NPort S9000 Series User's Manual

Edition 1.0, March 2017

www.moxa.com/product

NPort S9000 Series User's Manual

Copyright Notice

Trademarks

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

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 India

Tel:	+91-80-4172-9088
Fax:	+91-80-4132-1045

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

1

Introduction

The NPort S9000 series comprises substation grade 4-port RS-232/422/485 serial ports device servers with a full-function managed Ethernet switch by integrating a combination of fiber and copper Ethernet ports, allowing you to easily install, manage, and maintain the products and serial devices.

The following topics are covered in this chapter:

- ❐ **Overview**
  - ➢ Industrial Communications and Automation
  - ➢ Industrial vs. Commercial
  - ➢ Informative vs. Passive
- ❐ **Package Checklist**
- ❐ **Product Features**
- ❐ **Product Specifications**
  - ➢ NPort S9450I Series
- ❐ **EMI and Environmental Type Tests**

Overview

The NPort S9000 series supports a high level of surge protection to prevent damage from the types of power surges and EMI one finds in electrical substations and industrial automation applications. Combined with a -40 to 85 degree Celsius operating temperature range and galvanized steel housing, the NPort S9000 is suitable for a wide range of industrial environments.

Another plus is the NPort S9000's dual power supplies, which provide both redundancy, as well as a wide range of voltage inputs. The WV models accept a power 24/48 VDC power input (ranging from 18 to 72 VDC), and the HV models accept a power input of 88 to 300 VDC and 85 to 264 VAC.

Combining a device server and switch in one product allows you to reduce overall power consumption,extends the useful life of existing legacy IEDs, and minimizes capital expenditures on new equipment.

The NPort S9000 series includes the following models:

- **NPort S9450I-WV-T:**
  4 RS-232/422/485 ports rugged device server, five 10/100M Ethernet ports, 24/48VDC, -40 to 85°C operating temperature
- **NPort S9450I-HV-T:**
  4 RS-232/422/485 ports rugged device server, five 10/100M Ethernet ports, 88-300 VDC or 85-264 VAC, -40 to 85°C operating temperature
- **NPort S9450I-2M-SC-WV-T:**
  4 RS-232/422/485 ports rugged device server, three 10/100M Ethernet ports, two 100M multimode fiber ports with SC connector, 24/48VDC, -40 to 85°C operating temperature
- **NPort S9450I-2M-SC-HV-T:**
  4 RS-232/422/485 ports rugged device server, three 10/100M Ethernet ports, two 100M multimode fiber ports with SC connector, 88-300 VDC or 85-264 VAC, -40 to 85°C operating temperature
- **NPort S9450I-2M-ST-WV-T:**
  4 RS-232/422/485 ports rugged device server, three 10/100M Ethernet ports, two 100M multimode fiber ports with ST connector, 24/48VDC, -40 to 85°C operating temperature
- **NPort S9450I-2M-ST-HV-T:**
  4 RS-232/422/485 ports rugged device server, three 10/100M Ethernet ports, two 100M multimode fiber ports with ST connector, 88-300 VDC or 85-264 VAC, -40 to 85°C operating temperature
- **NPort S9450I-2S-SC-WV-T:**
  4 RS-232/422/485 ports rugged device server, three 10/100M Ethernet ports, two 100M single-mode fiber ports with SC connector, 24/48VDC, -40 to 85°C operating temperature
- **NPort S9450I-2S-SC-HV-T:**
  4 RS-232/422/485 ports rugged device server, three 10/100M Ethernet ports, two 100M single-mode fiber ports with SC connector, 88-300 VDC or 85-264 VAC, -40 to 85°C operating temperature
- **NPort S9450I-2S-ST-WV-T:**
  4 RS-232/422/485 ports rugged device server, three 10/100M Ethernet ports, two 100M single-mode fiber ports with ST connector, 24/48VDC, -40 to 85°C operating temperature
- **NPort S9450I-2S-ST-HV-T:**
  4 RS-232/422/485 ports rugged device server, three 10/100M Ethernet ports, two 100M single-mode fiber ports with ST connector, 88-300 VDC or 85-264 VAC, -40 to 85°C operating temperature

Industrial Communications and Automation

As the world’s networking and information technology becomes more complex, Ethernet has become the major communications interface in many industrial communications and automation applications. In fact, a whole new industry has sprung up to provide Ethernet products that comply with the requirements of demanding industrial applications.

Industrial vs. Commercial

Users have found that when transplanting Ethernet from comfortable office environments to harsh and less predictable industrial environments, commercial Ethernet equipment available in today's market simply cannot meet the high-reliability requirements demanded by industrial applications. This means that more robust networking equipment, commonly referred to as industrial Ethernet equipment, is required for these applications.

Informative vs. Passive

Since industrial Ethernet devices are often located at the endpoints of a system, such devices cannot always know what's happening elsewhere on the network. This means that industrial Ethernet communication equipment that connects these devices must provide system administrators with real-time alarm messages.

Package Checklist

The Moxa NPort S9000 Series products are shipped with the following items:

Standard

- 1 NPort S9000 combo switch/serial device server
- 1 CN20070 Connection CBL RJ45/10P/F9 150cm
- 1 DK/DC 50x131mm w/ Lock Natural (DIN-rail kit) for the NPort S9450I series only
- Document & software CD
- Quick installation guide
- Product warranty statement

NOTE Notify your sales representative if any of the aforementioned items is missing or damaged..

Product Features

The NPort S9000 Series products have the following features:

- IEC 61850-3, IEEE 1613 (power substations)-compliant
- Versatile socket operation modes, including TCP Server, TCP Client, and UDP
- Easy-to-use Windows Utility for mass installation
- Supports 10/100 Mbps Ethernet—auto detectable
- Supports SNMP MIB-II for network management
- Configuration auto-restore by LLDP (Link Layer Discovery Protocol)
- Configurable serial data transmission priority
- Supports IEC 62443 Level 2
- Ethernet redundancy by Turbo Ring (recovery time < 20 ms), RSTP/STP (IEEE 802.1w/D)
- QoS, IGMP snooping/GMRP, VLAN, LACP, SNMPv1/v2c/v3, RMON supported
- 4 serial ports device server, support RS-232/422/RS-485
- 2kV DC isolation protection for serial port
- Surge protection for serial/power/Ethernet
- Gateway supports DNP3 and Modbus protocols
- 2- or 4-wire RS-485 with patented ADDC™ (Automatic Data Direction Control)
- Supports IEC 61850 MMS Protocol

Product Specifications

NPort S9450I Series

General Specifications

Port Summary

Serial Ports: 4 RS-232/422/485 ports

Ethernet Switch Ports:

NPort S9450I all copper models: 5 RJ45 copper ports

NPort S9450I copper/fiber models: 3 RJ45 copper ports, 2 fiber ports

Magnetic Isolation Protection: 1.5 kV built in

Console Ports: 1 (10-pin RJ45 connector)

Physical Characteristics

Housing: Metal

Weight: 2.54 kg (5.60 lb)

Dimensions: 80 x 160 x 109 mm (3.15 x 6.30 x 4.29 inches)

Environmental Limits

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

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

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

Power Requirements

Input Voltage:

WV models: 24/48 VDC (18 to 72 VDC)

HV models: 110/220 VAC/VDC (88 to 300 VDC, 85 to 264 VAC)

Input Current:

520 mA @ 24 VDC

80 mA @ 110 VDC

Standards and Certifications

Safety: UL 508, UL 61010

EMC: EN 61000-6-2/61000-6-4

EMI: CISPR 22, FCC Part 15B Class A

EMS:

IEC 61000-4-2 ESD: Contact: 8 kV; Air: 15 kV

IEC 61000-4-3 RS: 80 MHz to 1 GHz: 10 V/m

IEC 61000-4-4 EFT: Power: 4 kV; Signal: 4 kV

IEC 61000-4-5 Surge: Power 6 kV; Signal: 4 kV

IEC 61000-4-6 CS: 150 kHz to 80 MHz: 10 V/m; Signal: 10 V/m

IEC 61000-4-8 PFMF

IEC 61000-4-11 DIPs

Hazardous Location: UL/cUL Class I Division 2 Groups A/B/C/D

Warranty

Warranty Period: 5 years

Details: See www.moxa.com/warranty

Device Server Specifications

Serial Interface

Number of Ports: 4

Serial Standards: RS-232/422/485

Connector: DB9 male

Serial Line Protection: 2 kV isolation protection

RS-485 Data Direction Control: ADDC® (Automatic Data Direction Control)

Console Port: Dedicated RS-232 console port (10-pin RJ45)

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 and XON/XOFF

Baudrate: 50 bps to 921.6 Kbps

Serial Signals

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

RS-422: Tx+, Tx-, Rx+, Rx-, GND

RS-485-4w: Tx+, Tx-, Rx+, Rx-, GND

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

Software

Configuration Options: Command Line Interface (CLI) through Serial/Telnet/SSH, Web Console (HTTP/HTTPS), Windows Utility

Windows Real COM Drivers: Windows 95/98/ME/NT/2000, Windows XP/2003/Vista/2008/7/8/8.1/10 (x86/x64), Windows 2008 R2/2012/2012 R2 (x64), Windows Embedded CE 5.0/6.0, Windows XP Embedded

Fixed TTY Drivers: SCO Unix, SCO OpenServer, UnixWare 7, QNX 4.25, QNX 6, Solaris 10, FreeBSD, AIX 5.x, HP-UX 11i, Mac OS X

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

Operation Modes: Real COM, TCP Server, TCP Client, UDP, RFC2217, Modbus, DNP3, DNP3 Raw Socket

Management: SNMP MIB-II, IEC 61850 MMS

Reliability

Alert Tools: Built-in buzzer and RTC (real-time clock)

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

MTBF (mean time between failures)

Time: 347,436 hrs

Standard: Telcordia (Bellcore) Standard TR/SR

Ethernet Switch Specifications

Ethernet Interface

Standards:

IEEE 802.3 for 10BaseT

IEEE 802.3u for 100BaseT(X) and 100BaseFX

IEEE 802.3x for Flow Control

IEEE 802.1D for Spanning Tree Protocol

IEEE 802.1w for Rapid STP

IEEE 802.1Q for VLAN Tagging

IEEE 802.1p for Class of Service

IEEE 802.1x for Authentication

IEEE 802.3ad for Port Trunk with LACP

Network Protocols: ICMP, IPv4, TCP, UDP, ARP, RARP, Telnet, DN, HTTP, SMTP, NTP, SNTP, IGMPv1/v2, GVRP, SNMPv1/v2c/v3, DHCP Server/Client, DHCP Option 82, BOOTP, TFTP, GMRP, LACP, RMON

MIB: MIB-II, Ethernet-Like MIB, P-BRIDGE MIB, Q-BRIDGE MIB, Bridge MIB, RSTP MIB, RMON MIB Group 1, 2, 3, 9

Flow Control: IEEE 802.3x flow control, back pressure flow control interface

Switch Properties

Priority Queues: 4

Max. Number of Available VLANs: 64

VLAN ID Range: VID 1 to 4094

IGMP Groups: 256

Cybersecurity: Ready for NERC CIP compliance system development

- Supports IEC 62443 Level 2
- Supports port access control list: MAC, 802.1x authentication
- Supports RADIUS, TACACS+
- Supports Syslog for system/event

Optical Fiber Interface

		100BaseFX		
		Multimode		**Single-mode**
Fiber Cable Type		**OM1**	**50/125 µm**	**G.652**
			800 MHz*km	
Typical Distance		4 km	5 km	40 km
Wavelength	Typical (nm)	1300		1310
	TX Range (nm)	1260 to 1360		1280 to 1340
	RX Range (nm)	1100 to 1600		1100 to 1600
Optical Power	TX Range (dBm)	-10 to -20		0 to -5
	RX Range (dBm)	-3 to -32		-3 to -34
	Link Budget (dB)	12		29
	Dispersion Penalty (dB)	3		1

Note: When connecting a single-mode fiber transceiver, we recommend using an attenuator to prevent damage caused by excessive optical power.

Note: Compute the "typical distance" of a specific fiber transceiver as follows: Link budget (dB) > dispersion penalty (dB) + total link loss (dB).

Switch Interface

RJ45 Ports: 10/100BaseT(X) auto negotiation speed, F/H duplex mode, and auto MDI/MDI-X connection

Alarm Contact: 2 relay outputs with current carrying capacity of 1A @ 24 VDC

EMI and Environmental Type Tests

IEC 61850-3 EMI Immunity Type Tests			**S9450I**
TEST	**Description**		**Test Levels**
IEC 61000-4-2	ESD	Enclosure Contact	+/- 8kV
		Enclosure Air	+/- 15kV
IEC 61000-4-3	Radiated RFI	Enclosure Ports	10 V/m
IEC 61000-4-4	Burst (Fast Transient)	Signal Ports	+/- 4kV @ 2.5kHz
		D.C. Power Ports	+/- 4kV
		A.C. Power Ports	+/- 4kV
		Earth Ground Ports3	+/- 4kV
IEC 61000-4-5	Surge	Signal Ports	L-E : 4KV, L-L : 2KV
		D.C. Power Ports	L-E : 6KV, L-L : 6KV
		A.C. Power Ports	L-E : 6KV, L-L : 6KV

IEC 61850-3 EMI Immunity Type Tests			S9450I
TEST	**Description**		**Test Levels**
IEC 61000-4-6	Induced (Conducted) RFI	Signal Ports	10 V
		D.C. Power Ports	10 V
		A.C. Power Ports	10 V
		Earth Ground Ports	10 V
IEC 61000-4-8	Magnetic Field	Enclosure Ports	100 A/m continuous; 1000A/m for 1 s
IEC 61000-4-29	Voltage Dips & Interrupts	D.C. Power Ports	30% for 0.1s, 60% fpr 0.1s
IEC 61000-4-11	Voltage Dips	A.C. Power Ports	100% for 5 periods
			100% for 50 periods
			60% for 50 periods,
			30% for 1 periods
			100% for 1 periods
IEC 61000-4-12	Dumped Oscillatory	Signal Ports	2.5kV common, 1kV
		D.C. Power Ports	2.5kV common, 1kV
		A.C. Power Ports	2.5kV common, 1kV
IEC 61000-4-16	Mains Frequency Voltage	Signal Ports	30V Continuous, 300V for 1s
		D.C. Power Ports	30V Continuous, 300V for 1s
IEC 61000-4-17	Ripple on D.C. Power Supply	D.C. Power Ports	10%

IEEE 1613 EMI Immunity Type Tests			S9450I
TEST	**Description**		**Test Levels**
IEEE C37.90.3	ESD	Enclosure Contact	+/- 8kV
		Enclosure Air	+/- 15kV
IEEE C37.90.2	Radiated RFI	Enclosure Ports	35 V/m
IEEE C37.90.1	Fast Transient	Signal Ports	+/- 4kV @ 2.5kHz
		D.C. Power Ports	+/- 4kV
		A.C. Power Ports	+/- 4kV
		Earth Ground Ports3	+/- 4kV
IEEE C37.90.1	Oscillatory	Signal Ports	2.5kV Common Mode @ 1MHz
		D.C. Power Ports	2.5kV Common & Differential Mode @ 1MHz
		A.C. Power Ports	2.5kV Common & Differential Mode @ 1MHz
IEEE C37.90	H.V. Impulse	Signal Ports	5kV (Fail-Safe Relay Output)
		D.C. Power Ports	5kV
		A.C. Power Ports	5kV
IEEE C37.90	Dielectric Strength	Signal Ports	2kVAC
		D.C. Power Ports	1.5kVDC
		A.C. Power Ports	2kVAC

2

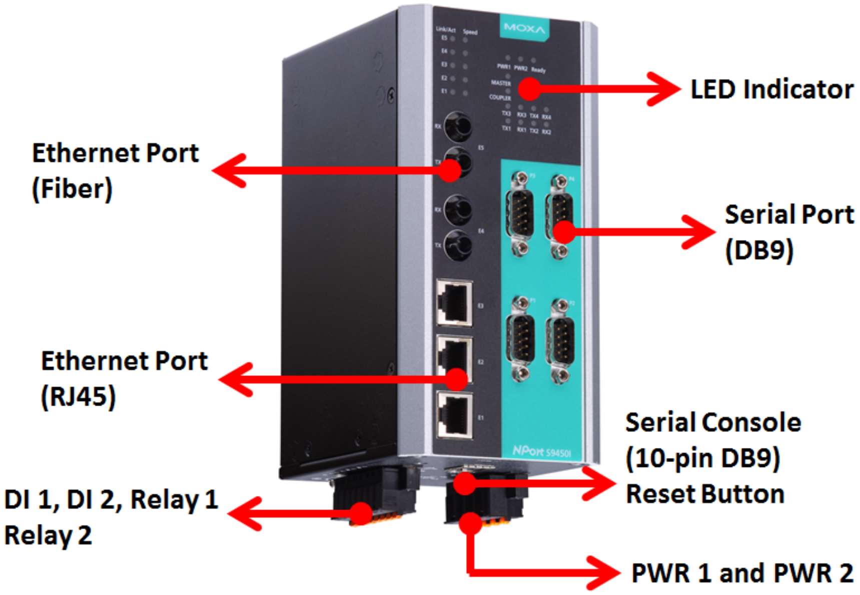
Getting Started

This chapter details the installation of NPort S9000 series device servers. Note that the manual uses the NPort S9000 series as an example to illustrate the functionality of NPort S9000 series in chapters 2, 3, 4, 5, 6, 7 and 8.

The following topics are covered in this chapter:

- ❒ **Panel Layout**
- ❒ **Dimensions**
  - ➢ NPort S9450I Series
- ❒ **Connecting the Hardware**
  - ➢ Wiring Requirements
  - ➢ Connecting the Power
  - ➢ Connecting to the Network
  - ➢ Connecting to a Serial Device
  - ➢ LED Indicators
  - ➢ Wiring the Relay Contact
  - ➢ Wiring the Digital Inputs
  - ➢ Cybersecurity Considerations

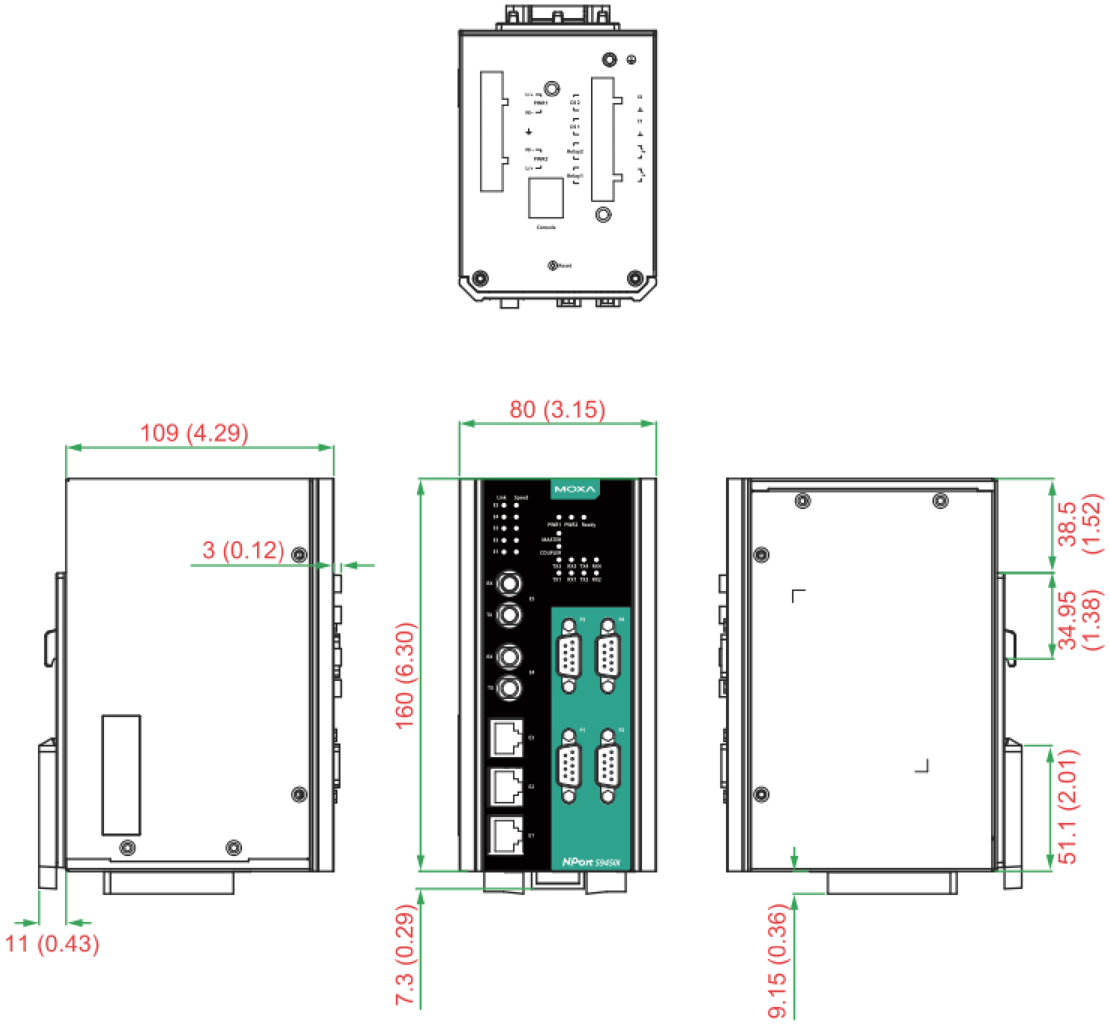
Panel Layout



NPort S9450I Series

Dimensions

NPort S9450I Series



Connecting the Hardware

This section describes how to connect the NPort S9000 to serial devices for initial testing purposes. We cover **Wiring Requirements**, **Connecting the Power**, **Grounding the NPort S9000**, **Connecting to the Network**, **Connecting to a Serial Device**, and **LED Indicators**.

Wiring Requirements

ATTENTION

Safety First!

Be sure to disconnect the power cord before installing and/or wiring your NPort S9000.

Wiring Caution!

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

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

Temperature Caution!

Please take care when handling the NPort S9000. When plugged in, the NPort S9000's internal components generate heat; consequently, the casing may be too hot to touch.

You should heed the following:

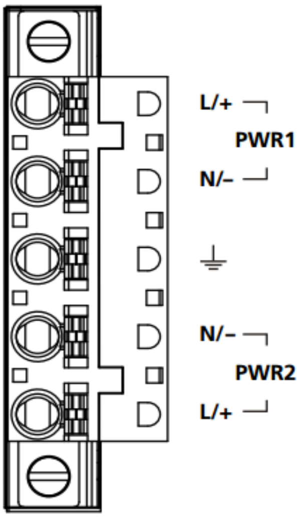
- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
  NOTE: Do not run signal or communication wiring and power wiring in the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
- You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- Keep input wiring and output wiring separate.
- Where necessary, it is strongly advised that you label wiring to all devices in the system.

Connecting the Power

Connect the power line with the NPort S9000's terminal block. If the power is properly supplied, the "Ready" LED will show a solid red color until the system is ready, at which time the "Ready" LED will change to green.

Take the following steps to wire the redundant power inputs:

1. Insert the negative/positive DC wires into the V-/V+ terminals.
2. To keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.
3. Insert the plastic terminal block connector prongs into the terminal block receptor.



NPort S9450I's bottom panel

Connecting to the Network

Connect one end of the Ethernet cable to the NPort S9000's 10/100M Ethernet port and the other end of the cable to the Ethernet network. If the cable is properly connected, the NPort S9000 will indicate a valid connection to the Ethernet in the following ways:

- The Ethernet LED maintains a solid green color when connected to a 100 Mbps Ethernet network.
- The Ethernet LED will flash when Ethernet packets are being transmitted or received.

Connecting to a Serial Device

Connect the serial data cable between the NPort S9000 and the serial device.

LED Indicators

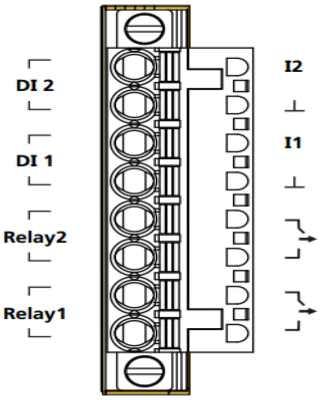
The LED indicators of NPort S9000 series are described in the following table.

Type	Color	Meaning
PW 1	Green	Power 1 input
PW 2	Green	Power 2 input
Ready	Red	Steady On: Power is on, and the NPort is booting up. Blinking: Indicates a LAN-IP conflict, or the DHCP or BOOTP server did not respond properly.
	Green	Steady On: Power is on, and the NPort is functioning normally. Blinking: The device server has been located by the DSU's (Device Search Utility) location function.
	Off	Power is off, or a power error condition exists.
Master	Green	Steady On: When the NPort is the Master of this Turbo Ring. Blinking: When the NPort is the Ring Master of this Turbo Ring and the Turbo Ring is disconnected.
Coupler	Green	When the NPort enables the coupling function to form a backup path
E1…E5		
Link	Green	Steady On: The Ethernet port is active. Blinking: When the Ethernet port is transmitting/receiving data.
Speed	Green	Steady On: 100 Mbps Ethernet connection.
	Yellow	Steady On: 10 Mbp Ethernet connection.
TX1…TX4	Green	The serial port is transmitting data.
RX1…RX4	Amber	The serial port is receiving data.

Wiring the Relay Contact

The NPort S9450I series has two sets of relay output: relay 1 and relay 2. Each relay contact consists of two contacts of the terminal block on the NPort S9450I's bottom panel. Refer to the next section for detailed instructions on how to connect the wires to the terminal block connector and how to attach the terminal block connector to the terminal block receptor.

The two contacts used to connect the relay contacts work as follow (illustrated below):



The fault circuit will open if

1. A relay warning event is triggered,

   OR

2. The NPort S9450I is the Master of this Turbo Ring, and the Turbo Ring is broken,

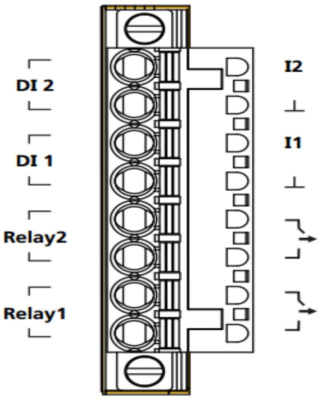
   OR

3. Start-up failure.

If none of these three conditions are met, the fault circuit will remain closed.

Wiring the Digital Inputs

The NPort S9450I unit has two sets of digital inputs: DI 1 and DI 2. Each DI consists of two contacts of the 6-pin terminal block connector on the NPort S9450I's top panel. The remaining contacts are used for the NPort S9450I's two DC inputs. The top and front views of one of the terminal block connectors are shown below.



Take the following steps to wire the digital inputs:

1. Insert the negative (ground)/positive DI wires into the ⊥/I1 terminals.
2. To keep the DI wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.
3. Insert the plastic terminal block connector prongs into the terminal block receptor, which is located on the NPort S9450I's top panel.

Cybersecurity Considerations

Security recommendations

With cyberattacks growing in number and sophistication, network device vendors are adding functions geared towards protecting sensitive business and personal information. Besides these devices that support those protective functions, network managers can follow a number of recommendations to protect their network and devices.

To prevent unauthorized access to a device, follow these recommendations:

- The device should be operated inside a secure network, protected by a firewall or router that blocks attacks via the Internet.
- Use your own passwords for the users of the devices. If possible, also change the default name of the account, for example, don't name admin group "admin" before the device is deployed.
- Use strong passwords. The devices support a function to check if the passwords are strong enough. You can enable the function to help you check whether the passwords are strong enough.

- Enable 802.1X or TACACS+ service for user authentication, which supports central management for the user accounts.
- Control the access to the serial console as any physical access to the device.
- Only enable the services that will be used on the device.
- If SNMP is enabled, remember to change the default community names and also set SNMP to send a trap if authentication failures happen.
- Avoid using insecure services such as Telnet and TFTP; the best way is to disable them completely.
- Limit the number of simultaneous Web Server, Telnet and SSH sessions allowed.
- Backup the configuration files periodically and compare the configurations to make sure the devices work properly.
- Audit the devices periodically to make sure they comply with these recommendations and/or any internal security policies.
- If there is a need to return the unit to Moxa, make sure encryption is disabled and you had already backup the current configuration before returning it.

Available Services by Port

The following table lists the services available by the device server, including the following information:

Process Name: The service supported by the device
Option: If the service can enabled/disabled, or it may be always enabled
Type: Is the service working on TCP or UDP port
Port Number: The port number associated with the service
Description: The purpose for enabling this service

Process Name	Option	Type	Port Number	Description
DSCI	**Enable/Disable**	TCP	4900	**For Utility communication**
		UDP	4800	
Dns_wins	Always Enable	UDP	53, 137, 949	Processing DNS & WINS (Client) Data
SNMP	Enable/Disable	UDP	161	SNMP Handle routine
RIPD_PORT	Always Enable	UDP	520, 521	RIP/RIPng handle routine
Http	Enable/Disable	TCP	80	Web console
Https	Enable/Disable	TCP	443	Secure web console
SSH	Enable/Disable	TCP	22	SSH console
Telnet	Enable/Disable	TCP	23	Telnet console
MMS	Enable/Disable	TCP	102	MMS Service
FTP	Enable/Disable	TCP	20, 21	For system file update
Radius	Enable/Disable	UDP	User Define(default: 1812)	Authentication Server
Tacacs+	Enable/Disable	UDP	User Define(default: 49)	Authentication Server
DHCP	Always Enable	UDP	68	
SNTP	Enable/Disable	UDP	Random Port	
Remote System Log	Enable/Disable	UDP	Random Port	
OPMode				
Real COM Mode	Enable/Disable	TCP	950+(Serial Port NO. - 1) 966+(Serial Port NO. - 1)	
RFC2217 Mode	Enable/Disable	TCP	User Define(default: 4000+Serial Port NO.)	
TCP Server Mode	Enable/Disable	TCP	User Define(default: 4000+Serial Port NO.) User Define(default: 966+Serial Port NO.)	
UDP Mode	Enable/Disable	UDP	User Define(default: 4000+Serial Port NO.)	
DNP3	Enable/Disable	TCP	User Define(default: 20000)	
DNP3 Raw Socket	Enable/Disable	TCP	User Define(default: 4000+Serial Port NO.)	
Modbus	Enable/Disable	TCP	User Define(default: 502)	

3

Initial IP Address Configuration

When setting up the NPort S9000 for the first time, the first thing you should do is configure its IP address. This chapter introduces the different methods that can be used.

The following topics are covered in this chapter:

- **Static and Dynamic IP Addresses**
- **Factory Default IP Address**
- **Configuration Options**
  - Web Console
  - ARP
  - SSH Console
  - Serial Console

Static and Dynamic IP Addresses

Determine whether your NPort S9000 needs to use a static IP or dynamic IP address (either DHCP or BOOTP application).

- ***If your NPort S9000 is used in a static IP environment***, you will assign a specific IP address using one of the tools described in this chapter.
- ***If your NPort S9000 is used in a dynamic IP environment***, the IP address will be assigned automatically over the network. In this case, set the IP configuration mode to DHCP, BOOTP.

ATTENTION

Consult your network administrator on how to reserve a fixed IP address for your NPort S9000 in the MAC-IP mapping table when using a DHCP server or BOOTP server. For most applications, you should assign a fixed IP address to your NPort S9000.

Factory Default IP Address

The NPort S9000 is configured with the following default private IP address:

192.168.127.254

Note that IP addresses that begin with "192.168" are referred to as private IP addresses. Devices configured with a private IP address are not directly accessible from a public network. For example, you would not be able to ping a device with a private IP address from an outside Internet connection. If your application requires sending data over a public network, such as the Internet, your NPort S9000 will need a valid public IP address, which can be leased from a local Internet service provider (ISP).

Configuration Options

Web Console

You may configure your NPort S9000 using a standard web browser. Please refer to chapters 6, 7, and 8 for details on how to access and use the NPort S9000 web console.

ARP

You may use the ARP (Address Resolution Protocol) command to set up an IP address for your NPort S9000. The ARP command tells your computer to associate the NPort S9000's MAC address with an IP address. Afterwards, use Telnet to access the NPort S9000, and its IP address will be reconfigured.

ATTENTION

In order to use the ARP setup method, both your computer and the NPort S9000 must be connected to the same LAN. Alternatively, you may use a crossover Ethernet cable to connect the NPort S9000 directly to your computer's Ethernet card. Before executing the ARP command, your NPort S9000 must be configured with the factory default IP address (192.168.127.254), and your computer and the NPort S9000 must be on the same subnet.

To use ARP to configure the IP address, complete the following:

1. Obtain a valid IP address for your NPort S9000 from your network administrator.
2. Obtain your NPort S9000's MAC address from the label on the bottom panel.

3. Execute the arp -s command from your computer's MS-DOS prompt as follows:

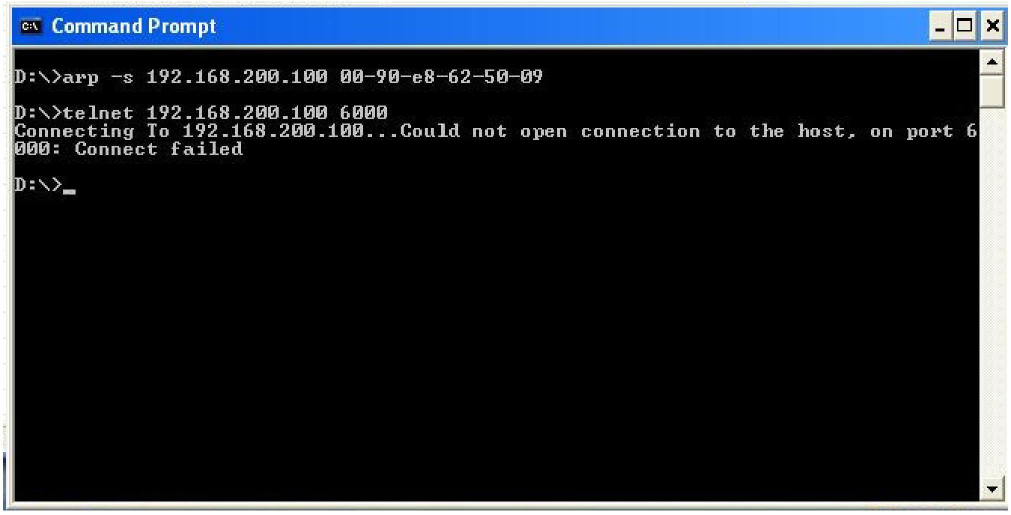
   arp -s <*IP address***> <***MAC address***>**

   For example,
   C:\> **arp -s 192.168.200.100 00-90-E8-04-00-11**

4. Next, execute a special Telnet command by entering the following exactly:

   telnet 192.168.200.100 6000

   When you enter this command, a **Connect failed** message will appear, as shown below.



