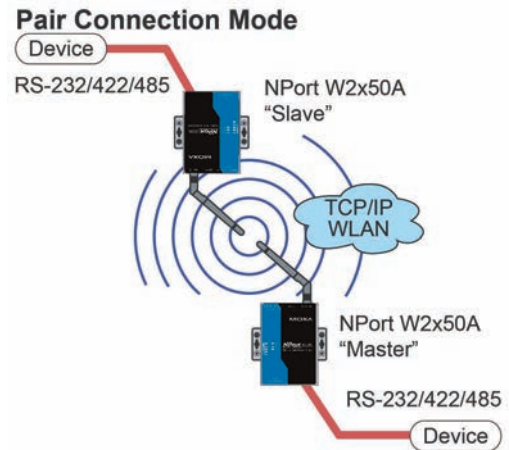
## UDP Mode

UDP is similar to TCP but is faster and more efficient. Data can be broadcast to or received from multiple network hosts. However, UDP does not support verification of data and would not be suitable for applications where data integrity is critical. It is ideal for message display applications.



## Pair Connection Modes

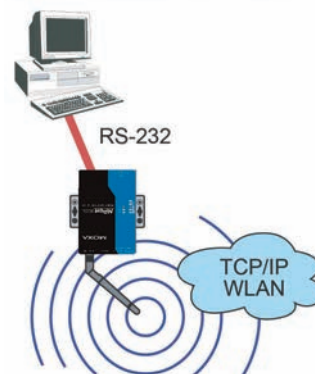
Pair Connection Master and Slave modes connect two NPort device servers over a network for serial-to-serial communication. A device attached to one NPort can then communicate transparently to a device attached to the other NPort, as if the two devices were connected by a serial cable. Both data and modem control signals are exchanged, except for DCD signals. This can be used to overcome traditional limitations with serial communication distance and introduces many new possibilities for serial-based device control.



## Ethernet Modem Mode

Ethernet Modem mode is designed for use with legacy operating systems, such as MS-DOS, that do not support TCP/IP Ethernet. By connecting the properly configured NPort serial port to the MS-DOS computer's serial port, it is possible to use legacy software to transmit data over the Ethernet when the software was originally designed to transmit data over a modem.

**Ethernet Modem Mode**



## Web Console: Basic Settings

---

The following topics are covered in this chapter:

- **Overview**
- **Basic Settings**

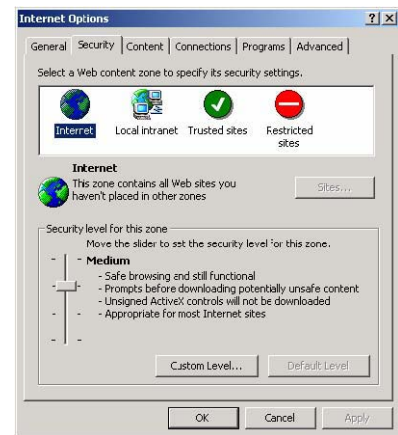
## Overview

This chapter introduces the NPort web console and explains how to configure the basic settings.

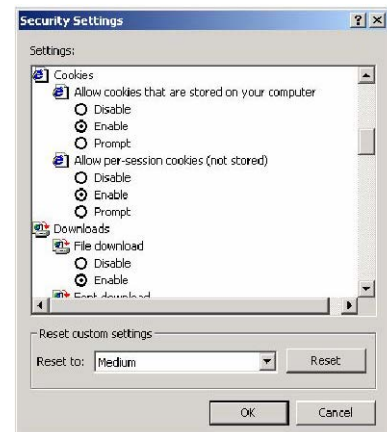
The NPort can be configured from anywhere on the network through its web console. Simply point the browser to the device server's IP address to open the web console. Network settings, operation mode, and other items can all be configured through the browser.

## Web Browser Settings

In order to use the web console, you will need to have cookies enabled for your browser. Please note that the web console uses cookies only for password transmission. For Internet Explorer, cookies can be enabled by right-clicking the Internet Explorer icon on your desktop and selecting Properties from the context menu.



On the Security tab, click "Custom Level..." and enable these two items:  
 Allow cookies that are stored on your computer.  
 Allow per-session cookies (not stored).



### ATTENTION

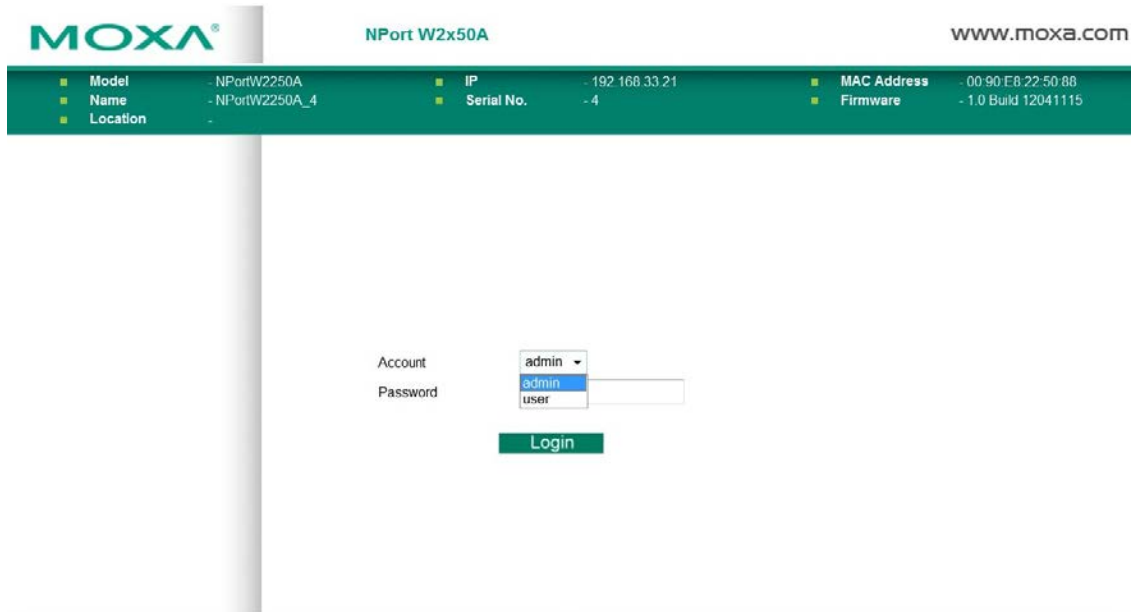
If you are not using Internet Explorer, cookies are usually enabled through a web browser setting such as "allow cookies that are stored on your computer" or "allow per-session cookies."

## Navigating the Web Console

To open the web console, enter your device server's IP address in the website address line. If you are configuring the NPort for the first time over an Ethernet cable, you will use the default IP address, **192.168.126.254**.

There are two account types: **admin** and **user**. If you enter the system with **admin** account, you will have the right to read and write. If you enter the system with **user** account, you will only have the right to read.

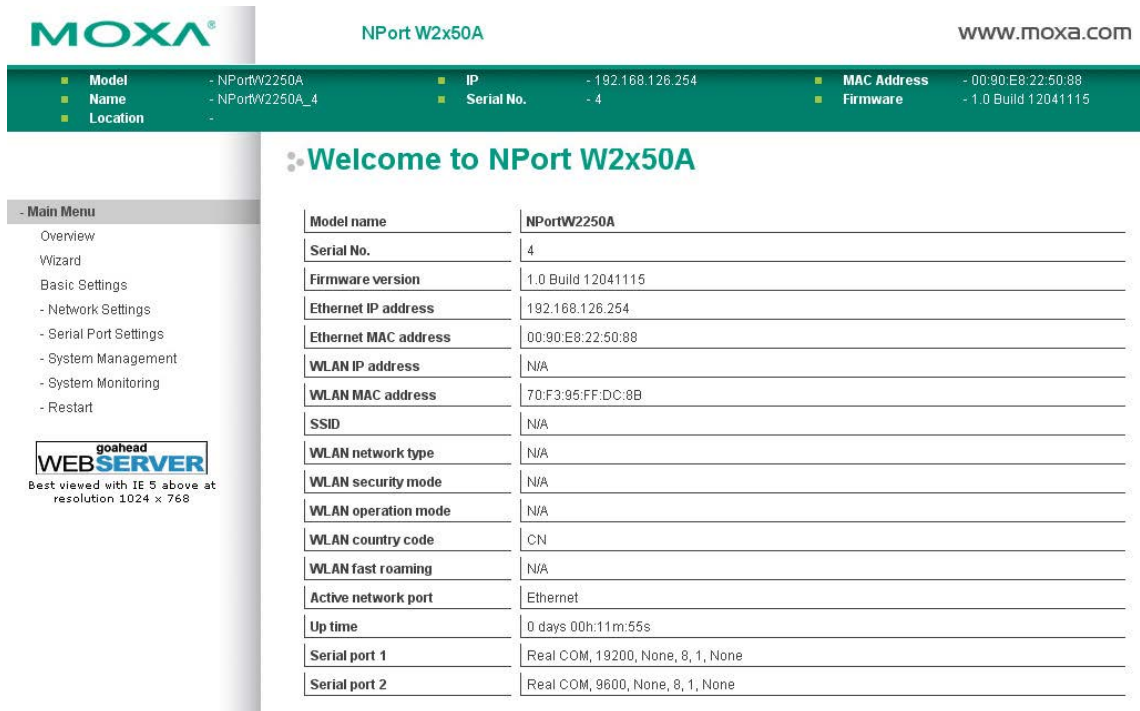
If prompted, enter the console password. You will only be prompted for a password if you have enabled password protection on the device server. The password will be transmitted with MD5 encryption over the Ethernet.



**ATTENTION**

If you have forgotten the password, you can use the reset button to load factory defaults, but this will erase all previous configuration information.

The web console will appear as shown below.



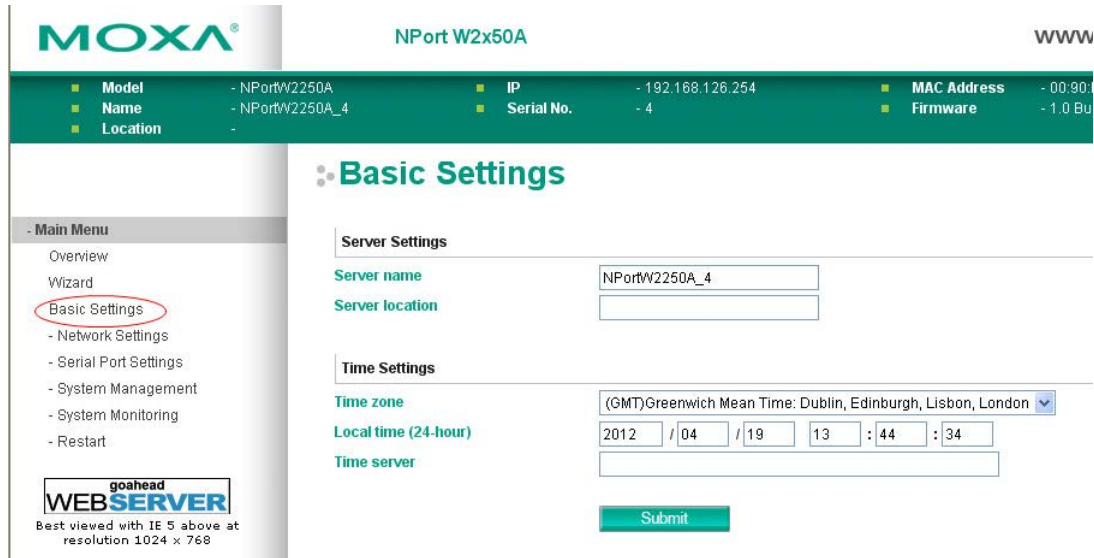
Settings are presented on pages that are organized by folder. Select the desired folder in the left navigation panel to open that page. The page will be displayed in the main window on the right. Certain folders can be expanded by clicking the adjacent “-” symbol.

For example, if you click **Basic Settings** in the navigation panel, the main window will show a page of basic settings that you can configure.

After you have made changes on a page, you must click **[Submit]** in the main window before jumping to another page. Your changes will be lost if you do not click **[Submit]**.

Once you click [Submit] button, the device server will reboot and with a beep alarm.

# Basic Settings



On the **Basic Settings** page, you can configure **Server name**, **Server location**, **Time zone (24-hour)**, **Local time**, and **Time server**.

## Server Name

<b>Default</b>	NPortW2150A_<serial no.> or NPortW2250A_<serial no.>
<b>Options</b>	free text (e.g., "Server 1")
<b>Description</b>	This is an optional free text field to help you differentiate one device server from another. It does not affect operation of the NPort device server.

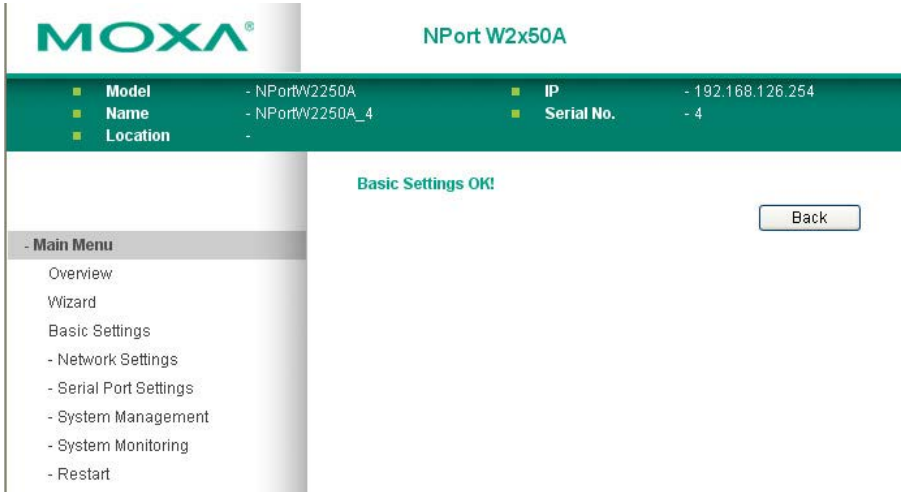
## Server Location

<b>Default</b>	
<b>Options</b>	free text (e.g., "Bldg 1, 2nd Floor")
<b>Description</b>	This is an optional free text field to help you differentiate one device server from another. It does not affect operation of the NPort device server.

## Time Zone

<b>Default</b>	(GMT)Greenwich Mean Time
<b>Options</b>	(GMT)Greenwich Mean Time (GMT-01:00)Azores, Cape Verde Is. (GMT-02:00)Mid-Atlantic etc.
<b>Description</b>	This field shows the currently selected time zone and allows you to select a different time zone.

**Local Time**

<b>Default</b>	
<b>Options</b>	Date (yy:mm:dd), Time (hh:mm:ss)
<b>Description</b>	<p>The NPort has a built-in real-time clock that allows you to add time information to functions such as the automatic warning e-mail or SNMP trap. This field shows the current time according to the NPort's built-in real-time clock. This is not a live field, so you will need to refresh the browser to get an updated reading.</p> <p>Change the correct date or time, and click <b>[Submit]</b>. The change will take effect directly, and shows <b>Basic Setting OK!</b>.</p>  <p>The screenshot shows the Moxa NPort W2x50A web console interface. At the top, there is a green header with the Moxa logo and the device name 'NPort W2x50A'. Below this is a green status bar displaying system information: Model (NPortW2250A), Name (NPortW2250A_4), Location (-), IP (192.168.126.254), and Serial No. (4). A central message box displays 'Basic Settings OK!' with a 'Back' button. On the left side, there is a 'Main Menu' with the following items: Overview, Wizard, Basic Settings, - Network Settings, - Serial Port Settings, - System Management, - System Monitoring, and - Restart.</p>



**ATTENTION**

There is a risk of explosion if the real-time clock battery is replaced incorrectly!  
 The real time clock is powered by a lithium battery. We strongly recommend that you obtain assistance from a Moxa support engineer before replacing the battery. Please contact the Moxa RMA service team if you need to change the battery.

**Time Server**

<b>Default</b>	
<b>Options</b>	IP address or domain name (e.g., "192.168.1.1" or "time.nist.gov")
<b>Description</b>	<p>This optional field specifies your time server's IP address or domain name, if a time server is used in your network. The NPort supports SNTP (RFC-1769) for automatic time calibration. The device server will request time information from the specified time server every 10 minutes.</p>

# Web Console: Network Settings

---

The following topics are covered in this chapter:

- **Overview**

- **Network Settings**

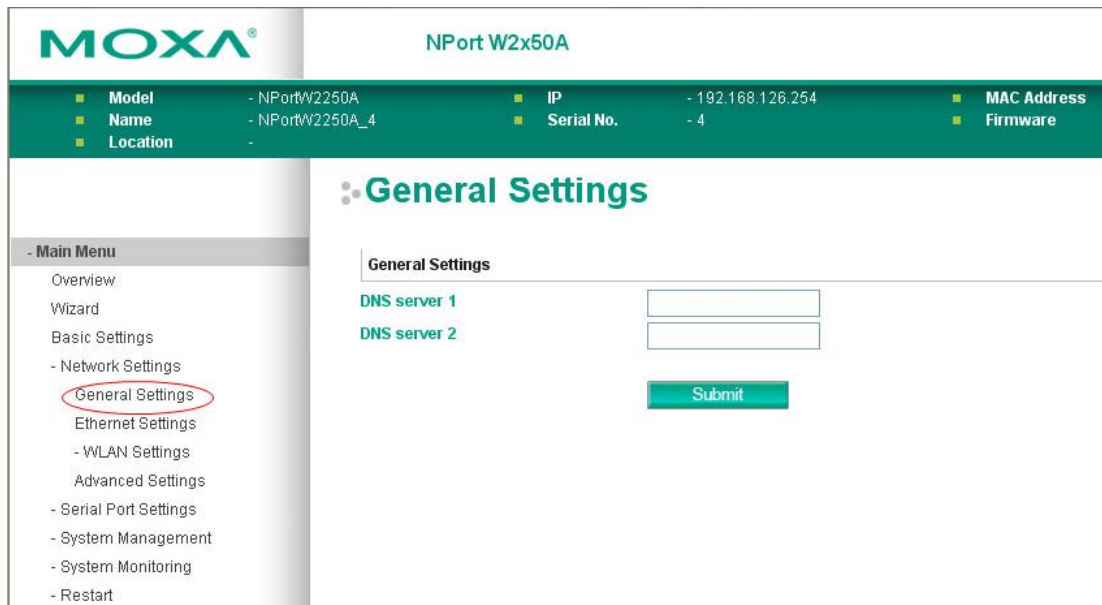
- General Settings
- Ethernet Settings
- WLAN Settings
- Advanced Settings

# Overview

This chapter explains how to configure all settings located under the **Network Settings** folder in the NPort web console.

## Network Settings

### General Settings



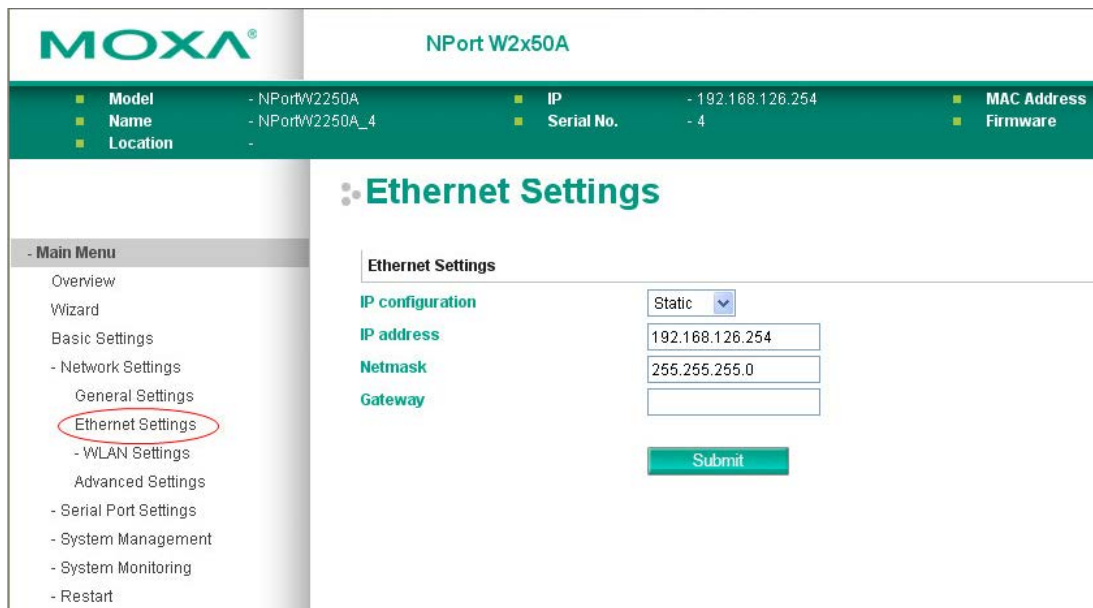
On the **General Settings** page in the **Network Settings** folder, you can modify **DNS server 1 and 2**.