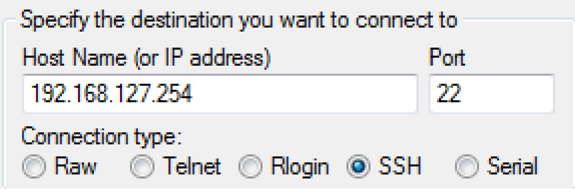
```
D:\>arp -s 192.168.200.100 00-90-e8-62-50-09

D:\>telnet 192.168.200.100 6000
Connecting To 192.168.200.100...Could not open connection to the host, on port 6
000: Connect failed

D:\>_
```

5. After the NPort S9000 reboots, its IP address will be assigned to the new address, and you can reconnect using Telnet to verify that the update was successful.

SSH Console

Depending on how your computer and network are configured, you may find it convenient to use network access to set up your NPort S9000's IP address. This can be done using Telnet.

1. It's easy to find SSH client software on the Internet. Please download, install and execute it and input the destination NPort's IP and the TCP port to accept the SSH session.



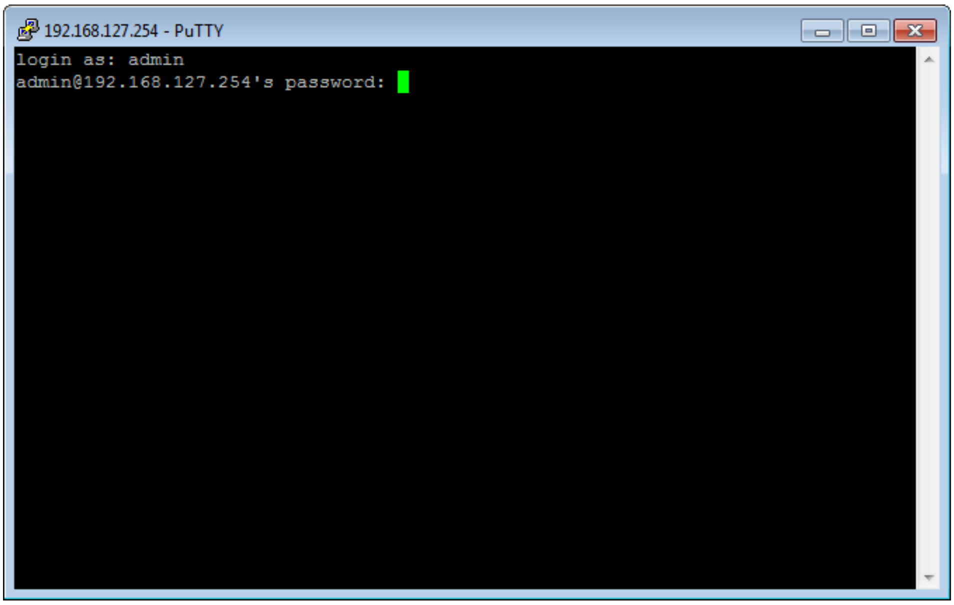
Specify the destination you want to connect to

Host Name (or IP address): 192.168.127.254

Port: 22

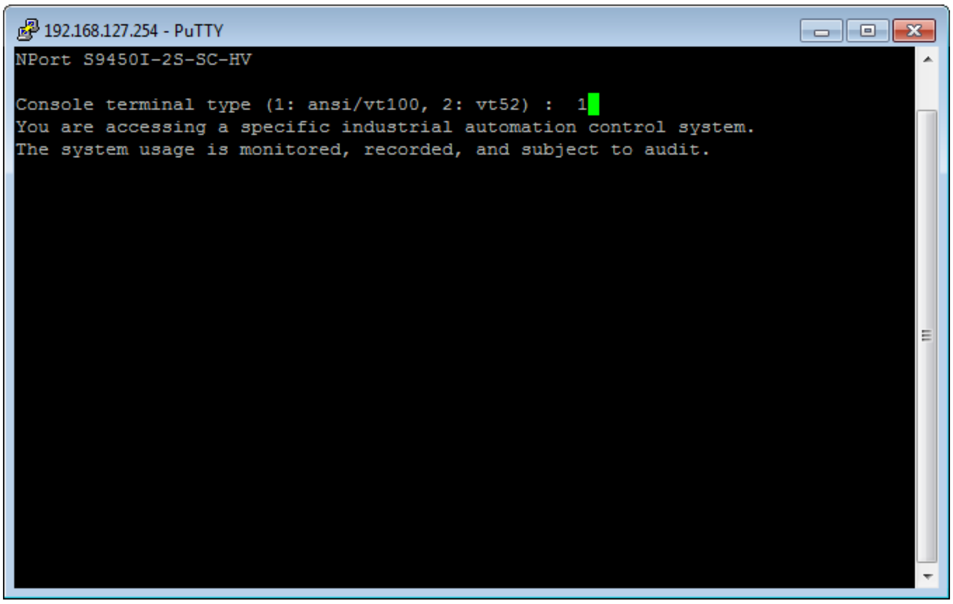
Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

2. The console terminal type selection is displayed as shown. Enter the username and password to log in to the SSH console. The default username and password are **admin** and **moxa**, respectively.



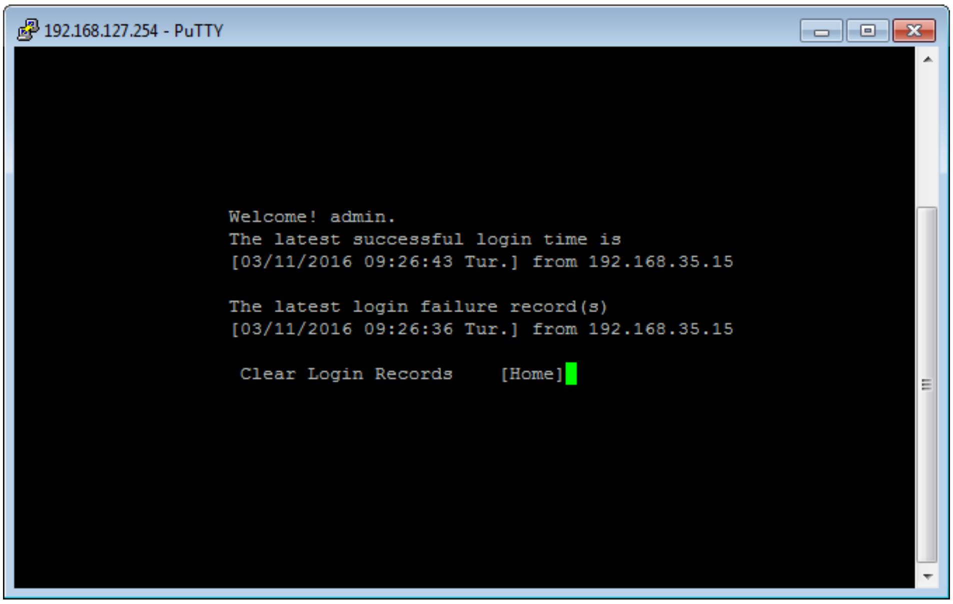
```
login as: admin
admin@192.168.127.254's password:
```

3. Enter **1** for **ansi/vt100** and press **ENTER** to continue.



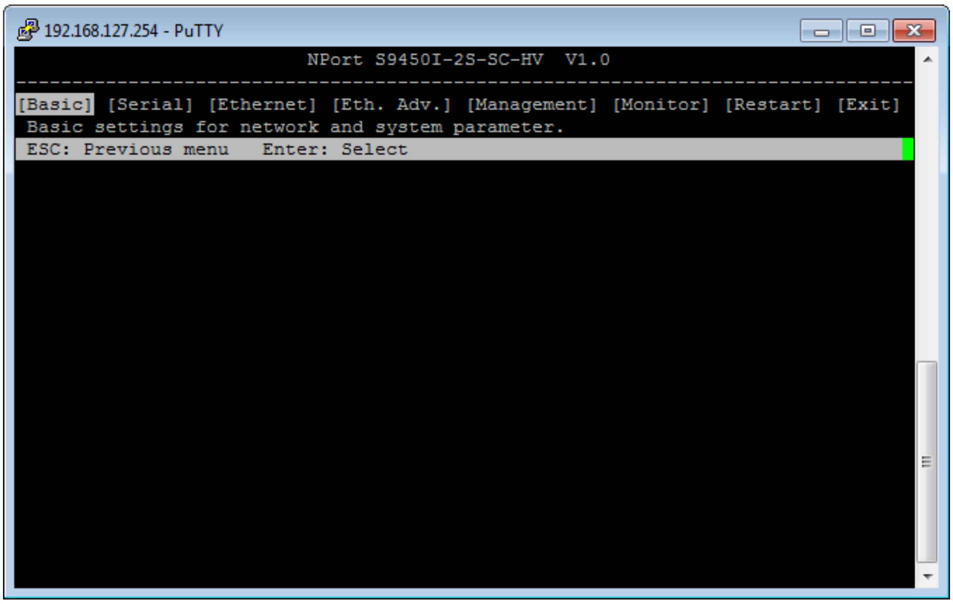
```
NPort S9450I-2S-SC-HV

Console terminal type (1: ansi/vt100, 2: vt52) :  1
You are accessing a specific industrial automation control system.
The system usage is monitored, recorded, and subject to audit.
```

4. The console will show a welcome message (which can be modified), the last successful login, and the last three failed login records. Press **ENTER** to continue.



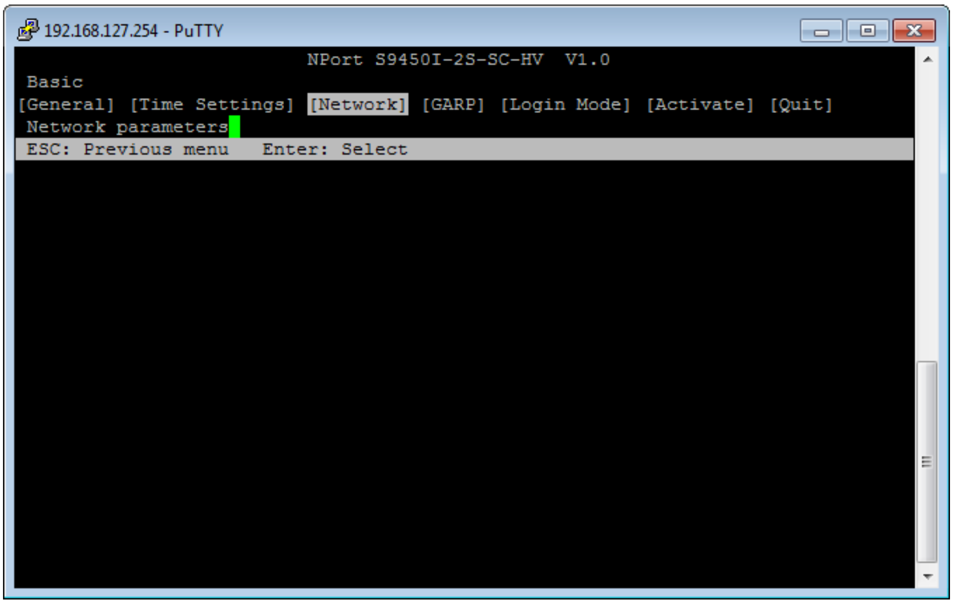
```
Welcome! admin.
The latest successful login time is
[03/11/2016 09:26:43 Tur.] from 192.168.35.15

The latest login failure record(s)
[03/11/2016 09:26:36 Tur.] from 192.168.35.15

 Clear Login Records    [Home]
```

5. Press **B**, or use the arrow keys to select **Basic** and then press **ENTER** to configure Basic settings.



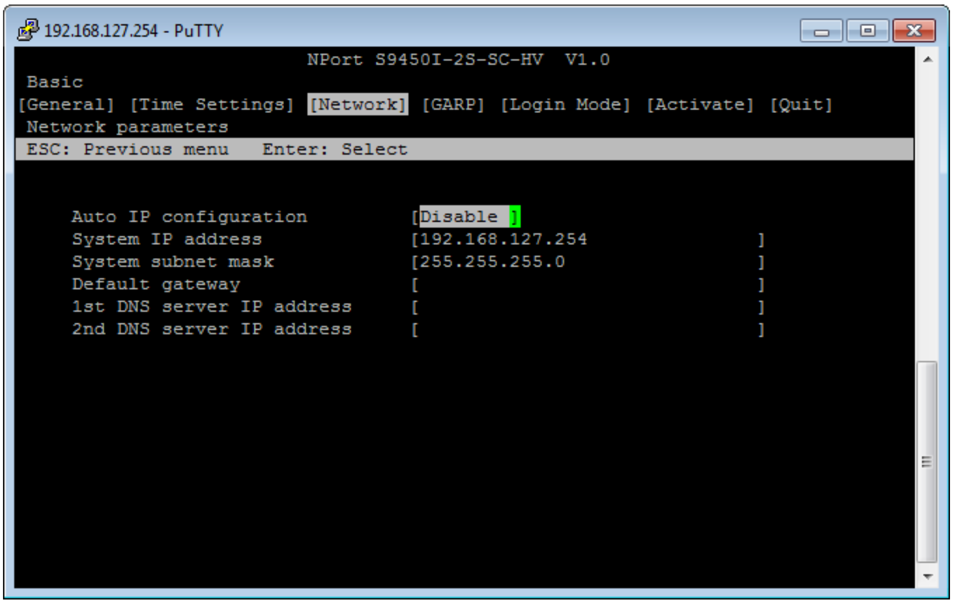
```
                          NPort S9450I-2S-SC-HV  V1.0
--------------------------------------------------------------------------------
[Basic] [Serial] [Ethernet] [Eth. Adv.] [Management] [Monitor] [Restart] [Exit]
 Basic settings for network and system parameter.
 ESC: Previous menu   Enter: Select
```

6. Press **N**, or use the arrow keys to select network and then press **ENTER** to configure Network parameters.



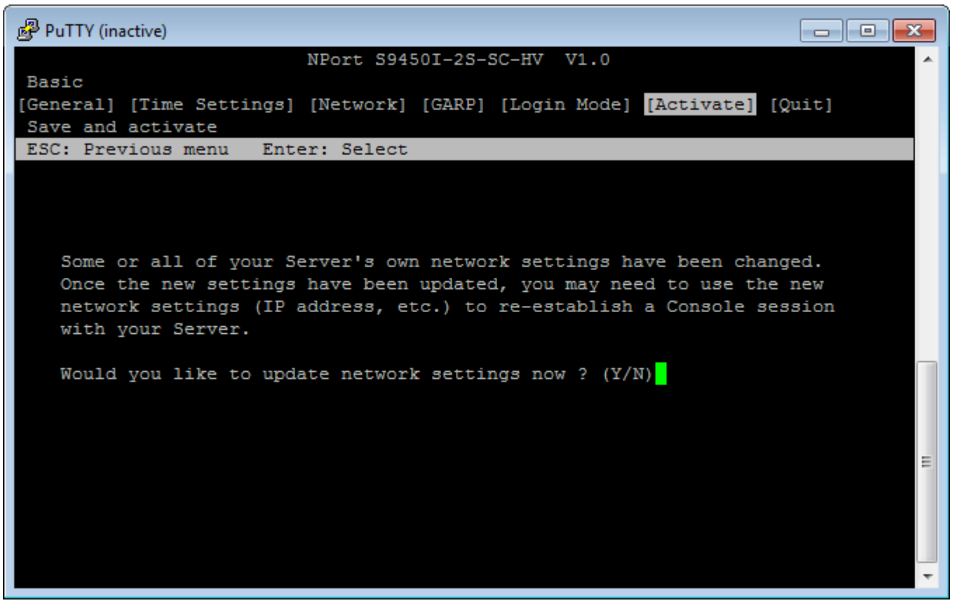
```
                              NPort S9450I-2S-SC-HV  V1.0
 Basic
[General] [Time Settings] [Network] [GARP] [Login Mode] [Activate] [Quit]
 Network parameters
 ESC: Previous menu    Enter: Select
```

7. Use the arrow keys to move the cursor to System IP address. Use the **Delete**, **Backspace**, or **Space** key to erase the current IP address, and then type in the new IP address and press **Enter**. If you are using a dynamic IP configuration (BOOTP or DHCP), you will need to go to the Auto IP configuration field and press **Enter** to select the appropriate configuration.



```
                              NPort S9450I-2S-SC-HV  V1.0
 Basic
[General] [Time Settings] [Network] [GARP] [Login Mode] [Activate] [Quit]
 Network parameters
 ESC: Previous menu    Enter: Select


     Auto IP configuration          [Disable ]
     System IP address              [192.168.127.254               ]
     System subnet mask             [255.255.255.0                 ]
     Default gateway                [                              ]
     1st DNS server IP address      [                              ]
     2nd DNS server IP address      [                              ]
```

8. Press **Esc** to return to the previous page. Select **Activate** and press **Y** to confirm the modification and activate the new settings.



```
                              NPort S9450I-2S-SC-HV  V1.0
 Basic
[General] [Time Settings] [Network] [GARP] [Login Mode] [Activate] [Quit]
 Save and activate
 ESC: Previous menu    Enter: Select



    Some or all of your Server's own network settings have been changed.
    Once the new settings have been updated, you may need to use the new
    network settings (IP address, etc.) to re-establish a Console session
    with your Server.

    Would you like to update network settings now ? (Y/N)
```

Serial Console

The NPort S9000 supports configuration through the serial console, which is the same as the Telnet console but accessed through the RS-232 console port rather than through the network. Once you have entered the serial console, the configuration options and instructions are the same as if you were using the Telnet console.

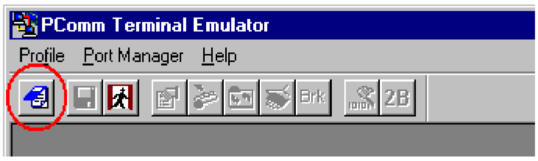
The following instructions and screenshots show how to enter the serial console using PComm Terminal Emulator, which is available free of charge as part of the PComm Lite suite. You may use a different terminal emulator utility, although your actual screens and procedures may vary slightly from the following instructions.

1. Use the serial console cable in the box to connect the NPort S9000's serial console port to your computer's male RS-232 serial port.

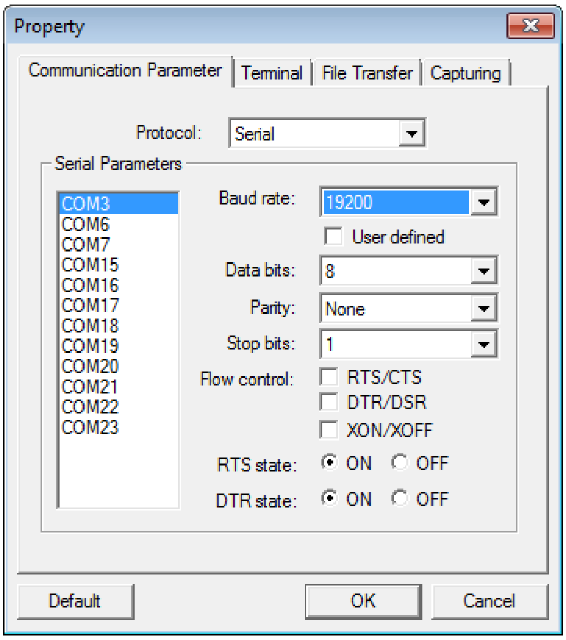
ATTENTION

The NPort S9000 has a dedicated serial console port.

2. From the Windows desktop select **Start → All Programs → PComm Lite → Terminal Emulator**.
3. The PComm Terminal Emulator window should appear. From the **Port Manager** menu, select **Open**, or simply click the **Open icon** as shown below:



4. The Property window opens automatically. Select the **Communication Parameter** tab, and then select the appropriate COM port for the connection (COM1 in this example). Configure the parameters for **19200, 8, N, 1** (**19200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits).



Protocol: Serial

Baud rate: 19200

□ User defined

Data bits: 8

Parity: None

Stop bits: 1

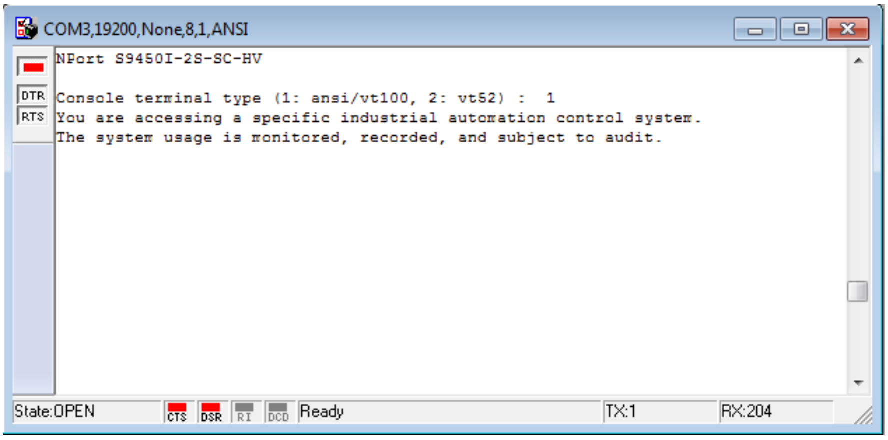
Flow control: □ RTS/CTS □ DTR/DSR □ XON/XOFF

RTS state: ● ON ○ OFF

DTR state: ● ON ○ OFF

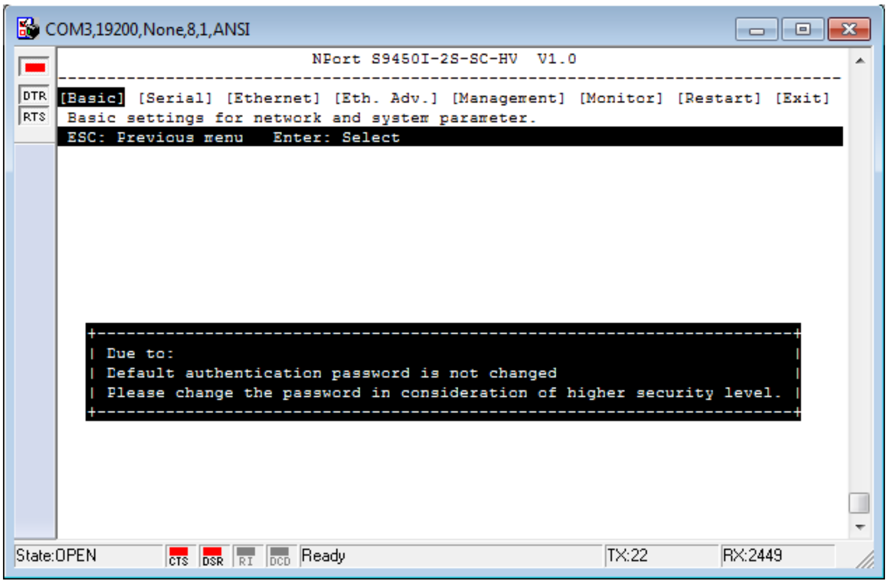
5. From the Property window's Terminal page, select **ANSI** or **VT100** for **Terminal Type** and click **OK**. The NPort S9000 will then automatically switch from data mode to console mode.

6. Press **Enter** then the message will pop up and Press 1 for ansi/vt100 and then press ENTER.



```
NPort S9450I-2S-SC-HV

Console terminal type (1: ansi/vt100, 2: vt52) :  1
You are accessing a specific industrial automation control system.
The system usage is monitored, recorded, and subject to audit.
```

7. Enter the username and password to log in to the console. The default username and password are admin and moxa, respectively. After showing the welcome message, the main menu should come up. Once you are in the console, you may configure the IP address through the **Network** menu item, just as with the Telnet console. Please refer to steps 4 to 8 in the *Telnet Console* section to complete the initial IP configuration.



```
                          NPort S9450I-2S-SC-HV  V1.0
--------------------------------------------------------------------------------
[Basic] [Serial] [Ethernet] [Eth. Adv.] [Management] [Monitor] [Restart] [Exit]
 Basic settings for network and system parameter.
 ESC: Previous menu   Enter: Select



   +-----------------------------------------------------------------------+
   | Due to:                                                               |
   | Default authentication password is not changed                        |
   | Please change the password in consideration of higher security level. |
   +-----------------------------------------------------------------------+
```

4

Choosing the Serial Operation Mode

In this chapter, we describe the various serial operation modes of the NPort S9000. The options include an operation mode that uses a driver installed on the host computer and operation modes that rely on TCP/IP socket programming concepts. After choosing the proper operation mode in this chapter, refer to Chapter 5 for detailed configuration parameter definitions.

The following topics are covered in this chapter:

Overview

The device server function of the NPort S9000 enables network operation of traditional RS-232/422/485 devices, in which a device server is a tiny computer equipped with a CPU, real-time OS, and TCP/IP protocols that can bidirectionally translate data between the serial and Ethernet formats. Your computer can access, manage, and configure remote facilities and equipment over the Internet from anywhere in the world.

Traditional SCADA and data collection systems rely on serial ports (RS-232/422/485) to collect data from various kinds of instruments. Since the NPort S9000 networks instruments are equipped with an RS-232/422/485 communication port, your SCADA and data collection system will be able to access all instruments connected to a standard TCP/IP network, regardless of whether the devices are used locally or at a remote site.

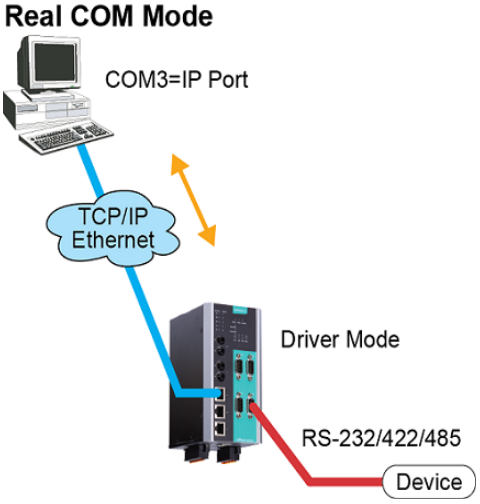
The NPort S9000 is an external IP-based network device that allows you to expand the number of serial ports for a host computer on demand. As long as your host computer supports the TCP/IP protocol, you won't be limited by the host computer's bus limitation (such as ISA or PCI), or lack of drivers for various operating systems.

In addition to providing socket access, the NPort also comes with a Real COM/TTY driver that transmits all serial signals intact. This means that your existing COM/TTY-based software can be preserved, without needing to invest in additional software.

Three different Socket Modes are available: TCP Server, TCP Client, and UDP Server/Client. 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 a speedier delivery. UDP also allows multicasting of data to groups of IP addresses.

Real COM Mode

The NPort S9000 comes equipped with COM drivers that work with Windows 9x/NT/2000/XP/2003/Vista/2008/7/8/8.1/10 (all x86/x64) systems, and also TTY drivers for Linux and Unix systems. The driver establishes a transparent connection between the host and serial device by mapping the IP port of the NPort's serial port to a local COM/TTY port on the host computer. This operation mode also supports up to eight simultaneous connections, so that multiple hosts can collect data from the same serial device at the same time.



The important point is that Real COM Mode allows users to continue using RS-232/422/485 serial communications software that was written for pure serial communications applications. The driver intercepts data sent to the host's COM port, packs it into a TCP/IP packet, and then redirects it through the host's Ethernet card. At the other end of the connection, the NPort accepts the Ethernet frame, unpacks the TCP/IP packet, and then transparently sends it to the appropriate serial device attached to one of the NPort's serial ports.

For more information about installing the driver and how Real COM Mode runs, refer to Chapter 5 for details.

ATTENTION

Real COM Mode allows several hosts to have access control over the same NPort. The driver that comes with your NPort controls the host's access to attached serial devices by checking the host's IP address. Modify the Accessible IP Setting table when the legal IP address is required in your application

RFC2217 Mode

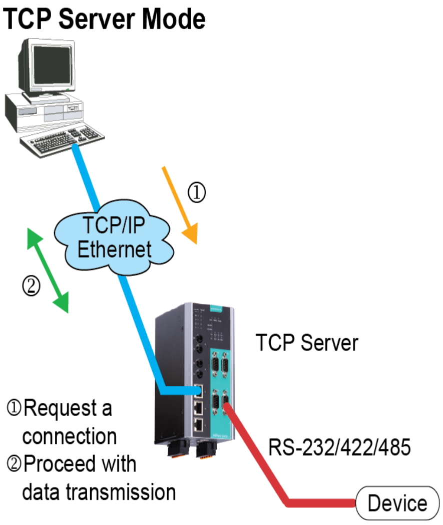
RFC-2217 mode is similar to Real COM mode. That is, a driver is used to establish a transparent connection between a host computer and a serial device by mapping the serial port on the NPort S9000 to a local COM port on the host computer. RFC2217 defines general COM port control options based on the Telnet protocol. Third-party drivers supporting RFC-2217 are widely available on the Internet and can be used to implement Virtual COM mapping to your NPort S9000 serial port(s).

TCP Server Mode

In TCP Server mode, the NPort S9000 provides a unique IP port address on a TCP/IP network. The NPort S9000 waits passively to be contacted by the host computer, allowing the host computer to establish a connection with and get data from the serial device. This operation mode also supports up to eight simultaneous connections, so that multiple hosts can collect data from the same serial device at the same time.

As illustrated in the figure, data transmission proceeds as follows:

1. The host requests a connection from the NPort configured for TCP Server Mode.
2. Once the connection is established, data can be transmitted in both directions—from the host to the NPort, and from the NPort to the host.

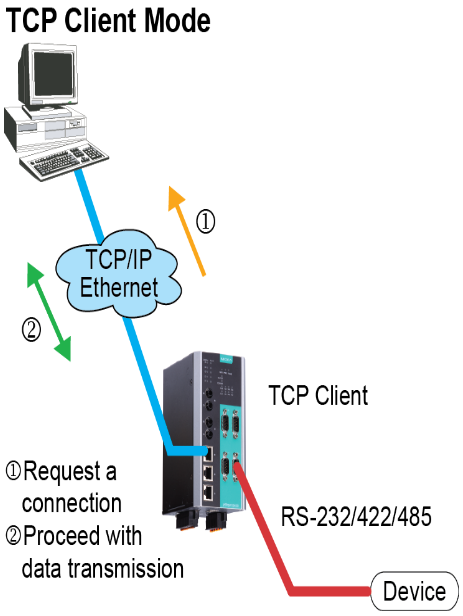


TCP Client Mode

In TCP Client mode, the NPort S9000 can actively establish a TCP connection to a predefined host computer when serial data arrives.
After the data has been transferred, the NPort S9000 can automatically disconnect from the host computer by using the **TCP alive check time** or **Inactivity time** settings. Refer to chapter 5 for more details.

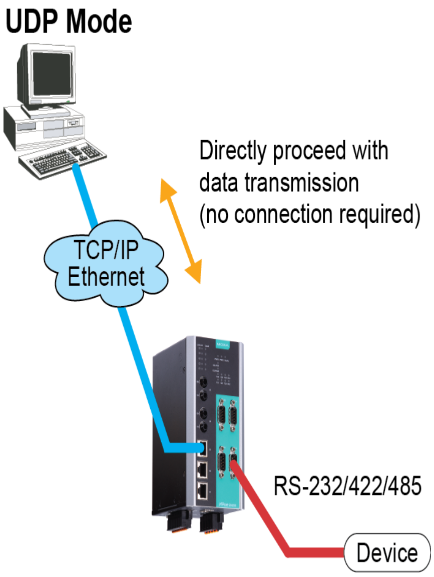
As illustrated in the figure, data transmission proceeds as follows:

1. The NPort configured for TCP Client Mode requests a connection from the host.
2. Once the connection is established, data can be transmitted in both directions—from the host to the NPort, and from the NPort to the host.



UDP Mode

Compared to TCP communication, UDP is faster and more efficient. In UDP mode, you can multicast data from the serial device to multiple host computers, and the serial device can also receive data from multiple host computers, making this mode ideal for message display applications.


UDP Mode
Directly proceed with data transmission (no connection required)
TCP/IP Ethernet
RS-232/422/485
Device

The NPort S9000 series also can be a gateway to support three kinds of communication protocols: DNP3, DNP3 Raw Socket and Modbus. For the NPort S9000 series, each serial port can be set to different protocols.

DNP3 Mode

In DNP3 mode, the NPort S9000 series convert DNP3 serial to DNP3 IP through the Ethernet interface.

DNP3 Raw Socket Mode

In DNP3 Raw Socket mode, it provides TCP server mode and TCP client mode to transmit raw data from the serial device to the Ethernet network.

Modbus Mode

In Modbus mode, the NPort S9000 series converts Modbus RTU/ASCII to Modbus TCP through the Ethernet interface.

Disabled Mode

When the Operation Mode for a particular port is set to **Disabled**, the port will be disabled.

5

Use Real COM mode to communicate with serial devices

The following topics are covered in this chapter:

Overview

The Documentation & software CD included with your NPort S9000 is designed to make the installation and configuration procedure easy and straightforward. This auto-run CD includes the Device Search Utility (DSU) (to broadcast search for all NPort S9000 accessible over the network and firmware upgrade), NPort driver for Windows and Linux platforms (for COM mapping), and the NPort S9000 User's Manual.