#### DNS Server 1 and 2

<b>Default</b>	
<b>Options</b>	IP address (e.g., "192.168.1.1")
<b>Description</b>	<p>This field is for the DNS server's IP address, if applicable. With the DNS server configured, the NPort device server can use domain names instead of IP addresses to access hosts.</p> <p>Domain Name System (DNS) is how Internet domain names are identified and translated into IP addresses. A domain name is an alphanumeric name, such as www.moxa.com, that it is usually easier to remember than the numeric IP address. A DNS server is a host that translates a text-based domain name into an IP address in order to establish a TCP/IP connection. When the user wants to visit a particular website, the user's computer sends the domain name (e.g., www.moxa.com) to a DNS server to request that website's numeric IP address. When the IP address is received from the DNS server, the user's computer uses that information to connect to the website's web server.</p> <p>The NPort will play the role of a DNS client, actively querying the DNS server for the IP address associated with a particular domain name.</p>



# Ethernet Settings



On the **Ethernet Settings** page in the **Network Settings** folder, you can modify **IP configuration**, **IP address**, **Netmask**, and **Gateway**.

You must assign a valid IP address to the NPort before it will work in your network environment. Your network system administrator should provide you with an IP address and related settings for your network. The IP address must be unique within the network; otherwise the NPort will not have a valid connection to the network. First-time users should refer to Chapter 3, "Initial IP Address Configuration," for more information.

## IP Configuration

<b>Default</b>	Static
<b>Options</b>	Static, DHCP, DHCP/BOOTP, BOOTP
<b>Description</b>	This field determines how the NPort's IP address will be assigned. Static: IP address, netmask, and gateway are user-defined. DHCP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. DHCP/BOOTP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. IP address is assigned by BOOTP server if DHCP server does not respond. BOOTP: IP address is assigned by BOOTP server.

## IP Address

<b>Default</b>	192.168.126.254
<b>Options</b>	IP address (e.g., "192.168.1.1")
<b>Description</b>	This field is for the IP address that will be assigned to your NPort device server. An IP address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IP address to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your network environment. If your device server will be assigned a dynamic IP address, set the "IP configuration" parameter appropriately.

**Netmask**

<b>Default</b>	255.255.255.0
<b>Options</b>	Netmask setting (e.g., "255.255.0.0")
<b>Description</b>	This field is for the subnet mask. A subnet mask represents all of the network hosts at one geographic location, in one building, or on the same local area network. When a packet is sent out over the network, the NPort device server will use the subnet mask to check whether the desired TCP/IP host specified in the packet is on the local network segment. If the address is on the same network segment as the device server, a connection is established directly from the device server. Otherwise, the connection is established through the gateway as specified in the "Gateway" parameter.

**Gateway**

<b>Default</b>	
<b>Options</b>	IP address (e.g., "192.168.1.1")
<b>Description</b>	This field is for the IP address of the gateway, if applicable. A gateway is a network computer that acts as an entrance to another network. Usually, the computers that control traffic within the network or at the local Internet service provider are gateway nodes. The NPort device server needs to know the IP address of the default gateway computer in order to communicate with the hosts outside the local network environment. Consult your network administrator if you do not know how to set this parameter.



**ATTENTION**

In dynamic IP environments, the NPort will send 3 requests every 30 seconds to the DHCP or BOOTP server until the network settings have successfully been assigned. The first request will time out after one second; the second request will time out after three seconds, and the third request will timeout after five second. If the DHCP or BOOTP server is unavailable, the NPort will use the factory default network settings.

**WLAN Settings**

**WLAN**

The screenshot shows the MOXA NPort W2x50A web console. At the top, the MOXA logo and device model 'NPort W2x50A' are visible. A green status bar displays system information: Model (NPortW2250A), Name (NPortW2250A\_4), Location (-), IP (192.168.126.254), Serial No. (- 4), MAC Address, and Firmware. The left navigation menu includes 'Main Menu', 'Overview', 'Wizard', 'Basic Settings', 'Network Settings', 'WLAN Settings' (with 'WLAN Profile' circled), 'Advanced Settings', 'Serial Port Settings', 'System Management', 'System Monitoring', and 'Restart'. The main content area is titled 'WLAN Settings' and contains a 'WLAN Settings' section with a 'Static' IP configuration dropdown. Below this, there are input fields for 'IP address' (192.168.127.254), 'Netmask' (255.255.255.0), and 'Gateway'. A green 'Submit' button is located at the bottom of the configuration area.

The **WLAN** page is located under **WLAN Settings** in the **Network Settings** folder. You can modify **IP configuration**, **IP address**, **Netmask**, and **Gateway** for your WLAN.

The NPort W2150A/W2250A Series supports IEEE 802.11a/b/g wireless network interfaces. The supported IP configurations are static and dynamic (BOOTP, DHCP, or BOOTP+DHCP). Users can set up the IP configuration with the serial console, or the Web/Telnet consoles through the NPort's Ethernet interface. For detailed information about configuring **IP configuration**, **IP address**, **Netmask**, and **Gateway**, see the previous section, Ethernet Configuration.

### IP Configuration

<b>Default</b>	Static
<b>Options</b>	Static, DHCP, DHCP/BOOTP, BOOTP
<b>Description</b>	This field determines how the NPort's IP address will be assigned. Static: IP address, netmask, and gateway are user-defined. DHCP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. DHCP/BOOTP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. IP address is assigned by BOOTP server if DHCP server does not respond. BOOTP: IP address is assigned by BOOTP server.

### IP Address

<b>Default</b>	192.168.127.254
<b>Options</b>	IP address (e.g., "192.168.1.1")
<b>Description</b>	This field is for the IP address that will be assigned to your NPort device server. An IP address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IP address to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your WLAN environment. If your device server will be assigned a dynamic IP address, set the "IP configuration" parameter appropriately.

### Netmask

<b>Default</b>	255.255.255.0
<b>Options</b>	Netmask setting (e.g., "255.255.0.0")
<b>Description</b>	This field is for the subnet mask. A subnet mask represents all of the network hosts at one geographic location, in one building, or on the same local area network. When a packet is sent out over the network, the NPort device server will use the subnet mask to check whether the desired TCP/IP host specified in the packet is on the local network segment. If the address is on the same network segment as the device server, a connection is established directly from the device server. Otherwise, the connection is established through the gateway as specified in the "Gateway" parameter.

### Gateway

<b>Default</b>	
<b>Options</b>	IP address (e.g., "192.168.1.1")
<b>Description</b>	This field is for the IP address of the gateway, if applicable. A gateway is a network computer that acts as an entrance to another network. Usually, the computers that control traffic within the network or at the local Internet service provider are gateway nodes. The NPort device server needs to know the IP address of the default gateway computer in order to communicate with the hosts outside the local network environment. Consult your network administrator if you do not know how to set this parameter.

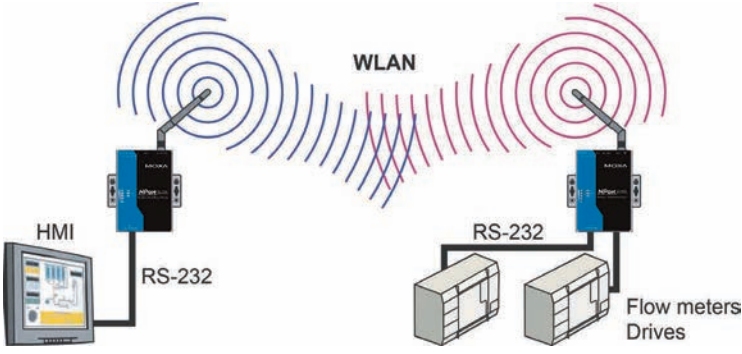
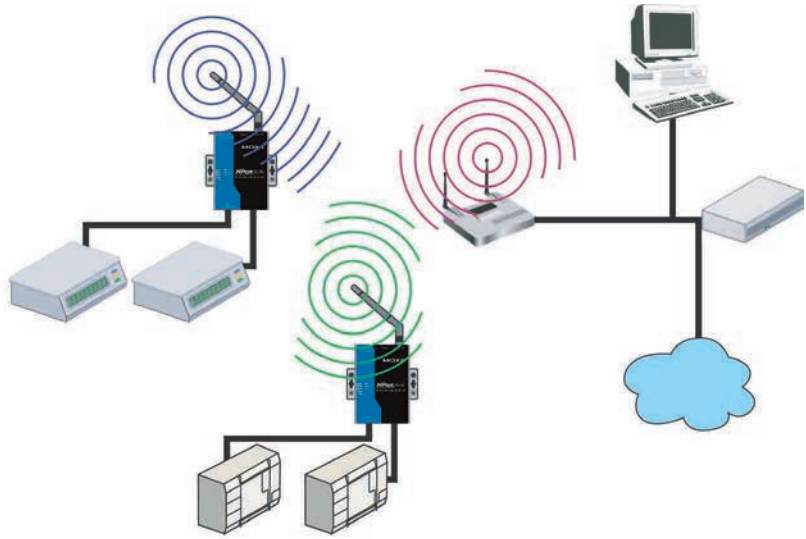
## Profile

The screenshot shows the MOXA NPort W2x50A web console interface. At the top, there is a header with the MOXA logo and the device model. Below the header is a status bar displaying system information: Model (NPortW2250A), Name (NPortW2250A\_4), Location (-), IP (192.168.126.254), Serial No. (- 4), MAC Address, and Firmware. A main menu is visible on the left side, with 'WLAN Profile' highlighted. The main content area is titled 'Wireless LAN Profile Settings'. It includes a 'Wireless LAN Profile' section with a 'Network type' dropdown menu set to 'Infrastructure Mode'. Below this, there is a 'Profile name' field and two buttons: 'General' and 'Security'. At the bottom of this section are 'Submit' and 'Activate' buttons. A note below the buttons reads: 'Please remember to activate Profile service by pressing "Activate" button after configuring.'

The screenshot shows the MOXA NPort W2x50A web console interface, specifically the 'WLAN Profile Properties' page. The header and status bar are identical to the previous screenshot. The main menu on the left shows 'WLAN Profile' selected. The main content area is titled 'WLAN Profile Properties' and contains a 'General Properties' section. This section includes fields for 'Profile name' (Infrastructure), 'Operation mode' (Auto), 'SSID' (profile1), 'Fast roaming' (Disable), and three 'Scan channels' (1, 2, and 3), each set to 'N/A'. A 'Submit' button is located at the bottom of the form.

The **Profile** page is located under **WLAN Settings** in the **Network Settings** folder. This is where you configure the NPort for Ad-hoc or Infrastructure operation. Different settings are available depending on whether you select Ad-hoc Mode or Infrastructure Mode.

**Network Type**

<b>Default</b>	Infrastructure Mode
<b>Options</b>	Infrastructure Mode, Ad-hoc Mode
<b>Description</b>	<p>This field specifies whether the NPort will operate in Ad-hoc or Infrastructure Mode. For all wireless networking devices, there are two possible modes for communication with another wireless device. Devices that are configured for Ad-hoc Mode automatically detect and communicate directly with each other and do not require a wireless access point (AP) or gateway. Wireless devices that are configured for Infrastructure Mode do not communicate directly with each other, but through a wireless access point (AP).</p> <p>Devices must be configured for the same mode in order to communicate with each other. Devices in Ad-Hoc Mode will only recognize other devices in Ad-Hoc Mode, and likewise for devices in Infrastructure Mode.</p> <p>Example of Ad-Hoc Mode</p>  <p>Example of Infrastructure Mode</p>  <p>After setting the Network type, you will need to adjust the General and Security settings for the profile. In Ad-hoc Mode, only one profile is available. In Infrastructure Mode, three profiles can be defined.</p>

## General Settings for WLAN Profile

The **General** page is opened through the **Profile** page, under **WLAN Settings** in the **Network Settings** folder. You can type a profile name to help you differentiate one profile from another. It does not affect operation of the NPort. After selecting Ad-hoc or Infrastructure Mode, click **[General]** to open the General page for the selected profile. In Ad-hoc Mode and Infrastructure Mode, only one profile is available.

**In Ad-hoc Mode**

The image shows two screenshots of the Moxa NPort W2x50A web console interface. The top screenshot is titled "Wireless LAN Profile Settings" and shows the "General" tab selected. The "Network type" is set to "Ad-hoc Mode" and the "Profile name" is "Adhoc". A red circle highlights the "General" tab, and a red arrow points down to the second screenshot. The second screenshot is titled "WLAN Profile Properties" and shows the "General Properties" tab. The "Profile name" is "Adhoc", "Operation mode" is "802.11b/g", "SSID" is empty, and "Channel" is "1".

**MOXA® NPort W2x50A**

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

### Wireless LAN Profile Settings

Wireless LAN Profile

Network type: Ad-hoc Mode

Profile name: Adhoc

General Security

Submit Activate

Please remember to activate Profile service by pressing "Activate" button after configuring.

---

**MOXA® NPort W2x50A**

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

### WLAN Profile Properties

General Properties

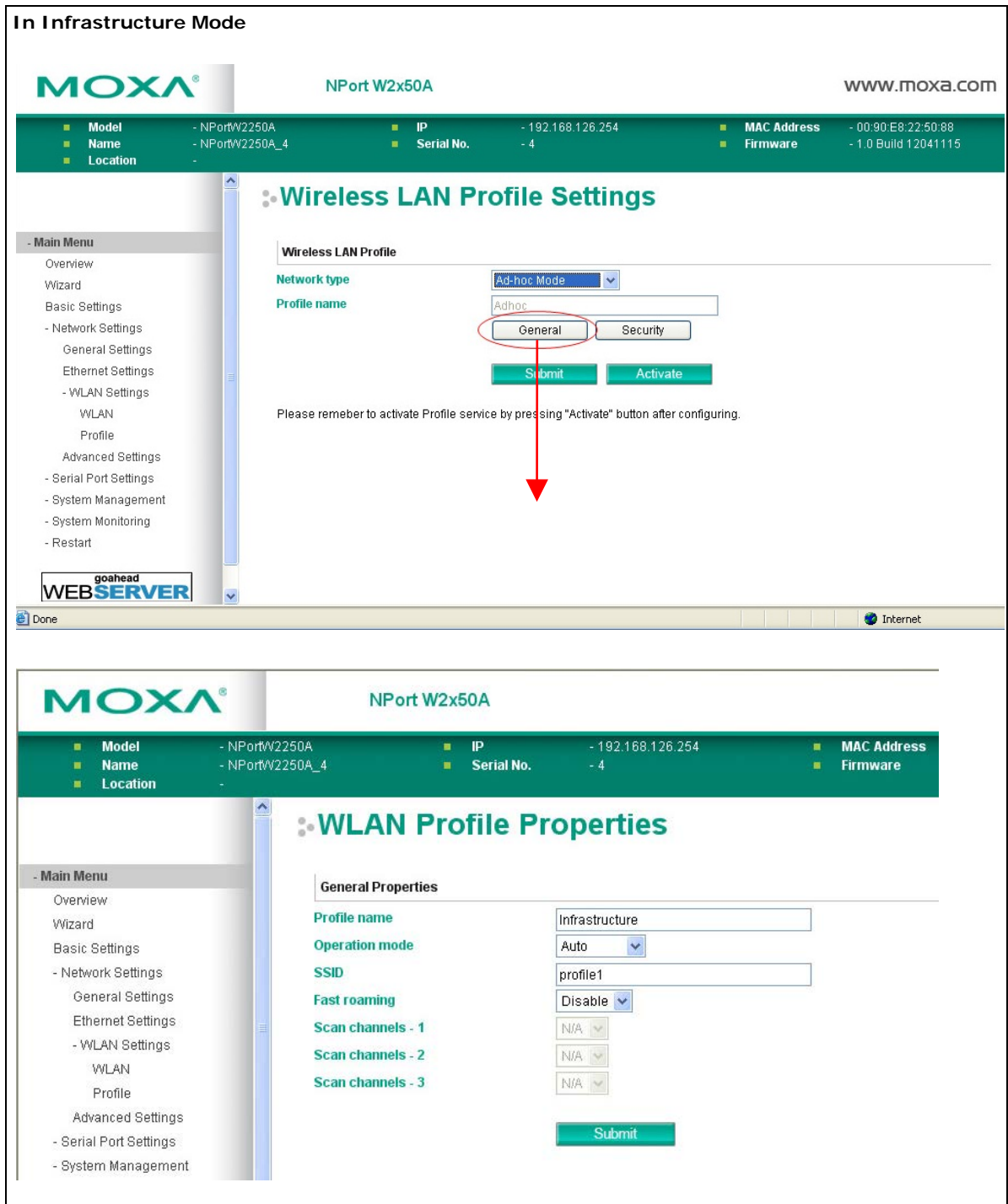
Profile name: Adhoc

Operation mode: 802.11b/g

SSID:

Channel: 1

Submit



On the General page, you can configure **Profile name**, **Operation mode**, and **SSID**. Additional settings are also available depending on whether you select Ad-hoc Mode or Infrastructure Mode.

**Profile Name**

<b>Default</b>	Ad-hoc (in Ad-hoc Mode) Infrastructure (in Infrastructure Mode)
<b>Options</b>	free text (e.g., "Primary Connection")
<b>Description</b>	This is a free text field to help you differentiate one profile from another. It does not affect operation of the NPort.

**Operation Mode**

<b>Default</b>	802.11b/g for Ad-Hoc Mode. Auto, 802.11b/g, and 802.11a for Infrastructure Mode.
<b>Options</b>	Auto, 802.11a, 802.11b/g
<b>Description</b>	<p>This field determines which wireless standard will be used by the selected profile. 802.11a, 802.11b, and 802.11g are supported.</p> <p>Auto: In Ad-hoc Mode, the NPort will scan the 2.4G wireless band and will automatically select the appropriate wireless standard for communication with any other wireless devices that are detected. In Infrastructure Mode, the NPort will automatically select between 802.11a, 802.11b and 802.11g according to the settings of the AP.</p> <p>802.11a: This setting is only available in Infrastructure Mode. The Unlicensed National Information Infrastructure (UNII) 5 GHz band is used for communication, which is different from the RF band used by 802.11b and 802.11g. Consequently, 802.11a devices will not be able to communicate with 802.11b or 802.11g devices. (Multi-mode 802.11a/b/g APs or client adapters can be used to resolve this.) Transmission rates up to 54Mbps are supported.</p> <p>802.11b/g: This option means our device will support for 802.11b or 802.11g.</p> <p>802.11b: This is the well-known "Wi-Fi" standard, also referred to as "802.11 High-Rate (HR)". Wireless communication is in the 2.4 GHz ISM band, using the DSSS spread spectrum transmission scheme. 802.11b supports data rates of 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps.</p> <p>802.11g: This is currently the most widely used standard for wireless LANS and is sometimes referred to as "54g™". Communication is in the 2.4 GHz ISM band and uses Orthogonal Frequency Division Multiplexing (OFDM). Data rates up to 54 Mbps are supported.</p>

**SSID**

<b>Default</b>	Default
<b>Options</b>	free text (e.g., "Coffeeshop WLAN")
<b>Description</b>	This field specifies the SSID, or name, of the wireless network (SSID) that will be used by the NPort. Wireless devices must use the same SSID in order to communicate with each other.

**Channel (Ad-hoc mode only)**

<b>Default</b>	1
<b>Options</b>	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
<b>Description</b>	This field is for Ad-Hoc Mode only and specifies the radio channel to use for the wireless network.



**Fast Roaming (Infrastructure mode only)**

<b>Default</b>	Disable
<b>Options</b>	Disable, Enable
<b>Description</b>	<p>This field is only available in Infrastructure Mode and is used to specify the W2150A/W2250A roaming behavior. Roaming is the ability to connect to different APs so wireless communication is not confined to one area or one particular AP. The W2150A/W2250A will only roam between APs, as specified by the SSID.</p> <p>Disable: Fast Roaming function will be disabled.</p> <p>W2150A/W2250A will scan all available channels and roam between APs as specified by the SSID. It scans the channel when booting up and will associate with the highest signal strength AP. Only when the associated AP is loses, then it will re-associate again.</p> <p>Enable: Fast Roaming function will be enabled.</p> <p>NPort W2150A/W2250A will only scan the pre-defined "<b>Scan Channels - 1, Scan Channels - 2 &amp; Scan Channels - 3</b>" and roam between APs as specified by the SSID.</p> <p>It scans the channel and will associate with the highest signal strength AP. It also scans the channel regularly and will re-associate with the highest signal strength AP (if there is) by automatically.</p>

**Scan channels – 1, Scan channels – 2, Scan channels – 3 (Infrastructure mode only)**

<b>Default</b>	N/A
<b>Options</b>	1 through 14, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161
<b>Description</b>	This field is for fast roaming under Infrastructure Mode and specifies the radio channel to use for the wireless network. Choose the channel according to the factory setting of AP.

**Security Settings for WLAN Profile**

The **Security** page is opened through the **Profile** page, under **WLAN Settings** in the **Network Settings** folder. After selecting Ad-hoc or Infrastructure Mode, click **[Security]** to open the Security page for the selected profile. In Ad-hoc Mode, only one profile is available, whereas three profiles are available in Infrastructure Mode.

In Ad-hoc Mode

---

**MOXA®** NPort W2x50A

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

---

**Wireless LAN Profile Settings**

Wireless LAN Profile

Network type: Ad-hoc Mode

Profile name: Adhoc

General Security

Submit Activate

Please remember to activate Profile service by pressing "Activate" button after configuring.

---

**MOXA®** NPort W2x50A

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

---

**WLAN Profile Properties**

Security Properties

Profile name: Adhoc

Authentication: Open System

Encryption: Disable

Submit

**In Infrastructure Mode**

MOXA® NPort W2x50A

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

### Wireless LAN Profile Settings

Wireless LAN Profile

Network type: Infrastructure Mode

Profile name: Infrastructure

General Security

Submit Activate

Please remember to activate Profile service by pressing "Activate" button after configuring.

---

MOXA® NPort W2x50A

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

### WLAN Profile Properties

Security Properties

Profile name: Infrastructure

Authentication: Open System

Encryption: Disable

Submit

You will need to configure **Authentication** and **Encryption**. These settings must match the settings on the wireless device at the other end of the connection (such as the AP). Different settings and options are available depending on how **Authentication** and **Encryption** are configured.

## Authentication

<b>Default</b>	Open System
<b>Options</b>	Open System, Shared Key, WPA, WPA-PSK, WPA2, WPA2-PSK
<b>Description</b>	<p>This field specifies how wireless devices will be authenticated. Only authenticated devices will be allowed to communicate with the NPort. If a RADIUS server is used, this setting must match the setting on the RADIUS server.</p> <p>Open System: The NPort will simply announce a desire to associate with another station or access point. No authentication is required. For Ad-hoc Mode, this is the only option for authentication, since Ad-hoc Mode was designed for open communication.</p> <p>Shared Key: This option is only available in Infrastructure Mode. Authentication involves a more rigorous exchange of frames to ensure that the requesting station is authentic. WEP encryption is required.</p> <p>WPA: This is a managed authentication option that is only available in Infrastructure Mode. WPA was created by the Wi-Fi Alliance, the industry trade group that owns the Wi-Fi trademark and certifies devices with the Wi-Fi name. It is based on Draft 3 of the IEEE 802.11i standard. Each user uses a unique key for authentication, distributed from an IEEE 802.1X authentication server, also known as a RADIUS server. This option is also referred to as WPA Enterprise Mode, since it is intended to meet rigorous enterprise security requirements. Tunneled authentication is supported, depending on the EAP method selected.</p> <p>WPA-PSK: This is an unmanaged authentication option that is only available in Infrastructure Mode. Instead of a unique key for each user, a pre-shared key (PSK) is manually entered on the access point to generate an encryption key that is shared among all users. Consequently, this method does not scale well for enterprise. A PSK that uses a mix of letters, numbers and non-alphanumeric characters is recommended. This option is also referred to as WPA Personal Mode, since it is designed for the needs and capabilities of small home and office WLANs.</p> <p>WPA2: This is a managed authentication option that is only available in Infrastructure Mode. WPA2 implements the mandatory elements of 802.11i. Supported encryption algorithms include TKIP, Michael, and AES-based CCMP, which is considered fully secure. Since March 13, 2006, WPA2 has been mandatory for all Wi-Fi-certified devices. This option may also be referred to as WPA Enterprise Mode. Tunneled authentication is supported, depending on the EAP method selected.</p> <p>WPA2-PSK: This is an unmanaged authentication option that is only available in Infrastructure Mode. It employs WPA2 encryption algorithms but relies on a PSK for authentication. A PSK that uses a mix of letters, numbers and non-alphanumeric characters is recommended. This option can also be referred to as WPA Personal Mode.</p>

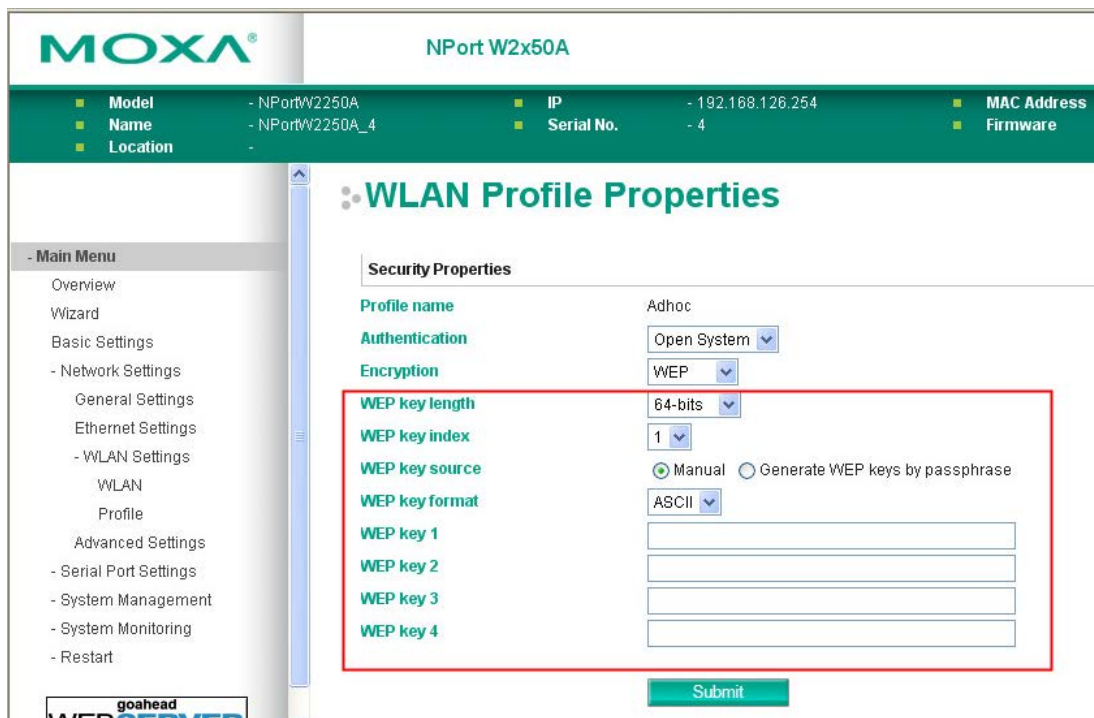
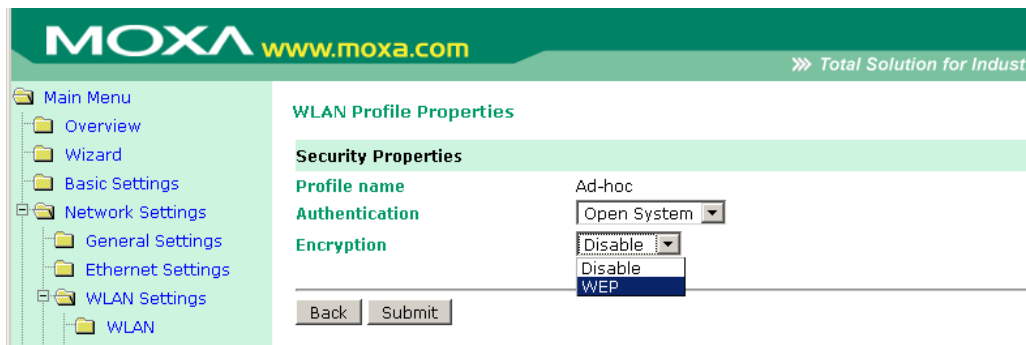
## Encryption

<b>Default</b>	Disable
<b>Options</b>	Disable, WEP, TKIP, AES-CCMP
<b>Description</b>	<p>This field specifies the type of encryption to use during wireless communication. Different encryption methods are available depending on the Authentication setting. Also, each encryption method has its own set of parameters that may also require configuration.</p> <p>Disable: No encryption is applied to the data during wireless communication. This option is only available if Authentication is set to Open System.</p> <p>WEP: Wired Equivalent Privacy (WEP) is only available for Open System and Shared Key authentication methods. Data is encrypted according to a key. The NPort supports both 64 and 128-bit keys. This method may deter casual snooping but is not considered very secure.</p> <p>TKIP: Temporal Key Integrity Protocol (TKIP) is only available for WPA, WPA2, WPA-PSK, and WPA2-PSK authentication methods. TKIP is part of a draft standard from the IEEE 802.11i working group and utilizes the RC4 stream cipher with 128-bit keys for encryption and 64-bit keys for authentication. TKIP improves on WEP by adding a per-packet key mixing function to de-correlate the public initialization vectors (IVs) from weak keys.</p> <p>AES-CCMP: This is a powerful encryption method that is only available for WPA, WPA2, WPA-PSK, and WPA2-PSK authentication methods. Advanced Encryption Standard (AES) is the block cipher system used by the Robust Secure Network (RSN) protocol and is equivalent to the RC4 algorithm used by WPA. CCMP is the security protocol used by AES, equivalent to TKIP for WPA. Data undergoes a Message Integrity Check (MIC) using a well-known and proven technique called Cipher Block Chaining Message Authentication Code (CBC-MAC). The technique ensures that even a one-bit alteration in a message produces a dramatically different result. Master keys are not used directly but are used to derive other keys, each of which expire after a certain amount of time. Messages are encrypted using a secret 128-bit key and a 128-bit block of data. The encryption process is complex, but the administrator does not need to be aware of the intricacies of the computations. The end result is encryption that is much harder to break than even WPA.</p>

## PSK Passphrase

<b>Default</b>	
<b>Options</b>	free text (e.g., "This is the WLAN passphrase")
<b>Description</b>	<p>This field is only available for WPA-PSK and WPA2-PSK authentication methods. If the NPort's passphrase does not match the AP's passphrase, the connection will be denied. A PSK of sufficient strength—one that uses a mix of letters, numbers and non-alphanumeric characters—is recommended.</p>

## Security Settings for WEP Encryption



When Encryption is set to WEP on the **Security** page for the WLAN profile, you will be able to configure **WEP key length**, **WEP key index**, and **WEP key source**. Other settings will be displayed depending on how **WEP key source** is configured.

### WEP Key Length

<b>Default</b>	64bits
<b>Options</b>	64bits, 128bits
<b>Description</b>	This field specifies the length of the WEP key. 64bits is the industry standard for WEP, but 128bits provides better protection.

### WEP Key Index

<b>Default</b>	1
<b>Options</b>	1 through 4
<b>Description</b>	This field specifies the primary WEP key to use for the WLAN.

**WEP Key Source**

<b>Default</b>	Manual
<b>Options</b>	Manual, Generate WEP keys by passphrase
<b>Description</b>	This field specifies whether the WEP key will be generated manually or through a user-specified passphrase. A passphrase is equivalent to a free-text password that will be used to generate the WEP key. A passphrase is typically easier to remember and enter than a long and complicated WEP key.

**WEP Passphrase**

<b>Default</b>	
<b>Options</b>	free text (e.g., "This is the WEP passphrase")
<b>Description</b>	This field is only available if WEP key source is set to "Generate WEP keys by passphrase". A standard hexadecimal password will be generated using the supplied passphrase. For example, if "404tech" is entered, the WEP key will be "DB971608E942FC39BD89FC4ADB".

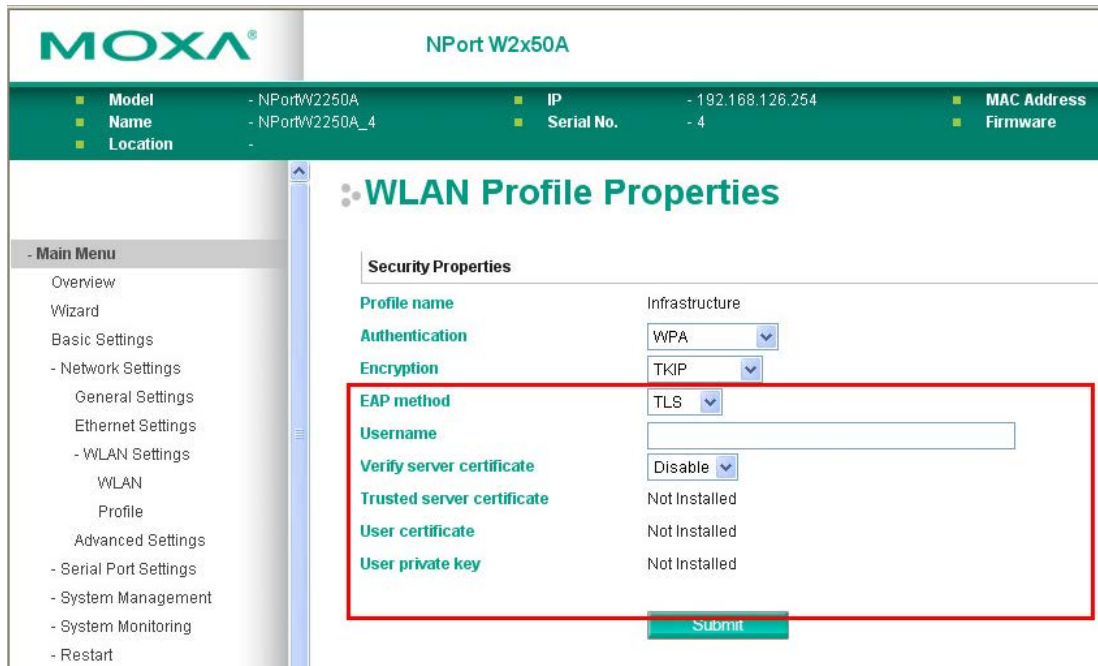
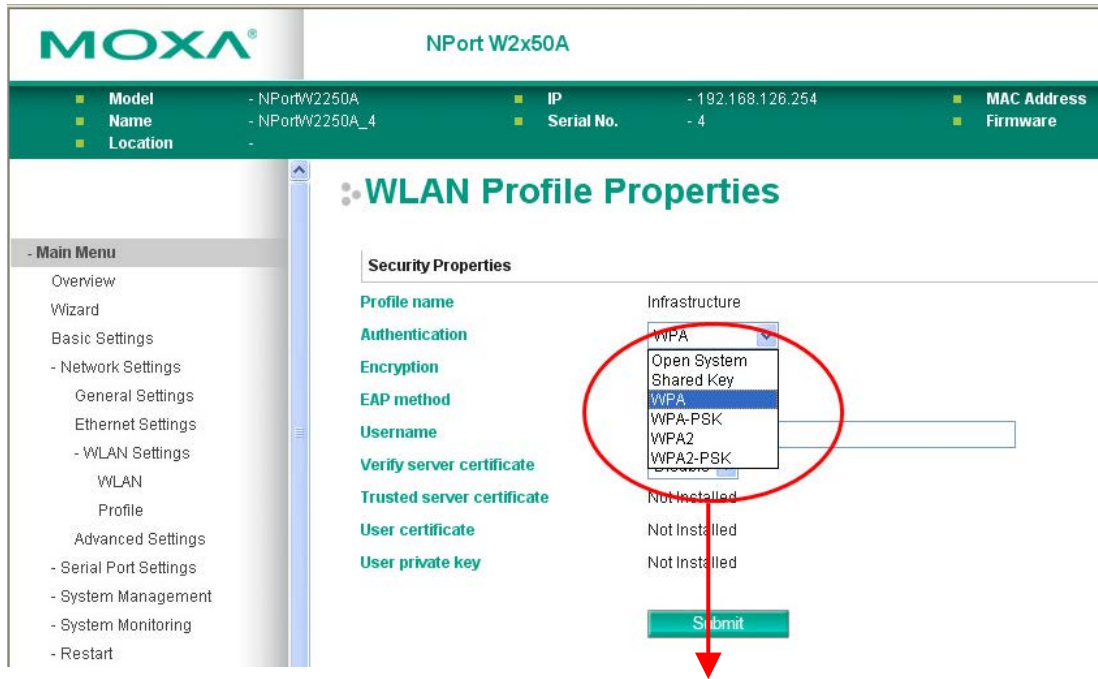
**WEP Key Format**

<b>Default</b>	ASCII
<b>Options</b>	ASCII, HEX
<b>Description</b>	This field is only available if WEP key source is set to "Manual". It specifies the format you will use to enter the WEP key.

**WEP Key 1 Through 4**

<b>Default</b>														
<b>Options</b>	free text in ASCII or HEX													
<b>Description</b>	<p>These fields are only available if WEP key source is set to "Manual". Enter each WEP key in ASCII or HEX as specified in WEP key format. The number of characters required for each key depends on WEP key length and WEP key format.</p> <table border="1"> <thead> <tr> <th>WEP Key Length</th> <th>WEP Key Format</th> <th>Key Length</th> </tr> </thead> <tbody> <tr> <td rowspan="2">64bits</td> <td>ASCII</td> <td>5 characters</td> </tr> <tr> <td>HEX</td> <td>10 characters</td> </tr> <tr> <td rowspan="2">128bits</td> <td>ASCII</td> <td>13 characters</td> </tr> <tr> <td>HEX</td> <td>26 characters</td> </tr> </tbody> </table>	WEP Key Length	WEP Key Format	Key Length	64bits	ASCII	5 characters	HEX	10 characters	128bits	ASCII	13 characters	HEX	26 characters
WEP Key Length	WEP Key Format	Key Length												
64bits	ASCII	5 characters												
	HEX	10 characters												
128bits	ASCII	13 characters												
	HEX	26 characters												

### Security Settings for WPA, WPA2

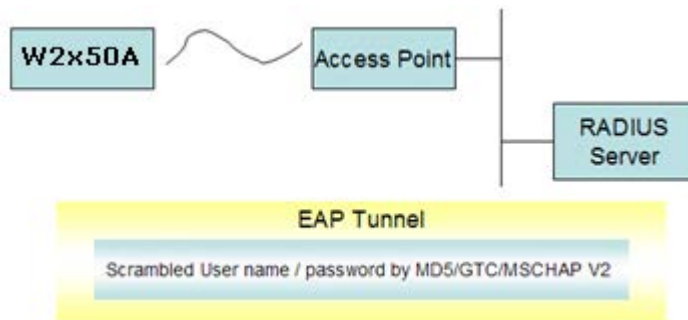


When WPA or WPA2 is used for authentication, you will also need to configure **EAP method** in the **Security** settings for the WLAN profile. Other settings will also be displayed depending on how **EAP method** is configured.



There are two parts to WPA and WPA2 security, authentication and data encryption.

- Authentication occurs before access is granted to a WLAN. Wireless clients such as the NPort W2150A/W2250A Series are first authenticated by the AP according to the authentication protocol used by the RADIUS server. Depending on the WLAN security settings, an EAP tunnel can be used to scramble the username and password that is submitted for authentication purposes.



- Encryption occurs after WLAN access has been granted. For all wireless devices, data is first encrypted before wireless transmission, using mutually agreed-upon encryption protocol.