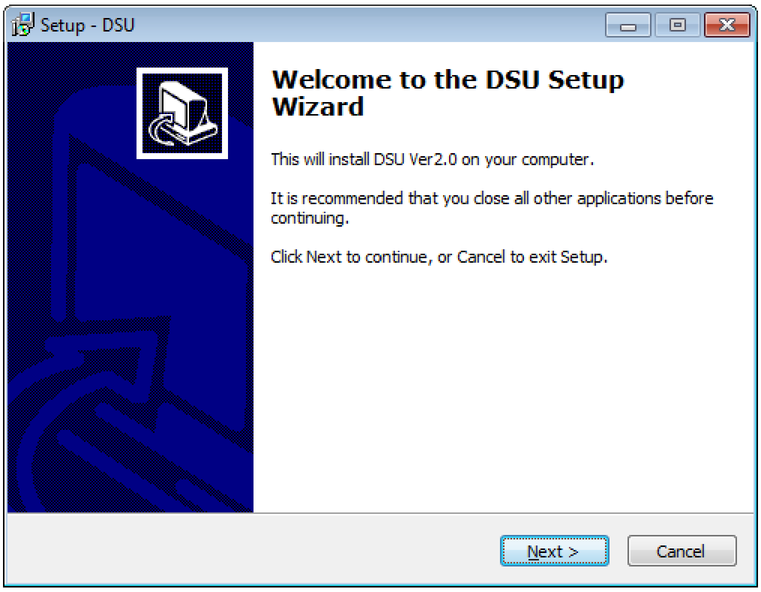
This chapter will instruct you on how to install the necessary software and provide the steps to mapping virtual COM port to help user's software keep working as usual.

1. Install the Device Search Utility to find the specific NPort on the Ethernet network.
2. Log in to the Web console to configure the device to work on Real COM mode.
3. Install the NPort driver and mapping COM port.
4. The original utility can open the COM port to transmit/receive data to/from the serial device.

Device Search Utility

Installing the Device Search Utility

1. Click the **INSTALL UTILITY** button in the NPort Installation CD auto-run window to install the NPort Search Utility. Once the program starts running, click **Yes** to proceed.
2. Click **Settings** when the Welcome screen opens, to proceed with the installation.



Setup - DSU

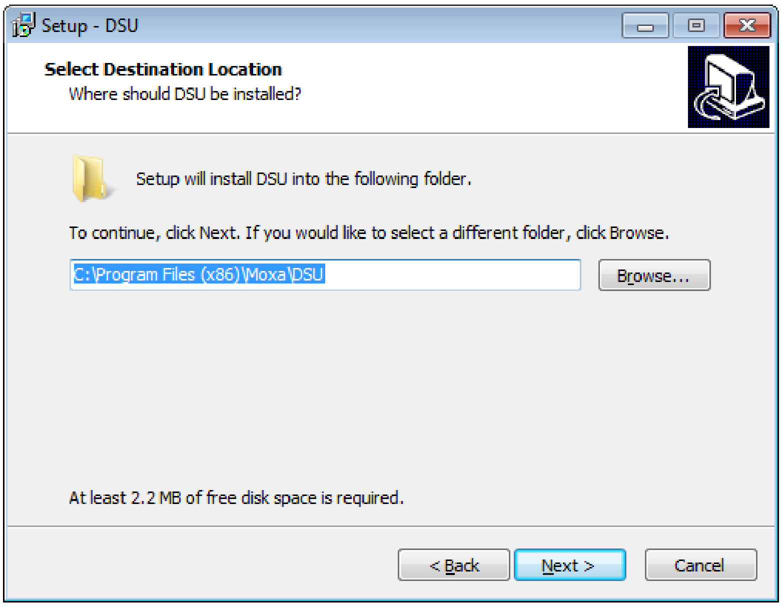
Welcome to the DSU Setup Wizard

This will install DSU Ver2.0 on your computer.

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

Click Next to continue, or Cancel to exit Setup.

3. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



Setup - DSU

Select Destination Location

Where should DSU be installed?

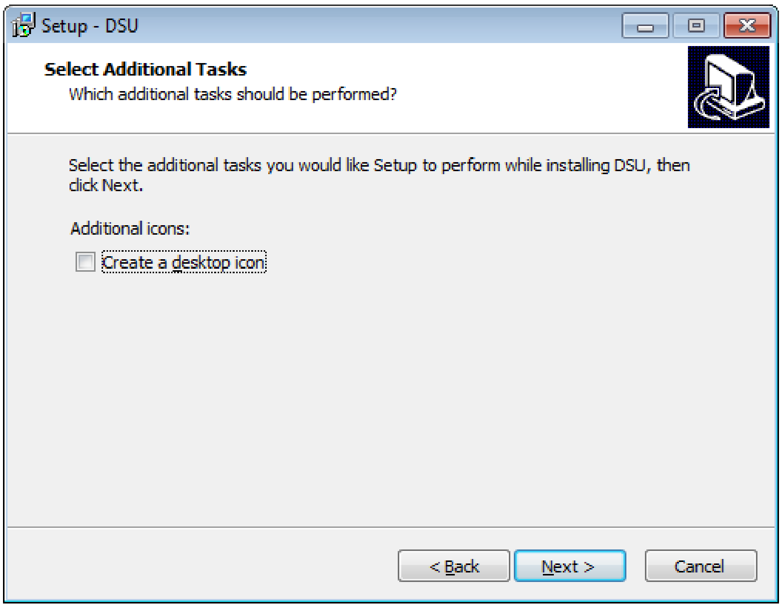
Setup will install DSU into the following folder.

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

C:\Program Files (x86)\Moxa\DSU

At least 2.2 MB of free disk space is required.

4. Check the checkbox if you want the DSU to create a desktop icon, or just click **Next** to install the program's shortcuts in the appropriate Start Menu folder.



Setup - DSU

Select Additional Tasks

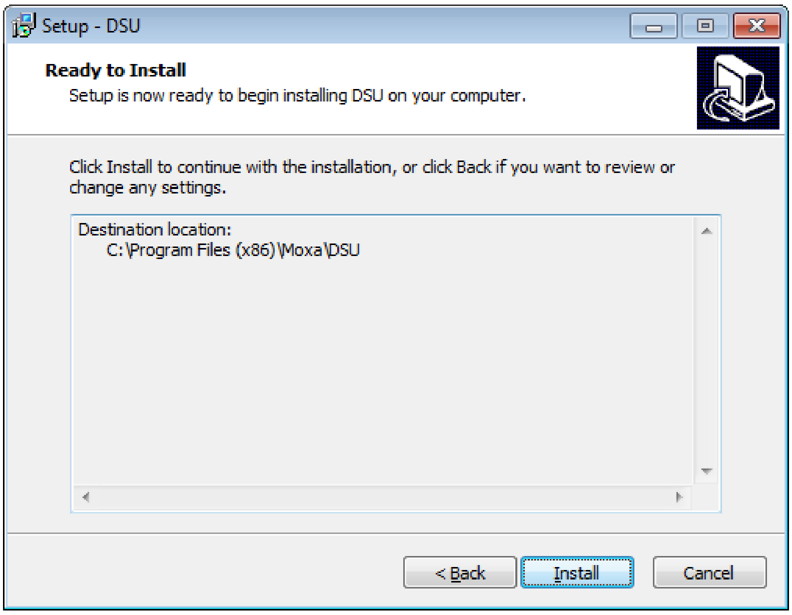
Which additional tasks should be performed?

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

Additional icons:

□ Create a desktop icon

5. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.

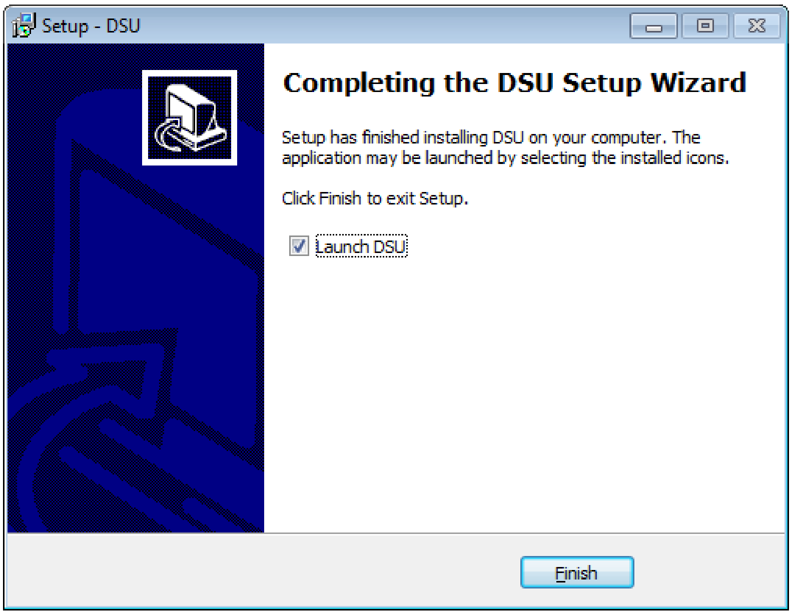


Ready to Install
Setup is now ready to begin installing DSU on your computer.

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

Destination location:
C:\Program Files (x86)\Moxa\DSU

6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.
7. Click **Finish** to complete the installation of the NPort Search Utility.



Completing the DSU Setup Wizard

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

Click Finish to exit Setup.

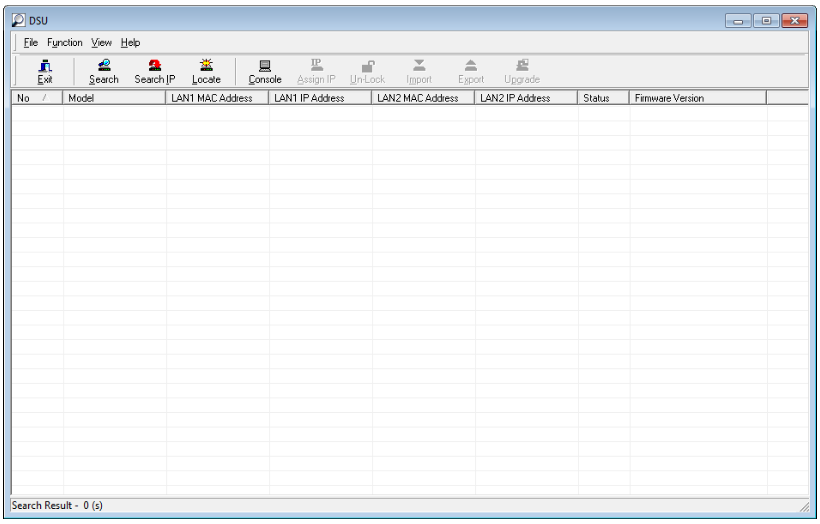
☑ Launch DSU

Find a Specific NPort on the Ethernet Network via the DSU

The Broadcast Search function is used to locate all the NPort S9000 servers that are connected to the same LAN as your computer. After locating an NPort S9000, you will be able to change its IP address.

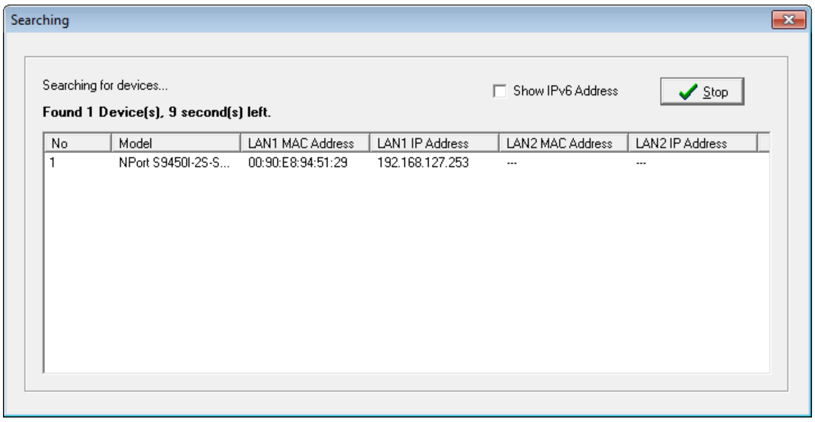
Since the Broadcast Search function searches by MAC address and not by IP address, all NPort S9000 servers connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

1. Open the DSU and then click the **Search** icon.



Search Result - 0 (s)

The Searching window indicates the progress of the search.



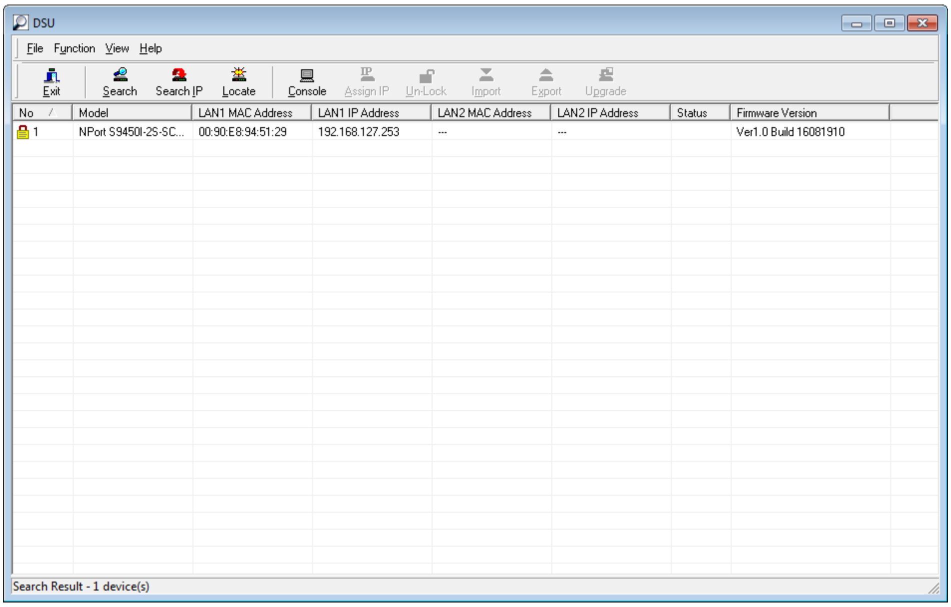
Searching for devices...

Found 1 Device(s), 9 second(s) left.

□ Show IPv6 Address

No	Model	LAN1 MAC Address	LAN1 IP Address	LAN2 MAC Address	LAN2 IP Address
1	NPort S9450I-2S-S...	00:90:E8:94:51:29	192.168.127.253	---	---

2. When the search is complete, all the NPort S9000 servers that were located will be displayed in the DSU window.



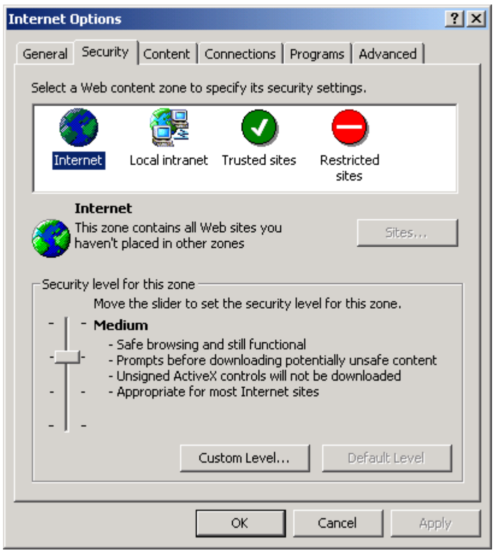
No	Model	LAN1 MAC Address	LAN1 IP Address	LAN2 MAC Address	LAN2 IP Address	Status	Firmware Version
1	NPort S9450I-2S-SC...	00:90:E8:94:51:29	192.168.127.253	---	---		Ver1.0 Build 16081910

Search Result - 1 device(s)

3. To modify the configuration of the highlighted NPort S9000, click on the Console icon to open the web console. This will take you to the web console, where you can make all configuration changes. Please refer to Chapter 6, "Configuration with the Web Console", for information on how to use the web console.

Opening Your Browser

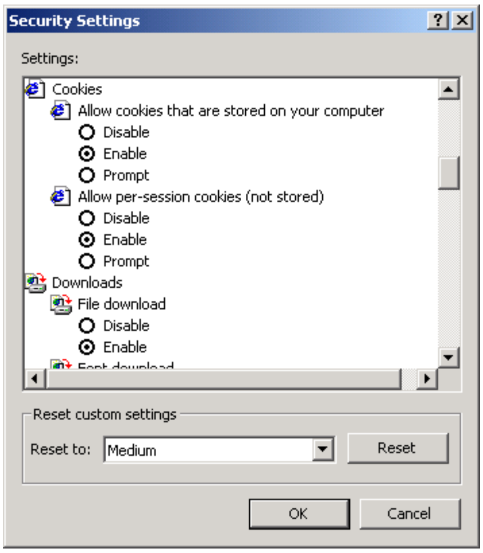
1. Open your browser with the cookie function enabled. (To enable your browser for cookies, right-click on your desktop Internet Explorer icon, select **Properties**, click on the Security tab, and then select the three Enable options as shown in the figure below.)



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone
Move the slider to set the security level for this zone.
Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites



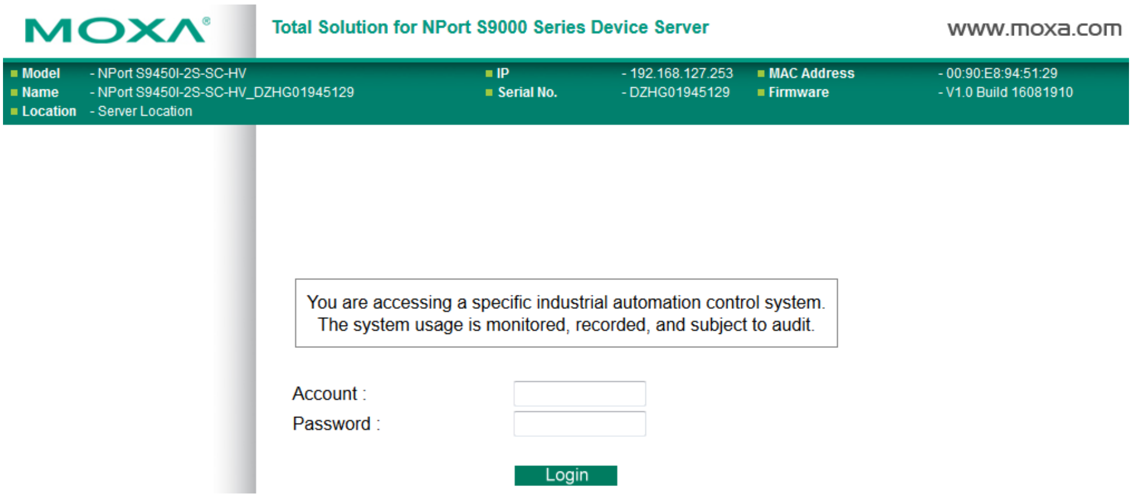
Settings:

Cookies
Allow cookies that are stored on your computer
○ Disable
● Enable
○ Prompt
Allow per-session cookies (not stored)
○ Disable
● Enable
○ Prompt
Downloads
File download
○ Disable
● Enable
Font download

Reset custom settings
Reset to: Medium

2. After using the DSU to find a specific NPort, type the IP address to log in to the web console. If this is the first time you configure the NPort, you may directly type the default IP address, 192.168.127.254 in the Address input box. Use the correct IP address if it is different from the default and then press Enter.

3. On the first page of the web console, type **admin** for the default account name and **moxa** for the default password.



Total Solution for NPort S9000 Series Device Server

www.moxa.com

Model	- NPort S9450I-2S-SC-HV	IP	- 192.168.127.253	MAC Address	- 00:90:E8:94:51:29
Name	- NPort S9450I-2S-SC-HV_DZHG01945129	Serial No.	- DZHG01945129	Firmware	- V1.0 Build 16081910
Location	- Server Location				

You are accessing a specific industrial automation control system.
The system usage is monitored, recorded, and subject to audit.

Account :

Password :

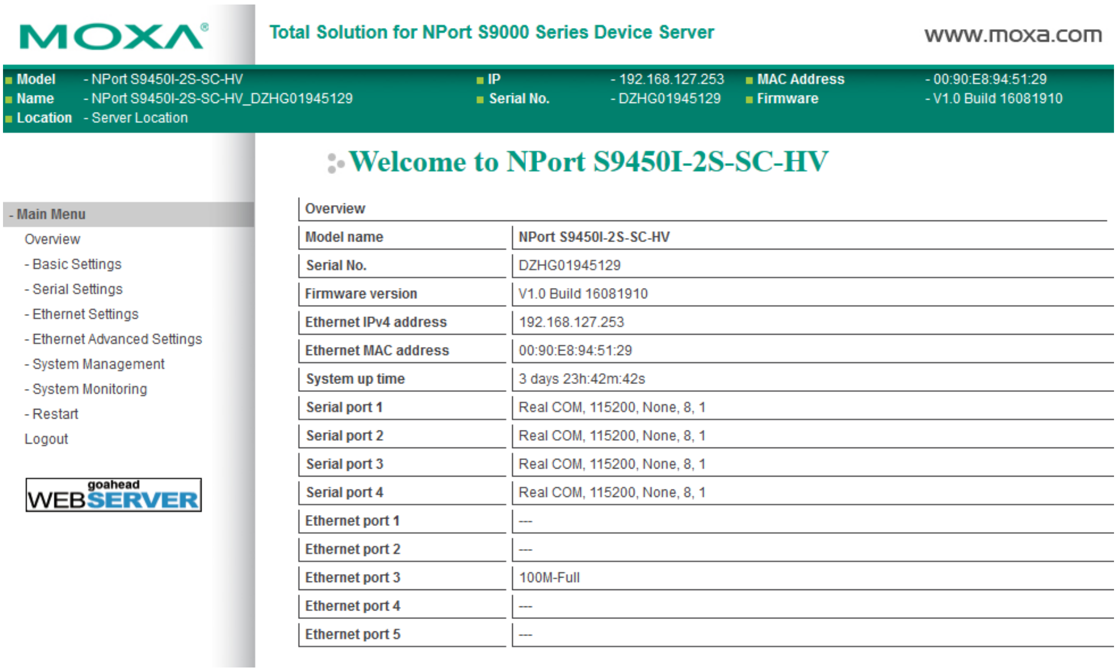
ATTENTION

If you use other web browsers, remember to Enable the functions **to allow cookies that are stored on your computer** or **allow per-session cookies**. Device servers use cookies only for "password" transmission.

ATTENTION

Refer to Chapter 3, "Initial IP Address Configuration," to see how to configure the IP address. Examples shown in this chapter use the Factory Default IP address (192.168.127.254).

The NPort S9000 homepage will open. On this page, you can see a brief description of the Web Console



Total Solution for NPort S9000 Series Device Server

www.moxa.com

Model	- NPort S9450I-2S-SC-HV	IP	- 192.168.127.253	MAC Address	- 00:90:E8:94:51:29
Name	- NPort S9450I-2S-SC-HV_DZHG01945129	Serial No.	- DZHG01945129	Firmware	- V1.0 Build 16081910
Location	- Server Location				

Welcome to NPort S9450I-2S-SC-HV

Overview	
Model name	NPort S9450I-2S-SC-HV
Serial No.	DZHG01945129
Firmware version	V1.0 Build 16081910
Ethernet IPv4 address	192.168.127.253
Ethernet MAC address	00:90:E8:94:51:29
System up time	3 days 23h:42m:42s
Serial port 1	Real COM, 115200, None, 8, 1
Serial port 2	Real COM, 115200, None, 8, 1
Serial port 3	Real COM, 115200, None, 8, 1
Serial port 4	Real COM, 115200, None, 8, 1
Ethernet port 1	---
Ethernet port 2	---
Ethernet port 3	100M-Full
Ethernet port 4	---
Ethernet port 5	---

ATTENTION

If you forgot the password, the ONLY way to start configuring the NPort is to load the factory defaults by using the reset button.

ATTENTION

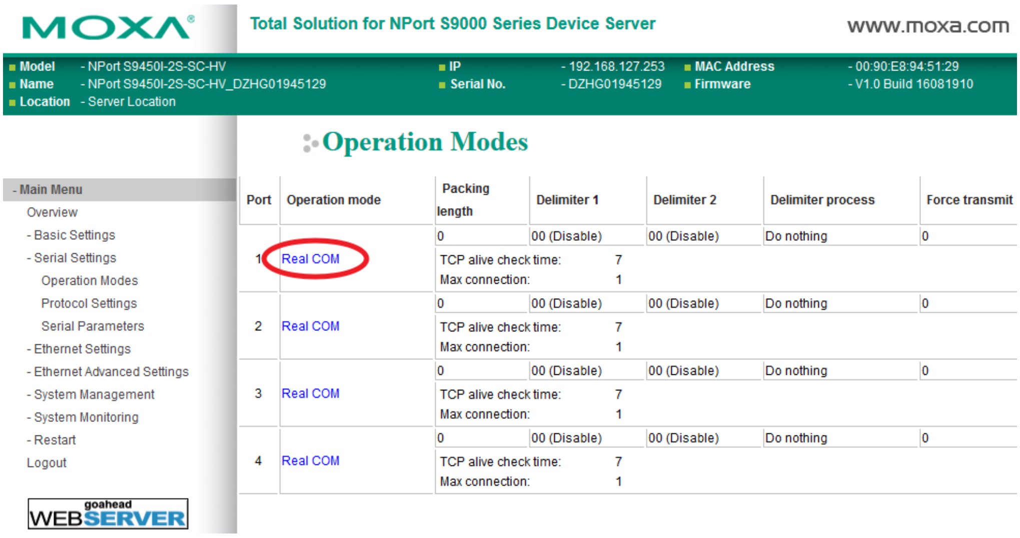
Remember to export the configuration file when you have finished the configuration. After using the reset button to load the factory defaults, your configuration can be easily reloaded into the NPort by using the Import function. Refer to Chapter 8, "Maintenance / Update System Files", for more details about using the Export and Import functions.

ATTENTION

If your NPort application requires using password protection, you must enable the cookie function in your browser. If the cookie function is disabled, you will not be allowed to enter the Web Console Screen.

Configure Operation Mode to Real COM Mode

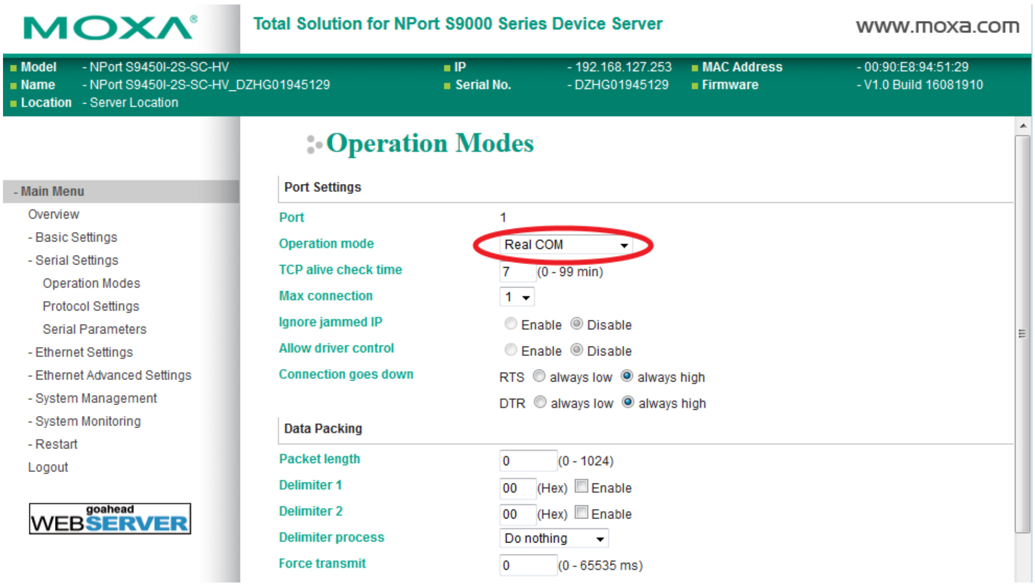
Click on **Operation Modes**, located under Serial Settings, to display the serial port settings for four serial ports. To modify the serial operation mode settings for a particular port, click on **Operation Modes** of the serial port in the window on the right-hand side..



Model	- NPort S9450I-2S-SC-HV	IP	- 192.168.127.253	MAC Address	- 00:90:E8:94:51:29
Name	- NPort S9450I-2S-SC-HV_DZHG01945129	Serial No.	- DZHG01945129	Firmware	- V1.0 Build 16081910
Location	- Server Location				

Operation Modes

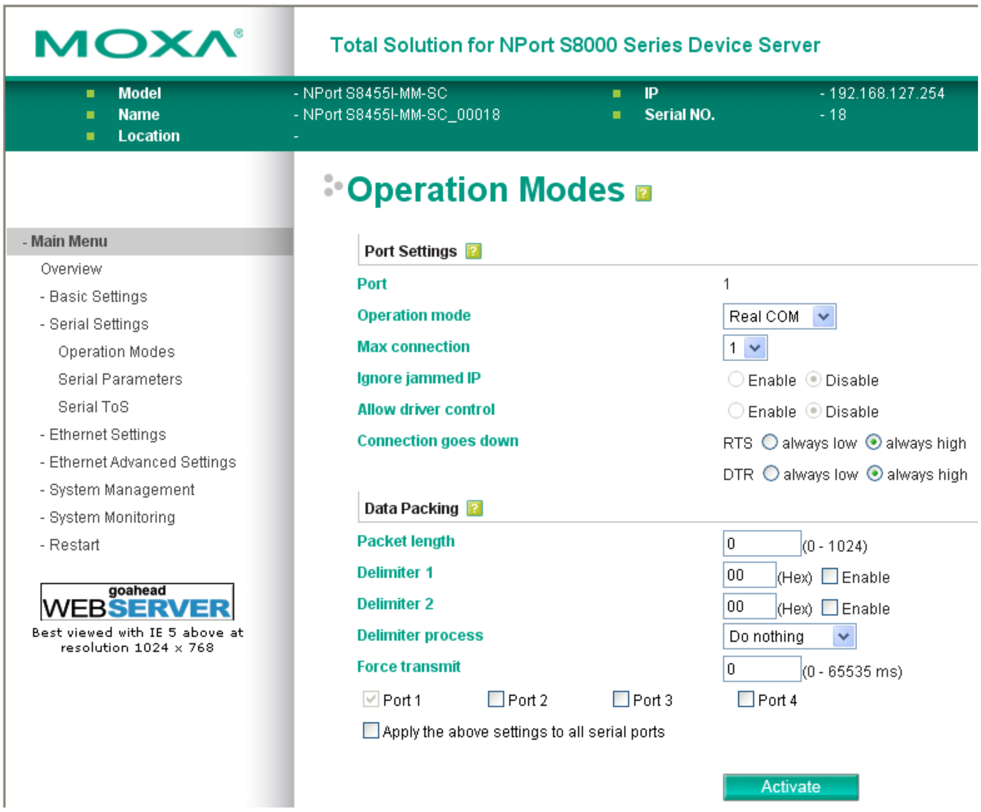
Port	Operation mode	Packing length	Delimiter 1	Delimiter 2	Delimiter process	Force transmit
1	Real COM	0 TCP alive check time: 7 Max connection: 1	00 (Disable)	00 (Disable)	Do nothing	0
2	Real COM	0 TCP alive check time: 7 Max connection: 1	00 (Disable)	00 (Disable)	Do nothing	0
3	Real COM	0 TCP alive check time: 7 Max connection: 1	00 (Disable)	00 (Disable)	Do nothing	0
4	Real COM	0 TCP alive check time: 7 Max connection: 1	00 (Disable)	00 (Disable)	Do nothing	0



Model	- NPort S9450I-2S-SC-HV	IP	- 192.168.127.253	MAC Address	- 00:90:E8:94:51:29
Name	- NPort S9450I-2S-SC-HV_DZHG01945129	Serial No.	- DZHG01945129	Firmware	- V1.0 Build 16081910
Location	- Server 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	○ Enable ● Disable
Allow driver control	○ Enable ● 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
Force transmit	0 (0 - 65535 ms)



Model - NPort S8455I-MM-SC
Name - NPort S8455I-MM-SC_00018
Location -
IP - 192.168.127.254
Serial NO. - 18

Operation Modes

Port Settings

Port 1

Operation mode Real COM

Max connection 1

Ignore jammed IP ○ Enable ● Disable

Allow driver control ○ Enable ● 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

Force transmit 0 (0 - 65535 ms)

☑ Port 1 □ Port 2 □ Port 3 □ Port 4

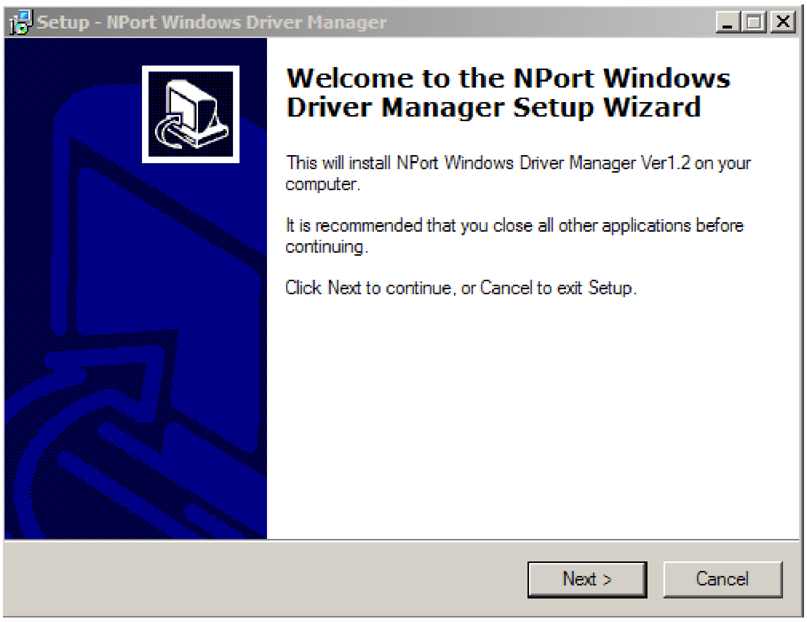
□ Apply the above settings to all serial ports

NPort Windows Driver Manager

Installing the NPort Windows Driver Manager

The NPort Windows Driver Manager is intended for use with NPort S9000 serial ports that are set to Real COM mode. The software manages the installation of drivers that allow you to map unused COM ports on your PC to serial ports on the NPort S9000. When the drivers are installed and configured, devices that are attached to serial ports on the NPort S9000 will be treated as if they were attached to your PC's own COM ports.