**EAP Method**

<b>Default</b>	PEAP
<b>Options</b>	TLS, PEAP, TTLS, LEAP
<b>Description</b>	<p>This field specifies the EAP method to use for authentication. Four methods are supported.</p> <p>TLS: Transport Layer Security (TLS) was created by Microsoft and accepted by the IETF as RFC 2716: PPP EAP TLS Authentication Protocol. Passwords and tunneled authentication are not used. A user certificate and user private key are used to identify the NPort. The NPort's user certificate and user private key must already be installed on the RADIUS server.</p> <p>PEAP: Protected Extensible Authentication Protocol (PEAP) is a proprietary protocol which was developed by Microsoft, Cisco and RSA Security.</p> <p>TTLS: Tunneled Transport Layer Security (TTLS) is a proprietary protocol which was developed by Funk Software and Certicom, and is supported by Agere Systems, Proxim, and Avaya. TTLS is being considered by the IETF as a new standard. For more information on TTLS, read the draft RFC EAP Tunneled TLS Authentication Protocol.</p> <p>LEAP: Lightweight Extensible Authentication Protocol (LEAP) is a proprietary protocol which was developed by Cisco. LEAP doesn't check certificate during the authentication process.</p>

**Tunneled Authentication**

<b>Default</b>	PAP (when using TTLS) GTC (when using PEAP)
<b>Options</b>	GTC, MD5, MSCHAP V2 (when using PEAP) PAP, CHAP, MSCHAP, MSCHAP V2, EAP-MSCHAP V2, EAP-GTC, EAP-MD5 (when using TTLS)
<b>Description</b>	This field specifies the encryption method to use during the authentication process. Different methods are available depending on the EAP Method setting.

**Username**

<b>Default</b>	
<b>Options</b>	free text (e.g., "Smith_John")
<b>Description</b>	This field specifies the username that will be used to gain access to the WLAN. The correct username and password must be provided for access to be granted.

**Password**

<b>Default</b>	
<b>Options</b>	free text (e.g., "Password123")
<b>Description</b>	This field specifies the password that will be used to gain access to the WLAN. The correct username and password must be provided for access to be granted.

**Anonymous Username**

<b>Default</b>	
<b>Options</b>	free text (e.g., "Anyuser")
<b>Description</b>	This field specifies the anonymous username to use when initiating authentication. After the RADIUS Server has been verified by certificate, the true username and password will be used to complete the authentication process.

**Verify Server Certificate**

<b>Default</b>	Disable
<b>Options</b>	Disable, Enable
<b>Description</b>	<p>Disable: The certificate from the RADIUS server will be ignored.</p> <p>Enable: The certificate from the RADIUS server will be used to authenticate access to the WLAN. The RADIUS server's trusted server certificate must already be installed on the NPort. To install a trusted server certificate, visit the corresponding page in the <b>System Management &gt; Certificate</b> folder.</p>

**Trusted Server Certificate**

This field is available for PEAP, TLS, and TTLS EAP methods only. It displays information on the trusted server certificate that is installed on the NPort. To install a trusted server certificate, visit the corresponding page in the **System Management > Certificate** folder.

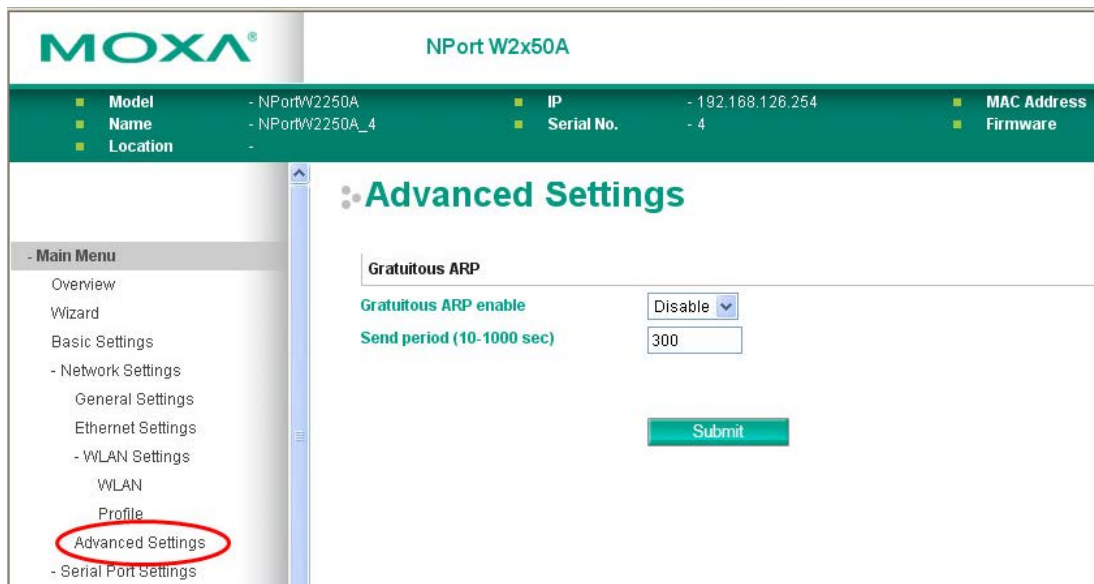
**User Certificate**

This field is available only when EAP method has been set to TLS. It displays information on the user certificate that is installed on the NPort. To install a user certificate, visit the corresponding page in the **System Management > Certificate** folder.

**User Private Key**

This field is available only when EAP method has been set to TLS. It displays information on the user private key on the NPort.

# Advanced Settings



On the **Advanced Settings** page in the **Network Settings** folder, you can modify **Gratuitous ARP**.

## Gratuitous ARP

<b>Default</b>	Disabled
<b>Options</b>	Disabled, Enabled, 10 to 1000 sec
<b>Description</b>	<p>This field specifies how often the NPort sends broadcast packets to update the ARP table. This may be required for certain applications.</p> <p>Disabled: The NPort will not send broadcast packets to update the ARP table.</p> <p>Enabled: The NPort will send periodically send broadcast packets at the time interval as specified by Send period.</p>

# Web Console: Serial Port Settings

---

The following topics are covered in this chapter:

▣ **Overview**

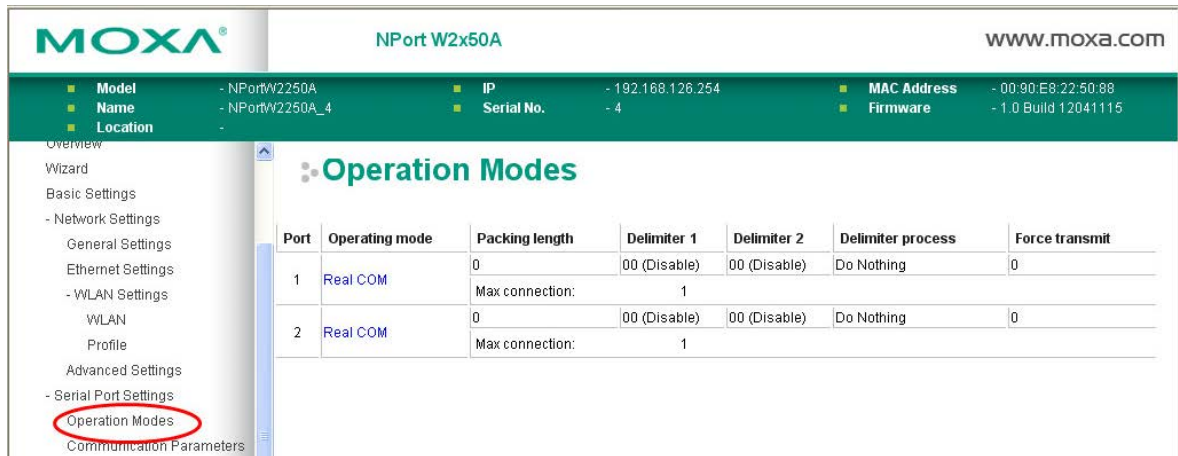
- Serial Port Settings
- Communication Parameters
- Data Buffering/Log

# Overview

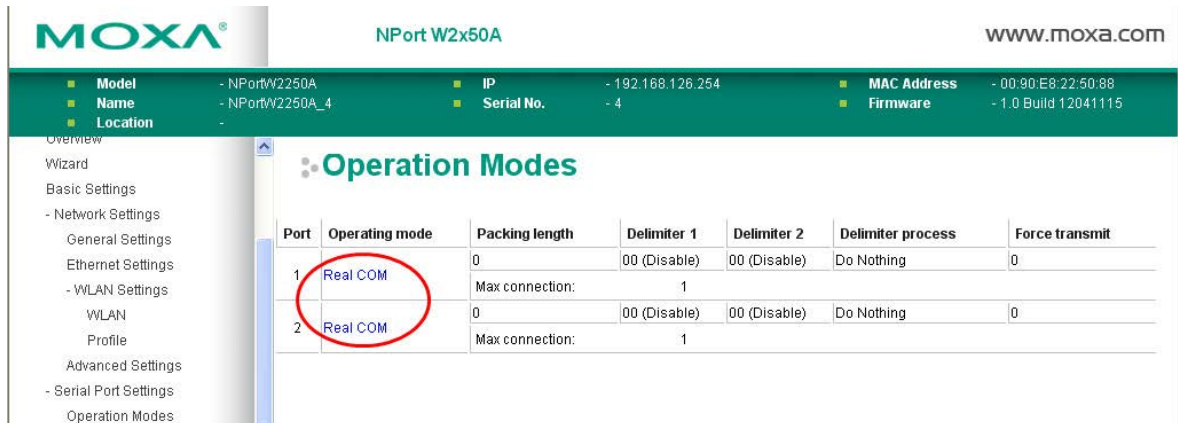
This chapter explains how to configure all settings located under the **Serial Port Settings** folder in the NPort web console.

## Serial Port Settings


### Operation Modes



Each serial port on the NPort is configured through the hyperlink below the column of **Operating mode**.



Click the link of **RealCOM**, it will show the Port settings page. The Operation Modes page for each serial port is where you configure the serial port's operation mode and related settings. For an introduction to the different operation modes, please refer to Chapter 4.



NPort W2x50A

■ <b>Model</b> - NPortW2250A	■ <b>IP</b> - 192.168.126.254	■ <b>MAC Address</b>
■ <b>Name</b> - NPortW2250A_4	■ <b>Serial No.</b> - 4	■ <b>Firmware</b>
■ <b>Location</b> -		

### Operation Modes

#### Port Settings

**Port** 1

**Operation mode** Real COM

**TCP alive check time**  (0 - 99 min)

**Max connection** 1

**Ignore jammed IP** Disable

**Allow driver control** Disable

**Connection goes down** RTS  always low  always high  
 DTR  always low  always high

---

#### Data Packing

**Packet length**  (0 - 1024)

**Delimiter 1**  (HEX)  Enable

**Delimiter 2**  (HEX)  Enable

**Delimiter process** Do Nothing (Processed only when Packing length is 0)

**Force transmit**  (0 - 65535 ms)

Apply the above settings to all serial ports

Submit

**goahead**  
**WEB SERVER**

Best viewed with IE 5 above at resolution 1024 x 768

### Operation Mode

<b>Default</b>	RealCOM
<b>Options</b>	RealCOM, RFC2217, TCP Server, TCP Client, UDP, Pair_Master, Pair_Slave, EModem
<b>Description</b>	<p>Along with Application, this field specifies the serial port's operation mode, or how it will interact with network devices. Depending on how Application is configured, different options are available for Mode. Depending on how Mode is configured, additional settings will be available for configuration. For an introduction to the different operation modes, please refer to Chapter 4.</p> <p><b>RealCOM:</b> This serial port will operate in RealCOM mode.</p> <p><b>RFC2217:</b> This serial port will operate in RFC2217 mode.</p> <p><b>TCP Server:</b> This serial port will operate in TCP Server mode.</p> <p><b>TCP Client:</b> This serial port will operate in TCP Client mode.</p> <p><b>UDP:</b> This serial port will operate in UDP mode.</p> <p><b>Pair_Master:</b> This serial port will operate in Pair Connection Master mode.</p> <p><b>Pair_Slave:</b> This serial port will operate in Pair Connection Slave mode.</p> <p><b>EModem:</b> This serial port will operate in Ethernet Modem mode.</p>

## Settings for RealCOM Mode

**MOXA** NPort W2x50A

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

**Operation Modes**

**Port Settings**

Port: 1

Operation mode: **Real COM**

TCP alive check time: 7 (0 - 99 min)

Max connection: 1

Ignore jammed IP: Disable

Allow driver control: Disable

Connection goes down: RTS  always low  always high  
DTR  always low  always high

**Data Packing**

Packet length: 0 (0 - 1024)

Delimiter 1: 00 (HEX)  Enable

Delimiter 2: 00 (HEX)  Enable

Delimiter process: Do Nothing (Processed only when Packing length is 0)

Force transmit: 0 (0 - 65535 ms)

Apply the above settings to all serial ports

Submit

When **Operation Mode** is set to RealCOM on a serial port's **Operation Modes** page, you will be able to configure additional settings including **TCP alive check time**, **Max connection**, **Ignore jammed IP**, **Allow driver Control**, **Connection goes down**, **Packet length**, **Delimiter 1**, **Delimiter 2**, **Delimiter process**, and **Force transmit**.

### TCP Alive Check Time

<b>Default</b>	7 min
<b>Options</b>	0 to 99 min
<b>Description</b>	<p>This field specifies how long the NPort will wait for a response to “keep alive” packets before closing the TCP connection. The NPort checks connection status by sending periodic “keep alive” packets.</p> <p>0: The TCP connection will remain open even if there is no response to the “keep alive” packets.</p> <p>1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.</p>

**Max connection**

<b>Default</b>	1
<b>Options</b>	1 to 8
<b>Description</b>	<p>This field specifies the maximum number of connections that will be accepted by the serial port.</p> <p>1: Only one specific host can access this serial port, and the RealCOM driver on that host will have full control over the port.</p> <p>2 to 8: This serial port will allow the specified number of connections to be opened simultaneously. With simultaneous connections, the RealCOM driver will only provide a pure data tunnel with no control ability. The serial communication will be determined by the NPort rather than by your application program. Application software that is based on the RealCOM driver will receive a driver response of "success" when using any of the Win32 API functions. The NPort will send data only to the RealCOM driver on the host. Data received from hosts will be sent to the attached serial device on a first-in-first-out basis.</p>

**ATTENTION**

When Max connection is 2 or greater, the serial port's communication settings (i.e., baudrate, parity, data bits, etc.) will be determined by the NPort. Any host that opens the COM port connection must use identical serial communication settings.

**Ignore jammed IP**

<b>Default</b>	Disable
<b>Options</b>	Disable, Enable
<b>Description</b>	<p>This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port.</p> <p>Disable: All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded.</p> <p>Enable: Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.</p>

**Allow driver control**

<b>Default</b>	Disable
<b>Options</b>	Disable, Enable
<b>Description</b>	<p>This field specifies how the port will proceed if driver control commands are received from multiple hosts that are connected to the port.</p> <p>Disable: Driver control commands will be ignored.</p> <p>Enable: Control commands will be accepted, with the most recent command received taking precedence.</p>



**Connection goes down**

<b>Default</b>	always high
<b>Options</b>	always low, always high
<b>Description</b>	<p>This field specifies what happens to the RTS and DTR signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent through the serial port.</p> <p>Always low: The selected signal will change to low when the Ethernet connection goes down.</p> <p>Always high The selected signal will remain high when the Ethernet connection goes down.</p>

**Packet length**

<b>Default</b>	0
<b>Options</b>	0 to 1024
<b>Description</b>	<p>This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending.</p> <p>0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full.</p> <p>1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.</p>

**Delimiter 1 and 2**

<b>Default</b>	Disabled
<b>Options</b>	Disabled, Enabled, 00 to FF
<b>Description</b>	<p>These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence.</p> <p>When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process.</p> <p>Delimiters must be incorporated into the data stream at the software or device level.</p>

**ATTENTION**

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

**Delimiter process**

<b>Default</b>	Do Nothing
<b>Options</b>	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
<b>Description</b>	<p>This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.</p> <p>Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters.</p> <p>Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed.</p> <p>Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed.</p> <p>Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.</p>

**Force transmit**

<b>Default</b>	0 ms
<b>Options</b>	0 to 65535
<b>Description</b>	<p>This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted.</p> <p>0: If serial data is not received, the NPort will wait indefinitely for additional data.</p> <p>1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.</p>

## Settings for RFC2217 Mode

The screenshot shows the MOXA NPort W2x50A web console interface. At the top, there is a header with the MOXA logo and the device name 'NPort W2x50A'. Below this is a green navigation bar with several menu items: Model, Name, Location, IP, Serial No., MAC Address, and Firmware. The main content area is titled 'Operation Modes' and contains a 'Port Settings' section. The 'Operation mode' dropdown menu is set to 'RFC2217' and is circled in red. Other settings in the 'Port Settings' section include 'TCP alive check time' (7 min), 'TCP port' (4001), 'Data Packing' section with 'Packet length' (0), 'Delimiter 1' (00), 'Delimiter 2' (00), and 'Delimiter process' (Do Nothing), and 'Force transmit' (0). A 'Submit' button is located at the bottom right of the settings area.

When **Operation Mode** is set to **RFC2217** on a serial port's **Operation Modes** page, you will be able to configure additional settings, including **TCP alive check time**, **TCP port**, **Packet length**, **Delimiter 1**, **Delimiter 2**, **Delimiter process**, and **Force transmit**.

### TCP alive check time

<b>Default</b>	7 min
<b>Options</b>	0 to 99 min
<b>Description</b>	<p>This field specifies how long the NPort will wait for a response to “keep alive” packets before closing the TCP connection. The NPort checks connection status by sending periodic “keep alive” packets.</p> <p>0: The TCP connection will remain open even if there is no response to the “keep alive” packets.</p> <p>1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.</p>

### TCP port

<b>Default</b>	4001
<b>Options</b>	
<b>Description</b>	This field specifies the TCP port number that the serial port will use to listen to connections, and that other devices must use to contact the serial port.

**Packet length**

<b>Default</b>	0
<b>Options</b>	0 to 1024
<b>Description</b>	<p>This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending.</p> <p>0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full.</p> <p>1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.</p>

**Delimiter 1 and 2**

<b>Default</b>	Disabled
<b>Options</b>	Disabled, Enabled, 00 to FF
<b>Description</b>	<p>These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence.</p> <p>When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process.</p> <p>Delimiters must be incorporated into the data stream at the software or device level.</p>

**Delimiter process**

<b>Default</b>	Do Nothing
<b>Options</b>	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
<b>Description</b>	<p>This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.</p> <p>Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters.</p> <p>Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed.</p> <p>Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed.</p> <p>Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.</p>

**Force transmit**

<b>Default</b>	0 ms
<b>Options</b>	0 to 65535
<b>Description</b>	<p>This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted.</p> <p>0: If serial data is not received, the NPort will wait indefinitely for additional data.</p> <p>1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.</p>

**Settings for TCP Server Mode**

The screenshot shows the MOXA NPort W2x50A Web Console interface. At the top, the device name 'NPort W2x50A' is displayed. Below it, a status bar shows system information: Model (NPortW2250A), Name (NPortW2250A\_4), Location (-), IP (192.168.126.254), Serial No. (- 4), MAC Address, and Firmware. The main navigation menu on the left includes 'Main Menu', 'Overview', 'Wizard', 'Basic Settings', 'Network Settings', 'Serial Port Settings', 'Operation Modes', 'Communication Parameters', 'Data Buffering/Log', 'System Management', 'System Monitoring', and 'Restart'. The 'Operation Modes' page is active, showing 'Port Settings' for port 1. The 'Operation mode' dropdown menu is set to 'TCP Server' and is circled in red. Other settings include 'TCP alive check time' (7 min), 'Inactivity time' (0 ms), 'Max connection' (1), 'Ignore jammed IP' (Disable), 'Allow driver control' (Disable), 'TCP port' (4001), 'Cmd port' (966), and 'Connection goes down' (RTS and DTR both set to 'always high'). The 'Data Packing' section includes 'Packet length' (0), 'Delimiter 1' (00), 'Delimiter 2' (00), 'Delimiter process' (Do Nothing), and 'Force transmit' (0). A 'Submit' button is at the bottom right.

When **Operation Mode** is set to **TCP Server** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, **Max connection**, **Ignore jammed IP**, **Allow driver control**, **TCP port**, **Cmd port**, **Connection goes down**, **Packet length**, **Delimiter 1**, **Delimiter 2**, **Delimiter process**, and **Force transmit**.

**TCP alive check time**

<b>Default</b>	7 min
<b>Options</b>	0 to 99 min
<b>Description</b>	<p>This field specifies how long the NPort will wait for a response to “keep alive” packets before closing the TCP connection. The NPort checks connection status by sending periodic “keep alive” packets.</p> <p>0: The TCP connection will remain open even if there is no response to the “keep alive” packets.</p> <p>1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.</p>

**Inactivity time**

<b>Default</b>	0 ms
<b>Options</b>	0 to 65535 ms
<b>Description</b>	<p>This field specifies the time limit for keeping the connection open if no data flows to or from the serial device.</p> <p>0: The connection will remain open even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting.</p> <p>1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, make sure that it is greater than the Force transmit time. Otherwise, the TCP connection may be closed before data in the buffer can be transmitted.</p>

**Max connection**

<b>Default</b>	1
<b>Options</b>	1 to 8
<b>Description</b>	<p>This field specifies the maximum number of connections that will be accepted by the serial port.</p> <p>1: Only one specific host can access this serial port, and the RealCOM driver on that host will have full control over the port.</p> <p>2 to 8: This serial port will allow the specified number of connections to be opened simultaneously. With simultaneous connections, the RealCOM driver will only provide a pure data tunnel with no control ability. The serial communication will be determined by the NPort rather than by your application program. Application software that is based on the RealCOM driver will receive a driver response of “success” when using any of the Win32 API functions. The NPort will send data only to the RealCOM driver on the host. Data received from hosts will be sent to the attached serial device on a first-in-first-out basis.</p>

**ATTENTION**

When Max connection is 2 or greater, the serial port’s communication settings (i.e., baudrate, parity, data bits, etc.) will be determined by the NPort. Any host that opens the COM port connection must use identical serial communication settings.

**Ignore jammed IP**

<b>Default</b>	Disable
<b>Options</b>	Disable, Enable
<b>Description</b>	<p>This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port.</p> <p>Disable: All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded.</p> <p>Enable: Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.</p>

**Allow driver control**

<b>Default</b>	Disable
<b>Options</b>	Disable, Enable
<b>Description</b>	<p>This field specifies how the port will proceed if driver control commands are received from multiple hosts that are connected to the port.</p> <p>Disable: Driver control commands will be ignored.</p> <p>Enable: Control commands will be accepted, with the most recent command received taking precedence.</p>

**TCP port**

<b>Default</b>	4001
<b>Options</b>	0 to 9999
<b>Description</b>	This field specifies the TCP port number that the serial port will use to listen to connections, and that other devices must use to contact the serial port.

**Cmd port**

<b>Default</b>	996
<b>Options</b>	
<b>Description</b>	This field specifies the TCP port number for listening to SSDK commands from the host.

The usage of other functions can be found in the subsection of **RealCOM** mode in page 7-4.

**Connection goes down**

<b>Default</b>	always high
<b>Options</b>	always low, always high
<b>Description</b>	<p>This field specifies what happens to the RTS and DTR signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent through the serial port.</p> <p>Always low: The selected signal will change to low when the Ethernet connection goes down.</p> <p>Always high: The selected signal will remain high when the Ethernet connection goes down.</p>

**Packet length**

<b>Default</b>	0
<b>Options</b>	0 to 1024
<b>Description</b>	<p>This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending.</p> <p>0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full.</p> <p>1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.</p>

**Delimiter 1 and 2**

<b>Default</b>	Disabled
<b>Options</b>	Disabled, Enabled, 00 to FF
<b>Description</b>	<p>These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence.</p> <p>When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process.</p> <p>Delimiters must be incorporated into the data stream at the software or device level.</p>

**ATTENTION**

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

**Delimiter process**

<b>Default</b>	Do Nothing
<b>Options</b>	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
<b>Description</b>	<p>This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.</p> <p>Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters.</p> <p>Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed.</p> <p>Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed.</p> <p>Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.</p>



**Force transmit**

<b>Default</b>	0 ms
<b>Options</b>	0 to 65535
<b>Description</b>	<p>This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted.</p> <p>0: If serial data is not received, the NPort will wait indefinitely for additional data.</p> <p>1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.</p>

**Settings for TCP Client Mode**

The screenshot shows the MOXA NPort W2x50A web console interface. At the top, the model is identified as NPortW2250A with IP 192.168.128.254 and MAC address 00:90:E8:22:50. The left sidebar contains a 'Main Menu' with options like Overview, Wizard, Basic Settings, Network Settings, Serial Port Settings, Operation Modes, Communication Parameters, Data Buffering/Log, System Management, System Monitoring, and Restart. The 'Serial Port Settings' page is active, showing 'Port Settings' for Port 1. The 'Operation mode' dropdown is highlighted with a red circle and set to 'TCP Client'. Below it, various settings are visible: 'TCP alive check time' (7 min), 'Inactivity time' (0 ms), 'Ignore jammed IP' (Disable), 'Destination address 1-4' (all 4001), 'Designated local port 1-4' (5010-5013), 'Connection control' (Startup/None), 'Data Packing' section with 'Packet length' (0), 'Delimiter 1-2' (00), 'Delimiter process' (Do Nothing), and 'Force transmit' (0). A 'Submit' button is located at the bottom of the settings area.

When **Operation Mode** is set to **TCP Client** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, **Ignore jammed IP**, **Destination address 1-4**, **Designated local port 1-4**, **Connection control**, and **Packet length**, **Delimiter 1**, **Delimiter 2**, **Delimiter process**, and **Force transmit**.

**TCP Alive Check Time**

<b>Default</b>	7 min
<b>Options</b>	0 to 99 min
<b>Description</b>	<p>This field specifies how long the NPort will wait for a response to “keep alive” packets before closing the TCP connection. The NPort checks connection status by sending periodic “keep alive” packets.</p> <p>0: The TCP connection will remain open even if there is no response to the “keep alive” packets.</p> <p>1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.</p>

**Inactivity time**

<b>Default</b>	0 ms
<b>Options</b>	0 to 65535 ms
<b>Description</b>	<p>This field specifies the time limit for keeping the connection open if no data flows to or from the serial device.</p> <p>0: The connection will remain open even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting.</p> <p>1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, make sure that it is greater than the Force transmit time. Otherwise, the TCP connection may be closed before data in the buffer can be transmitted.</p>

**Ignore jammed IP**

<b>Default</b>	Disable
<b>Options</b>	Disable, Enable
<b>Description</b>	<p>This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port.</p> <p>Disable: All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded.</p> <p>Enable: Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.</p>

**Destination address 1 to 4**

<b>Default</b>	
<b>Options</b>	IP address and port (e.g., “192.168.1.1” and “4001”)
<b>Description</b>	This field specifies the remote host(s) that will access the attached device. At least one destination must be provided. This field supports the use of domain names and names defined in the host table.

**ATTENTION**

In TCP Client mode, up to 4 connections can be established between the serial port and TCP hosts. The connection speed or throughput may be low if any one of the four connections is slow, since the one slow connection will slow down the other 3 connections.

**Designated local port 1 to 4**

<b>Default</b>	
<b>Options</b>	1 to 65535
<b>Description</b>	This field specifies the TCP port number that will be used for data transmission with the serial port.

**Connection control**

<b>Default</b>	Startup/None
<b>Options</b>	Startup/None, Any Character/None, Any Character/Inactivity Time, DSR On/DSR Off, DSR On/None, DCD On/DCD Off, DCD On/None
<b>Description</b>	<p>This field specifies how connections to the device are established and closed.</p> <p>Startup/None: The connection will be opened as the NPort starts up. The connection will only be closed manually.</p> <p>Any Character/None: The connection will be opened as soon as a character is received from the attached device. The connection will only be closed manually.</p> <p>Any Character/Inactivity Time: The connection will be opened as soon as a character is received from the attached device. The connection will be closed if no data is received for the time specified in Inactivity time.</p> <p>DSR On/DSR Off: The TCP connection is opened when the DSR signal is on, and closed when the DSR signal is off.</p> <p>DSR On/None: The TCP connection is opened when the DSR signal is on. The connection will only be closed manually.</p> <p>DCD On/DCD Off: The TCP connection is opened when the DCD signal is on, and closed when the DCD signal is off.</p> <p>DCD On/None: The TCP connection is opened when the DCD signal is on. The connection will only be closed manually.</p>

**Packet length**

<b>Default</b>	0
<b>Options</b>	0 to 1024
<b>Description</b>	<p>This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending.</p> <p>0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full.</p> <p>1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.</p>

**Delimiter 1 and 2**

<b>Default</b>	Disabled
<b>Options</b>	Disabled, Enabled, 00 to FF
<b>Description</b>	<p>These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence.</p> <p>When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process.</p> <p>Delimiters must be incorporated into the data stream at the software or device level.</p>

**ATTENTION**

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

**Delimiter process**

<b>Default</b>	Do Nothing
<b>Options</b>	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
<b>Description</b>	<p>This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.</p> <p>Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters.</p> <p>Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed.</p> <p>Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed.</p> <p>Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.</p>

**Force transmit**

<b>Default</b>	0 ms
<b>Options</b>	0 to 65535
<b>Description</b>	<p>This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted.</p> <p>0: If serial data is not received, the NPort will wait indefinitely for additional data.</p> <p>1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.</p>

## Settings for UDP Mode

The screenshot shows the Moxa NPort W2x50A Web Console interface. At the top, there is a header with the Moxa logo and the device model. Below the header is a navigation menu with options like Overview, Wizard, Basic Settings, Network Settings, Serial Port Settings, System Management, System Monitoring, and Restart. The main content area is titled 'Operation Modes' and contains a 'Port Settings' section for port 1. The 'Operation mode' dropdown menu is set to 'UDP' and is circled in red. Below this are fields for 'Destination address 1' through '4', each with 'Begin', 'End', and 'Port' sub-fields. The 'Local listen port' is set to 4001. There is also a 'Data Packing' section with fields for 'Packet length', 'Delimiter 1', 'Delimiter 2', 'Delimiter process', and 'Force transmit'.

When **Operation Mode** is set to **UDP** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **Destination address 1** through **4**, **Local listen port**, **Packet length**, **Delimiter 1**, **Delimiter 2**, **Delimiter process**, and **Force transmit**.

### Destination address 1 to 4

<b>Default</b>	
<b>Options</b>	IP address range and port (e.g., "192.168.1.1" to "192.168.1.64" and "4001")
<b>Description</b>	In UDP mode, you may specify up to 4 ranges of IP addresses for the serial port to connect to. At least one destination range must be provided.  The maximum selectable IP address range is 64 addresses. However, you can enter multicast addresses in the Begin field, in the form xxx.xxx.xxx.255. For example, enter "192.127.168.255" to allow the NPort to broadcast UDP packets to all hosts with IP addresses between 192.127.168.1 and 192.127.168.254.

### Local listen port

<b>Default</b>	4001
<b>Options</b>	
<b>Description</b>	This field specifies the UDP port that the NPort listens to and that other devices must use to contact the attached serial device.

### Packet length

<b>Default</b>	0
<b>Options</b>	0 to 1024
<b>Description</b>	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending.  0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full.  1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

**Delimiter 1 and 2**

<b>Default</b>	Disabled
<b>Options</b>	Disabled, Enabled, 00 to FF
<b>Description</b>	<p>These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence.</p> <p>When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process.</p> <p>Delimiters must be incorporated into the data stream at the software or device level.</p>

**ATTENTION**

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

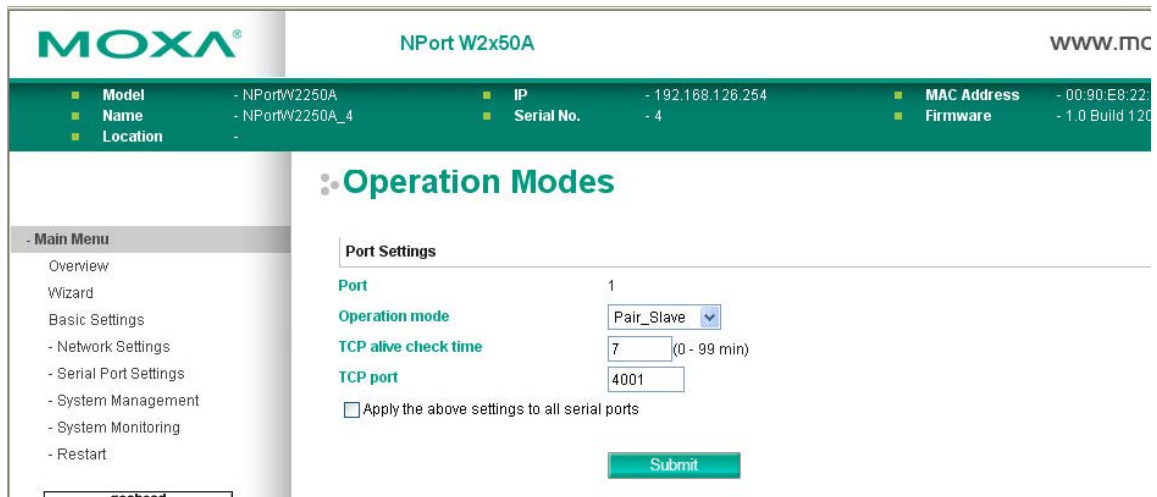
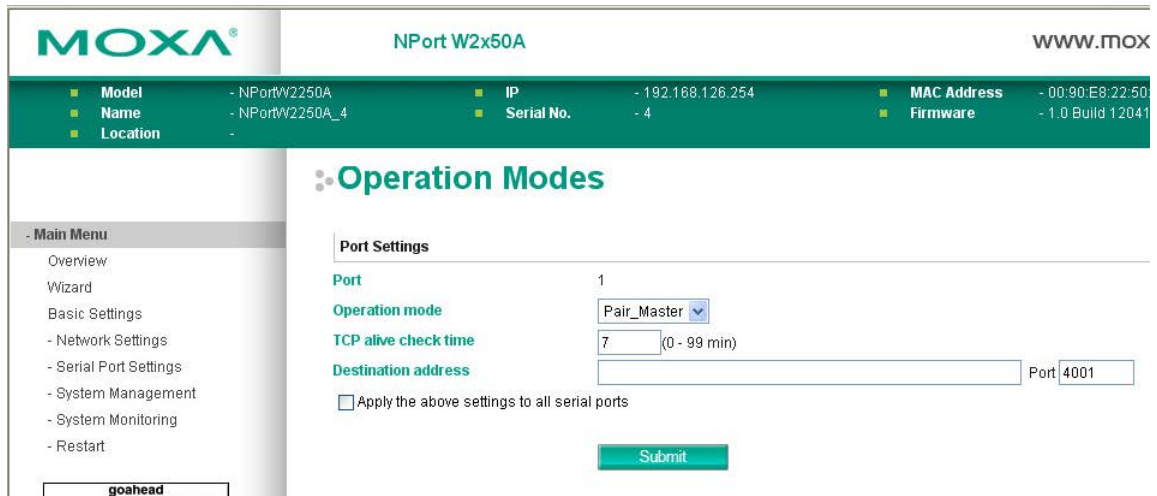
**Delimiter process**

<b>Default</b>	Do Nothing
<b>Options</b>	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
<b>Description</b>	<p>This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.</p> <p>Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters.</p> <p>Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed.</p> <p>Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed.</p> <p>Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.</p>

**Force transmit**

<b>Default</b>	0 ms
<b>Options</b>	0 to 65535
<b>Description</b>	<p>This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted.</p> <p>0: If serial data is not received, the NPort will wait indefinitely for additional data.</p> <p>1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.</p>

# Settings for Pair Connection Master Mode and Pair Connection Slave Mode



When **Operation Mode** is set to **Pair Connection Master** or **Pair Connection Slave** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Destination address** and **TCP port**. A Pair Connection application involves one serial port communicating over an IP network to another serial port as if the two serial ports were connected by a serial cable. Pair Connection modes can be used to extend RS-232 transmission to unlimited distances.

An NPort device server is needed at both ends of the connection. The serial port at one end must be set to Pair Connection Master mode, and the serial port at the other end must be set to Pair Connection Slave mode. It does not matter which serial port is master and which serial port is slave.

**TCP alive check time**

<b>Default</b>	7 min
<b>Options</b>	0 to 99 min
<b>Description</b>	<p>This field specifies how long the NPort will wait for a response to “keep alive” packets before closing the TCP connection. The NPort checks connection status by sending periodic “keep alive” packets.</p> <p>0: The TCP connection will remain open even if there is no response to the “keep alive” packets.</p> <p>1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.</p>

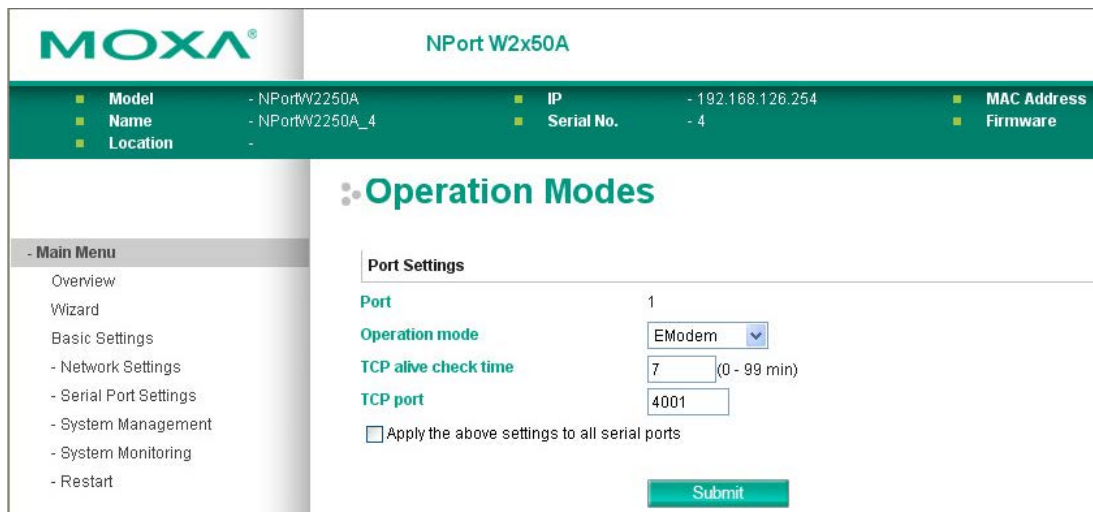
**Destination address**

<b>Default</b>	
<b>Options</b>	IP address and port (e.g., “192.168.1.1” and “4001”)
<b>Description</b>	This field specifies the IP address for the NPort at the opposite end of the Pair Connection, and the TCP port number for communication with the serial port. The port number must match with that serial port’s TCP port setting.

**TCP port**

<b>Default</b>	4001
<b>Options</b>	
<b>Description</b>	This field specifies the TCP port to use for communication with the attached serial device. The serial port at the opposite end of the Pair Connection must use this port number to establish the connection.

**Settings for Ethernet Modem Mode**



When **Application** is set to **Ethernet Modem Mode**, the NPort will accept AT commands such as “ATD 192.127.168.1:4001” from the serial port. A TCP connection will then be requested from the specified remote Ethernet Modem or PC. When the remote unit accepts this TCP connection, the NPort will return the “**CONNECT { baudrate}**” signal to the serial port and will then enter data mode. Please refer to Appendix C for details on Ethernet modem commands.



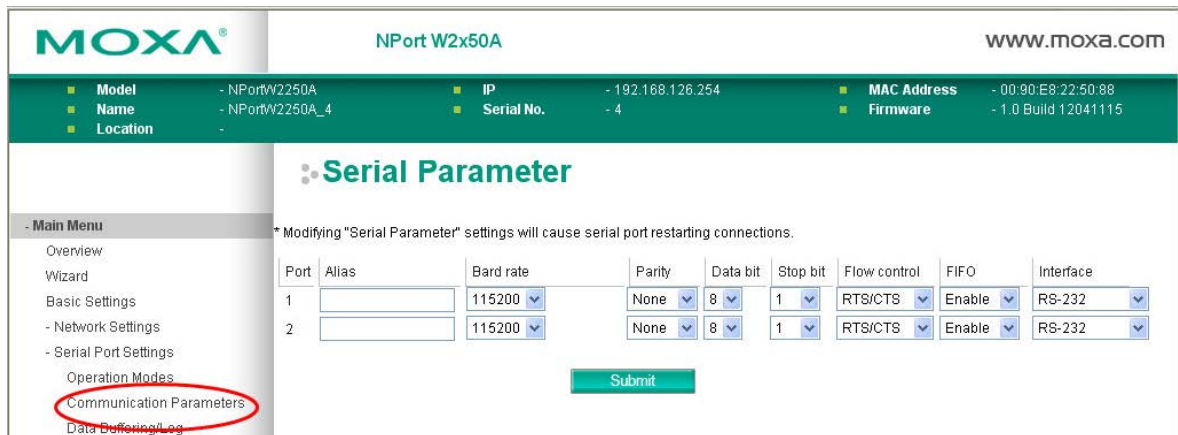
**TCP alive check time**

<b>Default</b>	7 min
<b>Options</b>	0 to 99 min
<b>Description</b>	<p>This field specifies how long the NPort will wait for a response to “keep alive” packets before closing the TCP connection. The NPort checks connection status by sending periodic “keep alive” packets.</p> <p>0: The TCP connection will remain open even if there is no response to the “keep alive” packets.</p> <p>1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.</p>

**TCP port**

<b>Default</b>	4001
<b>Options</b>	
<b>Description</b>	This field specifies the TCP port to use for communication with the attached serial device.