1. Click the **INSTALL COM Driver** button in the NPort Installation CD auto-run window to install the NPort Windows Driver. Once the installation program starts running, click **Yes** to proceed.
2. Click **Next** when the Welcome screen opens, to proceed with the installation.



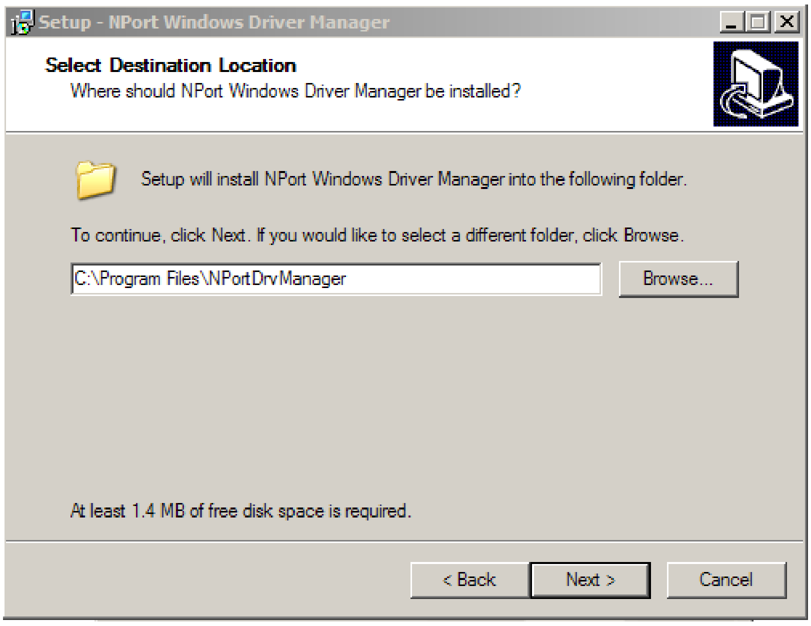
Welcome to the NPort Windows Driver Manager Setup Wizard

This will install NPort Windows Driver Manager Ver1.2 on your computer.

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

Click Next to continue, or Cancel to exit Setup.

Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



Select Destination Location

Where should NPort Windows Driver Manager be installed?

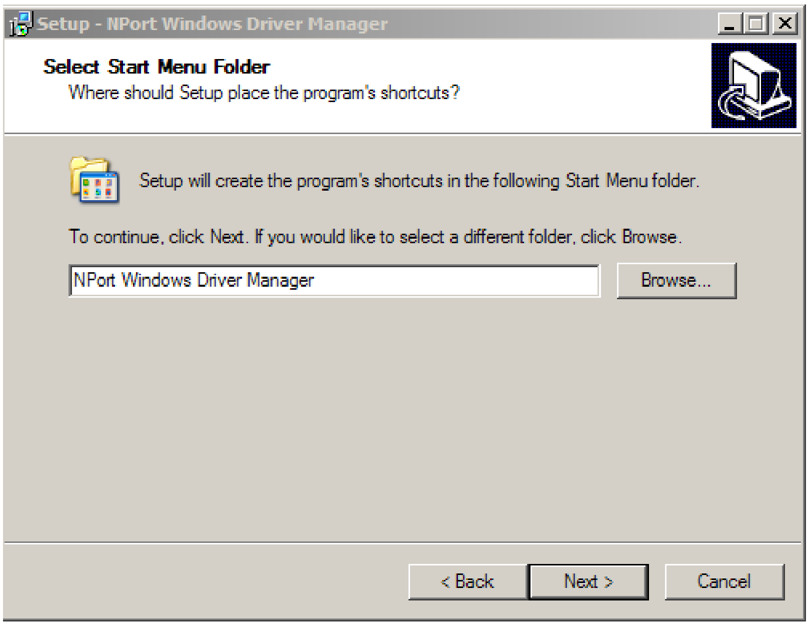
Setup will install NPort Windows Driver Manager into the following folder.

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

C:\Program Files\NPortDrvManager

At least 1.4 MB of free disk space is required.

3. Click **Next** to install the program's shortcuts in the appropriate Start Menu folder.



Select Start Menu Folder

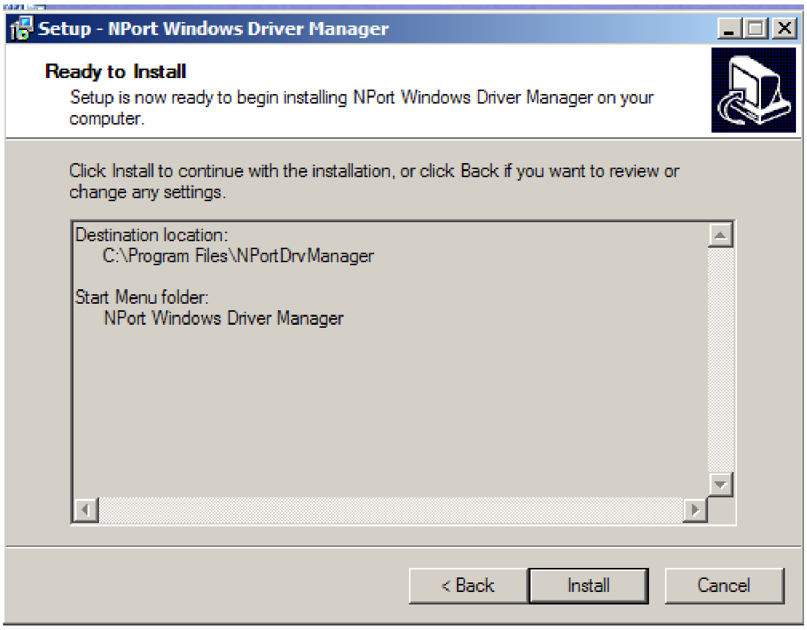
Where should Setup place the program's shortcuts?

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

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

NPort Windows Driver Manager

4. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.



Ready to Install

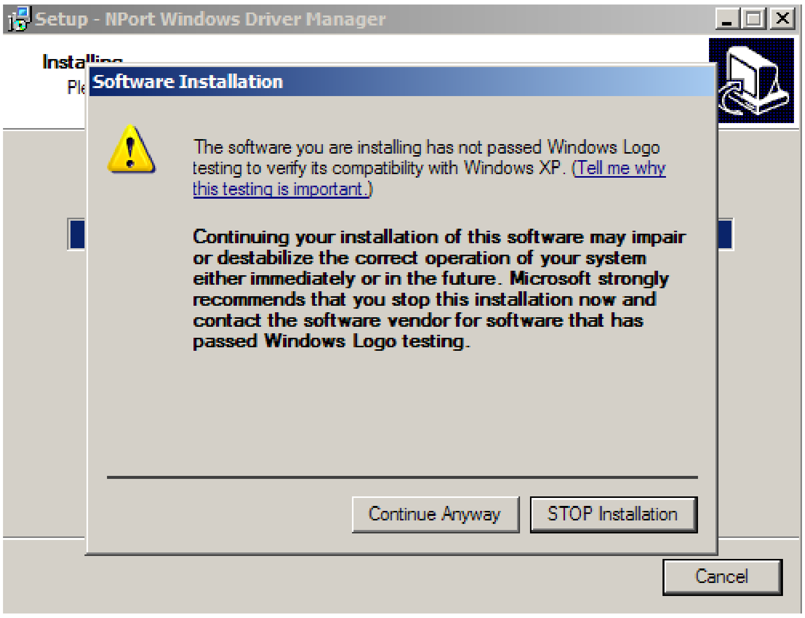
Setup is now ready to begin installing NPort Windows Driver Manager on your computer.

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

Destination location:
C:\Program Files\NPortDrvManager

Start Menu folder:
NPort Windows Driver Manager

5. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen. The installer will display a message that the software has not passed Windows Logo testing. This is shown as follows:

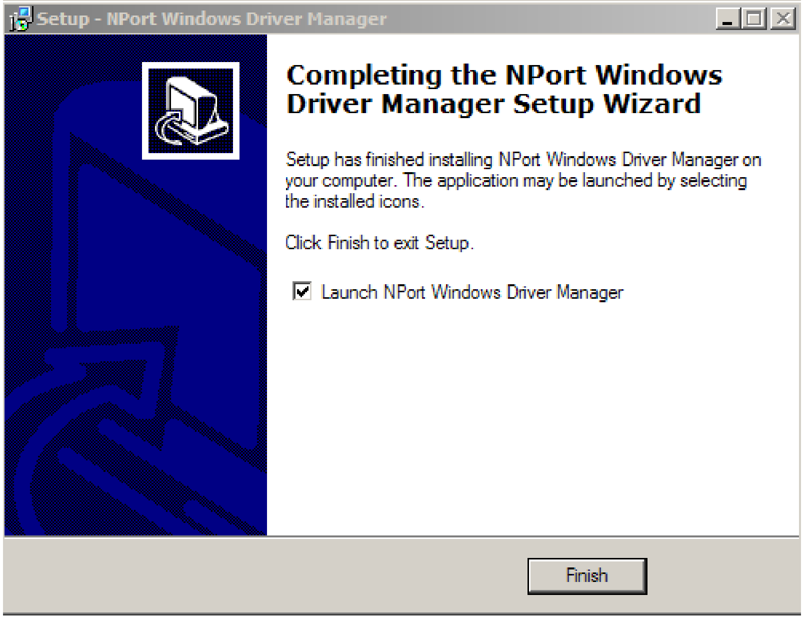


The software you are installing has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

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

Click **Continue Anyway** to finish the installation.

6. Click **Finish** to complete the installation of the NPort Windows Driver Manager.



Completing the NPort Windows Driver Manager Setup Wizard

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

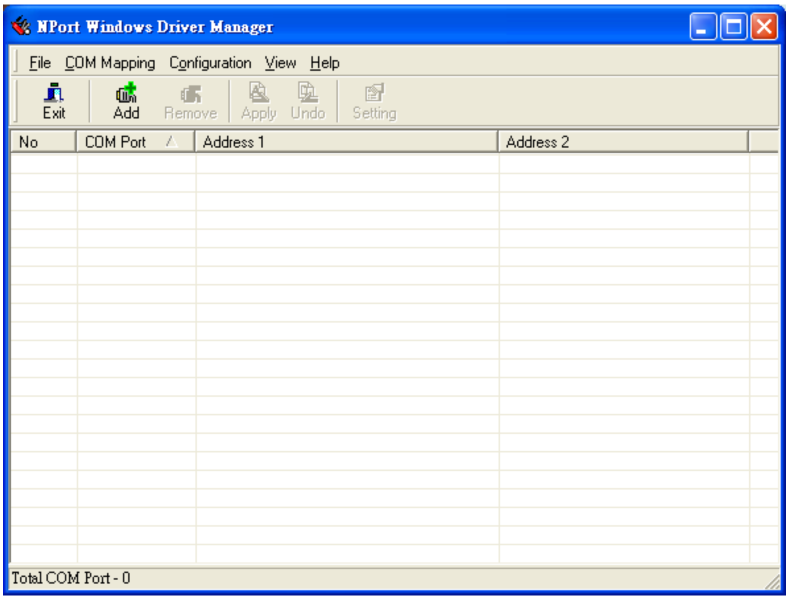
Click Finish to exit Setup.

☑ Launch NPort Windows Driver Manager

Using NPort Windows Driver Manager

After you have installed the NPort Windows Driver Manager, you can set up the NPort S9000's serial ports as remote COM ports for your PC host. Make sure that the serial port(s) on your NPort S9000 are set to Real COM mode before mapping COM ports with the NPort Windows Driver Manager.

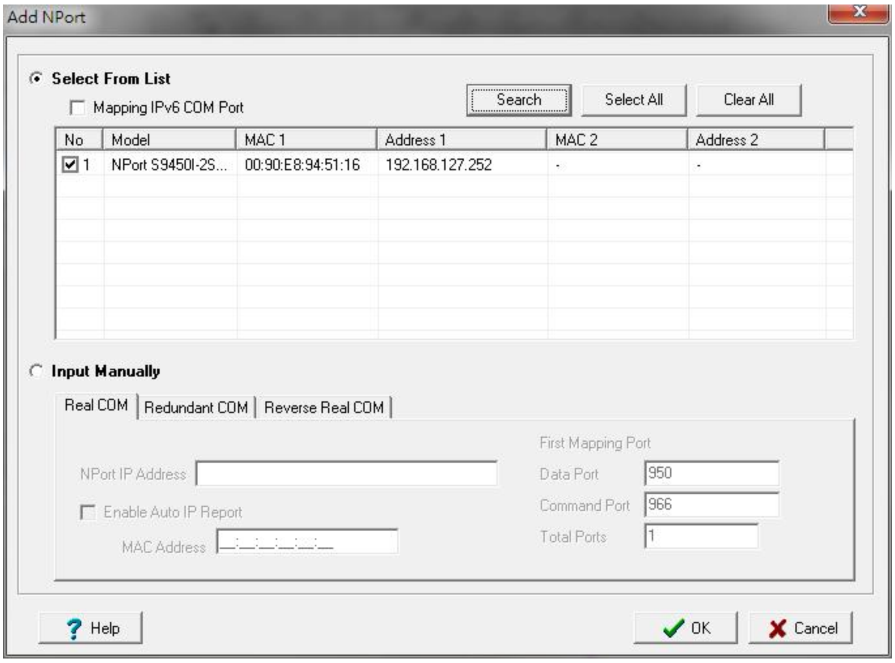
1. Go to **Start** → **NPort Windows Driver Manager** → **NPort Windows Driver Manager** to start the COM mapping utility.
2. Click the **Add** icon.



No	COM Port	Address 1	Address 2

Total COM Port - 0

3. Click **Search** to search for the NPort device servers. From the list that is generated, select the server to which you will map COM ports, and then click **OK**.



● Select From List

□ Mapping IPv6 COM Port

No	Model	MAC 1	Address 1	MAC 2	Address 2
☑ 1	NPort S9450I-2S...	00:90:E8:94:51:16	192.168.127.252	-	-

○ Input Manually

NPort IP Address

□ Enable Auto IP Report

MAC Address __:__:__:__:__:__

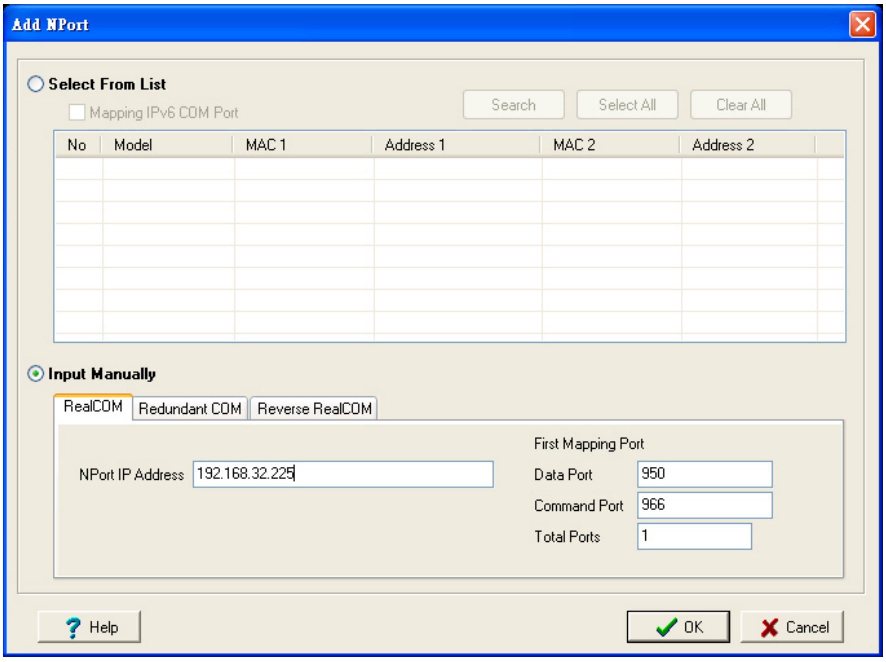
First Mapping Port

Data Port 950

Command Port 966

Total Ports 1

4. Alternatively, you can select **Input Manually** and then manually enter the NPort IP Address, 1st Data Port, 1st Command Port, and Total Ports to which COM ports will be mapped. Click **OK** to proceed to the next step. Note that the Add NPort page supports FQDN (Fully Qualified Domain Name), in which case the IP address will be filled in automatically.



○ Select From List

□ Mapping IPv6 COM Port

No	Model	MAC 1	Address 1	MAC 2	Address 2

● Input Manually

NPort IP Address 192.168.32.225

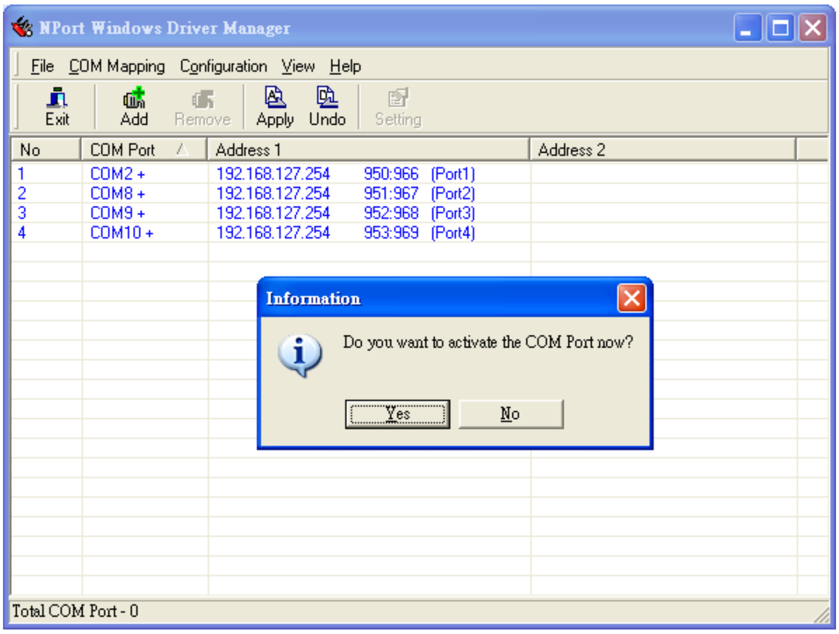
First Mapping Port

Data Port 950

Command Port 966

Total Ports 1

5. COM ports and their mappings will appear in blue until they are activated. Activating the COM ports saves the information in the host system registry and makes the COM port available for use. The host computer will not have the ability to use the COM port until the COM ports are activated. Click **Yes** to activate the COM ports at this time, or click **No** to activate the COM ports later.



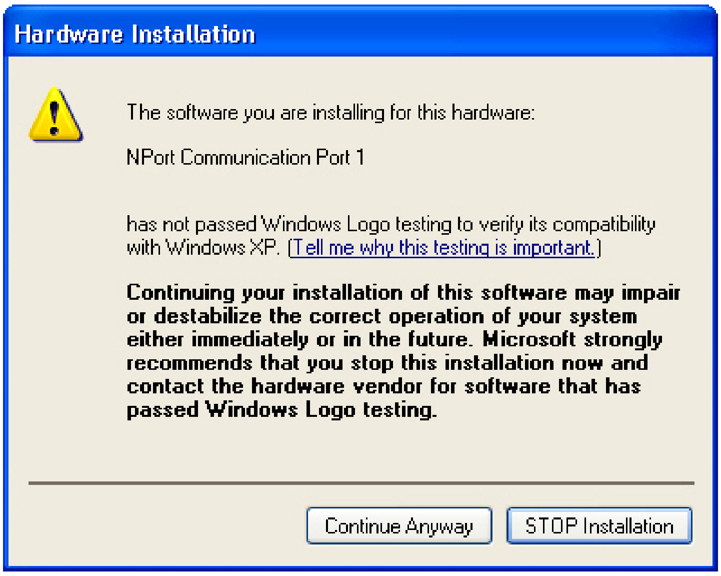
No	COM Port	Address 1	Address 2
1	COM2 +	192.168.127.254 950:966 (Port1)	
2	COM8 +	192.168.127.254 951:967 (Port2)	
3	COM9 +	192.168.127.254 952:968 (Port3)	
4	COM10 +	192.168.127.254 953:969 (Port4)	

Information

Do you want to activate the COM Port now?

Total COM Port - 0

6. A message will display during activation of each port, indicating that the software has not passed Windows Logo certification. Click **Continue Anyway** to proceed.



Hardware Installation

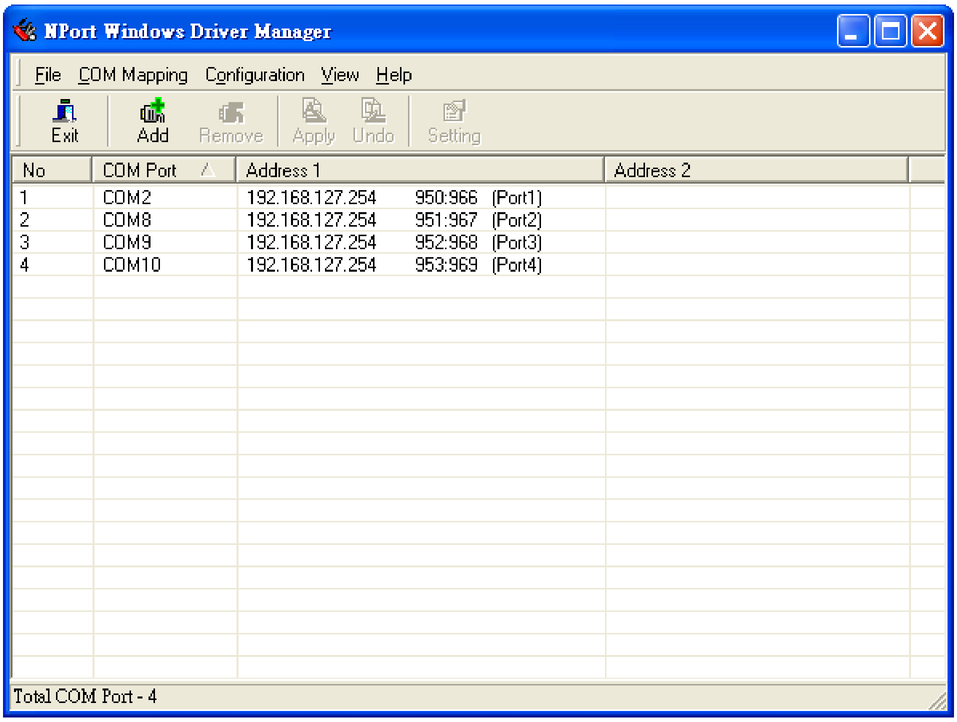
The software you are installing for this hardware:

NPort Communication Port 1

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

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

7. Ports that have been activated will appear in black.


NPort Windows Driver Manager
File COM Mapping Configuration View Help
Exit Add Remove Apply Undo Setting

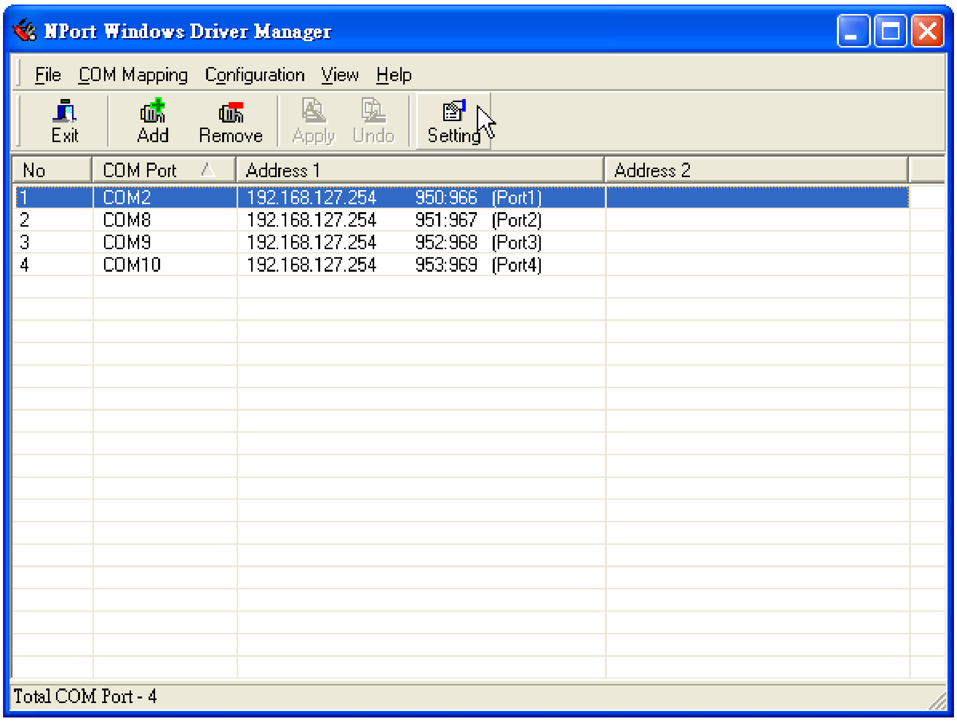
No	COM Port	Address 1	Address 2
1	COM2	192.168.127.254 950:966 (Port1)	
2	COM8	192.168.127.254 951:967 (Port2)	
3	COM9	192.168.127.254 952:968 (Port3)	
4	COM10	192.168.127.254 953:969 (Port4)	

Total COM Port - 4

8. Use terminal software to open the mapped COM port to communicate with the serial device. You may download PComm Lite, a useful tool to check the serial communication, from Moxa's website: http://www.moxa.com/support/download.aspx?type=support&id=167

Configure the mapped COM ports with Advanced Functions

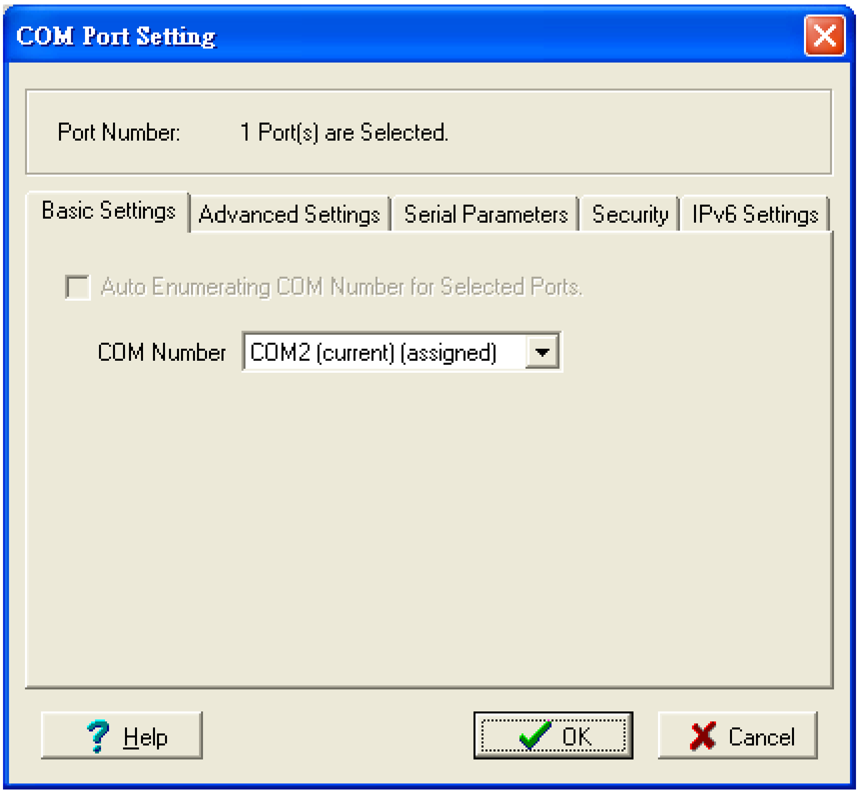
For Real COM Mode, to reconfigure the settings for a particular serial port on the NPort S9000, select the row corresponding to the desired port and then click the **Setting** icon.


NPort Windows Driver Manager
File COM Mapping Configuration View Help
Exit Add Remove Apply Undo Setting

No	COM Port	Address 1	Address 2
1	COM2	192.168.127.254 950:966 (Port1)	
2	COM8	192.168.127.254 951:967 (Port2)	
3	COM9	192.168.127.254 952:968 (Port3)	
4	COM10	192.168.127.254 953:969 (Port4)	

Total COM Port - 4

1. On the **Basic Setting** window, use the **COM Number** drop-down list to select a COM number to be assigned to the NPort S9000's serial port that is being configured. Select the **Auto Enumerating COM Number for Selected Ports** option to automatically assign available COM numbers in sequence to selected serial ports. Note that ports that are "in use" will be labeled accordingly.



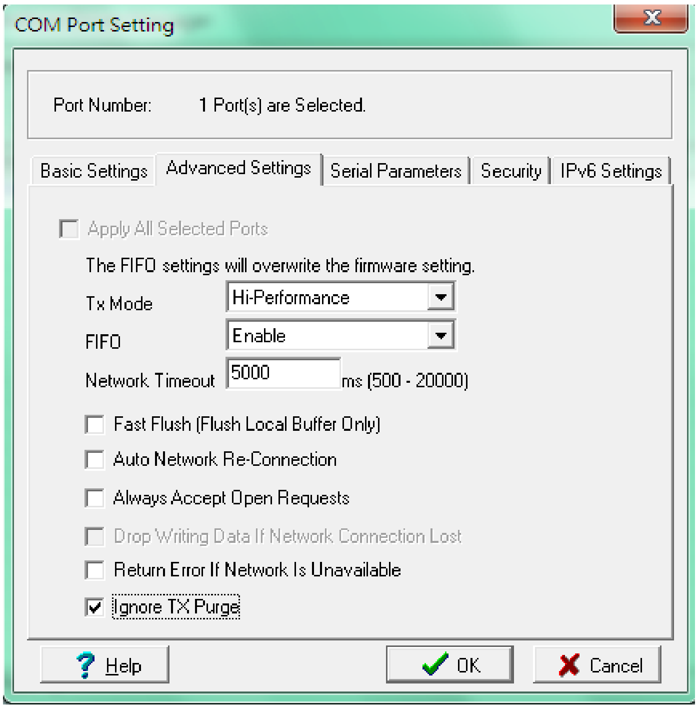
COM Port Setting

Port Number: 1 Port(s) are Selected.

□ Auto Enumerating COM Number for Selected Ports.

COM Number: COM2 (current) (assigned)

2. Click the **Advanced Settings** tab to modify Tx Mode, FIFO, and Flash Flush.



COM Port Setting

Port Number: 1 Port(s) are Selected.

□ Apply All Selected Ports

The FIFO settings will overwrite the firmware setting.

Tx Mode: Hi-Performance

FIFO: Enable

Network Timeout: 5000 ms (500 - 20000)

□ Fast Flush (Flush Local Buffer Only)

□ Auto Network Re-Connection

□ Always Accept Open Requests

□ Drop Writing Data If Network Connection Lost

□ Return Error If Network Is Unavailable

☑ Ignore TX Purge

Tx Mode

Hi-Performance is the default for Tx mode. After the driver sends data to the NPort S9000, the driver immediately issues a "Tx Empty" response to the program. Under **Classical** mode, the driver will not send the "Tx Empty" response until after confirmation is received from the NPort S9000's serial port. This causes lower throughput. Classical mode is recommended if you want to ensure that all data is sent out before further processing.

FIFO

If FIFO is **Disabled**, the NPort S9000 will transmit one byte each time the Tx FIFO becomes empty, and an Rx interrupt will be generated for each incoming byte. This will result in a faster response and lower throughput.

Network Timeout

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

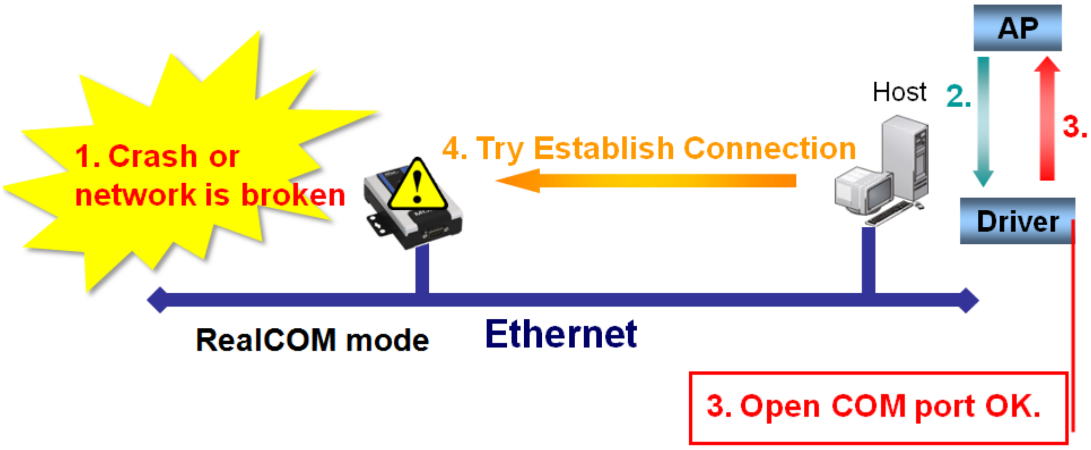
Auto Network Re-Connection

With this option enabled, the driver will repeatedly attempt to reestablish the TCP connection if the NPort S9000 does not respond to background "check alive" packets.

Always Accept Open Requests

When the driver cannot establish a connection with the NPort, the user's software can still open the mapped COM port, just like an onboard COM port.

For example, if the NPort is down or the network is broken as described in figure below. At that moment, the terminal software tries to open the mapped COM port, and the driver will respond with the message:"Success" for the terminal software to open the COM port. At the same time, the driver will try to establish the connection to the specific NPort. If the connection is established, then the mapped COM port will work properly.



Return error if network is unavailable

If this option is disabled, the driver will not return any error even when a connection cannot be established with the NPort S9000. With this option enabled, calling the Win32 Comm function will result in the error return code "STATUS_NETWORK_UNREACHABLE" when a connection cannot be established to the NPort S9000. This usually means that your host's network connection is down, perhaps due to a cable being disconnected. However, if you can reach other network devices, it may be that the NPort S9000 is not powered on or is disconnected. Note that **Auto Network Re-Connection** must be enabled in order to use this function.

Fast Flush (only flushes the local buffer)

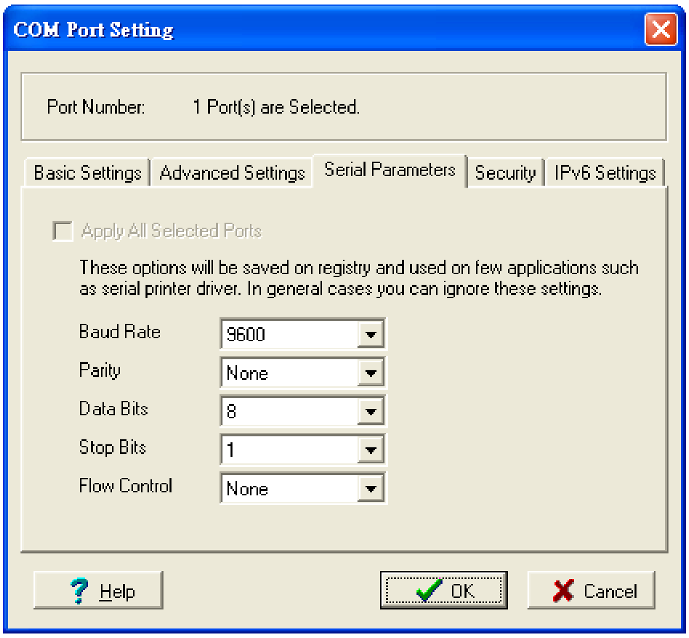
For some applications, the user's program will use the Win32 "PurgeComm()" function before it reads or writes data. After a program uses this PurgeComm() function, the NPort driver continues to query the NPort's firmware several times to make sure no data is queued in the NPort's firmware buffer, rather than just flushing the local buffer. This design is used to satisfy some special considerations. However, it may take more time (about several hundred milliseconds) than a native COM1 due to the additional time spent communicating across the Ethernet. This is why PurgeComm() works significantly faster with native COM ports on a PC than with mapped COM ports on the NPort S9000. In order to accommodate other applications that require a faster response time, the new NPort driver implements a new Fast Flush option. By default, this function is enabled.

If you have disabled Fast Flush and find that COM ports mapped to the NPort S9000 perform markedly slower than when using a native COM port, try to verify if "PurgeComm()" functions are used in your application. If so, try enabling the Fast Flush function and see if there is a significant improvement in performance.

Ignore TX Purge

Applications can use the Win32 API PurgeComm to clear the output buffer. Outstanding overlapping write operations will be terminated. Select the **Ignore TX Purge** checkbox to ignore the effect on output data.

3. The **Serial Parameters** window in the following figure shows the default settings when the NPort S9000 is powered on. However, the program can redefine the serial parameters to different values after the program opens the port via Win 32 API.



COM Port Setting

Port Number: 1 Port(s) are Selected.

□ Apply All Selected Ports

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

Baud Rate: 9600

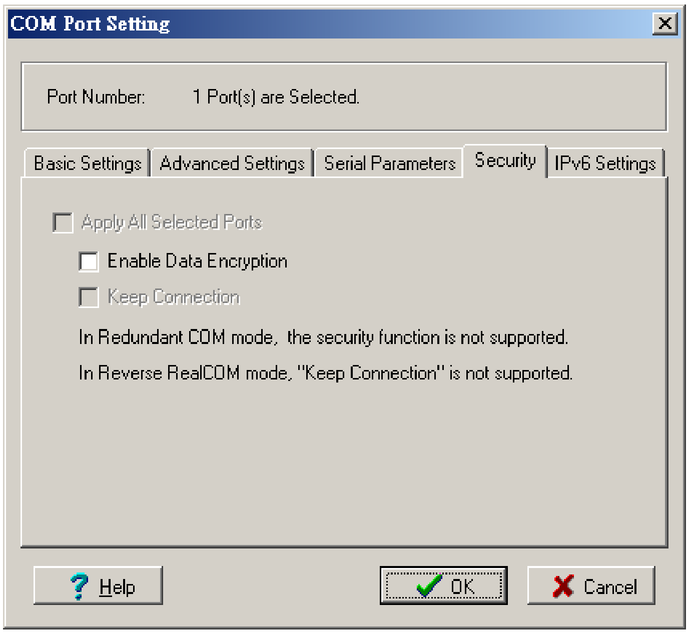
Parity: None

Data Bits: 8

Stop Bits: 1

Flow Control: None

4. The Security function is available only for the NPort 6000 series. The NPort S9000 doesn’t support this function.



COM Port Setting

Port Number: 1 Port(s) are Selected.

□ Apply All Selected Ports

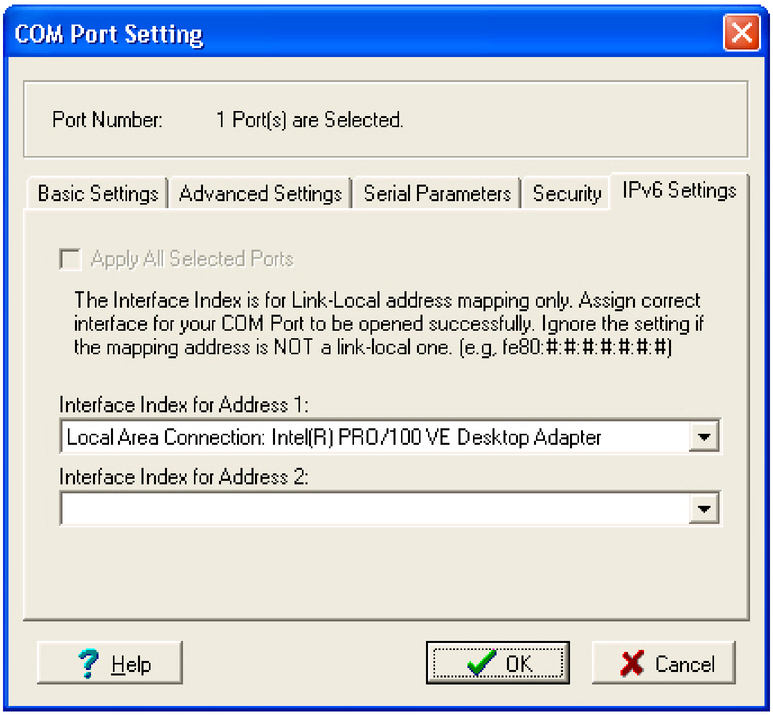
□ Enable Data Encryption

□ Keep Connection

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

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

5. The IPv6 Settings function is available only for the NPort 6000 series. The NPort S9000 doesn’t support this function.



Port Number: 1 Port(s) are Selected.

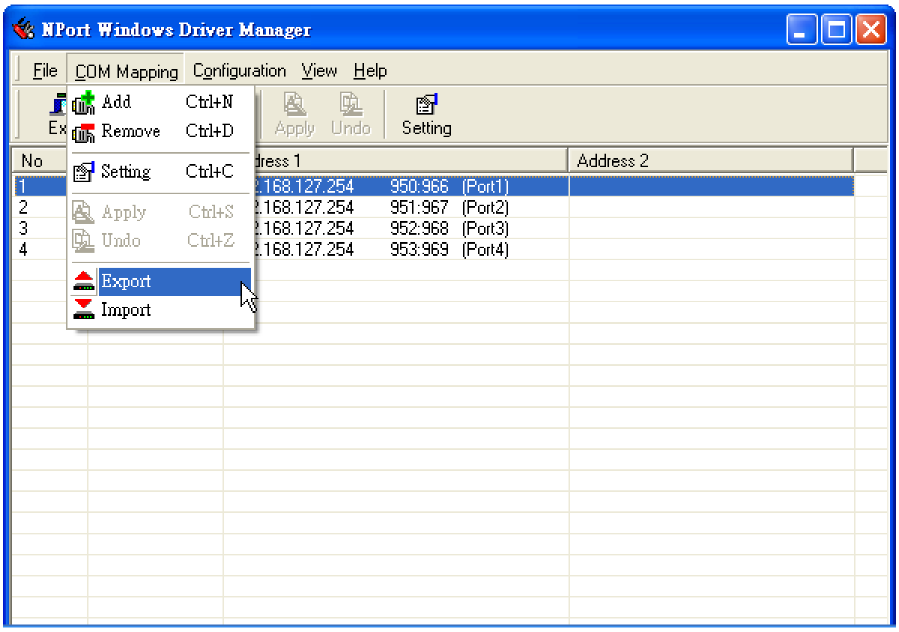
□ Apply All Selected Ports

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

Interface Index for Address 1: Local Area Connection: Intel(R) PRO/100 VE Desktop Adapter

Interface Index for Address 2:

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



No	ress 1		Address 2
1	.168.127.254	950:966 (Port1)	
2	.168.127.254	951:967 (Port2)	
3	.168.127.254	952:968 (Port3)	
4	.168.127.254	953:969 (Port4)	

Linux Real TTY Drivers

Basic Procedures

To map an NPort S9000 serial port to a Linux host’s tty port, follow these instructions:

1. Set up the NPort S9000. After verifying that the IP configuration works, and you can access the NPort S9000 (by using ping, telnet, etc.), configure the desired serial port on the NPort S9000 to Real COM mode.
2. Install the Linux Real tty driver files on the host

3. Map the NPort serial port to the host's tty port

Hardware Setup

Before proceeding with the software installation, make sure you have completed the hardware installation. Note that the default IP address for the NPort S9000 is **192.168.127.254,** and the default username and password are admin and moxa, respectively.

NOTE After installing the hardware, you must configure the operating mode of the serial port on your NPort S9000 to Real COM mode.

Installing Linux Real TTY Driver Files

1. Obtain the driver file from the included CD-ROM or the Moxa website, at http://www.moxa.com.
2. Log in to the console as a superuser (root).
3. Execute **cd /** to go to the root directory.
4. Copy the driver file **npreal2xx.tgz** to the **/** directory.
5. Execute **tar xvfz npreal2xx.tgz** to extract all files into the system.
6. Execute **/tmp/moxa/mxinst**.
   For RedHat AS/ES/WS and Fedora Core1, append an extra argument as follows:
   # /tmp/moxa/mxinst SP1
   The shell script will install the driver files automatically.
7. After installing the driver, you will be able to see several files in the **/usr/lib/npreal2/driver** folder:

> **mxaddsvr**	(Add Server, mapping tty port)
> **mxdelsvr**	(Delete Server, unmapping tty port)
> **mxloadsvr**	(Reload Server)
> **mxmknod**	(Create device node/tty port)
> **mxrmnod**	(Remove device node/tty port)
> **mxuninst**	(Remove tty port and driver files)

At this point, you will be ready to map the NPort serial port to the system tty port.

Mapping TTY Ports

Make sure that you set the operation mode of the desired NPort S9000 serial port to Real COM mode. After logging in as a superuser, enter the directory **/usr/lib/npreal2/driver** and then execute **mxaddsvr** to map the target NPort serial port to the host tty ports. The syntax of **mxaddsvr** is as follows:

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

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

1. Modifies npreal2d.cf.
2. Creates tty ports in directory /dev with major & minor number configured in **npreal2d.cf**.
3. Restarts the driver.

Mapping tty ports automatically

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

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

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

Mapping tty ports manually

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

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

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

Removing Mapped TTY Ports

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

mxdelsvr [*IP Address*]

Example:

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

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

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

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

Removing Linux Driver Files

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

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

The UNIX Fixed TTY Driver

Installing the UNIX Driver

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

   ```
   # mkdir –p /usr/etc
   ```

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

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

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

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

   The following files will be extracted:

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

4. Compile and Link

   For SCO UNIX:

   ```
   # make sco
   ```

   For UnixWare 7:

   ```
   # make svr5
   ```

   For UnixWare 2.1.x, SVR4.2:

   ```
   # make svr42
   ```

Configuring the UNIX Driver

Modify the configuration

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

```
ttyp1 192.168.1.1 950
```

For more configuration information, view the file **moxattyd.cf,** which contains detailed descriptions of the various configuration parameters.

NOTE The "Device Name" depends on the OS. See the Device Naming Rule section in README.TXT for more information.

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

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

Device naming rule

For UnixWare 7, UnixWare 2.1.x, and SVR4.2, use:

pts/[*n*]

For all other UNIX operating systems, use:

ttyp[*n*]

Starting moxattyd

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

Adding an additional server

1. Modify the text file **moxattyd.cf** to add an additional server. Users may use vi or any text editor to modify the file. For more configuration information, look at the file **moxattyd.cf**, which contains detailed descriptions of the various configuration parameters.
2. Find the process ID (PID) of the program **moxattyd**.

   # ps -ef | grep moxattyd
3. Update configuration of **moxattyd** program.

   # kill -**USR1 [*PID*]**
   (e.g., if moxattyd PID = 404, **kill -USR1 404**)
   This completes the process of adding an additional server.

6

Basic Settings and Device Server Configuration

In the following chapters, we explain how to access the NPort S9000's various configuration, monitoring, and administration functions. There are three ways to access these functions: RS-232 console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect the NPort S9000 to a PC's COM port, can be used if you do not know the NPort S9000's IP address. The Telnet console and web browser connection methods can be used to access the NPort S9000 over an Ethernet LAN or over the Internet.

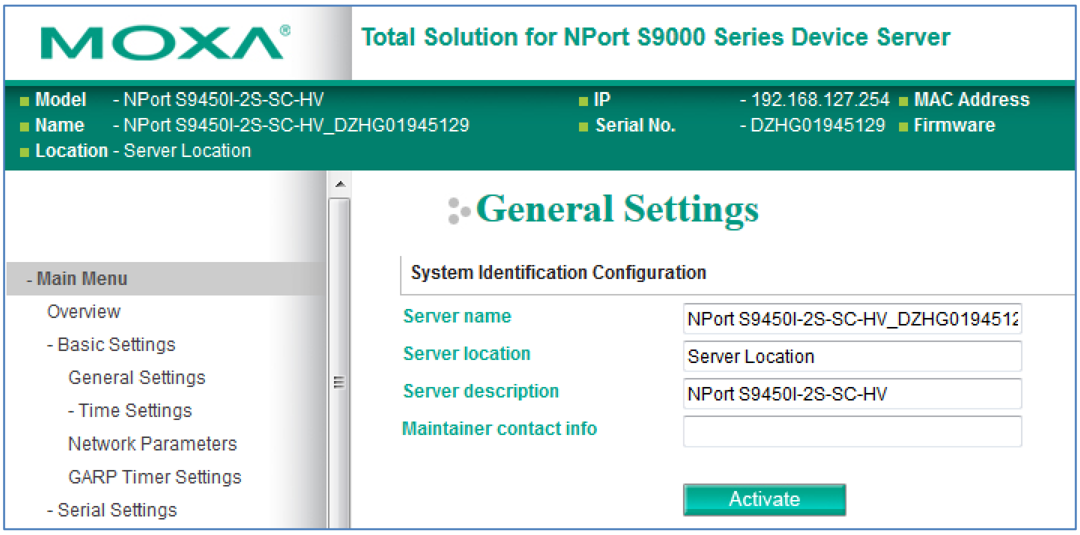
The Web Console is the most user-friendly way to configure the NPort S9000. In this chapter, we use the Web Console interface to introduce the functions that focus on the Basic Settings and Device Server Configuration.

This chapter covers the following topics:

- **Basic Settings**
  - General Settings
  - Time Settings
  - Network Settings
  - GARP Timer Settings
- **Serial Settings**
  - Operation Modes
  - DNP3 Mode
- **DNP3 Raw Socket Mode**
  - Modbus Mode
  - Protocol Settings
  - Serial Parameters

Basic Settings

General Settings



Total Solution for NPort S9000 Series Device Server

Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address
Firmware

General Settings

System Identification Configuration

Server name	NPort S9450I-2S-SC-HV_DZHG0194512
Server location	Server Location
Server description	NPort S9450I-2S-SC-HV
Maintainer contact info	

Server name

Setting	Factory Default	Necessity
1 to 40 characters	[model name]_[Serial No.]	Optional

This column is useful for specifying the application of this NPort device server.

Server Location

Setting	Factory Default	Necessity
1 to 80 characters	Empty	Optional

This column is useful for specifying the location of this NPort device server.

Server Description

Setting	Factory Default	Necessity
1 to 40 characters	Empty	Optional

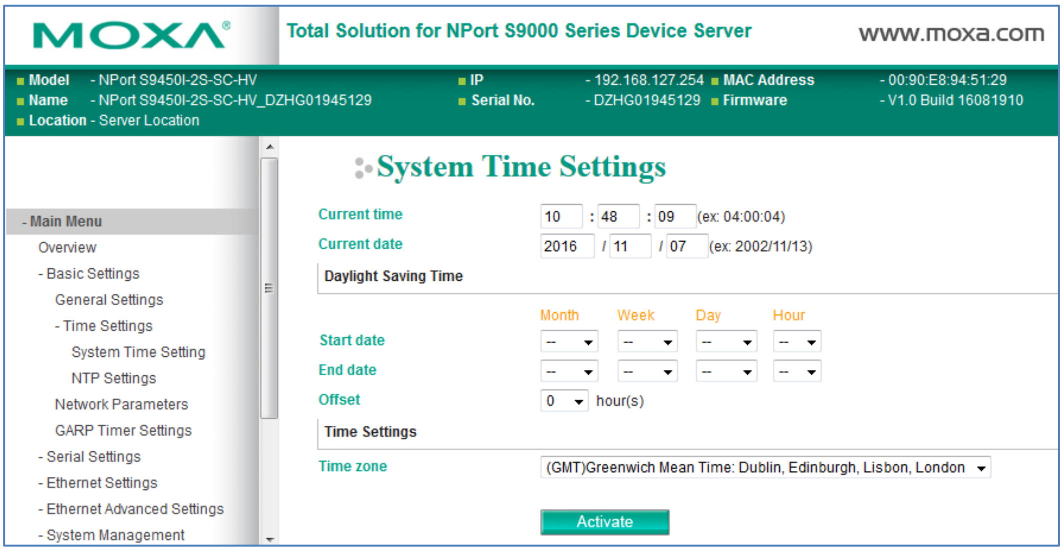
This column is useful for specifying more detailed description of this NPort S9000, such as the serial devices connected to the NPort S9000.

Maintainer contact info

Setting	Factory Default	Necessity
1 to 40 characters	Empty	Optional

This column is useful for specifying the contact information of the administrator responsible for maintaining this NPort S9000.

Time Settings



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

System Time Settings

Current time 10 : 48 : 09 (ex: 04:00:04)
Current date 2016 / 11 / 07 (ex: 2002/11/13)

Daylight Saving Time

	Month	Week	Day	Hour
Start date	--	--	--	--
End date	--	--	--	--

Offset 0 hour(s)

Time Settings

Time zone (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

System Time Settings

The NPort S9000 has a time-calibration function based on information from an NTP server or user-specified Time and Date information. Functions such as Auto warning "Email" can add real-time information to the message.

ATTENTION

The risk of an explosion is very high if the real-time clock battery is replaced with the wrong type!

The NPort S9000's real-time clock is powered by a rechargeable battery. We strongly recommend that you do not replace a rechargeable battery without help from a qualified Moxa support engineer. If you need to change the battery, please contact the Moxa RMA service team.

Current Time

Setting	Description	Factory Default
User adjustable time.	The time parameter allows configuration of the local time in local 24-hour format.	None (hh:mm:ss)

Current Date

Setting	Description	Factory Default
User adjustable date.	The date parameter allows configuration of the local date in yyyy/mm/dd format.	None (yyyy/mm/dd)

Daylight Saving Time

Daylight saving time (also know as **DST** or **summer time**) involves advancing clocks (usually one hour) during the summer time to provide an extra hour of daylight in the afternoon.

Start Date

Setting	Description	Factory Default
User adjustable date.	The Start Date parameter allows users to enter the date that daylight saving time begins.	None

End Date

Setting	Description	Factory Default
User adjustable date.	The End Date parameter allows users to enter the date that daylight saving time ends.	None

Offset

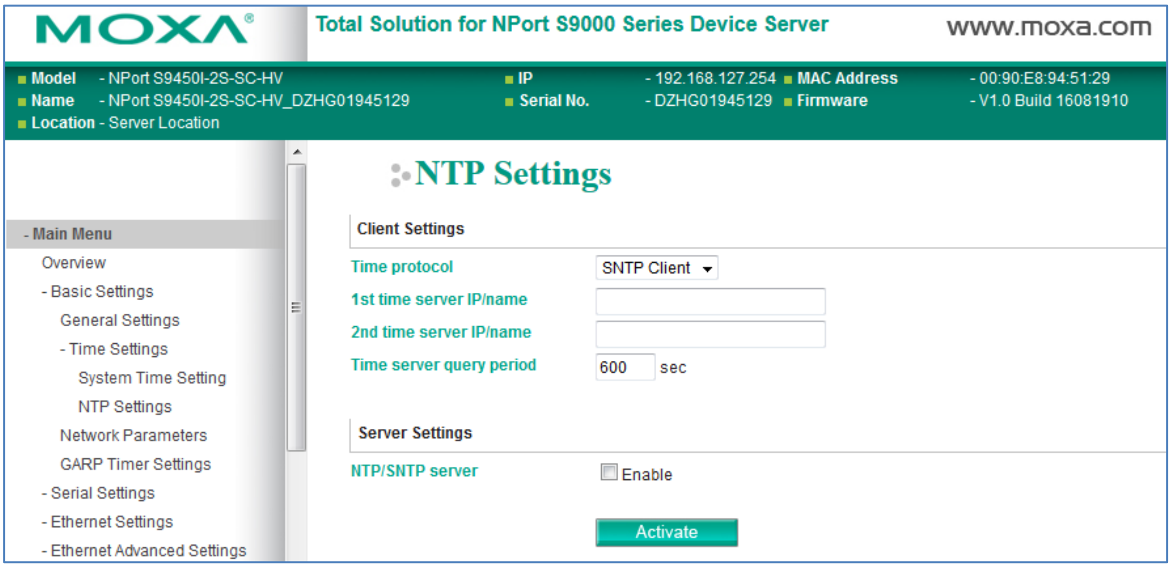
Setting	Description	Factory Default
User adjustable hour.	The offset parameter indicates how many hours forward the clock should be advanced.	None

Time Settings

Time Zone

Setting	Description	Factory Default
User selectable time zone.	The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time.	GMT (Greenwich Mean Time)

NOTE Changing the time zone will automatically correct the current time. You should configure the time zone before setting the time.



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

NTP Settings

Client Settings

Time protocol: SNTP Client
1st time server IP/name:
2nd time server IP/name:
Time server query period: 600 sec

Server Settings

NTP/SNTP server: □ Enable

NTP Settings

Time protocol

Setting	Description	Factory Default
Disable	Disable NTP/SNTP service	None

SNTP Client

Setting	Description	Factory Default
SNTP Client	Use SNTP protocol to sync the time with the destination SNTP server	None

NTP Client

Setting	Description	Factory Default
NTP Client	Use NTP protocol to sync the time with the destination NTP server	None

Time Server IP/Name

Setting	Description	Factory Default
1st Time Server IP/Name	IP or Domain address (e.g., 192.168.1.1 or time.stdtime.gov.tw or time.nist.gov).	None
2nd Time Server IP/Name	The NPort S8450I-MM-SC will try to locate the second time server if the first time server fails to connect.	

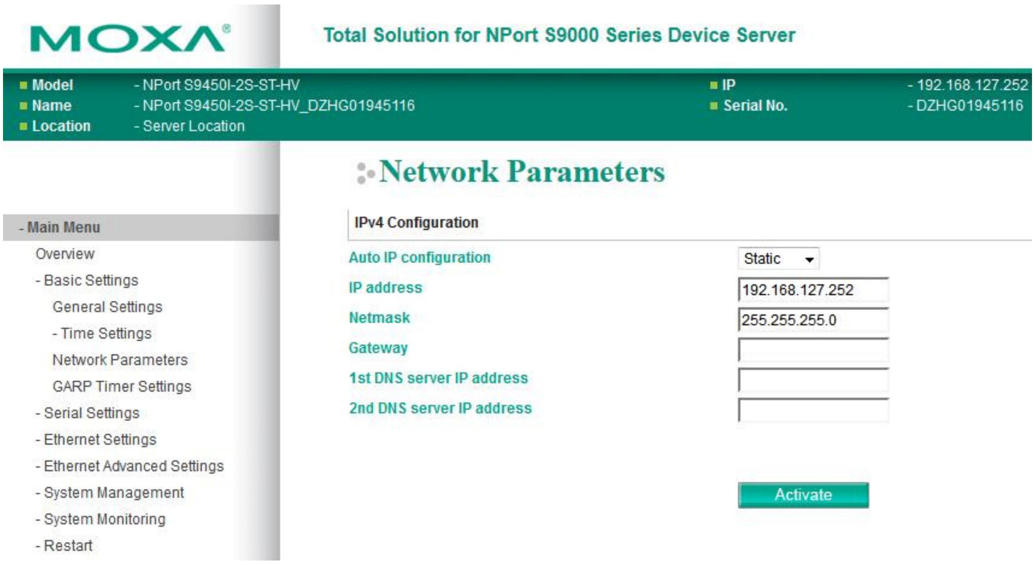
Time Server Query Period

Setting	Description	Factory Default
Query Period	This parameter determines how frequently the time is updated from the time server.	600 seconds

Server Settings

Setting	Description	Factory Default
NTP/SNTP server	Configure S9000 as a NTP/SNTP server to align the time to the NTP/SNTP clients	Disable

Network Settings



Total Solution for NPort S9000 Series Device Server

Model	- NPort S9450I-2S-ST-HV	IP	- 192.168.127.252
Name	- NPort S9450I-2S-ST-HV_DZHG01945116	Serial No.	- DZHG01945116
Location	- Server Location		

Network Parameters

IPv4 Configuration

Auto IP configuration	Static
IP address	192.168.127.252
Netmask	255.255.255.0
Gateway	
1st DNS server IP address	
2nd DNS server IP address	

You must assign a valid IP address to the NPort S9000 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 S9000 will not have a valid connection to the network. First-time users can refer to Chapter 3, “Initial IP Address Configuration,” for more information.

You can choose from four possible IP Configuration modes—**Static, By DHCP** and **By BOOTP**—located under the web console screen’s IP configuration drop-down box.

Auto IP Configuration

Setting	Description	Factory Default
Static	Set up the NPort S9000’s IP address manually.	Disable
By DHCP	The NPort S9000’s IP address will be assigned automatically by the network’s DHCP server.	
By BOOTP	The NPort S9000’s IP address will be assigned automatically by the network’s BOOTP server.	

ATTENTION

In Dynamic IP environments, the firmware will retry three times every 30 seconds until the network settings are assigned by the DHCP or BOOTP server. The timeout for each try increases from 1 second, to 3 seconds, to 5 seconds.

If the DHCP/BOOTP Server is unavailable, the firmware will use the default IP address (192.168.127.254), Netmask, and Gateway for IP settings.

IP Address

Setting	Description	Factory Default
IP Address of the NPort S9000	Identifies the NPort S9000 on a TCP/IP network.	192.168.127.254

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 addresses to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your network environment.

Subnet Mask

Setting	Description	Factory Default
Subnet mask of the NPort S9000	Identifies the type of network to which the NPort S9000 is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

A subnet mask represents all the network hosts at one geographic location, in one building, or on the same LAN. When a packet is sent out over the network, the NPort 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 NPort, a connection is established directly from the NPort. Otherwise, the connection is established through the given default gateway.

Default Gateway

Setting	Description	Factory Default
Default Gateway of the NPort S9000	The IP address of the router that connects the LAN to an outside network.	None

A gateway is a network gateway 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 needs to know the IP address of the default gateway computer in order to communicate with the hosts outside the local network environment. For the correct gateway IP address information, consult the network administrator.

DNS IP Address

Setting	Description	Factory Default
1st DNS Server's IP Address	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the NPort S9000's URL (e.g., www.NPortS9000.company.com) in your browser's address field, instead of entering the IP address.	None
2nd DNS Server's IP Address	The IP address of the DNS Server used by your network. The NPort S9000 will try to locate the 2nd DNS Server if the 1st DNS Server fails to connect.	None

When the user wants to visit a particular website, the computer asks a Domain Name System (DNS) server for the website's correct IP address and the computer user the response to connect to the web server. DNS is the way Internet domain names are identified and translated into IP addresses. A domain name is an alphanumeric name, such as moxa.com, that is usually easier to remember. A DNS server is a host that translates this kind of text-based domain name into the numeric IP address used to establish a TCP/IP connection.

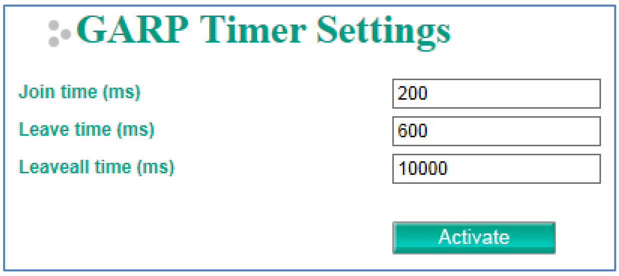
In order to use the NPort's DNS feature, you need to set the IP address of the DNS server to be able to access the host with the domain name. The NPort provides **DNS server 1** and **DNS server 2** configuration items to configure the IP address of the DNS server. DNS Server 2 is included for use when DNS sever 1 is unavailable.

The NPort plays the role of DNS client. Functions that support domain name in the NPort are **Time Sever IP Address**, **TCP Client-Destination IP Address**, **Mail Server**, **SNMP Trap IP Address**, and **IP Location Server**.

GARP Timer Settings

Generic Attribute Registration Protocol (GARP) was defined by the IEEE 802.1 working group to provide a generic framework. GARP defines the architecture, rules of operation, state machines, and variables for the registration and deregistration of attribute values.

The GARP Timer Settings are exchanged by creating the applications via GVRP (GARP VLAN Registration Protocol) to set the attributes of timer.



GARP Timer Settings

Join time (ms): 200

Leave time (ms): 600

Leaveall time (ms): 10000

Join Time

Setting	Description	Factory default
None	Specifies the period of the join time	200

Leave Time

Setting	Description	Factory default
None	Specifies the period of leave time	600

Leaveall Time

Setting	Description	Factory default
None	Specifies the period of leaveall time	10000

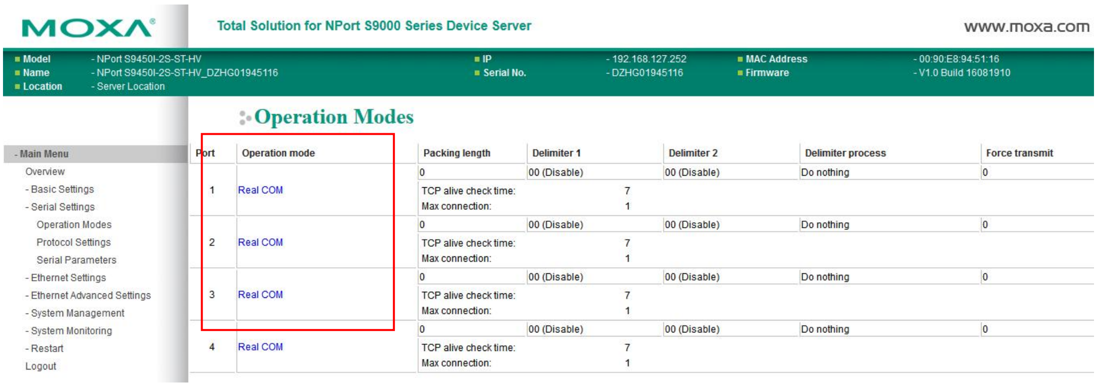
NOTE **Leave Time** should be at least twice more than **Join Time,** and **Leaveall Time** should be larger than **Leave Time**.

Moxa switches support IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol), which is different from IGMP (Internet Group Management Protocol). GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or deregister Group membership information dynamically. GMRP functions similarly to GVRP, except that GMRP registers multicast addresses on ports. When a port receives a GMRP-join message, it will register the multicast address to its database if the multicast address is not registered, and all the multicast packets with that multicast address are able to be forwarded from this port. When a port receives a GMRP-leave message, it will deregister the multicast address from its database, and all the multicast packets with this multicast address will not be able to be forwarded from this port.

Serial Settings

Operation Modes

Click on **Operation Modes**, located under **Serial Settings**, to display serial port settings for four serial ports. To modify serial operation mode settings for a particular port, click on **Operation Modes** of the serial port in the window on the right-hand side.