**Communication Parameters**



The **Communication Parameters** page for each serial port is where serial communication settings are specified, such as **Baud rate**, **Data bits**, and **Stop bits**.

**Alias**

<b>Default</b>	
<b>Options</b>	free text (e.g., “Secondary console connection”)
<b>Description</b>	This is an optional free text field to help you differentiate one serial port from another. It does not affect operation of the NPort device server.



**ATTENTION**

Serial communication settings should match the attached serial device. Check the communication settings in the user’s manual for your serial device.

**Baud rate**

<b>Default</b>	115200
<b>Options</b>	50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600, Other
<b>Description</b>	<p>This field specifies the baudrate for the serial port. Nonstandard baudrates are supported through the "Other" setting. When set to "Other", you may manually enter a baudrate of your choice, up to 921600.</p> <p>50 to 921600: The serial port will operate at the specified baudrate</p> <p>Other: The serial port will operate at a baudrate that is manually entered by the user.</p>

**Parity**

<b>Default</b>	None
<b>Options</b>	None, Odd, Even, Space, Mark
<b>Description</b>	This field specifies the type of parity bit used for each character frame.

**Data bit**

<b>Default</b>	8
<b>Options</b>	5, 6, 7, 8
<b>Description</b>	This field specifies the number of data bits used to encode each character of data.

**Stop bit**

<b>Default</b>	1
<b>Options</b>	1, 1.5, 2
<b>Description</b>	This field specifies the number of stop bits used for each character frame.

**Flow control**

<b>Default</b>	RTS/CTS
<b>Options</b>	None, RTS/CTS, XON/XOFF, DTR/DSR
<b>Description</b>	This field specifies the type of flow control used by the serial port.

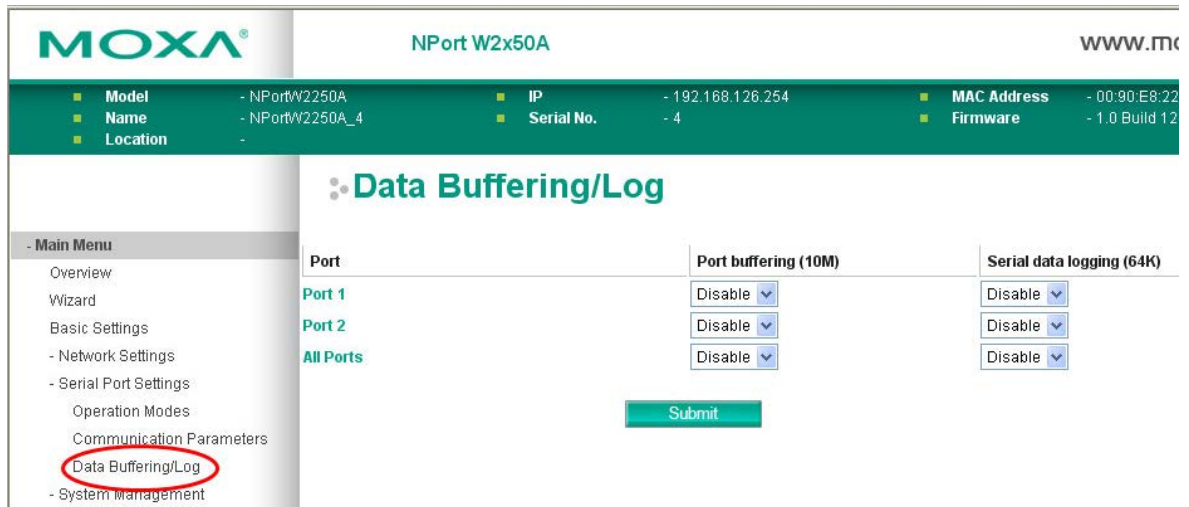
**FIFO**

<b>Default</b>	Enable
<b>Options</b>	Enable, Disable
<b>Description</b>	This field specifies whether the serial port will use the built-in FIFO. A 128-byte FIFO is provided to each serial port for both Tx and Rx directions. To prevent data loss during serial communication, this should be set to Disabled if the attached serial device does not have a FIFO.

**Interface**

<b>Default</b>	RS-232
<b>Options</b>	RS-232, RS-422, RS-485 2-wire, RS-485 4-wire
<b>Description</b>	This field specifies the type of interface the serial port will use.

## Data Buffering/Log



On the serial port's **Data Buffering/Log** page, you can enable or disable **Port buffering** and **Serial data logging**.

### Port buffering

<b>Default</b>	Disable
<b>Options</b>	Enable, Disable
<b>Description</b>	This field specifies whether the serial port will use port buffering when the network connection (Ethernet or WLAN) is down. Port buffering can be used in RealCOM mode, TCP Server mode, TCP Client mode, and Pair Connection mode. For other modes, the port buffering settings will have no effect.

### Serial data logging(64K)

<b>Default</b>	Disable
<b>Options</b>	Enable, Disable
<b>Description</b>	This field specifies whether data logs for the serial port will be stored on system RAM. Each serial port is allotted 64 KB for data logging. The data log is not saved when the NPort is powered off.

# Web Console: System Management

---

The following topics are covered in this chapter:

- **Overview**

- **System Management**

- Misc. Network Settings
- Auto Warning Settings
- Maintenance
- Maintenance
- Certificate

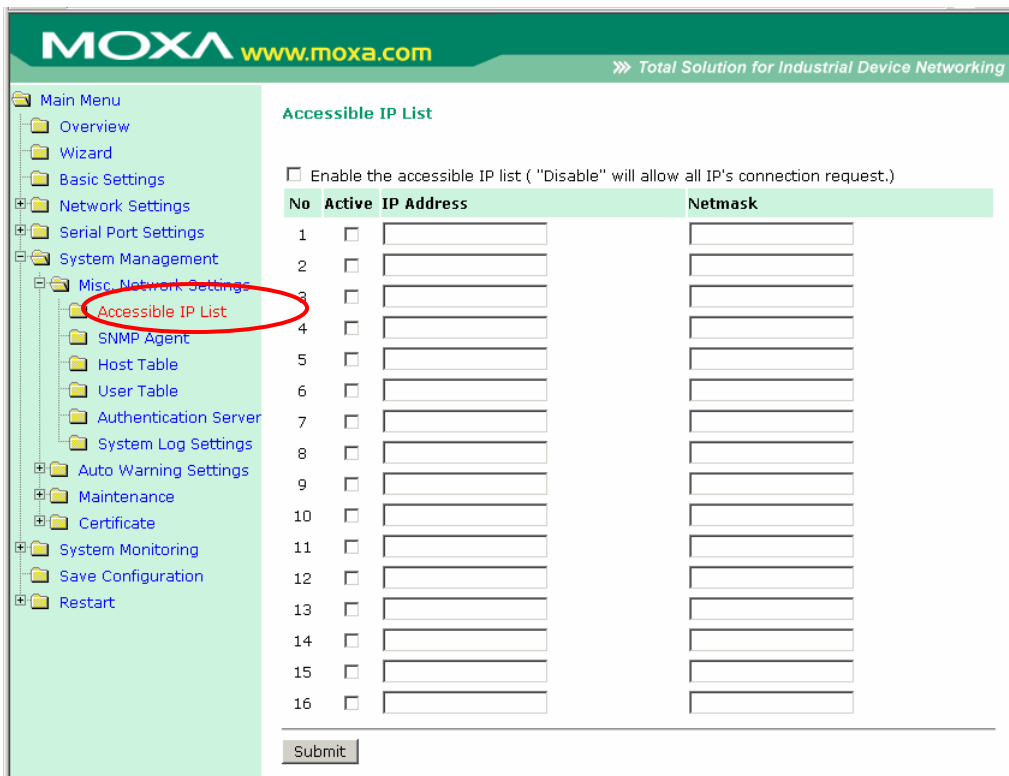
# Overview

This chapter explains how to configure all settings located under the **System Management** folder in the NPort web console.

## System Management

### Misc. Network Settings

#### Accessible IP List



The **Accessible IP List** page is located under **Misc. Network Settings** in the **System Management** folder. This page is used to restrict access to the NPort by IP address. Only IP addresses on the list will be allowed access to the NPort. You may add a specific address or range of addresses by using a combination of IP address and netmask, as follows:

**To allow access to a specific IP address**

Enter the IP address in the corresponding field; enter 255.255.255.255 for the netmask.

**To allow access to hosts on a specific subnet**

For both the IP address and netmask, use 0 for the last digit (e.g., "192.168.1.0" and "255.255.255.0").

**To allow access to all IP addresses**

Make sure that **Enable the accessible IP list** is not checked.

Refer to the following table for more configuration examples.

Desired IP Range	IP Address Field	Netmask Field
Any host	Disable	Disable
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

## SNMP Agent Settings

The screenshot shows the Moxa NPort W2x50A web console interface. At the top, there is a header with the Moxa logo and the device model. Below the header is a navigation bar with various system information items like Model, Name, Location, IP, Serial No., MAC Address, and Firmware. The main content area is titled "SNMP Agent Settings" and contains a "Configuration" section. This section includes a table of system information and a detailed configuration form for the SNMP Agent. The configuration form has fields for enabling/disabling the agent, contact name, location, community strings, agent version, and various read/write authentication and privacy modes. A "Submit" button is located at the bottom of the configuration form.

The **SNMP Agent** page is located under **Misc. Network Settings** in the **System Management** folder. This page is used to configure the SNMP Agent on the NPort.

### SNMP

<b>Default</b>	Enable
<b>Options</b>	Enable, Disable
<b>Description</b>	This field enables or disables the SNMP Agent. If enabled, you will need to configure other SNMP Agent settings. You will need to enter a community name under Read community string.

### Contact Name

<b>Default</b>	
<b>Options</b>	free text (e.g., "J Smith")
<b>Description</b>	This is an optional free text field that can be used to specify the SNMP emergency contact name, telephone, or pager number.

**Location**

<b>Default</b>	
<b>Options</b>	free text (e.g., "Building XYZ")
<b>Description</b>	This is an optional free text field that can be used to specify the location for SNMP agents such as the NPort.

**Read Community String**

<b>Default</b>	public
<b>Options</b>	free text (e.g., "public community")
<b>Description</b>	This field specifies the read community string used for the SNMP Agent. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.

**Write Community String**

<b>Default</b>	private
<b>Options</b>	free text (e.g., "private community")
<b>Description</b>	This field specifies the write community string used for the SNMP Agent. This is a text password mechanism that is used to weakly authenticate changes to agents of managed network devices.

**SNMP Agent Version**

<b>Default</b>	V1, V2c, V3
<b>Options</b>	V1, V2c, V3 / V1, V2c / V3 only
<b>Description</b>	This field specifies which version(s) of SNMP to support.

**Read Only User Name**

<b>Default</b>	rouser
<b>Options</b>	free text (e.g., "guest")
<b>Description</b>	This field specifies a user name to use for read only access.

**Read Only Authentication Mode**

<b>Default</b>	Disable
<b>Options</b>	Disable, MD5, SHA
<b>Description</b>	This field specifies the type of authentication to use for read-only access.

**Read Only Password**

<b>Default</b>	
<b>Options</b>	free text (e.g., "password123")
<b>Description</b>	This field specifies the password that users must enter for read-only access, if read only authentication is enabled.

**Read Only Privacy mode**

<b>Default</b>	Disable
<b>Options</b>	Disable, DES_CBC
<b>Description</b>	This field specifies whether DES_CBC data encryption will be used during read-only access.

**Read Only Privacy**

<b>Default</b>	
<b>Options</b>	free text (e.g., "read only key")
<b>Description</b>	This field specifies the encryption key for read-only access, if read-only privacy is enabled.

**Read/Write User Name**

<b>Default</b>	rwuser
<b>Options</b>	free text (e.g., "admin")
<b>Description</b>	This field specifies a user name to use for read/write access.

**Read/Write Authentication Mode**

<b>Default</b>	Disable
<b>Options</b>	Disable, MD5, SHA
<b>Description</b>	This field specifies the type of authentication to use for read/write access.

**Read/Write Password**

<b>Default</b>	
<b>Options</b>	free text (e.g., "password123")
<b>Description</b>	This field specifies the password that users must enter for read/write access, if read only authentication is enabled.

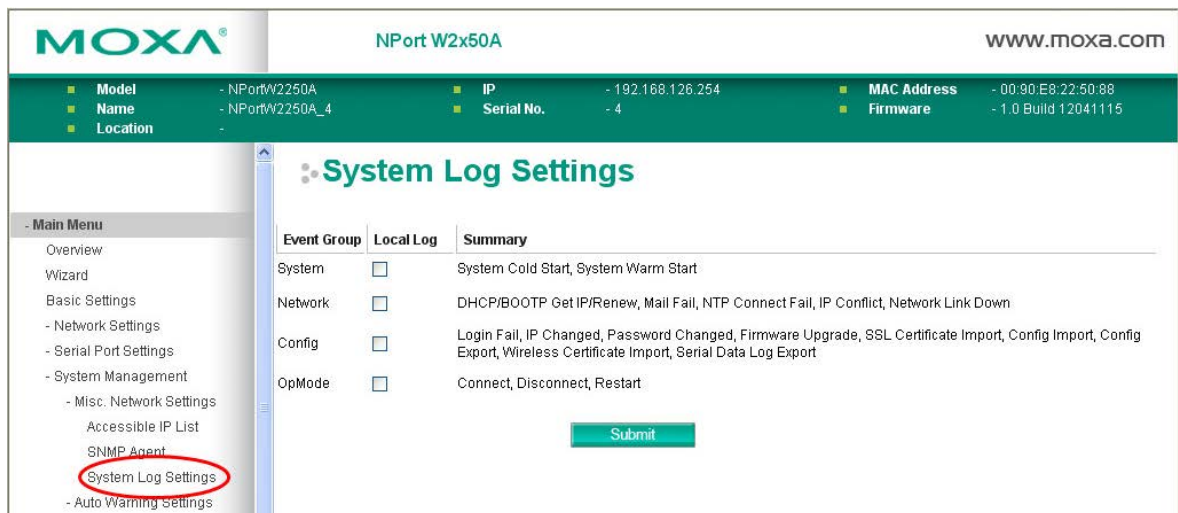
**Read/Write Privacy mode**

<b>Default</b>	Disable
<b>Options</b>	Disable, DES_CBC
<b>Description</b>	This field specifies whether DES_CBC data encryption will be used during read/write access.

**Read/Write Privacy**

<b>Default</b>	
<b>Options</b>	free text (e.g., "read write key")
<b>Description</b>	This field specifies the encryption key for read/write access, if read-/write privacy is enabled.

**System Log Settings**



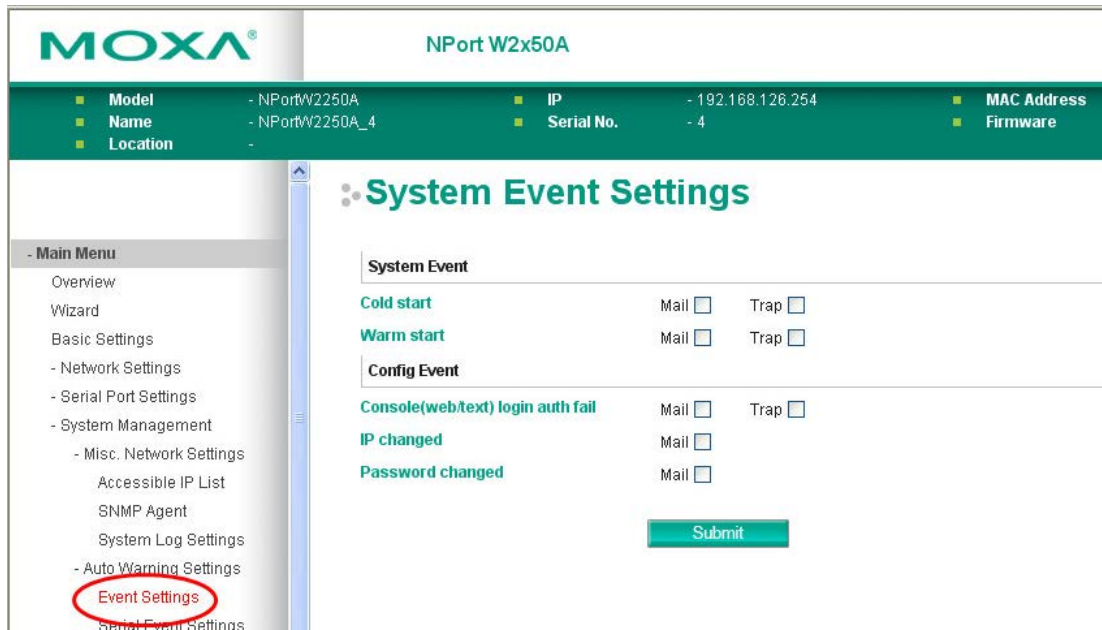
The **System Log** page is located under **Misc. Network Settings** in the **System Management** folder. This is where you select the type of events that will be logged by the NPort.

Group	Event
System	System Cold Start, System Warm Start
Network	DHCP/BOOTP, Get IP/Renew, Mail Fail, NTP Connect Fail, IP Conflict, Network Link Down
Config	Login Fail, IP Changed, Password Changed, Firmware Upgrade, SSL Certificate Import, Config Import, Config Export, Wireless Certificate Import, Serial Data Log Export
Op Mode	Connect, Disconnect, Restart



# Auto Warning Settings

## Event Settings



The **Event Settings** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how the NPort will notify you of system and configuration events. Depending on the event, different options for notification are available, as shown above. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending an SNMP trap.

Event	Description
Cold start	The NPort was powered on, or was restarted after a firmware upgrade.
Warm start	The NPort restarted without powering off.
Console login auth fail	An attempt has been made to open the web, Telnet, or serial console, but the password was incorrect.
IP changed	The IP address has been changed.
Password changed	The password to the console has been changed.

## Serial Event Settings

**MOXA** NPort W2x50A WWW.MOXA

Model - NPortW2250A IP - 192.168.126.254 MAC Address - 00:90:E8:22:50:88  
 Name - NPortW2250A\_4 Serial No. - 4 Firmware - 1.0 Build 120411  
 Location -

### Serial Event Settings

Serial Port Event	DCD changed		DSR changed	
Port 1	Mail <input type="checkbox"/>	Trap <input type="checkbox"/>	Mail <input type="checkbox"/>	Trap <input type="checkbox"/>
Port 2	Mail <input type="checkbox"/>	Trap <input type="checkbox"/>	Mail <input type="checkbox"/>	Trap <input type="checkbox"/>
All Ports	Mail <input type="checkbox"/>	Trap <input type="checkbox"/>	Mail <input type="checkbox"/>	Trap <input type="checkbox"/>

Submit

**Main Menu**  
 Overview  
 Wizard  
 Basic Settings  
 - Network Settings  
 - Serial Port Settings  
 - System Management  
   - Misc. Network Settings  
     Accessible IP List  
     SNMP Agent  
     System Log Settings  
   - Auto Warning Settings  
     Event Settings  
     Serial Event Settings

The **Serial Event Settings** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how the NPort will notify you of DCD and DSR events for each serial port. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending an SNMP trap.

A change in the DCD (Data Carrier Detect) signal indicates that the modem connection status has changed. If the DCD signal changes to low, it indicates that the connection line is down. A change in the DSR (Data Set Ready) signal indicates that the data communication equipment is powered off. If the DSR signal changes to low, it indicates that the data communication equipment is powered down.



### ATTENTION

SNMP indicates a change in DCD or DSR signals but does not differentiate between the two. A change in either signal from “-” to “+” is indicated by “link up” and a change in either signal from “+” to “-” is indicated by “link down.”

## E-mail Alert

The **E-mail Alert** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how and where e-mail is sent when e-mail is used for automatic notification of system and serial port events.



### ATTENTION

Consult your network administrator or ISP for the mail server settings to use for your network. If these settings are not configured correctly, e-mail notification may not work properly.