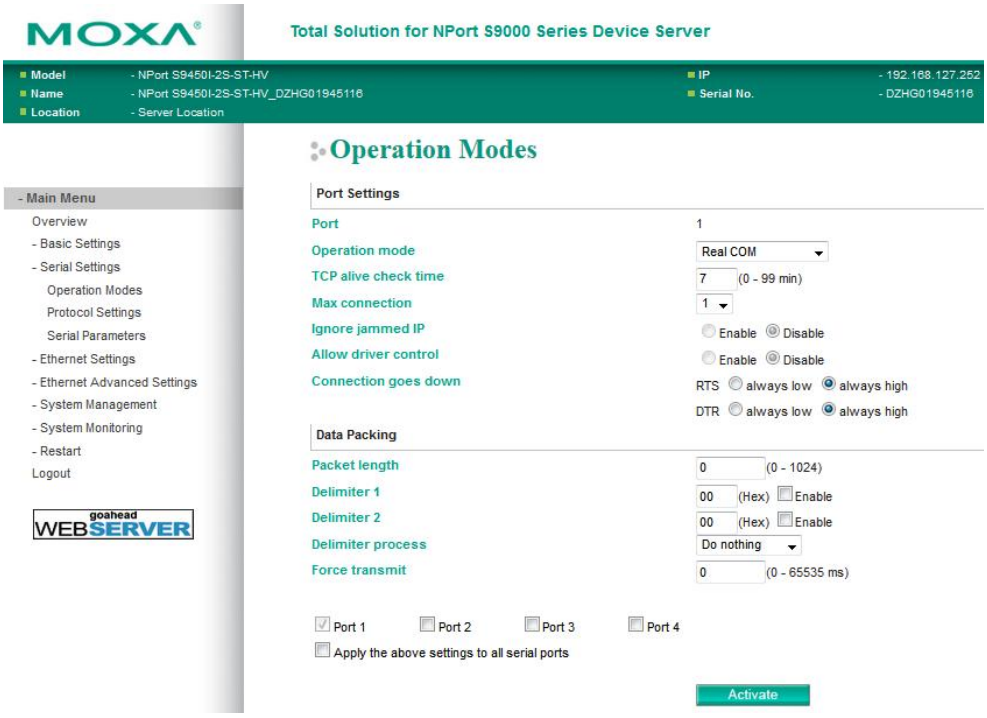
Model	- NPort S9450I-2S-ST-HV	IP	- 192.168.127.252
Name	- NPort S9450I-2S-ST-HV_DZHG01945116	Serial No.	- DZHG01945116
Location	- Server Location		

MAC Address	- 00:90:E8:94:51:16
Firmware	- V1.0 Build 16081910

Operation Modes

Port	Operation mode	Packing length	Delimiter 1	Delimiter 2	Delimiter process	Force transmit
1	Real COM	0 TCP alive check time: 7 Max connection: 1	00 (Disable)	00 (Disable)	Do nothing	0
2	Real COM	0 TCP alive check time: 7 Max connection: 1	00 (Disable)	00 (Disable)	Do nothing	0
3	Real COM	0 TCP alive check time: 7 Max connection: 1	00 (Disable)	00 (Disable)	Do nothing	0
4	Real COM	0 TCP alive check time: 7 Max connection: 1	00 (Disable)	00 (Disable)	Do nothing	0

Real COM Mode



Model	- NPort S9450I-2S-ST-HV	IP	- 192.168.127.252
Name	- NPort S9450I-2S-ST-HV_DZHG01945116	Serial No.	- DZHG01945116
Location	- Server 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	○ Enable ● Disable
Allow driver control	○ Enable ● 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
Force transmit	0 (0 - 65535 ms)

☑ Port 1 □ Port 2 □ Port 3 □ Port 4

□ Apply the above settings to all serial ports

Port Settings

Max connection

Setting	Factory Default	Necessity
1, 2, 3, 4, 5, 6, 7, 8	1	Required

This field is used if you need to receive data from different hosts simultaneously. When set to 1, only one specific host can access this port on the NPort S9000, and the Real COM driver on that host will have full control over the port. When set to 2 or greater, the Real COM drivers for up to the specified number of hosts may open this port at the same time. When multiple hosts' Real COM drivers open the port at the same time, the COM driver only provides a pure data tunnel—no control capability provided. The serial port parameters will use firmware settings instead of your application program (AP) settings.

Application software that is based on the COM driver will receive a driver response of "success" when the software uses any of the Win32 API functions. The firmware will only send data back to the driver on the host.

Data will be sent first-in-first-out when data enters the NPort S9000 from the Ethernet interface.

⚠ **ATTENTION**

When Max connection is set to 2 to 8, this means that the NPort use a "multiconnection application" (i.e., two to eight hosts are allowed access to the port at the same time). When using a multiconnection application, the NPort will use the serial communication parameters set in the console. All of the hosts connected to that port must use the same serial settings. If one of the hosts opens the COM port with parameters that are different from the NPort's console setting, data communication may not work properly.

Ignore jammed IP

Setting	Factory Default	Necessity
Enable or Disable	Disable	Optional

Previously, if **Max connection** was greater than 1, the serial device was transmitting data, and a connected host was not responding, then the NPort would wait until the data was transmitted successfully before transmitting the second group of data to all hosts. Currently, if you select Enable for **Ignore jammed IP**, the host that is not responding will be ignored, but the data will still be transmitted to the other hosts.

Allow driver control

Setting	Factory Default	Necessity
Enable or Disable	Disable	Optional

If **Max connection** is greater than 1, the NPort will ignore driver control commands from all connected hosts. However, if you set **Allow driver control** to **YES**, control commands will be accepted. Note that since the NPort S9000 may get configuration changes from multiple hosts, the most recent command received will take precedence.

Connection goes down

Setting	Factory Default	Necessity
Always High or Always Low	Always High	Optional

You can configure 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. Use **always low** if you want the RTS and DTR signals to change their status to low when the Ethernet connection goes down. Use **always high** if you do not want the Ethernet connection status to affect the RTS or DTR signals.

Data Packing

Packet length

Setting	Factory Default	Necessity
0 to 1024	0	Optional

Default = 0, The Delimiter Process will be followed, regardless of the length of the data packet. If the data length (in bytes) matches the configured value, the data will be forced out. The data length can be configured for 0 to 1024 bytes. Set to 0 if you do not need to limit the length.

Delimiter 1

Setting	Factory Default	Necessity
00 to FF	None	Optional

Delimiter 2

Setting	Factory Default	Necessity
00 to FF	None	Optional

When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in a hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to indicate when data should be sent.

ATTENTION

Delimiter 2 is optional. If left blank, then Delimiter 1 alone trips clearing of the buffer. If the size of the serial data received is greater than 1 KB, the NPort will automatically pack the data and send it to the Ethernet. However, to use the delimiter function, you must at least enable Delimiter 1. If Delimiter 1 is left blank and Delimiter 2 is enabled, the delimiter function will not work properly.

Delimiter process

Setting	Factory Default	Necessity
Do nothing Delimiter + 1 Delimiter + 2 Strip Delimiter	Do Nothing	Optional

[Delimiter + 1] or [Delimiter + 2]: The data will be transmitted when an additional byte (for Delimiter +1), or an additional 2 bytes (for Delimiter +2) of data is received after receiving the delimiter.

[Strip Delimiter]: When the delimiter is received, the delimiter is deleted (i.e., stripped), and the remaining data is transmitted.

[Do nothing]: The data will be transmitted when the delimiter is received.

Force transmit

Setting	Factory Default	Necessity
0 to 65535 ms	0 ms	Optional

0: Disable the Force Transmit timeout.

1 to 65535: Forces the NPort's TCP/IP protocol software to try to pack serial data received during the specified time into the same data frame.

This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full, or if the Force Transmit time interval reaches the time specified under Force Transmit timeout.

Optimal Force Transmit timeout differs according to 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

10 (bits) / 1200 (bits/s) * 1000 (ms/s) = 8.3 ms.

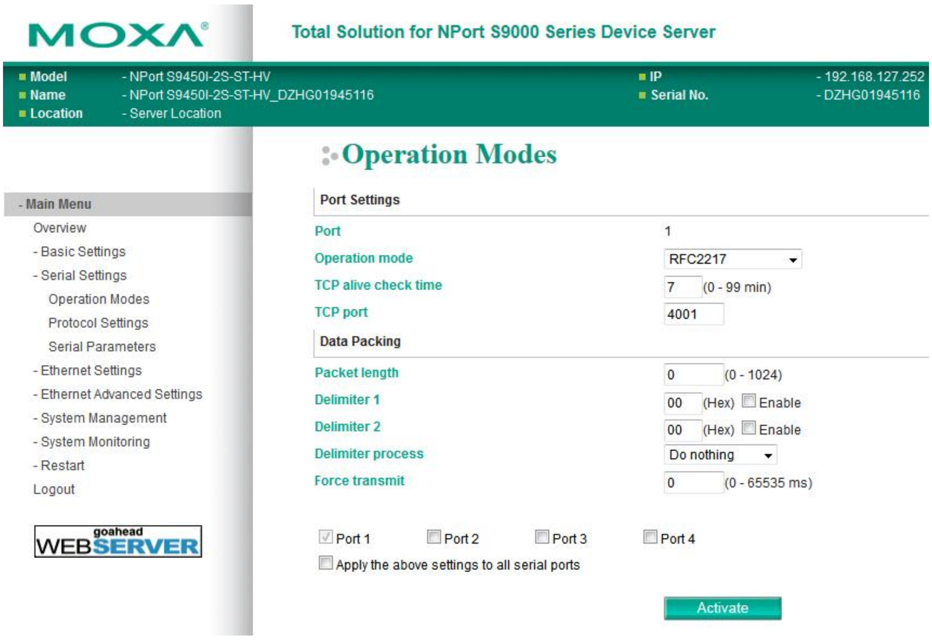
Therefore, you should set Force Transmit timeout to be larger than 8.3 ms. Force Transmit timeout is specified in milliseconds and must be larger than 10 ms.

If the user wants to send the series of characters in a packet, the serial device attached to the NPort should send characters without time delay larger than Force Transmit timeout between characters and the total length of data must be smaller than or equal to the NPort’s internal buffer size. The serial communication buffer size of the NPort is 1 Kbytes per port.

Parameter Copy

Apply the above setting to other serial ports, you may use the checkboxes at the bottom of the window to apply the settings to one or more ports.

RFC2217 Mode



Model - NPort S9450I-2S-ST-HV
Name - NPort S9450I-2S-ST-HV_DZHG01945116
Location - Server Location
IP - 192.168.127.252
Serial No. - DZHG01945116

Operation Modes

Port Settings

Port	1
Operation mode	RFC2217
TCP alive check time	7 (0 - 99 min)
TCP port	4001

Data Packing

Packet length	0 (0 - 1024)
Delimiter 1	00 (Hex) □ Enable
Delimiter 2	00 (Hex) □ Enable
Delimiter process	Do nothing
Force transmit	0 (0 - 65535 ms)

☑ Port 1 □ Port 2 □ Port 3 □ Port 4
□ Apply the above settings to all serial ports

Port Settings

TCP port (default=4001)

This is the TCP port number assignment for the serial port on the NPort S9000. It is the port number that the serial port uses to listen to connections and that other devices must use to contact the serial port. To avoid conflicts with well-known TCP ports, the default is set to 4001.

Data Packing

Packet length

Setting	Factory Default	Necessity
0 to 1024	0	Optional

Default = 0, The Delimiter Process will be followed, regardless of the length of the data packet. If the data length (in bytes) matches the configured value, the data will be forced out. The data length can be configured for 0 to 1024 bytes. Set to 0 if you do not need to limit the length.

Delimiter 1

Setting	Factory Default	Necessity
00 to FF	None	Optional

Delimiter 2

Setting	Factory Default	Necessity
00 to FF	None	Optional

When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in a hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to indicate when data should be sent.

ATTENTION

Delimiter 2 is optional. If left blank, then Delimiter 1 alone trips clearing of the buffer. If the size of the serial data received is greater than 1 KB, the NPort will automatically pack the data and send it to the Ethernet. However, to use the delimiter function, you must at least enable Delimiter 1. If Delimiter 1 is left blank and Delimiter 2 is enabled, the delimiter function will not work properly.

Delimiter process

Setting	Factory Default	Necessity
Do nothing Delimiter + 1 Delimiter + 2 Strip Delimiter	Do Nothing	Optional

[Delimiter + 1] or [Delimiter + 2]: The data will be transmitted when an additional byte (for Delimiter +1), or an additional 2 bytes (for Delimiter +2) of data is received after receiving the Delimiter.

[Strip Delimiter]: When the Delimiter is received, the Delimiter is deleted (i.e., stripped), and the remaining data is transmitted.

[Do nothing]: The data will be transmitted when the Delimiter is received.

Force transmit

Setting	Factory Default	Necessity
0 to 65535 ms	0 ms	Optional

0: Disable the Force Transmit timeout.

1 to 65535: Forces the NPort's TCP/IP protocol software to try to pack serial data received during the specified time into the same data frame.

This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full or if the Force Transmit time interval reaches the time specified under Force Transmit timeout.

Optimal Force Transmit timeout differs according to 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

10 (bits) / 1200 (bits/s) * 1000 (ms/s) = 8.3 ms.

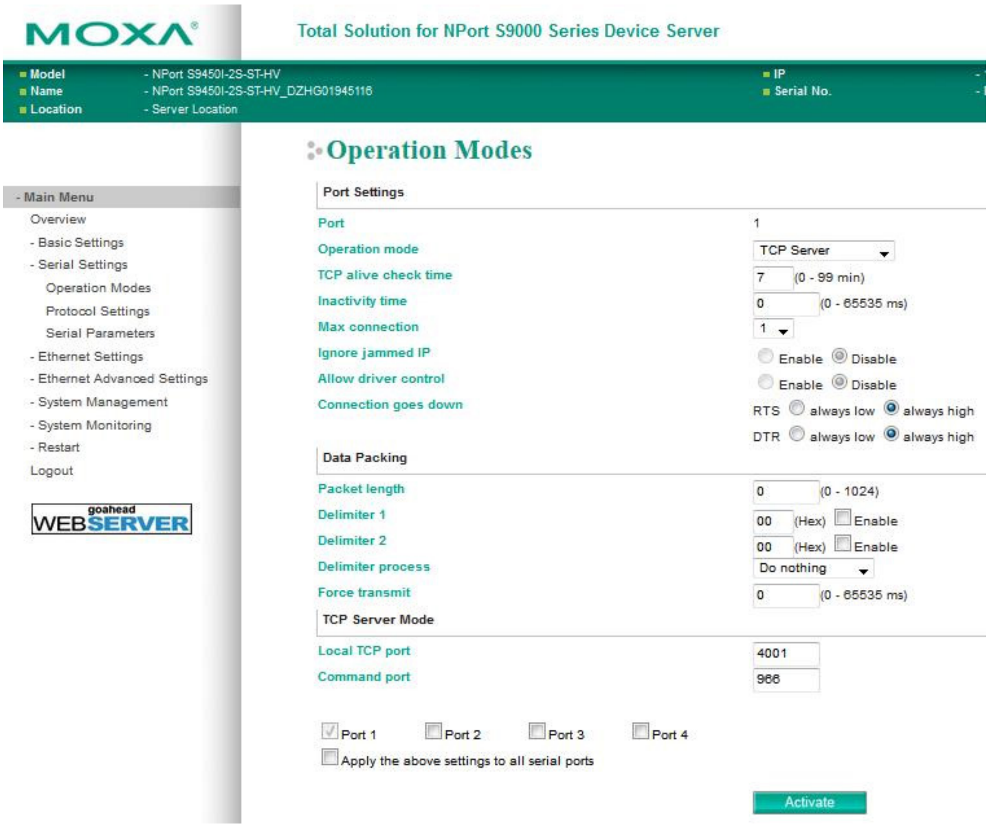
Therefore, you should set Force Transmit timeout to be larger than 8.3 ms. Force Transmit timeout is specified in milliseconds and must be larger than 10 ms.

If the user wants to send the series of characters in a packet, the serial device attached to the NPort should send characters without time delay larger than Force Transmit timeout between characters and the total length of data must be smaller than or equal to the NPort's internal buffer size. The serial communication buffer size of the NPort is 1 Kbytes per port.

Parameter Copy

Apply the above setting to other serial ports; you may use the checkboxes at the bottom of the window to apply the settings to one or more ports.

TCP Server Mode



Model - NPort S9450I-2S-ST-HV
Name - NPort S9450I-2S-ST-HV_DZHG01945116
Location - Server Location
IP -
Serial No. -

Operation Modes

Port Settings

Port	1
Operation mode	TCP Server
TCP alive check time	7 (0 - 99 min)
Inactivity time	0 (0 - 65535 ms)
Max connection	1
Ignore jammed IP	○ Enable ● Disable
Allow driver control	○ Enable ● 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
Force transmit	0 (0 - 65535 ms)

TCP Server Mode

Local TCP port	4001
Command port	966

☑ Port 1 □ Port 2 □ Port 3 □ Port 4
□ Apply the above settings to all serial ports

Port Settings

Inactivity time

Setting	Factory Default	Necessity
0 to 65535 ms	0 ms	Optional

0 ms: TCP connection is not closed due to an idle serial line.

0-65535 ms: The NPort automatically closes the TCP connection if there is no serial data activity for the given time. After the connection is closed, the NPort starts listening for another host's TCP connection.

This parameter defines the maintenances status as Closed or Listen on the TCP connection. The connection is closed if there is no incoming or outgoing data through the serial port during the specific Inactivity time.

If the value of inactivity time is set to 0, the current TCP connection is maintained until there is a connection close request. Although inactivity time is disabled, the NPort will check the connection status between the NPort and remote host by sending "keep alive" packets periodically. If the remote host does not respond to the packet, it assumes that the connection was closed down unintentionally. The NPort will then force the existing TCP connection to close.

ATTENTION

The Inactivity time should at least be set larger than that of Force Transmit timeout. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.

Max connection

Setting	Factory Default	Necessity
1, 2, 3, 4, 5, 6, 7, 8	1	Required

This field is used if you need to receive data from different hosts simultaneously. When set to 1, only one specific host can access this port of the NPort S9000, and the Real COM driver on that host will have full control over the port. When set to 2 or greater, up to the specified number of hosts' Real COM drivers may open this port at the same time. When multiple hosts' Real COM drivers open the port at the same time, the COM driver only provides a pure data tunnel—no control ability. The serial port parameters will use firmware settings instead of depending on your application program (AP).

Application software that is based on the COM driver will receive a driver response of "success" when the software uses any of the Win32 API functions. The firmware will only send data back to the driver on the host.

Data will be sent first-in-first-out when data enters the NPort S9000 from the Ethernet interface.

ATTENTION

When Max connection is set to 2 to 8, this means that the NPort will be using a "multiconnection application" (i.e., two to eight hosts are allowed access to the port at the same time). When using a multiconnection application, the NPort will use the serial communication parameters set in the console. All of the hosts connected to that port must use the same serial settings. If one of the hosts opens the COM port with parameters that are different from the NPort's console setting, data communication may not work properly.

Ignore jammed IP

Setting	Factory Default	Necessity
Enable or Disable	Disable	Optional

Previously, if Max connection was greater than 1 and the serial device was transmitting data, and a connected host was not responding, then the NPort would wait until the data was transmitted successfully before transmitting the second group of data to all hosts. Currently, if you select **Enable** for **Ignore jammed IP**, the host that is not responding will be ignored, but the data will still be transmitted to the other hosts.

Allow driver control

Setting	Factory Default	Necessity
Enable or Disable	Disable	Optional

If Max connection is greater than 1, the NPort will ignore driver control commands from all connected hosts. However, if you set **Allow driver control** to **YES**, control commands will be accepted. Note that since the NPort S9000 may get configuration changes from multiple hosts, the most recent command received will take precedence.

Connection goes down

Setting	Factory Default	Necessity
Always High or Always Low	Always High	Optional

You can configure 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. Use **always low** if you want the RTS and DTR signal to change their state to low when the Ethernet connection goes down. Use **always high** if you do not want the Ethernet connection status to affect the RTS or DTR signals.

Data Packing

Packet length

Setting	Factory Default	Necessity
0 to 1024	0	Optional

Default = 0, The Delimiter Process will be followed, regardless of the length of the data packet. If the data length (in bytes) matches the configured value, the data will be forced out. The data length can be configured for 0 to 1024 bytes. Set to 0 if you do not need to limit the length.

Delimiter 1

Setting	Factory Default	Necessity
00 to FF	None	Optional

Delimiter 2

Setting	Factory Default	Necessity
00 to FF	None	Optional

When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in a hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to indicate when data should be sent.

ATTENTION

Delimiter 2 is optional. If left blank, then Delimiter 1 alone trips clearing of the buffer. If the size of the serial data received is greater than 1 KB, the NPort will automatically pack the data and send it to the Ethernet. However, to use the delimiter function, you must at least enable Delimiter 1. If Delimiter 1 is left blank and Delimiter 2 is enabled, the delimiter function will not work properly.

Delimiter process

Setting	Factory Default	Necessity
Do nothing Delimiter + 1 Delimiter + 2 Strip Delimiter	Do Nothing	Optional

[Delimiter + 1] or [Delimiter + 2]: The data will be transmitted when an additional byte (for Delimiter +1), or an additional 2 bytes (for Delimiter +2) of data is received after receiving the delimiter.

[Strip Delimiter]: When the delimiter is received, the delimiter is deleted (i.e., stripped), and the remaining data is transmitted.

[Do nothing]: The data will be transmitted when the delimiter is received.

Force transmit

Setting	Factory Default	Necessity
0 to 65535 ms	0 ms	Optional

0: Disable the Force Transmit timeout.

1 to 65535: Forces the NPort's TCP/IP protocol software to try to pack serial data received during the specified time into the same data frame.

This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full or if the Force Transmit time interval reaches the time specified under Force Transmit timeout.

Optimal Force Transmit timeout differs according to 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

10 (bits) / 1200 (bits/s) * 1000 (ms/s) = 8.3 ms.

Therefore, you should set Force Transmit timeout to be larger than 8.3 ms. Force Transmit timeout is specified in milliseconds and must be larger than 10 ms.

If the user wants to send the series of characters in a packet, the serial device attached to the NPort should send characters without time delay larger than Force Transmit timeout between characters, and the total length of data must be smaller than or equal to the NPort's internal buffer size. The serial communication buffer size of the NPort is 1 Kbytes per port.

TCP Server Mode

Local TCP port

Setting	**Factory Default**	**Necessity**
1 to 65535	4001	Required

The TCP port that the NPort uses to listen to connections and that other devices must use to contact the NPort. To avoid conflicts with well-known TCP ports, the default is set to 4001.

Command port

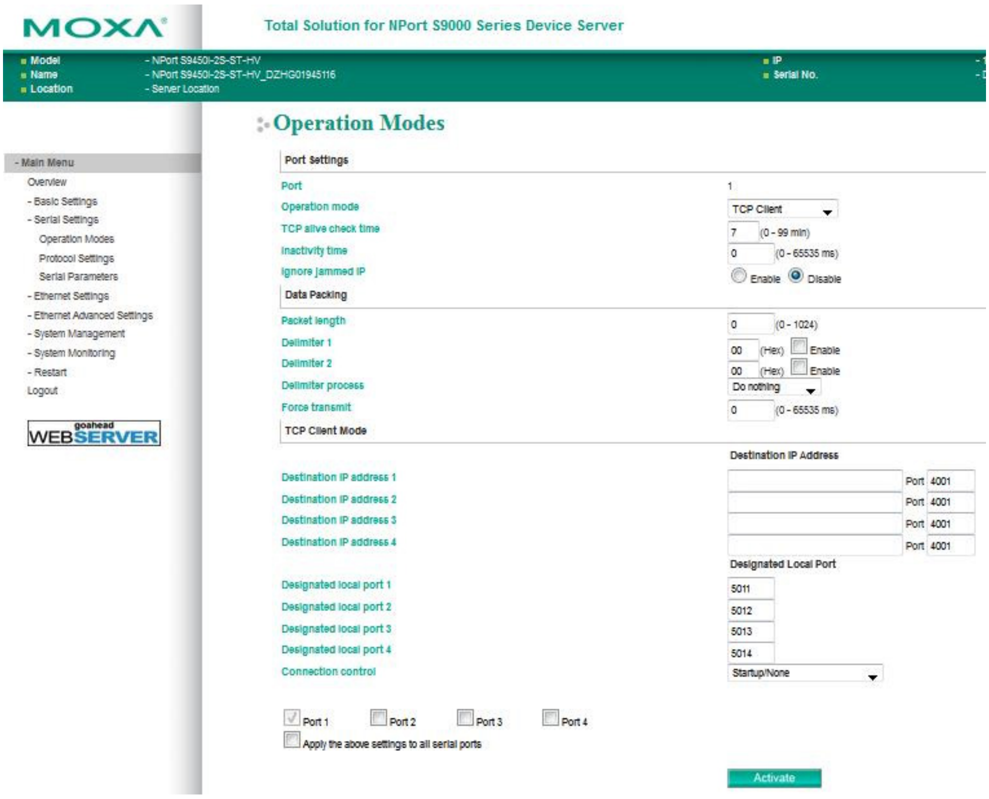
Setting	**Factory Default**	**Necessity**
1 to 65535	966	Optional

The Command port is the TCP port for listening to SSDK commands from the host. In order to prevent a TCP port conflict with other applications, the user can adjust the command port to another port if needed. And SSDK Commands will automatically check out the Command Port on the NPort so that the user does not need to configure the program.

Parameter Copy

Apply the above setting to other serial ports, you may use the checkboxes at the bottom of the window to apply the settings to one or more ports.

TCP Client Mode



Model - NPort S9450I-2S-ST-HV
Name - NPort S9450I-2S-ST-HV_DZHG01945116
Location - Server Location
IP
Serial No.

Operation Modes

Port settings

Port	1
Operation mode	TCP Client
TCP alive check time	7 (0 - 99 min)
Inactivity time	0 (0 - 65535 ms)
Ignore jammed IP	○ Enable ● Disable

Data Packing

Packet length	0 (0 - 1024)
Delimiter 1	00 (Hex) □ Enable
Delimiter 2	00 (Hex) □ Enable
Delimiter process	Do nothing
Force transmit	0 (0 - 65535 ms)

TCP Client Mode

	Destination IP Address	
Destination IP address 1		Port 4001
Destination IP address 2		Port 4001
Destination IP address 3		Port 4001
Destination IP address 4		Port 4001
	Designated Local Port	
Designated local port 1	5011	
Designated local port 2	5012	
Designated local port 3	5013	
Designated local port 4	5014	
Connection control	Startup/None	

☑ Port 1 □ Port 2 □ Port 3 □ Port 4
□ Apply the above settings to all serial ports

Port Settings

Inactivity time

Setting	Factory Default	Necessity
0 to 65535 ms	0 ms	Optional

0 ms: TCP connection is not closed due to an idle serial line.

0-65535 ms: The NPort automatically closes TCP connection, if there is no serial data activity for the given time.

This parameter defines the maintenance status as Closed or Listen on the TCP connection. The connection is closed if there is no incoming or outgoing data through the serial port during the specific Inactivity time.

If the value of inactivity time is set to 0, the current TCP connection is maintained until there's connection close request. Although the inactivity time is disabled, the NPort will check the connection status between the NPort and remote host by sending "keep alive" packets periodically. If the remote host does not respond to the packets, it treats the connection as being down unintentionally. The NPort will then force the existing TCP connection to close.

ATTENTION

The Inactivity time should at least be set larger than that of Force transmit timeout. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.

ATTENTION

Inactivity time is ONLY active when "TCP connect on" is set to "Any character."

Ignore jammed IP

Setting	Factory Default	Necessity
Enable or Disable	Disable	Optional

Previously, if Max connection was greater than 1 and the serial device was transmitting data, and a connected host was not responding, then the NPort would wait until the data was transmitted successfully before transmitting the second group of data to all hosts. Currently, if you select **Enable** for **Ignore jammed IP**, the host that is not responding will be ignored, but the data will still be transmitted to the other hosts.

Data Packing

Packet length

Setting	Factory Default	Necessity
0 to 1024	0	Optional

Default = 0, The Delimiter Process will be followed, regardless of the length of the data packet. If the data length (in bytes) matches the configured value, the data will be forced out. The data length can be configured for 0 to 1024 bytes. Set to 0 if you do not need to limit the length.

Delimiter 1

Setting	Factory Default	Necessity
00 to FF	None	Optional

Delimiter 2

Setting	Factory Default	Necessity
00 to FF	None	Optional

When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in a hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to indicate when data should be sent.

ATTENTION

Delimiter 2 is optional. If left blank, then Delimiter 1 alone trips clearing of the buffer. If the size of the serial data received is greater than 1 KB, the NPort will automatically pack the data and send it to the Ethernet. However, to use the delimiter function, you must at least enable Delimiter 1. If Delimiter 1 is left blank and Delimiter 2 is enabled, the delimiter function will not work properly.

Delimiter process

Setting	Factory Default	Necessity
Do nothing Delimiter + 1 Delimiter + 2 Strip Delimiter	Do Nothing	Optional

[Delimiter + 1] or [Delimiter + 2]: The data will be transmitted when an additional byte (for Delimiter +1), or an additional two bytes (for Delimiter +2) of data is received after receiving the delimiter.

[Strip Delimiter]: When the delimiter is received, the delimiter is deleted (i.e., stripped), and the remaining data is transmitted.

[Do nothing]: The data will be transmitted when the delimiter is received.

Force transmit

Setting	Factory Default	Necessity
0 to 65535 ms	0 ms	Optional

0: Disable the Force Transmit timeout.

1 to 65535: Forces the NPort's TCP/IP protocol software to try to pack serial data received during the specified time into the same data frame.

This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full or if the Force Transmit time interval reaches the time specified under Force Transmit timeout.

Optimal Force Transmit timeout differs according to 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

10 (bits) / 1200 (bits/s) * 1000 (ms/s) = 8.3 ms.

Therefore, you should set Force Transmit timeout to be larger than 8.3 ms. Force Transmit timeout is specified in milliseconds and must be larger than 10 ms.

If the user wants to send the series of characters in a packet, the serial device attached to the NPort should send characters without time delay larger than Force Transmit timeout between characters and the total length of data must be smaller than or equal to the NPort's internal buffer size. The serial communication buffer size of the NPort is 1 Kbytes per port.

TCP Client Mode

Destination IP address 1

Setting	Factory Default	Necessity
IP address or Domain Address (E.g., 192.168.1.1)	None	Required

Allows the NPort to connect actively to the remote host whose address is set by this parameter.

Destination IP address 2/3/4

Setting	Factory Default	Necessity
IP address or Domain Address (E.g., 192.168.1.1)	None	Optional

Allows the NPort to connect actively to the remote host whose address is set by this parameter.

TCP port (default=4001): This is the TCP port number assignment for the serial port on the NPort S9000. It is the port number that the serial port uses to listen to connections and that other devices must use to contact the serial port. To avoid conflicts with well-known TCP ports, the default is set to 4001.

ATTENTION

Up to four connections can be established between the NPort and hosts. The connection speed or throughput may be low if one of the four connections is slow, since the slow connection will slow down the other three connections.

ATTENTION

The **Destination IP address** parameter can use both IP address and Domain Name. For some applications, the user may need to send the data actively to the remote destination domain name.

Designated Local Port 1/2/3/4

Setting	Factory Default	Necessity
TCP Port No.	5001 (Port 1)	Required

Setting	Factory Default	Necessity
	5002 (Port 2) 5003 (Port 3) 5004 (Port 4)	

Connection control

Setting	Factory Default	Necessity
Startup/None, Any Character/None, Any Character/Inactivity Time, DSR ON/DSR OFF, DSR ON/None, DCD ON/DCD OFF, DCD ON/None	Startup/None	Required

The meaning of each of the above settings is given in the table below. In general, both the Connect condition and Disconnect condition are given.

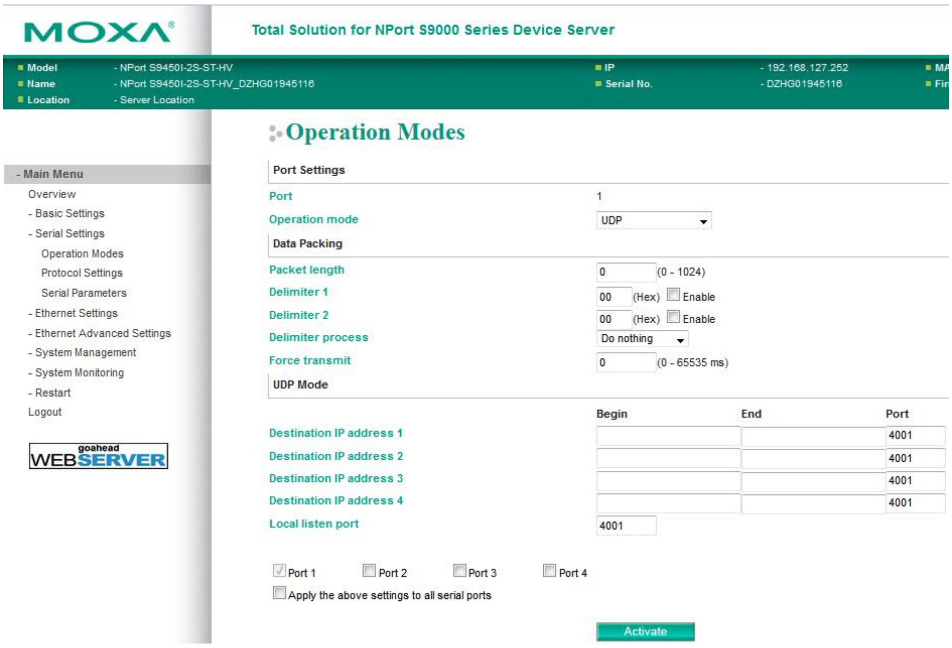
TCP Connection on

Connect/Disconnect	Description
Startup/None (default)	A TCP connection will be established on startup and will remain active indefinitely.
Any Character/None	A TCP connection will be established when any character is received from the serial interface and will remain active indefinitely.
Any Character/ Inactivity Time	A TCP connection will be established when any character is received from the serial interface and will be disconnected when the Inactivity time out is reached.
DSR On/DSR Off	A TCP connection will be established when a DSR "On" signal is received and will be disconnected when a DSR "Off" signal is received.
DSR On/None	A TCP connection will be established when a DSR "On" signal is received and will remain active indefinitely.
DCD On/DCD Off	A TCP connection will be established when a DCD "On" signal is received and will be disconnected when a DCD "Off" signal is received.
DCD On/None	A TCP connection will be established when a DCD "On" signal is received and will remain active indefinitely.

Parameter Copy

Apply the above setting to other serial ports; you may use the checkboxes at the bottom of the window to apply the settings to one or more ports.

UDP Mode



Total Solution for NPort S9000 Series Device Server

■ Model	- NPort S9450I-2S-ST-HV	■ IP	- 192.168.127.252
■ Name	- NPort S9450I-2S-ST-HV_DZHG01945116	■ Serial No.	- DZHG01945116
■ Location	- Server Location		

Operation Modes

Port Settings

Port: 1

Operation mode: UDP

Data Packing

Packet length: 0 (0 - 1024)

Delimiter 1: 00 (Hex) □ Enable

Delimiter 2: 00 (Hex) □ Enable

Delimiter process: Do nothing

Force transmit: 0 (0 - 65535 ms)

UDP Mode

	Begin	End	Port
Destination IP address 1			4001
Destination IP address 2			4001
Destination IP address 3			4001
Destination IP address 4			4001

Local listen port: 4001

☑ Port 1 □ Port 2 □ Port 3 □ Port 4

□ Apply the above settings to all serial ports

Data Packing

Packing length

Setting	Factory Default	Necessity
0 to 1024	0	Optional

Default = 0, The Delimiter Process will be followed, regardless of the length of the data packet. If the data length (in bytes) matches the configured value, the data will be forced out. The data length can be configured for 0 to 1024 bytes. Set to 0 if you do not need to limit the length.

Delimiter 1

Setting	Factory Default	Necessity
00 to FF	None	Optional

Delimiter 2

Setting	Factory Default	Necessity
00 to FF	None	Optional

When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in a hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to indicate when data should be sent.

ATTENTION

Delimiter 2 is optional. If left blank, then Delimiter 1 alone trips clearing of the buffer. If the size of the serial data received is greater than 1 KB, the NPort will automatically pack the data and send it to the Ethernet. However, to use the delimiter function, you must at least enable Delimiter 1. If Delimiter 1 is left blank and Delimiter 2 is enabled, the delimiter function will not work properly.

Delimiter process

Setting	Factory Default	Necessity
Do nothing Delimiter + 1 Delimiter + 2 Strip Delimiter	Do Nothing	Optional

[Delimiter + 1] or [Delimiter + 2]: The data will be transmitted when an additional byte (for Delimiter +1), or an additional 2 bytes (for Delimiter +2) of data is received after receiving the delimiter.

[Strip Delimiter]: When the delimiter is received, the delimiter is deleted (i.e., stripped), and the remaining data is transmitted.

[Do nothing]: The data will be transmitted when the delimiter is received.

Force transmit

Setting	Factory Default	Necessity
0 to 65535 ms	0 ms	Optional

0: Disable the Force Transmit timeout.

1 to 65535: Forces the NPort's TCP/IP protocol software to try to pack serial data received during the specified time into the same data frame.

This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full or if the Force Transmit time interval reaches the time specified under Force Transmit timeout.

Optimal Force Transmit timeout differs according to 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

10 (bits) / 1200 (bits/s) * 1000 (ms/s) = 8.3 ms.

Therefore, you should set Force Transmit timeout to be larger than 8.3 ms. Force Transmit timeout is specified in milliseconds and must be larger than 10 ms.

If the user wants to send the series of characters in a packet, the serial device attached to the NPort should send characters without time delay larger than Force Transmit timeout between characters and the total length of data must be smaller than or equal to the NPort's internal buffer size. The serial communication buffer size of the NPort is 1 Kbytes per port.

UDP Mode

Destination IP address 1

Setting	Factory Default		Necessity
IP address range	Begin:	Empty	Required
E.g., Begin: 192.168.1.1	End:	Empty	
End: 192.168.1.10	Port:	4001	

Destination IP address 2/3/4

Setting	Factory Default		Necessity
IP address range	Begin:	Empty	Optional
E.g., Begin: 192.168.1.11	End:	Empty	
End: 192.168.1.20	Port:	4001	

Local listen port

Setting	Factory Default	Necessity
1 to 65535	4001	Required

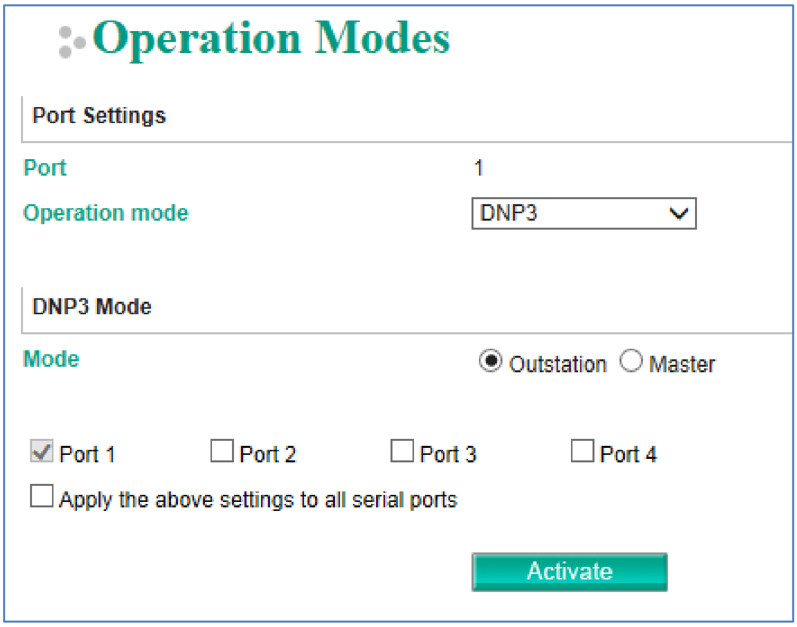
The UDP port that the NPort listens to, and that other devices must use to contact the NPort. To avoid conflicts with well-known UDP ports, the default is set to 4001.

Parameter Copy

Apply the above setting to other serial ports; you may use the checkboxes at the bottom of the window to apply the settings to one or more ports.

DNP3 Mode

The NPort S9000 gateway series supports three operation modes to communicate with Modbus and DNP3 protocols. With the NPort S9000 series, two serial ports can be set to different operation modes. In DNP3 mode, the NPort converts DNP3 serial to DNP3 IP. In DNP3 Raw Socket mode, users can assign a specific TCP port's DNP3 IP data to be converted to DNP3 serial data in a specific serial port of the NPort S9000 series. In Modbus mode, the NPort converts Modbus RTU/ASCII to Modbus TCP.


Operation Modes

Port Settings

Port 1

Operation mode DNP3

DNP3 Mode

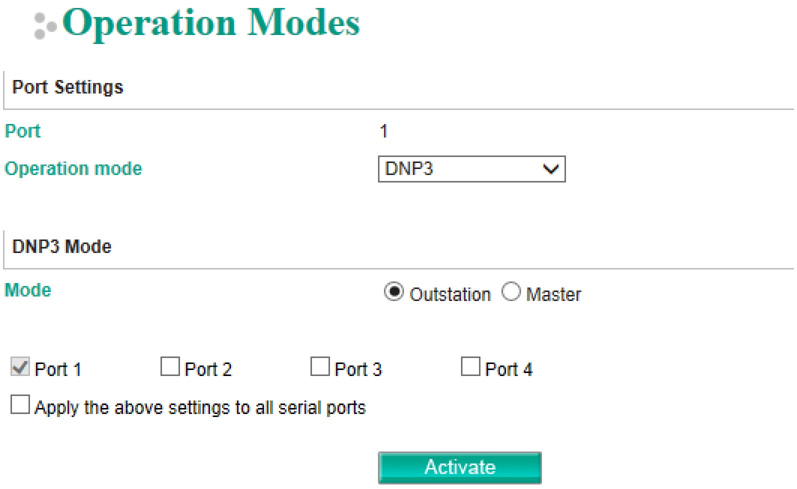
Mode ● Outstation ○ Master

☑ Port 1 □ Port 2 □ Port 3 □ Port 4

□ Apply the above settings to all serial ports

DNP3 Protocol

The NPort S9000 series gateways support DNP3 protocols. The NPort converts the outstation and master's data between DNP3 IP and DNP3 serial. If the serial port is connecting with an outstation device, set the operation mode of the port as Outstation. On the contrary, if the serial port is connecting with a master device, set the operation mode of the port as Master.



Port Settings

Port: 1

Operation mode: DNP3

DNP3 Mode

Mode: ● Outstation ○ Master

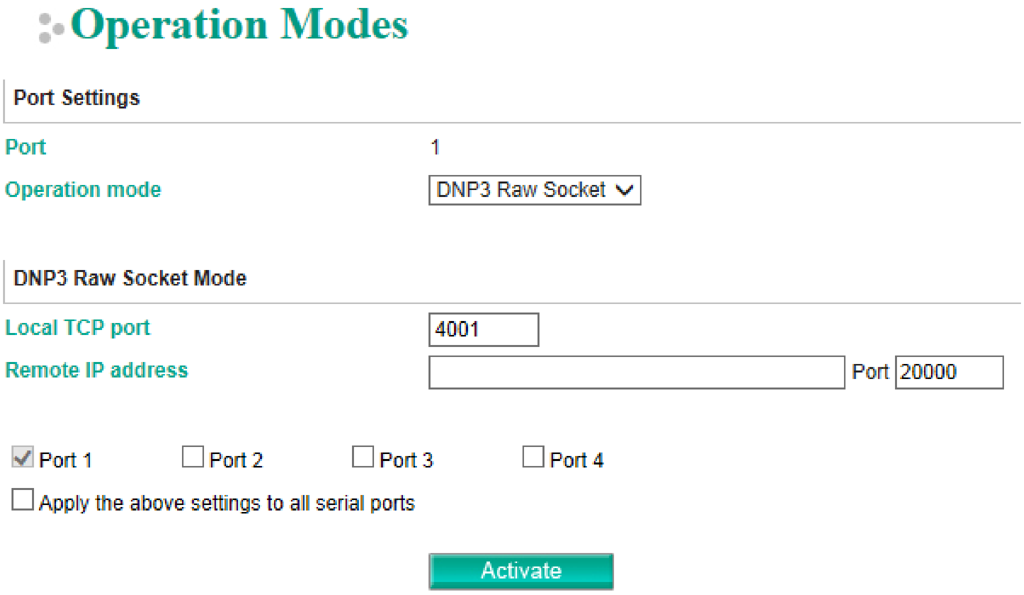
☑ Port 1 □ Port 2 □ Port 3 □ Port 4

□ Apply the above settings to all serial ports

Outstation and master devices have a logical device address for identification in the DNP3 system. You need to set the address table to indicate the routing destination of the DNP3 packet frames received by the gateway. Please go to Serial Settings --> Protocol Settings under the DNP3 tab for relative settings. A default device address routing table is shown in the Address table page under Protocol Settings.

DNP3 Raw Socket Mode

The NPort S9000 series gateways support users to define the routing table by different TCP ports via DNP3 Raw Socket Mode. When configuring the Local TCP port as 4001, all the DNP3 packets coming in from TCP port 4001 will be forwarded to serial port 1 of the NPort S9000. Those unsolicited packets generated by the serial device actively will be forwarded to the IP address and TCP port configured by the Remote IP address.



Port Settings

Port: 1

Operation mode: DNP3 Raw Socket

DNP3 Raw Socket Mode

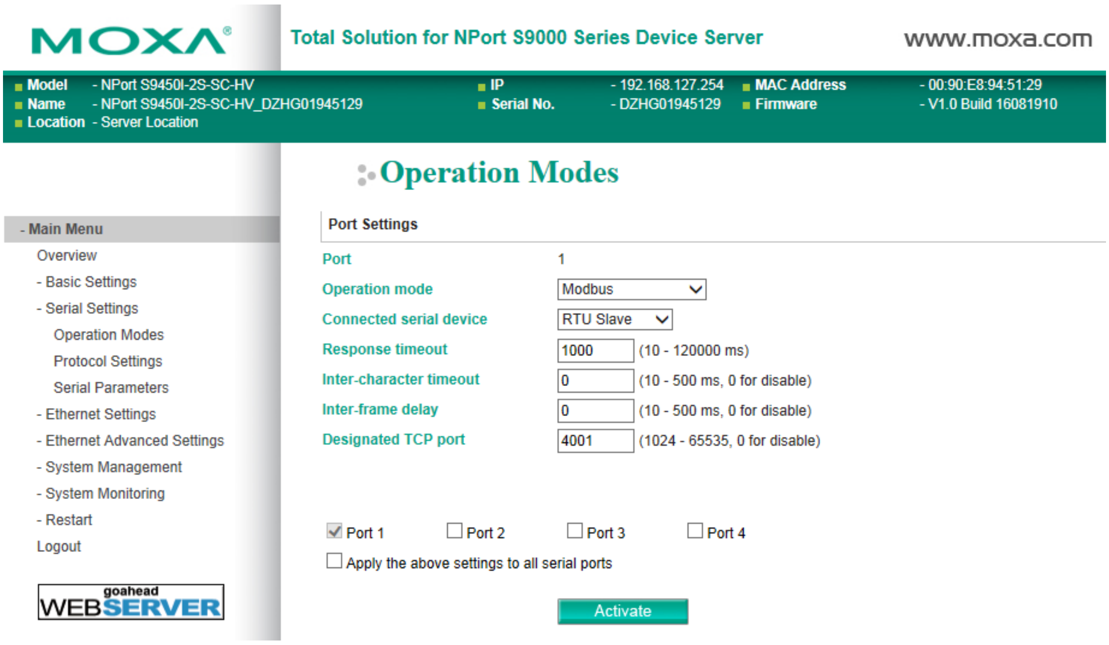
Local TCP port: 4001

Remote IP address: Port 20000

☑ Port 1 □ Port 2 □ Port 3 □ Port 4

□ Apply the above settings to all serial ports

Modbus Mode


MOXA
Total Solution for NPort S9000 Series Device Server
www.moxa.com
Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910
- Main Menu
Overview
- Basic Settings
- Serial Settings
Operation Modes
Protocol Settings
Serial Parameters
- Ethernet Settings
- Ethernet Advanced Settings
- System Management
- System Monitoring
- Restart
Logout
goahead WEBSERVER
Activate

Operation Modes

Port Settings

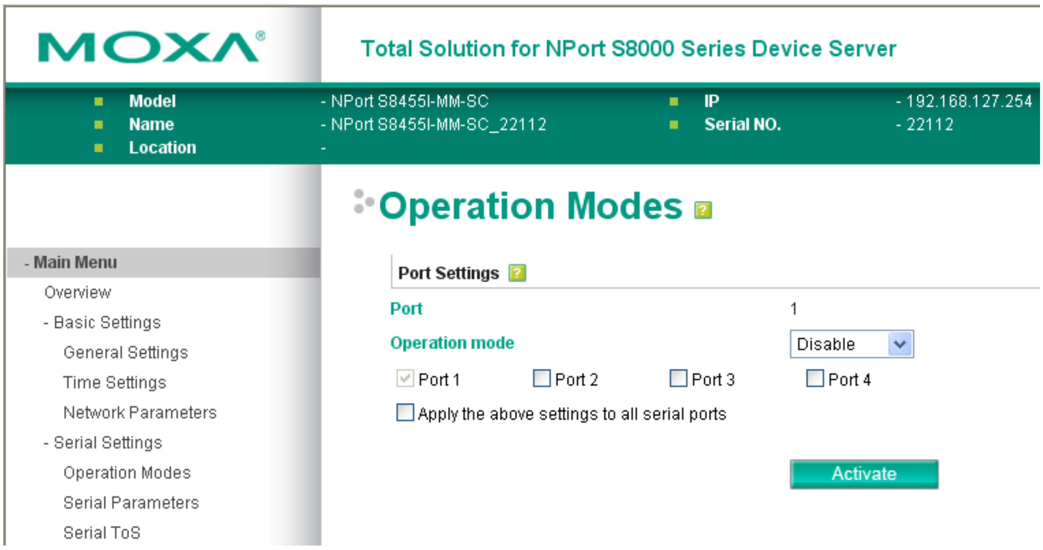
Port: 1
Operation mode: Modbus
Connected serial device: RTU Slave
Response timeout: 1000 (10 - 120000 ms)
Inter-character timeout: 0 (10 - 500 ms, 0 for disable)
Inter-frame delay: 0 (10 - 500 ms, 0 for disable)
Designated TCP port: 4001 (1024 - 65535, 0 for disable)

☑ Port 1 □ Port 2 □ Port 3 □ Port 4
□ Apply the above settings to all serial ports

Port Settings

Parameters	Description
Connected serial device	Select the role of the device that is connected to the serial port.
Response timeout	According to the Modbus standard, the time it takes for a slave device to respond to a request is defined by the device manufacturer. Based on this response time, a master can be configured to wait a certain amount of time for a slave's response. If no response is received within the specified time, the master will disregard the request and continue operation. This allows the Modbus system to continue operation even if a slave device is disconnected or faulty.
Inter-character timeout (only for Modbus RTU)	Use this function to determine the timeout interval between characters for Modbus devices that cannot receive Rx signals within an expected time interval. If the response is timed out, all received data will be discarded. The NPort S9000 will automatically determine the timeout interval if the timeout value is set to 0.
Inter-frame delay (only for Modbus RTU)	The users can determine the time delay to transmit the data frame received from the slave device to the upstream. The NPort S9000 will automatically determine the time interval if it is set to 0.
Designated TCP Port	By default, when configure NPort S9000 as a Modbus gateway, it will listen to the TCP port 502 and base on the Slave ID Map to pass the Modbus packet frames. This function will allow you to assign a TCP port for a specific serial port which means all the Modbus requests sent to this TCP port will be directly forward to the relative serial port no matter what the Slave ID Map routing is.

Disabled Mode



Total Solution for NPort S8000 Series Device Server

- Model - NPort S8455I-MM-SC
- Name - NPort S8455I-MM-SC_22112
- Location -
- IP - 192.168.127.254
- Serial NO. - 22112

Operation Modes

Port Settings

Port 1

Operation mode Disable

☑ Port 1 □ Port 2 □ Port 3 □ Port 4

□ Apply the above settings to all serial ports

When Operation mode is set to Disabled, that particular port will be disabled. Check the **Apply the above settings to all serial ports** to apply this setting to the other port.

With regard to **Apply the above setting to other serial ports**, you may use the checkboxes at the bottom of the window to apply the settings to one or more ports.

Protocol Settings

Modbus Settings

Initial Delay

Some Modbus slaves may take more time to boot up than other devices. For certain environments, this may cause the entire system to suffer from repeated exceptions during the initial boot-up. You can force the NPort to wait after booting up before sending the first request with the Initial Delay setting.

Modbus TCP Exception

The NPort S9000 is a protocol gateway that transparently passes requests and responses between Ethernet and serial interfaces. In some situations, it may be necessary for the gateway to return an exception in response to a request from a Modbus TCP master. This is enabled or disabled with the Modbus TCP Exception setting. When enabled, the unit can return two types of exception:

Exception	Conditions
Timeout	There is no response from the slave. Maybe the device is offline or the serial cable is broken.
Request dropped	There are two situations that will result in this exception: The request queue is full (32 request queue for each master) The destination ID is not included in the slave ID map.

Not all Modbus TCP masters require this exception, so it is up to you to determine if this setting should be enabled.

Modbus TCP Listen Port

Allow you to change Modbus TCP listen port from the default value (502).

Modbus TCP Response Timeout

According to the Modbus standard, the time that it takes for a slave device to respond to a request is defined by the device manufacturer. Based on this response time, a master can be configured to wait a certain amount of time for a slave's response. If no response is received within the specified time, the master will disregard the request and continue operation. This allows the Modbus system to continue operation even if a slave device is disconnected or faulty.

On the NPort S9000, the Modbus TCP response timeout field is used to configure how long the gateway will wait for a response from a Modbus ASCII or RTU slave. Refer to your device manufacturer's documentation to manually set the response time-out.

Slave ID Map

The Slave ID Map is where slave IDs are managed. The definitions on this tab determine how requests will be routed by the unit. To configure the Slave ID Map, double-click the row of the serial port to configure, or click Edit to enter the settings page.

How Slave IDs are Mapped on the NPort S9000

With the slave ID table, smart routing is achieved for units with multiple serial ports. Since each virtual slave ID is routed to a specific Modbus network, requests are not broadcast over all serial ports. This keeps communication efficient and prevents devices on one port from slowing down the entire system.

When a Modbus master requests information from a Modbus slave device, the request is addressed to the desired slave's ID, which must be unique on the network. When Modbus networks are integrated by a Modbus gateway, complications can arise if the same slave ID is being used on different networks. If this is not properly addressed, a request sent to that slave ID would receive more than one response, causing communication problems.

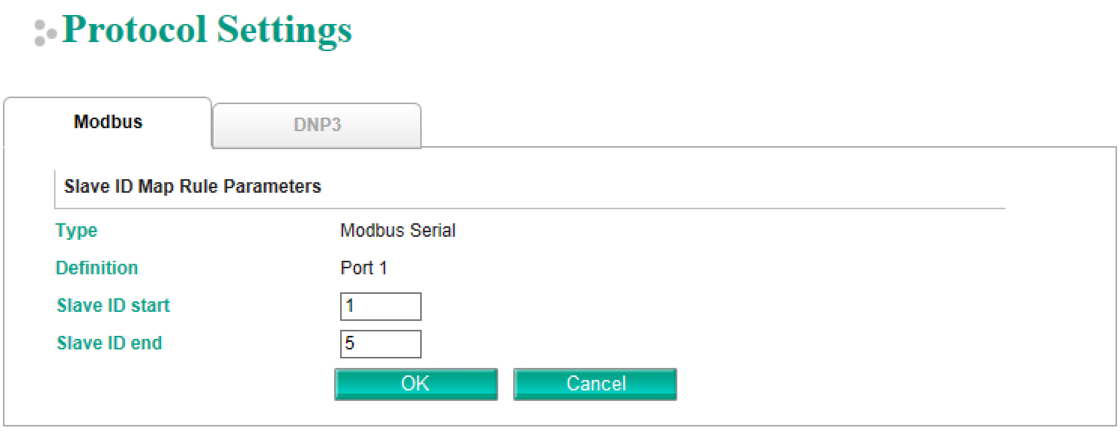
With the NPort S9000, this situation is addressed by using a slave ID map. While configuring the NPort, users set up a range of "virtual" slave IDs that are mapped to slave devices on a specific Modbus network. To send a request to a slave device that is on a different Modbus network, a Modbus master would address the request to the appropriate (virtual) slave ID. The NPort then routes that request as specified by the slave ID map.

For example, if a TCP master needs information from an ASCII slave, it addresses the request to the corresponding virtual slave ID as defined on the NPort's slave ID map. The NPort identifies the request as within its virtual slave ID range and forwards the request to the Modbus ASCII by the device's actual slave ID.

Virtual slave IDs must not conflict with each other or with other TCP slave IDs.

How Slave ID Map Is Defined

The slave ID map consists of entries (channels), the range of virtual ID versus real ID, and the destination of the serial port.



Protocol Settings

Slave ID Map Rule Parameters

Type: Modbus Serial
Definition: Port 1
Slave ID start: 1
Slave ID end: 5

Setting	Value	Notes
Virtual Slaves ID Range	(numeric range from 1 to 254)	This specifies the range of IDs that will be routed to the selected set of slave devices. For example, you can specify that IDs between 8 and 24 be routed to the devices on Port 3. The ID 255 is reserved for the gateway itself.

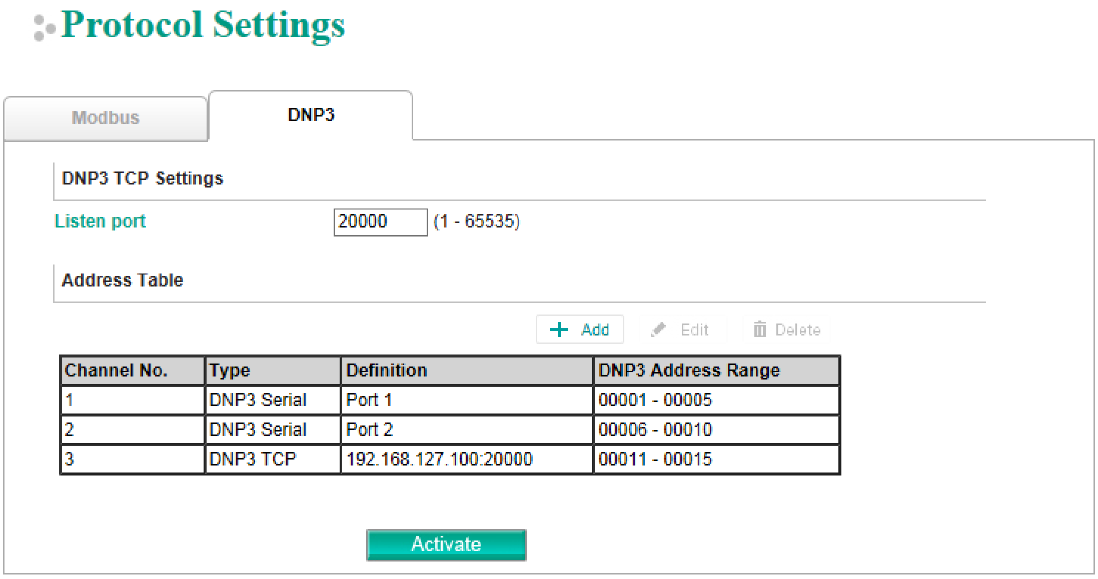
When a serial port is set to RTU slave or ASCII slave mode, a virtual ID range will already be created for you. Simple select the entry in the table. For TCP slaves, you can add an entry that assigns a range of virtual IDs to a specific IP address, using the Remote TCP Slave IP setting.

ATTENTION

The NPort S9000 will disregard any request that is not addressed to a virtual slave ID on its slave ID map. If a device has not been assigned a virtual slave ID, it will not be accessible by the masters on the other side of the Modbus gateway.

DNP3 Settings

The DNP3 tab is where certain adjustments can be made to fine-tune the communication between different DNP3 networks. You can configure DNP3 TCP Settings and Address Table.



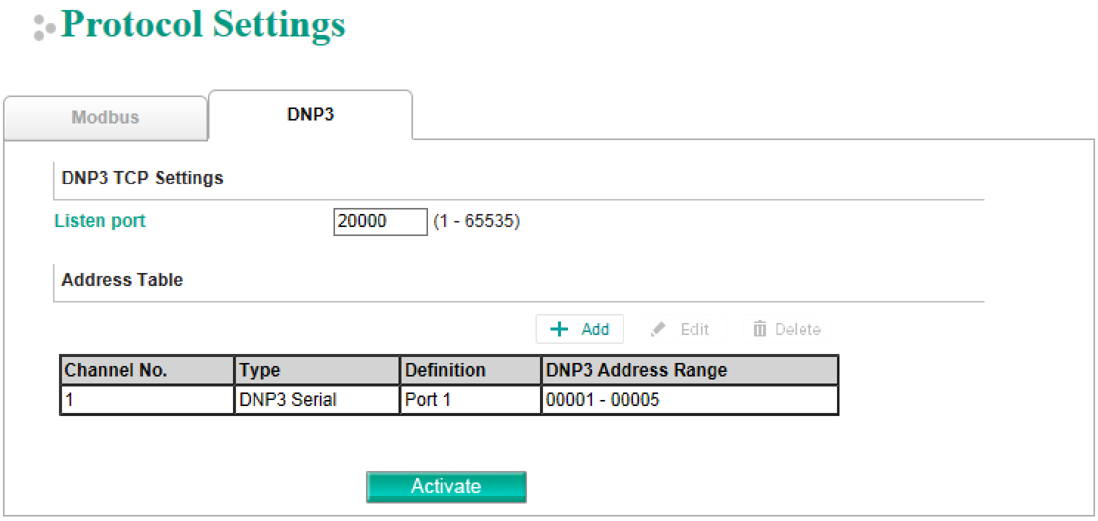
DNP3 TCP Settings

Listen port 20000 (1 - 65535)

Address Table

Channel No.	Type	Definition	DNP3 Address Range
1	DNP3 Serial	Port 1	00001 - 00005
2	DNP3 Serial	Port 2	00006 - 00010
3	DNP3 TCP	192.168.127.100:20000	00011 - 00015

When you click **Add**, you can add the master (or outstation) devices on the Ethernet side. You will need to add these devices' IP address and DNP3 address to the routing table.



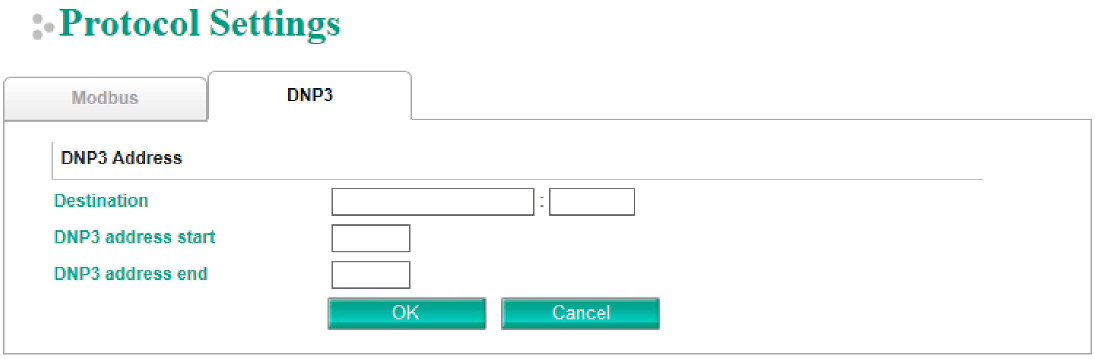
DNP3 TCP Settings

Listen port 20000 (1 - 65535)

Address Table

Channel No.	Type	Definition	DNP3 Address Range
1	DNP3 Serial	Port 1	00001 - 00005

For the DNP3 TCP Settings, you may modify which TCP port should the device server listen to for DNP3 packet frames. The default port is 20000.For the Address Table, you may Add/Edit/Delete for the device address routing table.



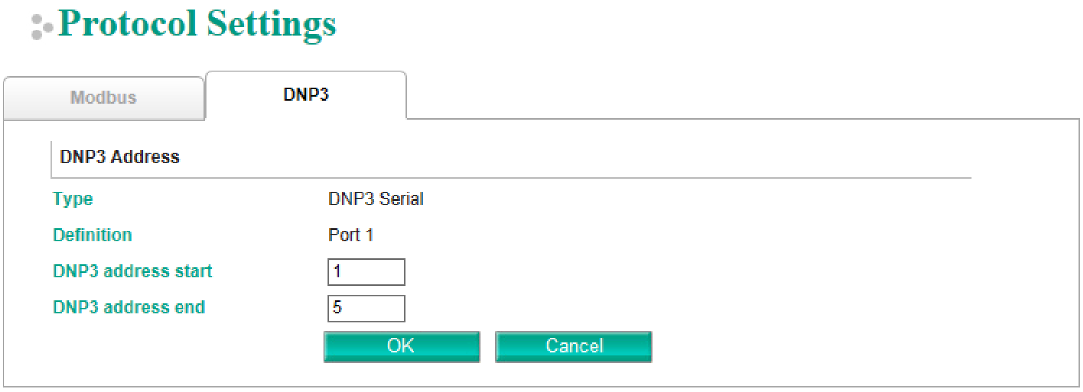
DNP3 Address

Destination: __________ : ______

DNP3 address start: ______

DNP3 address end: ______

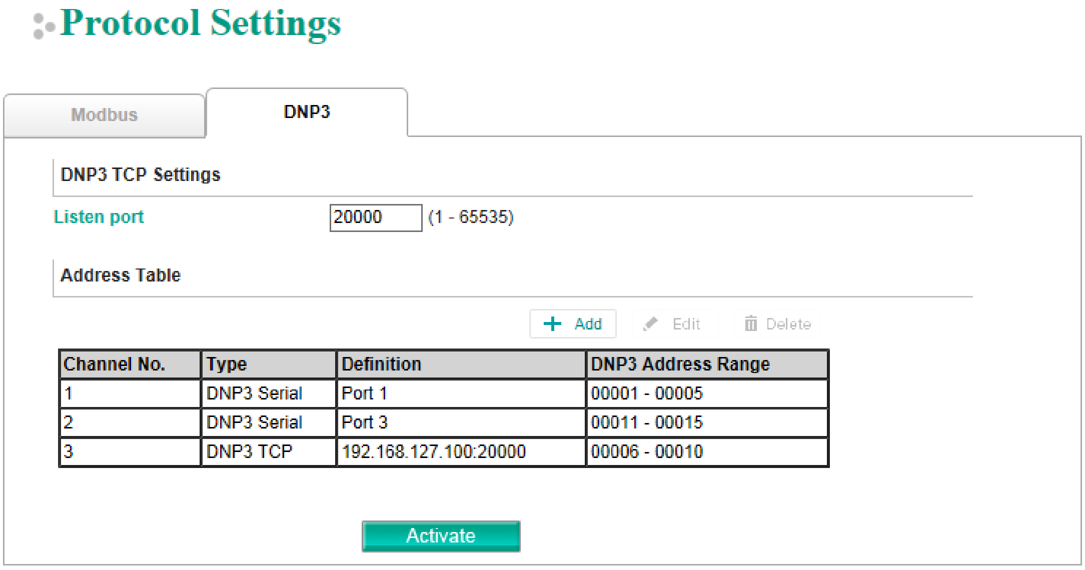
When you click Add, you can add the master (or outstation) devices on the Ethernet side. You will need to add these devices' IP address and DNP3 address to the routing table.



DNP3 Address

Type	DNP3 Serial
Definition	Port 1
DNP3 address start	1
DNP3 address end	5

When you select a serial routing and click **Edit**, you can assign the configuration for DNP3 packet frames coming from the serial side and will need to assign the DNP3 slave IDs.