### Mail Server (SMTP)

<b>Default</b>	
<b>Options</b>	free text (e.g., "192.168.3.3")
<b>Description</b>	This field specifies the IP address of the mail server that will be used when sending automatic warning e-mails. If the mail server requires authentication, select "My server requires authentication" and enter the username and password.

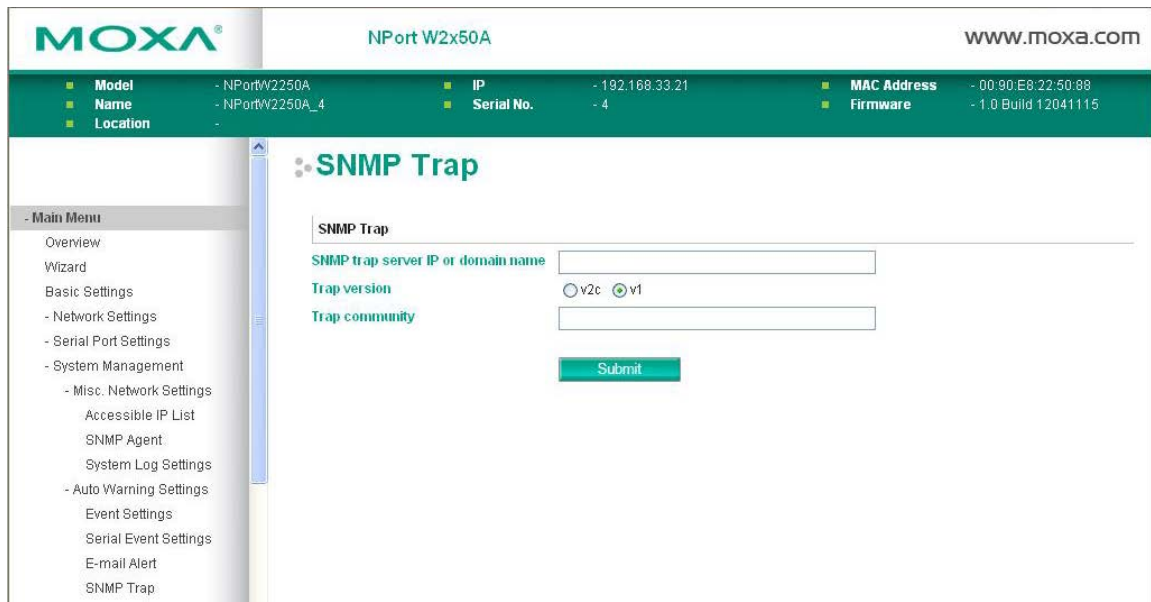
### From e-mail address

<b>Default</b>	
<b>Options</b>	free text (e.g., "jsmith@xyz.com")
<b>Description</b>	This field specifies the e-mail address that will be listed in the e-mail's "From" field.

### To e-mail address 1 to 4

<b>Default</b>	
<b>Options</b>	free text (e.g., "admin@abc.com")
<b>Description</b>	These fields specify the destination e-mail address(es) for the automatic e-mail warnings.

## SNMP Trap



The **SNMP Trap** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify the SNMP trap settings to use for automatic notification of system and serial port events.

### SNMP Trap Server IP

<b>Default</b>	
<b>Options</b>	IP address (e.g., "192.168.5.5")
<b>Description</b>	This field specifies the IP address of the SNMP trap server that will receive SNMP traps.

### Trap Version

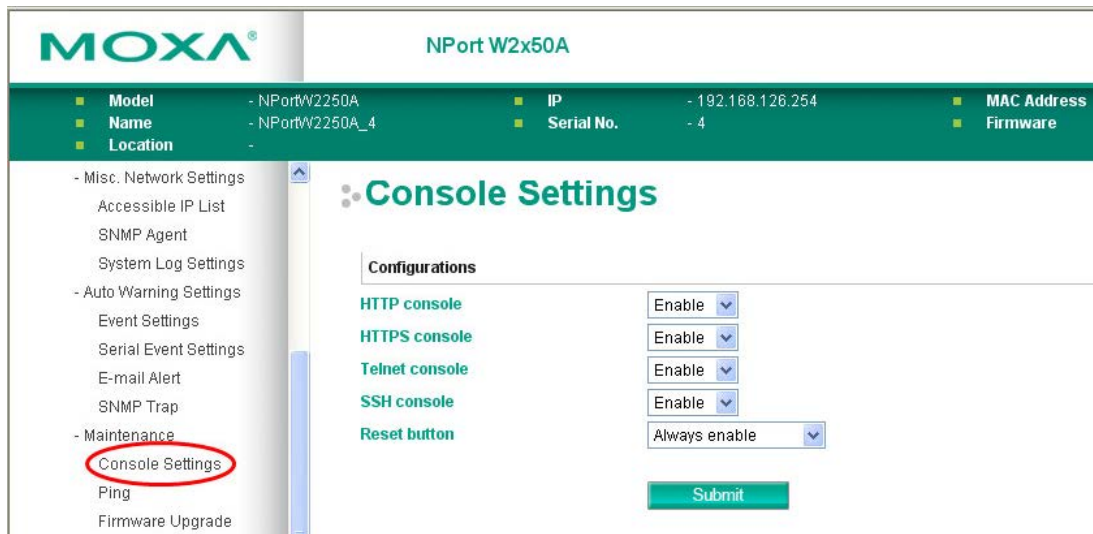
<b>Default</b>	v1
<b>Options</b>	v1, v2c
<b>Description</b>	This field specifies the SNMP trap version to use.

### Trap Community

<b>Default</b>	
<b>Options</b>	free text (e.g., "public access")
<b>Description</b>	This field specifies the SNMP trap community.

# Maintenance

## Console Settings



The **Console Settings** page is located under **Maintenance** in the **System Management** folder. This is where you enable or disable access to the various NPort configuration consoles, as well as the behavior of the reset button. You may modify **HTTP console**, **HTTPS console**, **Telnet console**, **SSH console**, and **Reset button**.

### HTTP Console

<b>Default</b>	Enable
<b>Options</b>	Enable, Disable
<b>Description</b>	This field enables or disables access to the HTTP (web) console.

### HTTPS Console

<b>Default</b>	Enable
<b>Options</b>	Enable, Disable
<b>Description</b>	This field enables or disables access to the HTTPS (web) console.

### Telnet Console

<b>Default</b>	Enable
<b>Options</b>	Enable, Disable
<b>Description</b>	This field enables or disables access to the Telnet console.

### SSH Console

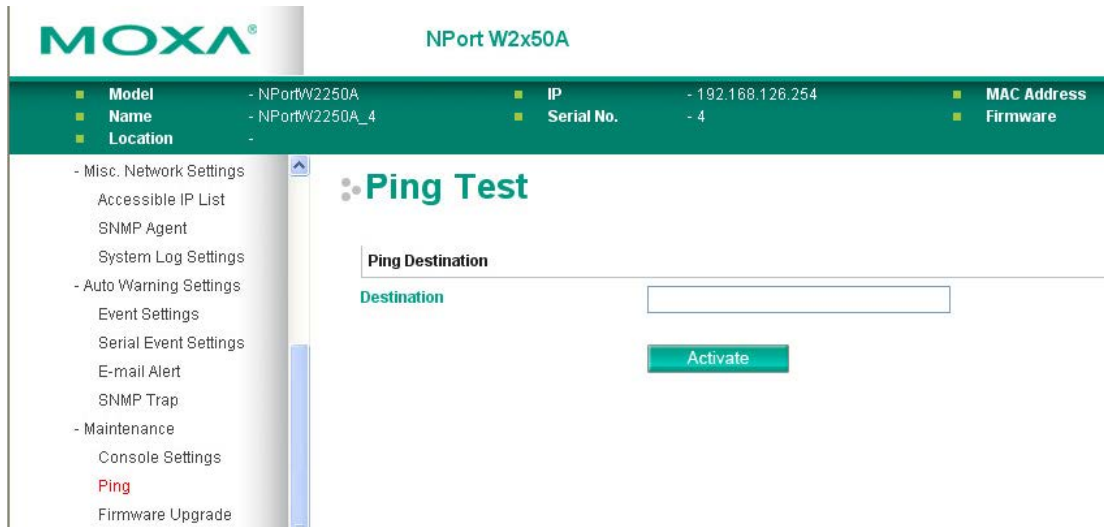
<b>Default</b>	Enable
<b>Options</b>	Enable, Disable
<b>Description</b>	This field enables or disables access to the SSH console.

### Reset Button

<b>Default</b>	Always Enable
<b>Options</b>	Always Enable, Disable after 60 sec
<b>Description</b>	<p>This field specifies the behavior of the hardware reset button.</p> <p>Always Enable: The reset button will be operate as usual.</p> <p>Disable after 60 sec: The reset button will only be effective for the first 60 seconds that the NPort is powered on.</p>

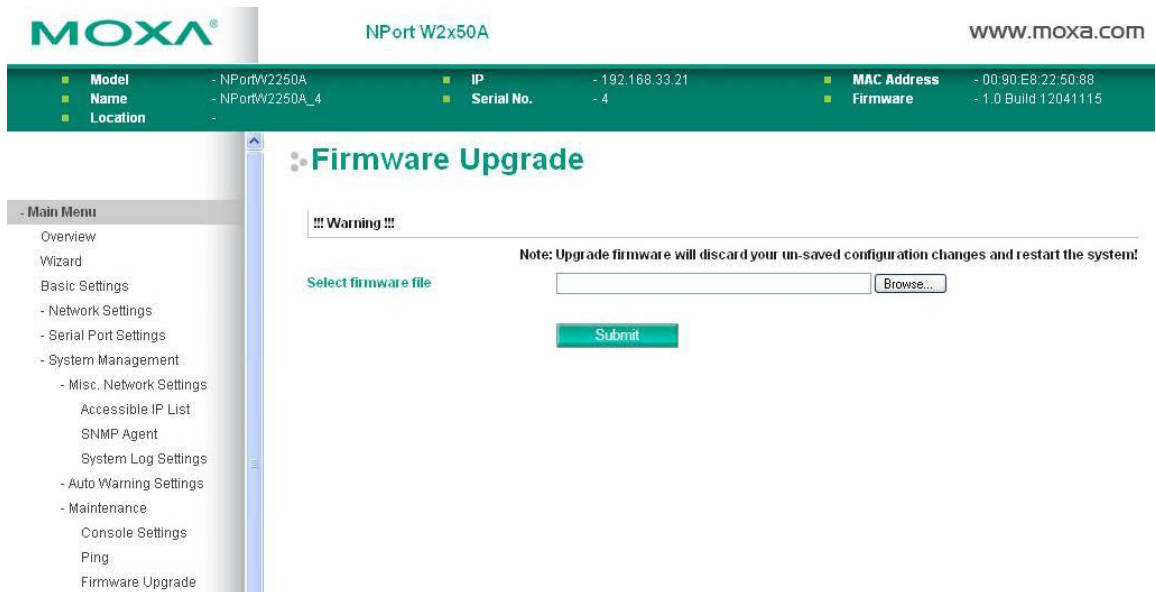
# Maintenance

## Ping



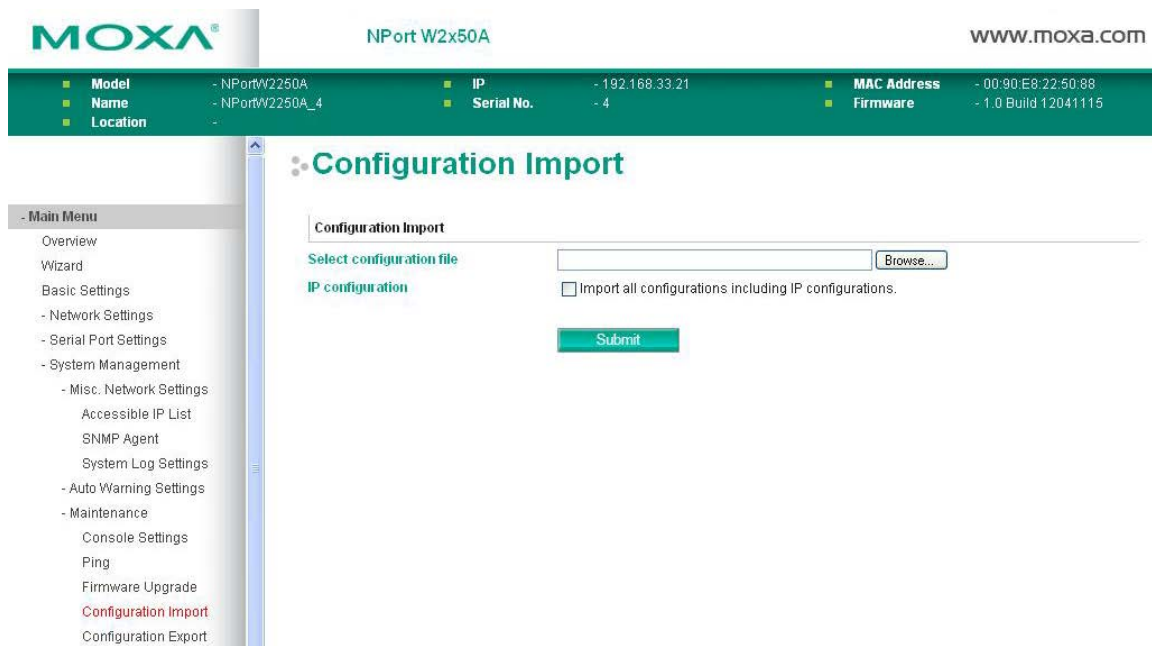
The **Ping** page is located under **Maintenance** in the **System Management** folder. It provides a convenient way to test an Ethernet connection or verify an IP address. Enter the IP address or domain name in the Destination field and click **[Activate]**. The results will be displayed immediately.

## Firmware Upgrade



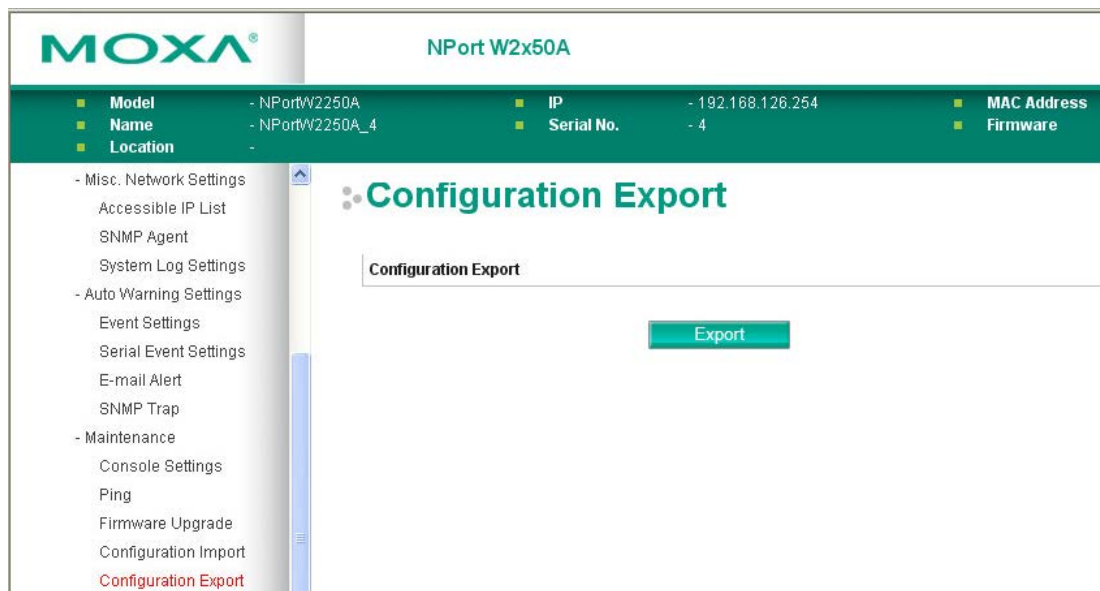
The **Firmware Upgrade** page is located under **Maintenance** in the **System Management** folder. This is where you can update the NPort firmware. After obtaining the latest firmware from [www.moxa.com](http://www.moxa.com), select or browse for the firmware file in the **Select firmware file** field. Before clicking **[Submit]**, it is a good idea to save the NPort configuration using the **Configuration Export** page, since the firmware upgrade process may cause all settings to revert to factory defaults.

## Configuration Import



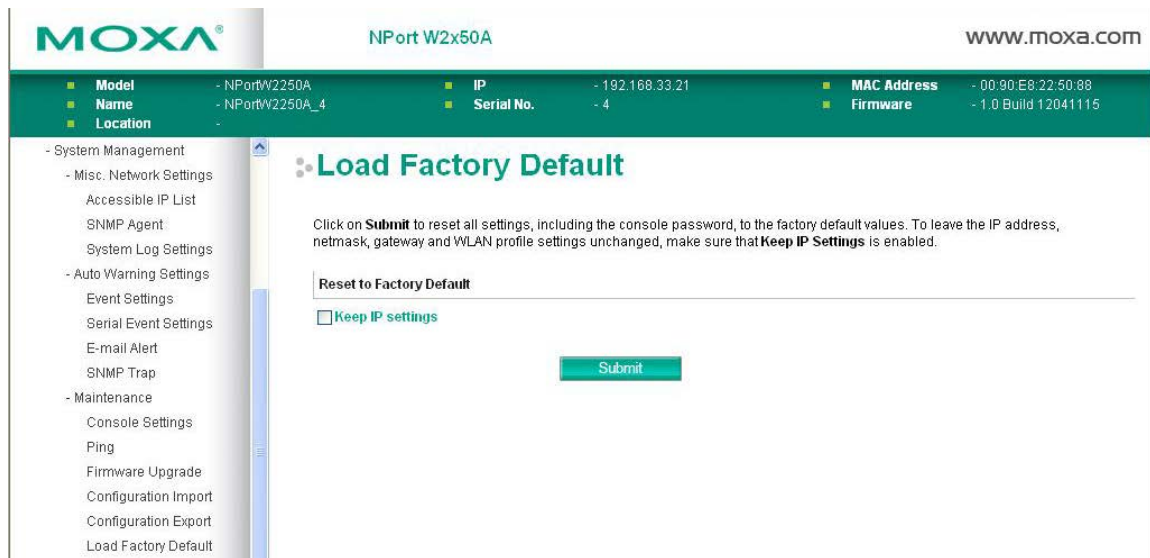
The **Configuration Import** page is located under **Maintenance** in the **System Management** folder. This is where you can load a previously saved or exported configuration. Select or browse for the configuration file in the **Select configuration file** field. If you also wish to import the IP configuration (i.e., IP address, netmask, and gateway), make sure that **Import all configurations including IP configurations** is checked.

## Configuration Export



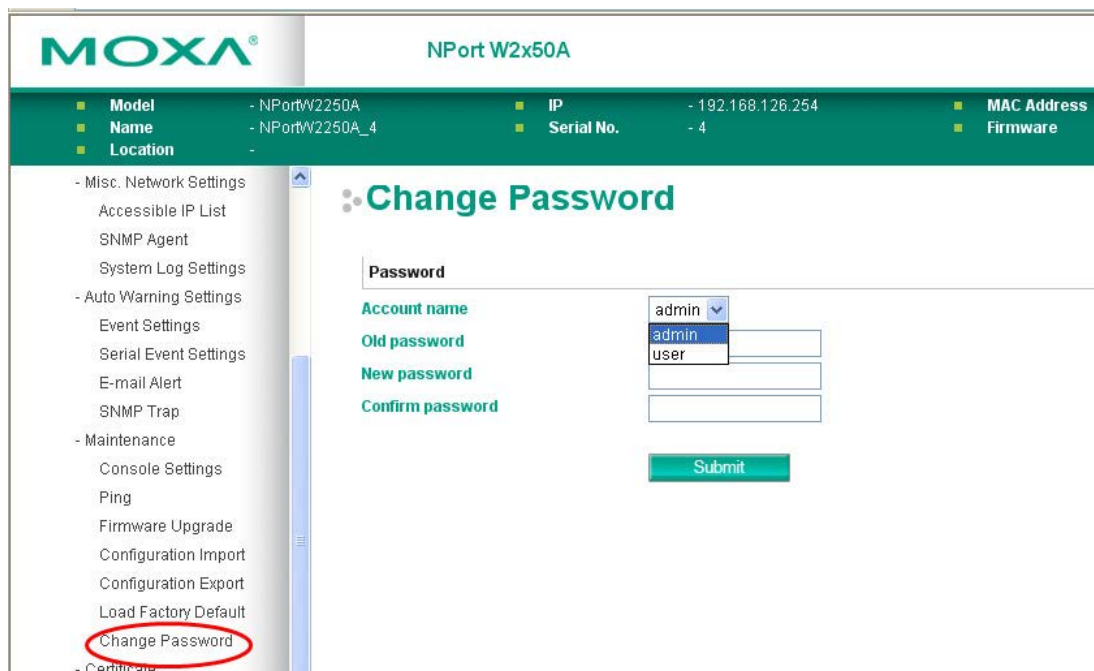
The **Configuration Export** page is located under **Maintenance** in the **System Management** folder. This is where you can save the NPort's current configuration to a file on the local host. Click **[Download]** to begin the process. A window should appear asking you to open or save the configuration text file.

## Load Factory Default



The **Load Factory Default** page is located under **Maintenance** in the **System Management** folder. Click **[Submit]** to reset all settings to the factory defaults. You can preserve the NPort’s existing IP settings (i.e., IP address, netmask, gateway, WLAN profile, and all certificates) by making sure **Keep IP settings** is checked before clicking **[Submit]**.

## Change Password



The **Change Password** page is located under **Maintenance** in the **System Management** folder. To change the password, choose the account name first, and then enter the old password in the **Old password** field. Leave this blank if the NPort is not currently password-protected. Enter the new password twice, once in the **New password** field and once in the **Confirm password**. Leave these fields blank to remove password protection.





### ATTENTION

If you forget the password, the ONLY way to configure the NPort is by loading the factory defaults with the reset button. All settings will be lost.  
Before setting the password, you may want to first export the configuration to a file. Your configuration can then be easily imported back into the NPort if necessary.

## Certificate

### Ethernet SSL Certificate Import

The screenshot shows the MOXA NPort W2x50A web console interface. At the top, the MOXA logo and 'NPort W2x50A' are visible. Below this is a status bar with fields for Model, Name, Location, IP, Serial No., MAC Address, and Firmware. The left sidebar contains a navigation menu with 'Certificate' expanded, and 'Ethernet SSL Certificate Imp' highlighted with a red circle. The main content area is titled 'Ethernet SSL Certificate Import' and contains the following information:

Installed Certificate	
Issued to	192.168.126.254
Issued by	192.168.126.254
Valid	from 2012/4/19 to 2017/4/4
Select SSL certificate/key file	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

The **Ethernet SSL Certificate Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the Ethernet SSL certificate. Select or browse for the certificate file in the **Select SSL certificate/key file** field.

### WLAN SSL Certificate Import

The screenshot shows the MOXA NPort W2x50A web console interface. At the top, the MOXA logo and 'NPort W2x50A' are visible. Below this is a status bar with fields for Model, Name, Location, IP, Serial No., MAC Address, and Firmware. The left sidebar contains a navigation menu with 'Certificate' expanded, and 'WLAN SSL Certificate Imp' highlighted. The main content area is titled 'WLAN SSL Certificate Import' and contains the following information:

Installed Certificate	
Issued to	Not installed
Issued by	Not installed
Valid	from Not installed to Not installed
Select SSL certificate/key file	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

The **WLAN SSL Certificate Import** page is located under **Certificate** in the **System Management** folder. By default, the WLAN SSL certificate is automatically generated by the NPort based on the IP address of the wireless interface. You can also import a certificate. Select or browse for the certificate file in the **Select SSL certificate/key file** field.

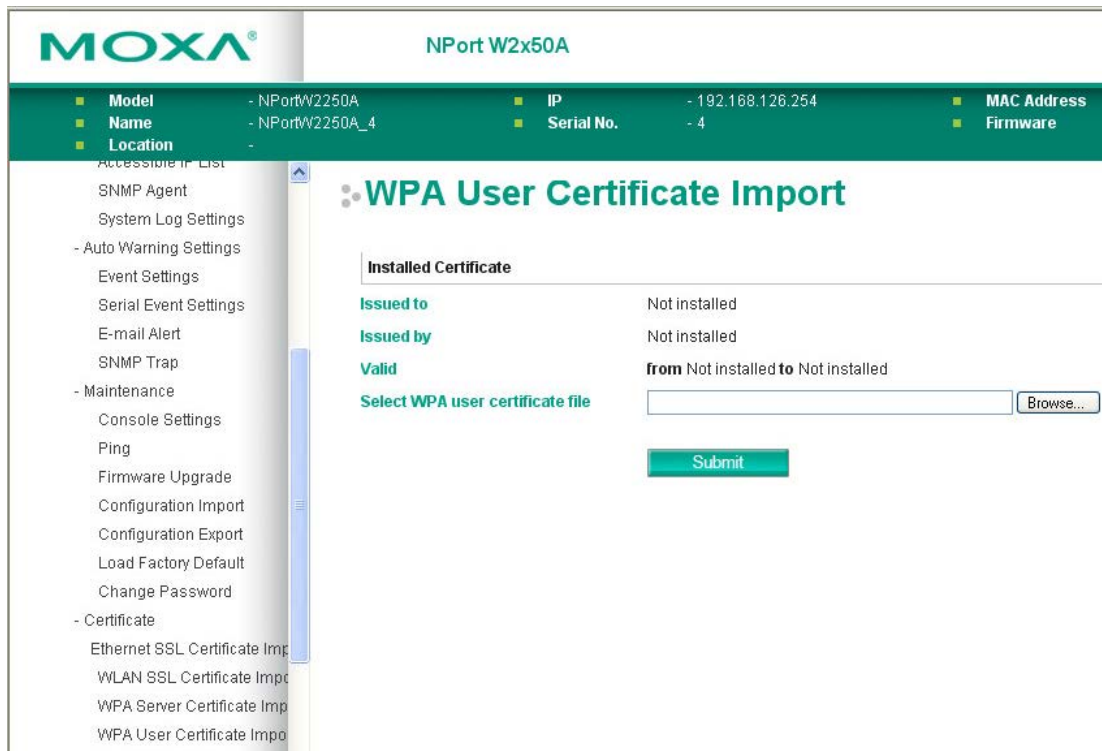
## WPA Server Certificate Import



The **WPA Server Certificate Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the WPA server certificate. Select or browse for the certificate file in the **Select WPA server certificate file** field.

You must install the trusted server certificate from the RADIUS server in order to enable **Verify server certificate** in the **WLAN Security** settings. This certificate will then be used by the NPort to authenticate the RADIUS server.

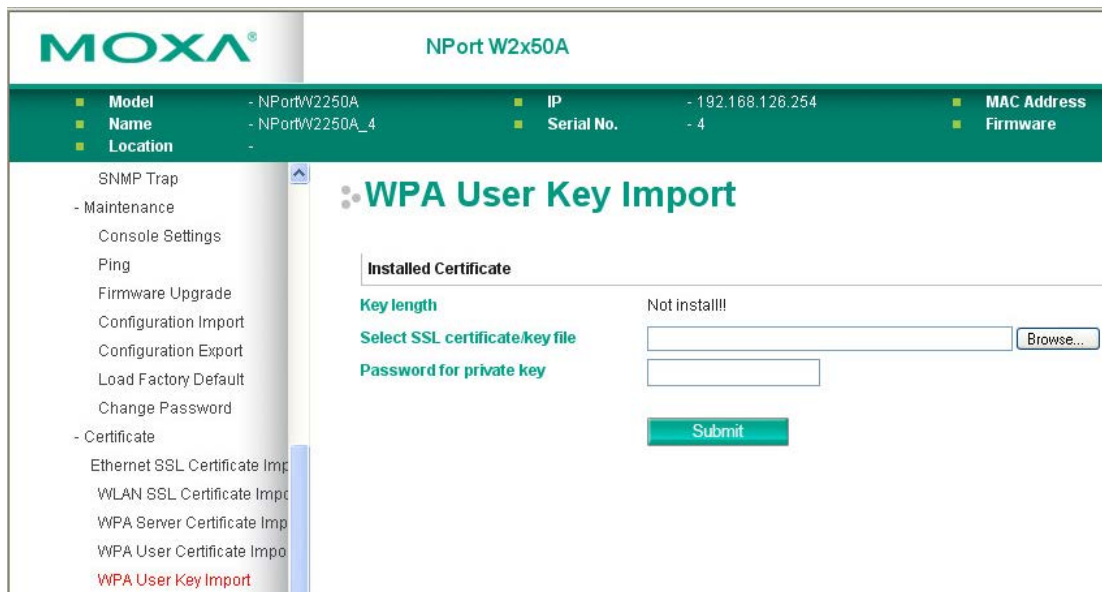
## WPA User Certificate Import



The **WPA User Certificate Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the WPA user certificate. Select or browse for the certificate file in the **Select WPA user certificate file** field.

The user certificate of the NPort must be installed in the RADIUS server when the NPort uses WPA (WPA2)/TLS. The trusted server certificate of the RADIUS server must also be installed in the NPort.

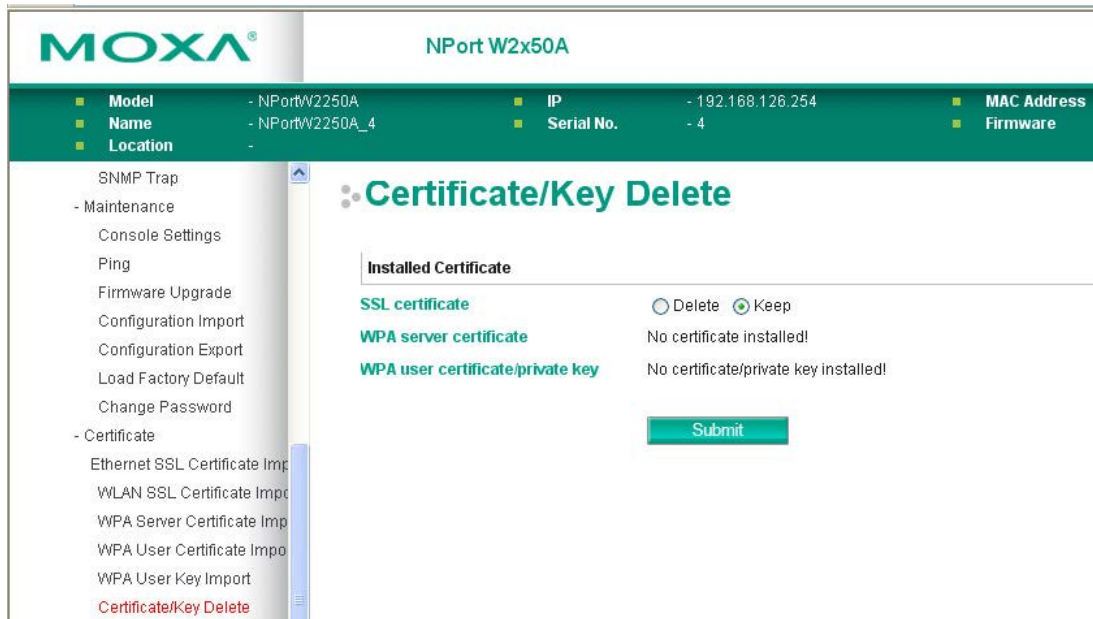
## WPA User Key Import



The **WPA User Key Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the WPA user certificate. Select or browse for the user private key file in the **Select WPA user privacy key file** field and enter the **Password for the private key**.

The user private key of the NPort must be installed in the RADIUS server when the NPort uses WPA(WPA2)//TLS. The trusted server certificate of RADIUS server must also be installed on the NPort.

## Certificate/Key Delete



The **Certificate/Key Delete** page is located under **Certificate** in the **System Management** folder. This page is where you can delete certificates or WPA keys that have been installed on the model. When you click **[Submit]**, any certificate or key that has been set to “Delete” will be deleted from the NPort.

# Web Console: System Monitoring

---

The following topics are covered in this chapter:

- **Overview**
- **System Monitoring**
  - Serial Status
  - System Status

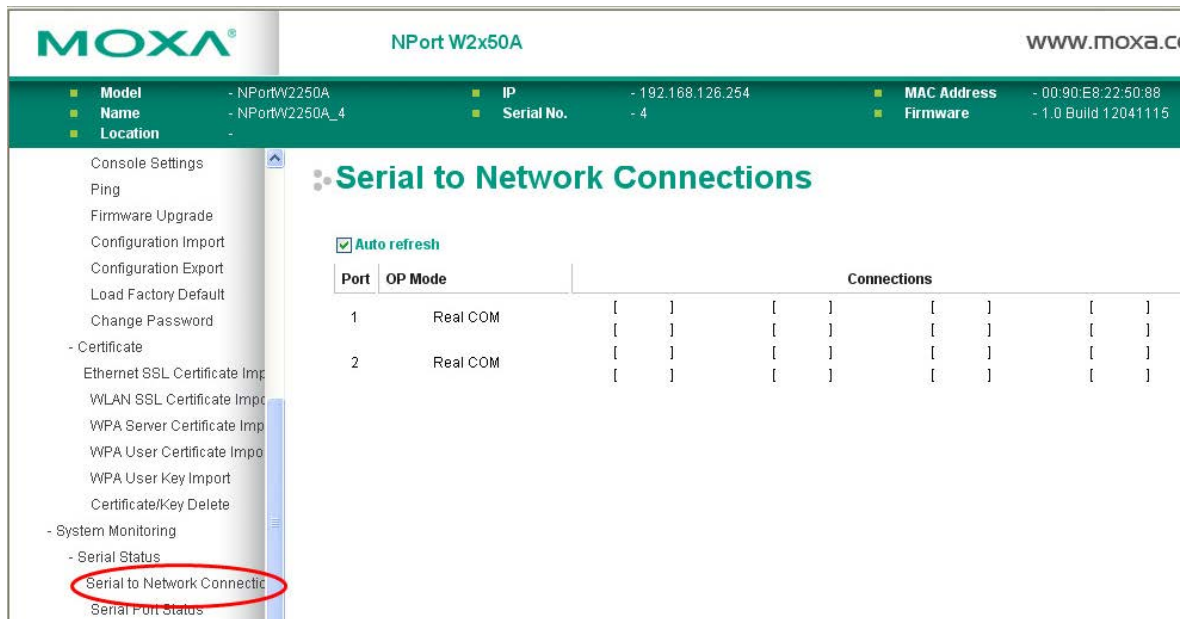
# Overview

This chapter explains how to use the **System Monitoring** functions on the NPort web console. These functions allow you to monitor many different aspects of operation.

## System Monitoring

### Serial Status

#### Serial to Network Connections



The **Serial to Network Connections** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can monitor the current operation mode and host connection status for each serial port.

## Serial Port Status

**MOXA®** NPort W2x50A www.moxa.com

- 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

### Serial Port Status

Auto refresh

Port	TxCnt	RxCnt	TxTotalCnt	RxTotalCnt	DSR	DTR	RTS	CTS	DCD
1	0	0	0	0	●	●	●	●	●
2	0	0	0	0	●	●	●	●	●

The **Serial Port Status** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can monitor the signal and data transmission status for each serial port.

**TxCnt**: number of Tx packets (to device) for the current connection

**RxCnt**: number of Rx packets (from device) for the current connection

**TxTotalCnt**: number of Tx packets since the NPort was powered on

**RxTotalCnt**: number of Rx packets since the NPort was powered on

## Serial Port Error Count

**MOXA®** NPort W2x50A www.moxa.com

- 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

### Serial Port Error Count

Auto refresh

Port	ErrCnt			
	Frame	Parity	Overrun	Break
1	0	0	0	0
2	0	0	0	0

The **Serial Port Error Count** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can view the current number of frame, parity, overrun and break errors for each serial port.

## Serial Port Settings

**MOXA®** NPort W2x50A www.moxa.com

- 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

### Serial Port Settings

Auto refresh

Port	Baud Rate	Data Bits	Stop Bits	Parity	Flow Control		FIFO	Interface
					RTS/CTS	XON/XOFF		
1	19200	8	1	None	OFF	OFF	Enable	RS-232
2	9600	8	1	None	OFF	OFF	Enable	RS-232

The **Serial Port Settings** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can view the current communication settings for each serial port.

## System Status

### Network Connections

**MOXA®** NPort W2x50A www.moxa.com

- 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

### Network Connections

Auto refresh

Protocol	Recv-Q	Send-Q	Local Address	Foreign Address	State
TCP	0	0	*:4900	*:0	LISTEN
TCP	0	0	*:966	*:0	LISTEN
TCP	0	0	*:967	*:0	LISTEN
TCP	0	0	*:80	*:0	LISTEN
TCP	0	0	*:950	*:0	LISTEN
TCP	0	0	*:22	*:0	LISTEN
TCP	0	0	*:951	*:0	LISTEN
TCP	0	0	*:23	*:0	LISTEN
TCP	0	0	*:443	*:0	LISTEN
TCP	0	0	192.168.126.254:80	192.168.126.11:3891	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3892	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3898	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3868	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3878	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3884	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3863	TIME_WAIT
TCP	0	1275	192.168.126.254:80	192.168.126.11:3908	ESTABLISHED
TCP	0	0	192.168.126.254:80	192.168.126.11:3873	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3883	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3897	TIME_WAIT

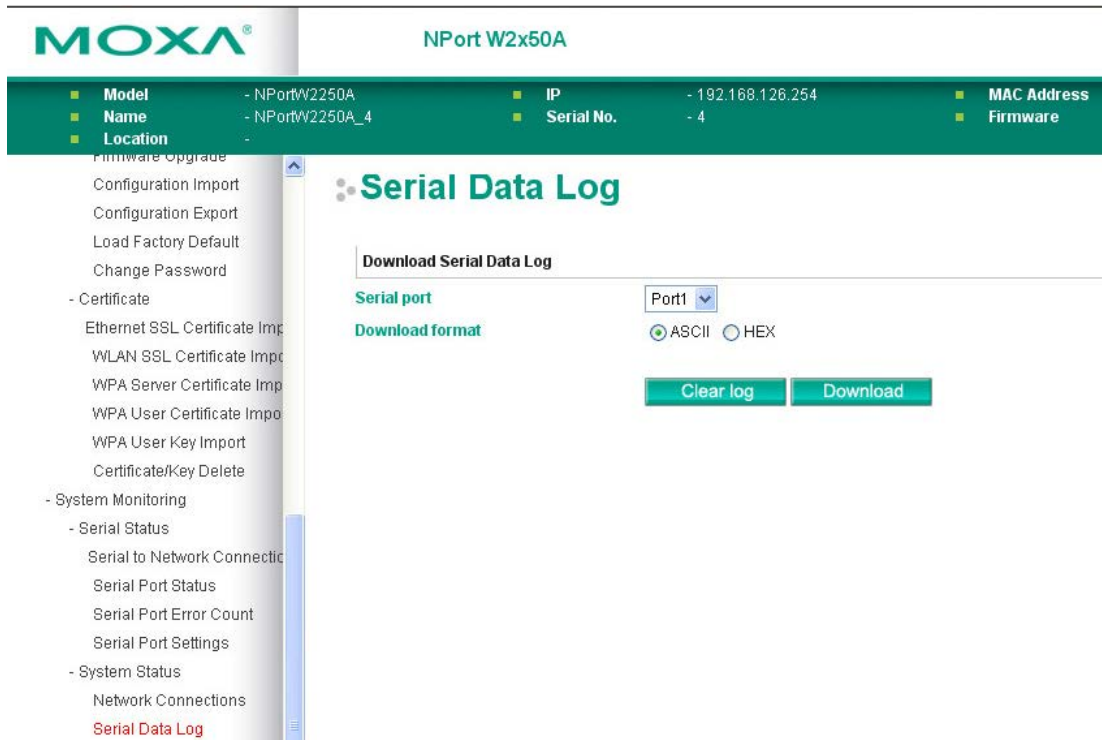
goahead  
**WEB SERVER**  
Best viewed with IE 5 above at resolution 1024 x 768



The **Network Connections** page is located under **System Status** in the **System Monitoring** folder. On this page, you can view the current status of any network connection to the NPort.

## Serial Data Log

Data logs for each serial port can be viewed in ASCII or HEX format. After selecting the serial port and format, you may click **Select** all to select the entire log if you wish to copy and paste the contents into a text file. The **Clear log** and **Refresh** buttons allow you to clear or refresh the log contents.



The **Serial Data Log** page is located under **System Status** in the **System Monitoring** folder. This is where you can download the current data log for a serial port. Select the desired serial port in the **Select port** field. Select the desired data format in the **Download format** field. Click **[Clear log]** to clear the log contents.

The data log includes all data sent or received by the specified serial port since the NPort was powered on. The maximum size of the log is 64 KB.