DNP3 TCP Settings

Listen port: 20000 (1 - 65535)

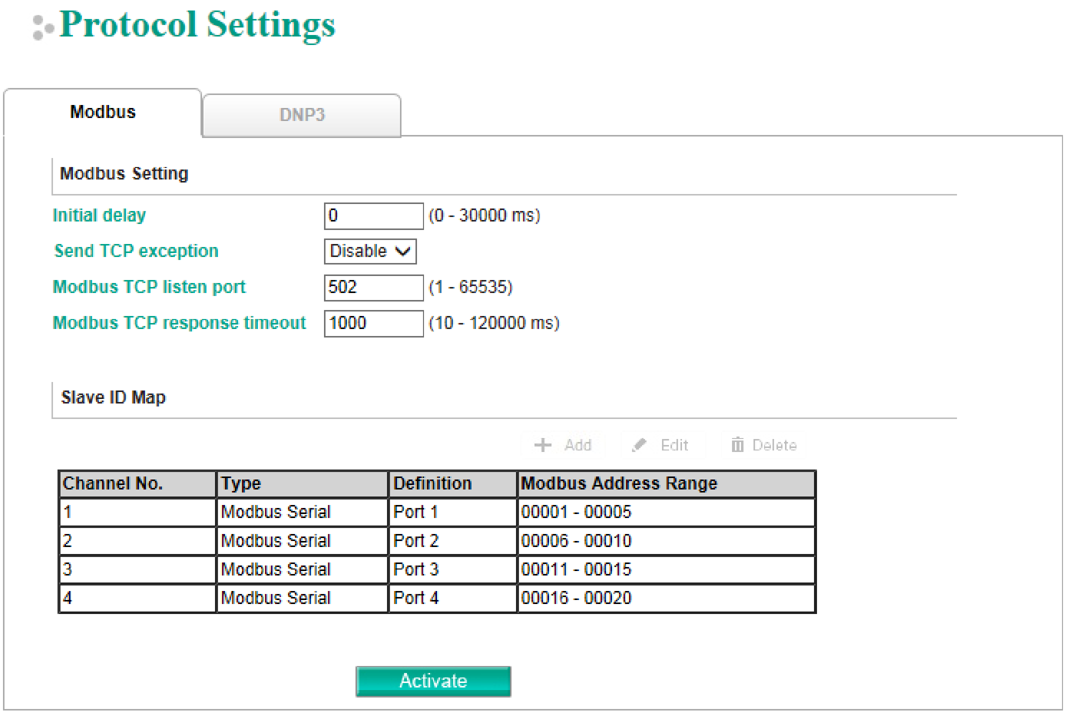
Address Table

Channel No.	Type	Definition	DNP3 Address Range
1	DNP3 Serial	Port 1	00001 - 00005
2	DNP3 Serial	Port 3	00011 - 00015
3	DNP3 TCP	192.168.127.100:20000	00006 - 00010

The gateway will drop a DNP3 packet frame if the destination DNP3 device address or IP address is not defined in the gateway.

Modbus Settings

The Modbus tab is where certain adjustments can be made to fine-tune the communication between different Modbus networks. You can configure Initial Delay, Modbus TCP Exception, Modbus TCP listen port, Modbus TCP Response Time-out, and Slave ID Map.



Protocol Settings

Modbus Setting

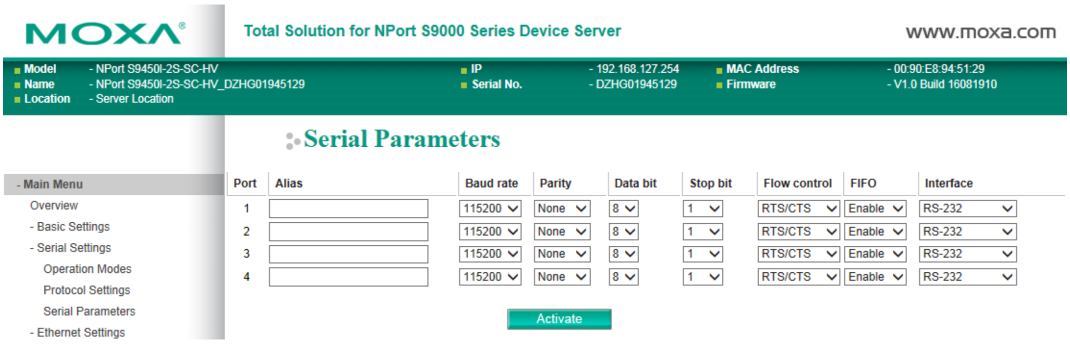
Initial delay: 0 (0 - 30000 ms)
Send TCP exception: Disable
Modbus TCP listen port: 502 (1 - 65535)
Modbus TCP response timeout: 1000 (10 - 120000 ms)

Slave ID Map

Channel No.	Type	Definition	Modbus Address Range
1	Modbus Serial	Port 1	00001 - 00005
2	Modbus Serial	Port 2	00006 - 00010
3	Modbus Serial	Port 3	00011 - 00015
4	Modbus Serial	Port 4	00016 - 00020

Parameter	Value
Initial delay	0-30000 ms
Modbus TCP exception	Enable or Disable
Modbus TCP listen port	1-65535
Modbus TCP response timeout	10-120000 ms

Serial Parameters



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

Serial Parameters

Port	Alias	Baud rate	Parity	Data bit	Stop bit	Flow control	FIFO	Interface
1		115200	None	8	1	RTS/CTS	Enable	RS-232
2		115200	None	8	1	RTS/CTS	Enable	RS-232
3		115200	None	8	1	RTS/CTS	Enable	RS-232
4		115200	None	8	1	RTS/CTS	Enable	RS-232

Port alias

Setting	Factory Default	Necessity
1 to 16 characters (E.g., PLC-No.1)	None	Optional

Port Alias is specially designed to allow the easy identification of the serial devices that are connected to the NPort's serial port.

Baudrate

Setting	Factory Default	Necessity
50 bps to 921600 bps	115200 bps	Required

Select one of the standard baudrates from 50 bps to 921.6 Kbps in the dropdown box, or select **Other** and then type the desired baudrate in the input box.

ATTENTION

If the port requires a special baudrate that is not listed, such as 500000 bps, you can select the **Other** option and enter the desired baudrate into the text box. The NPort S9000 will automatically calculate the closest supported baudrate. The margin for error will be less than 1.7% for all baudrates under 921600 bps.

Parity

Setting	Factory Default	Necessity
None, Even, Odd, Space, Mark	None	Required

Data bits

Setting	Factory Default	Necessity
5, 6, 7, 8	8	Required

When the user sets **Data bits** to 5 bits, the stop bits setting will automatically change to 1.5 bits.

Stop bits

Setting	Factory Default	Necessity
1, 2	1	Required

Stop bits will be set to 1.5 when **Data bits** is set to 5 bits.

Flow control

Setting	Factory Default	Necessity
None, RTS/CTS, Xon/Xoff	RTS/CTS	Required

FIFO

Setting	Factory Default	Necessity
Enable, Disable	Enable	Required

The NPort's serial ports provide a 16-byte FIFO both in the Tx and Rx directions. Disable the FIFO setting when your serial device does not have a FIFO to prevent data loss during communication.

Interface

Setting	Factory Default	Necessity
RS-232, RS-422, RS-485 2-wire, RS-485 4-wire	RS-232	Required

ATTENTION

Check the serial communication parameters in your serial device's user's manual. You should set up the NPort's serial parameters with the same communication parameters used by your serial devices.

7

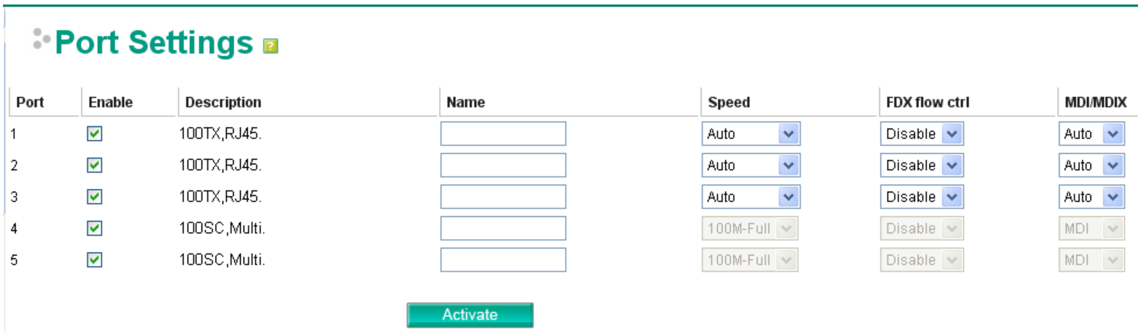
Switch Featured Functions

In this chapter, we use the Web Console interface to introduce the functions that focuses on the Switch Featured Functions. The following topics are covered in this chapter:

- **Ethernet Settings**
  - Port Settings
  - Port Trunking
  - Communication Redundancy
  - Configuring STP/RSTP
  - The Difference between STP and RSTP
- **Bandwidth Management**
  - Using Bandwidth Management
  - Configuring Bandwidth Management
- **Line Swap Fast Recovery**
  - Using Line-Swap-Fast-Recovery
  - Configuring Line-Swap Fast Recovery
  - Loop Protection
- **Ethernet Advanced Settings**
  - Ethernet Traffic Prioritization
  - The Traffic Prioritization Concept
  - Configuring Ethernet Traffic Prioritization
- **Virtual LAN**
  - Using Virtual LAN
  - The Virtual LAN (VLAN) Concept
  - Configuring Virtual LAN
- **Multicast Filtering**
  - Using Multicast Filtering
  - The Concept of Multicast Filtering
  - Configuring IGMP Snooping
  - IGMP Snooping Settings
  - Configuring GMRP
- **Set Device IP**
  - Using Set Device IP
  - Configuring Set Device IP

Ethernet Settings

Port Settings



Port Settings

Port	Enable	Description	Name	Speed	FDX flow ctrl	MDI/MDIX
1	☑	100TX,RJ45.		Auto	Disable	Auto
2	☑	100TX,RJ45.		Auto	Disable	Auto
3	☑	100TX,RJ45.		Auto	Disable	Auto
4	☑	100SC,Multi.		100M-Full	Disable	MDI
5	☑	100SC,Multi.		100M-Full	Disable	MDI

Enable

Setting	Description	Factory Default
Checked	Allows data transmission through the port.	Enabled
Unchecked	Immediately shuts off port access.	

ATTENTION

If a connected device or sub-network is wreaking havoc on the rest of the network, the **Disable** option under **Advanced Settings/Port** gives the administrator a quick way to shut off access through this port immediately.

Description

Setting	Description	Factory Default
Media type	Displays the media type for each module's port	N/A

Name

Setting	Description	Factory Default
Max. 63 Characters	Specify an alias for each port and assist the administrator in remembering important information about the port. E.g., PLC 1	None

Speed (Copper Port Only)

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
100M-Full	Choose one of these fixed speed options if the opposing Ethernet device has trouble auto-negotiating line speed.	
100M-Half		
10M-Full		
10M-Half		

***FDX Flow Ctrl*.**

This setting enables or disables the flow control capability of this port when the **port transmission speed** setting is in auto mode. The final result will be determined by the "auto" process between the NPort S9000 and connected devices.

Setting	Description	Factory Default
Enable	Enables flow control for this port when in auto-negotiate mode.	Disable
Disable	Disables flow control for this port when in auto-negotiate mode.	

MDI/MDIX

Setting	Description	Factory Default
Auto	Allows the port to auto detect the port type of the opposing Ethernet device and change the port type accordingly.	Auto
MDI	Choose the MDI or MDIX option if the opposing Ethernet device has trouble auto-negotiating port type.	
MDIX		

Port Trunking

Using Port Trunking

Link Aggregation allows one or more links to be aggregated together to form a Link Aggregation Group. A MAC client can treat Link Aggregation Groups as if they were a single link.

NPort S9000's Port Trunking feature allows devices to communicate by aggregating up to two trunk groups on the NPort S9000. If one of the ports fails, the other ports in the same trunk group will provide back up and share the traffic automatically.

The Port Trunking Concept

Moxa has developed a proprietary Port Trunking protocol that provides the following benefits:

- Gives you more flexibility in setting up your network connections, because the bandwidth of a link can be doubled, tripled, or quadrupled.
- Provides redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.
- Load sharing—MAC Client traffic may be distributed across multiple links.
- To avoid broadcast storms or loops in your network while configuring a trunk, first disable or disconnect all ports that you want to add to the trunk or remove from the trunk. After you have finished configuring the trunk, enable or re-connect the ports.

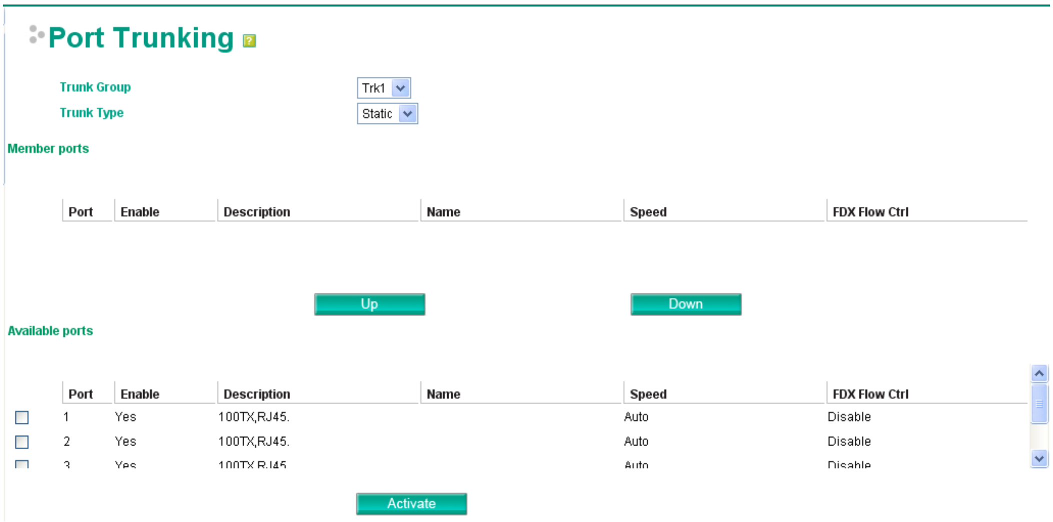
If all ports on both switches are configured as 100BASE-TX, and they are operating in full duplex, then the potential bandwidth of the connection will be up to 1 Gbps on an NPort S9000- switching device server. This means that users can connect one NPort S9000 to another NPort S9000 by port trunking to double, triple, or quadruple the bandwidth of the connection.
When configuring Port Trunking, note that:

Each NPort S9000 can set a maximum of two Port Trunking groups (designated Trk1, Trk2).

When you activate Port Trunking settings, some advanced functions that you setup with the original ports will either be set to factory default values, or disabled:

- Communication Redundancy will be set to the factory default
- Traffic Prioritization will be set to the factory default
- Port-based VLAN or 802.1Q VLAN will be set to the factory default
- Multicast Filtering will be set to the factory default
- Rate Limiting will be set to the factory default
- Port Access Control will be set to the factory default
- Email and Relay Warning will be set to the factory default
- Set Device IP will be set to the factory default
- Mirror Port will be set to the factory default
- You can setup these features again on your Trunking Port.

The **Port Trunking Settings** page is used to assign ports to a Trunk Group.



Port Trunking

Trunk Group: Trk1

Trunk Type: Static

Member ports

	Port	Enable	Description	Name	Speed	FDX Flow Ctrl

Available ports

	Port	Enable	Description	Name	Speed	FDX Flow Ctrl
□	1	Yes	100TX,RJ45.		Auto	Disable
□	2	Yes	100TX,RJ45.		Auto	Disable
□	3	Yes	100TX,RJ45		Auto	Disable

1. Select **Trk1, Trk2** from the Trunk Group drop-down box.
2. Select **Static** or **LACP** from the Trunk Type drop-down box.
3. Under Member Ports and Available Ports, select the specific ports.
4. Use the Up / Down buttons to add/remove designated ports to/from a trunk group.

Trunk Group (Maximum of two trunk groups on NPort S9000

Setting	Description	Factory Default
Trk1, Trk2 on NPort S9000	Display or designate the Trunk Type and Member Ports for Trunk Groups 1, 2	Trk1

Trunk Type

Setting	Description	Factory Default
Static	Designated Moxa proprietary trunking protocol	Static
LACP	Designated LACP (IEEE 802.3ad, Link Aggregation Control Protocol)	Static

Available Ports/Member Port

Setting	Description	Factory Default
Member/Available Ports	Use Up/Down buttons to add/remove specific ports from available ports to/from trunk group.	N/A
Checkbox	Check to designate which ports to add or remove.	Unchecked
Port	Port number	N/A
Port description	Displays the media type for each module’s port	N/A
Name	Max. 63 Characters	N/A
Speed	Indicates the transmission speed (100M-Full, 100M-Half, 10M-Full, or 10M-Half)	N/A
FDX Flow Control	Indicates if the FDX flow control of this port is “Enabled” or “Disabled.”	N/A
Up	Add designated ports into trunk group from available ports.	N/A
Down	Remove designated ports from trunk group to available port.	N/A

Communication Redundancy

Using Communication Redundancy

Setting up Communication Redundancy on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum.

The Communication Redundancy function allows the user to set up *redundant loops* in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This feature is particularly important for industrial applications, since it could take several minutes to locate the disconnected or severed cable. For example, if the NPort S9000 is used as a key communications component of a production line, several minutes of downtime could result in a big loss in production and revenue. The NPort S9000 supports three different protocols to support this communication redundancy function— **Rapid Spanning Tree/ Spanning Tree Protocol (IEEE 802.1W/1D), Turbo Ring**, and **Turbo Ring V2**.

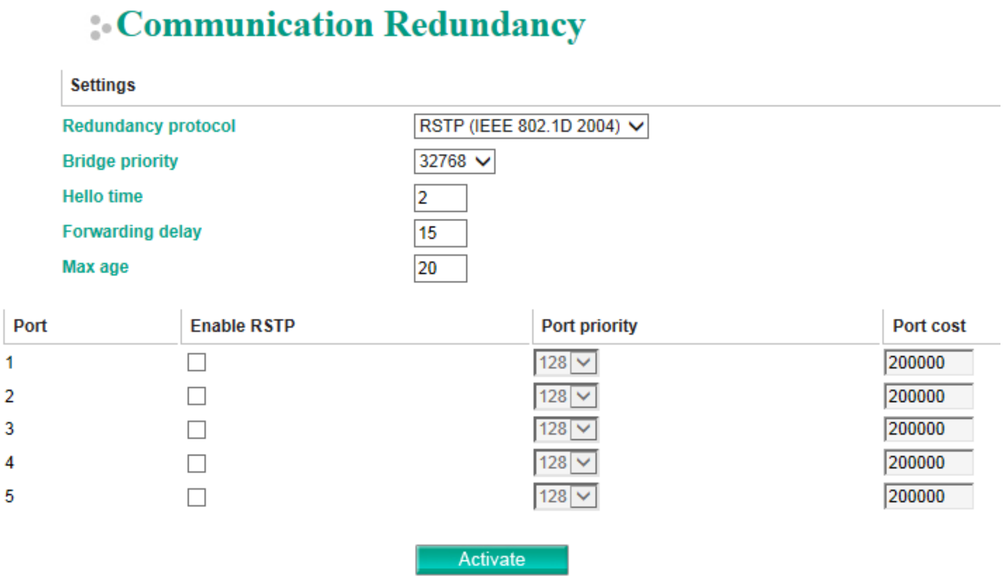
When configuring a redundant ring, all NPort S9000s on the same ring must be configured to use the same redundancy protocol. You cannot mix the "Turbo Ring," "Turbo Ring V2," and RSTP protocols on the same ring. The following table lists the key differences between each feature. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network.

	Turbo Ring V2	Turbo Ring	RSTP
Topology	Ring	Ring	Ring, Mesh
Recovery Time	< 20 ms	< 300 ms	Up to 5 sec

NOTE Most of Moxa's managed switches now support two proprietary Turbo Ring protocols:
"Turbo Ring" refers to the original version of Moxa's proprietary redundant ring protocol, which has a recovery time of under 300 ms.
"Turbo Ring V2" refers to the new generation Turbo Ring, which has a recovery time of under 20 ms.
In this manual, we use the terminology "Turbo Ring" ring and "Turbo Ring V2" ring to differentiate between rings configured for one or the other of these protocols.

Configuring STP/RSTP

The following figures indicate which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter follows.



Communication Redundancy

Settings

Redundancy protocol	RSTP (IEEE 802.1D 2004)
Bridge priority	32768
Hello time	2
Forwarding delay	15
Max age	20

Port	Enable RSTP	Port priority	Port cost
1	□	128	200000
2	□	128	200000
3	□	128	200000
4	□	128	200000
5	□	128	200000

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	
Turbo Ring 2	Select this item to change to the Turbo Ring 2 configuration page.	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	default

Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Hello time (sec.)

Setting	Description	Factory Default
Numerical value input by user	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2

Forwarding Delay

Setting	Description	Factory Default
Numerical value input by user	The amount of time this device waits before checking to see if it should change to a different state.	15

Max. Age (sec.)

Setting	Description	Factory Default
Numerical value input by user	If this device is not the root, and it has not received a hello message from the root in an amount of time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20

Enable RSTP per Port

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as a node on the Spanning Tree topology.	Disabled

NOTE We suggest not enabling the Spanning Tree Protocol once the port is connected to a device (PLC, RTU, etc.) as opposed to network equipment. The reason is that it will cause unnecessary negotiation.

Port Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by entering a lower number.	128

Port Cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology.	200000

Configuration Limits of STP/RSTP

The Spanning Tree Algorithm places limits on three of the configuration items described previously:

[Eq. 1]: 1 sec ≦ Hello Time ≦ 10 sec

[Eq. 2]: 6 sec ≦ Max. Age ≦ 40 sec

[Eq. 3]: 4 sec ≦ Forwarding Delay ≦ 30 sec

These three variables are further restricted by the following two inequalities:

[Eq. 4]: 2 * (Hello Time + 1 sec) ≦ Max. Age ≦ 2 * (Forwarding Delay – 1 sec)

The NPort S9000's firmware will alert you immediately if any of these restrictions are violated. For example, setting

Hello Time = 5 sec, Max. Age = 20 sec, and Forwarding Delay = 4 sec does not violate Eqs. 1 through 3, but does violate Eq. 4, since in this case,

2 * (Hello Time + 1 sec) = 12 sec, and 2 * (Forwarding Delay – 1 sec) = 6 sec.

You can remedy the situation in many ways. One solution is simply to increase the Forwarding Delay value to at least 11 sec.

HINT: Perform the following steps to avoid guessing:

Step 1: Assign a value to "Hello Time" and then calculate the left most part of Eq. 4 to get the lower limit of "Max. Age".

Step 2: Assign a value to "Forwarding Delay" and then calculate the right most part of Eq. 4 to get the upper limit for "Max. Age".

Step 3: Assign a value to "Forwarding Delay" that satisfies the conditions in Eq. 3 and Eq. 4.

The STP/RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures in a network and provide protection from loops. Networks that have a complicated architecture are prone to broadcast storms caused by unintended loops in the network. The NPort S9000's STP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every NPort S9000 connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE Std 802.1w-2001. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy. For example:

□ Defaults to sending 802.1D style BPDUs if packets with this format are received.

□ STP (802.1D) and RSTP (802.1w) can operate on different ports of the same NPort S9000. This feature is particularly helpful when the NPort S9000' s ports connect to older equipment, such as legacy switches.

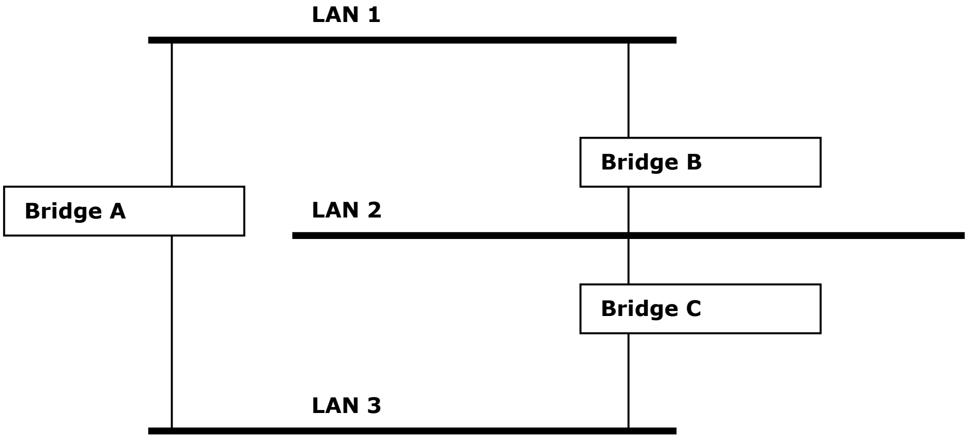
You get essentially the same functionality with RSTP and STP. To see how the two systems differ, see the Differences between RSTP and STP section in this chapter.

NOTE The STP protocol is part of the IEEE Std 802.1D, 1998 Edition bridge specification. The following explanation uses bridge instead of switch.

What is STP?

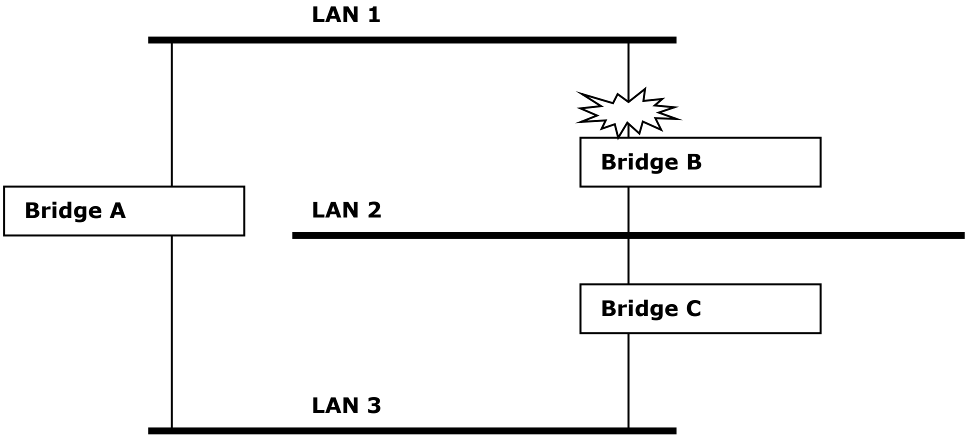
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

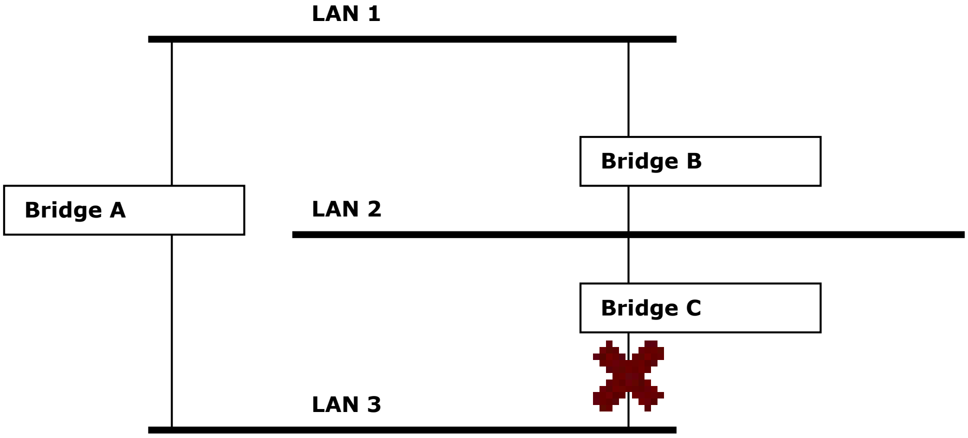
- Locate and then disable less efficient paths (i.e., paths that have a lower bandwidth).
- Enable one of the less efficient paths if the most efficient path fails.



The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.

If STP is enabled, it will detect duplicate paths and prevent, or block, one of them from forwarding traffic. In the following example, STP determined that traffic from LAN segment 2 to LAN segment 1 should flow through Bridges C and A because this path has a greater bandwidth and is therefore more efficient.





What happens if a link failure is detected? As shown in the previous figure, the STP process reconfigures the network so that traffic from LAN segment 2 flows through Bridge B.

STP will determine which path between each bridged segment is most efficient, and then assigns a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous three figures, STP first determined that the path through Bridge C was the most efficient, and as a result, blocked the path through Bridge B. After the failure of Bridge C, STP re-evaluated the situation and opened the path through Bridge B.

How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the sections below.

STP Required

Before STP can configure the network, the system must satisfy the following requirements:

□ Communication between all the bridges. This communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.

□ Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. The default priority of the NPort S9000 is 32768.

□ Each port has a cost that specifies the efficiency of each link. The efficiency cost is usually determined by the bandwidth of the link, with less efficient links assigned a higher cost. The following table shows the default port costs for a switch:

Port Speed	Path Cost 802.1D, 1998 Edition	Path Cost 802.1w, 2001
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1000 Mbps	4	20,000

STP Calculation

The first step of the STP process is to perform calculations. During this stage, each bridge on the network transmits BPDUs. The following items will be calculated:

- Which bridge should be the Root Bridge. The Root Bridge is the central reference point from which the network is configured.
- The Root Path Costs for each bridge. This is the cost of the paths from each bridge to the Root Bridge.
- The identity of each bridge's Root Port. The Root Port is the port on the bridge that connects to the Root Bridge via the most efficient path. In other words, the port connected to the Root Bridge via the path with the lowest Root Path Cost. The Root Bridge, however, does not have a Root Port.
- The identity of the Designated Bridge for each LAN segment. The Designated Bridge is the bridge with the lowest Root Path Cost from that segment. If several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge. Traffic transmitted in the direction of the Root Bridge will flow through the Designated Bridge. The port on this bridge that connects to the segment is called the Designated Bridge Port.

STP Configuration

After all the bridges on the network agree on the identity of the Root Bridge, and all other relevant parameters have been established, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they will not be allowed to receive or forward traffic.

STP Reconfiguration

Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has gone down. This will trigger the bridge to reconfigure the network to account for the change. If you have configured an SNMP trap destination, the first bridge to detect the change sends out an SNMP trap when the topology of your network changes.

The Difference between STP and RSTP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

An STP Example

The LAN shown in the following figure has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.

- Bridge A has been selected as the Root Bridge since it was determined to have the lowest Bridge Identifier on the network.

- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.

- Ports 1 of Bridges B, C, X, and Y are all Root Ports since they are nearest to the Root Bridge, and therefore have the most efficient path.

- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B was selected as the Designated Bridge for that segment since it has a lower Bridge Identifier. Port 2 on Bridge B is selected as the Designated Bridge Port for LAN Segment 2.

- Bridge C is the Designated Bridge for LAN segment 3, because it has the lowest Root Path Cost for LAN Segment 3:

□ The route through Bridges C and B costs 200 (C to B=100, B to A=100)

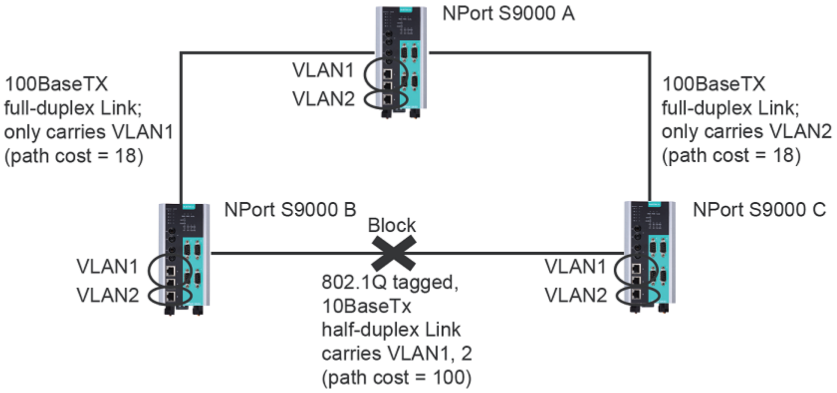
□ The route through Bridges Y and B costs 300 (Y to B=200, B to A=100)Item 3.3

- The Designated Bridge Port for LAN Segment 3 is Port 2 on Bridge C.

Using STP on a Network with Multiple VLANs

IEEE Std 802.1D, 1998 Edition, does not take into account VLANs when calculating STP information—the calculations only depend on the physical connections. Consequently, some network configurations will result in VLANs being subdivided into a number of isolated sections by the STP system. You must ensure that every VLAN configuration on your network takes into account the expected STP topology and alternative topologies that may result from link failures.

The following figure shows an example of a network that contains VLANs 1 and 2. The VLANs are connected using the 802.1Q-tagged link between Switch B and Switch C. By default, this link has a port cost of 100 and is automatically blocked because the other Switch-to-Switch connections have a port cost of 36 (18+18). This means that both VLANs are now subdivided—VLAN 1 on Switch units A and B cannot communicate with VLAN 1 on Switch C, and VLAN 2 on Switch units A and C cannot communicate with VLAN 2 on Switch B.


NPort S9000 A
VLAN1
VLAN2
100BaseTX full-duplex Link; only carries VLAN1 (path cost = 18)
100BaseTX full-duplex Link; only carries VLAN2 (path cost = 18)
NPort S9000 B
Block
NPort S9000 C
VLAN1
VLAN2
802.1Q tagged, 10BaseTx half-duplex Link carries VLAN1, 2 (path cost = 100)
VLAN1
VLAN2

To avoid subdividing VLANs, all inter-switch connections should be made members of all available 802.1Q VLANs. This will ensure connectivity at all times. For example, the connections between Switches A and B, and between Switches A and C should be 802.1Q tagged and carrying VLANs 1 and 2 to ensure connectivity.

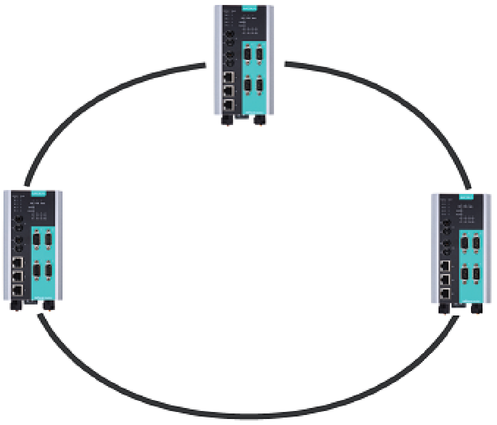
See the "Configuring Virtual LANs" section for more information about VLAN Tagging.

The Turbo Ring Concept

Moxa developed the proprietary Turbo Ring protocol to optimize communication redundancy and achieve a faster recovery time on the network.

The Turbo Ring and Turbo Ring V2 protocols identify one NPort S9000 as the ***master*** of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network.

Initial setup of a "Turbo Ring" or "Turbo Ring V2" ring



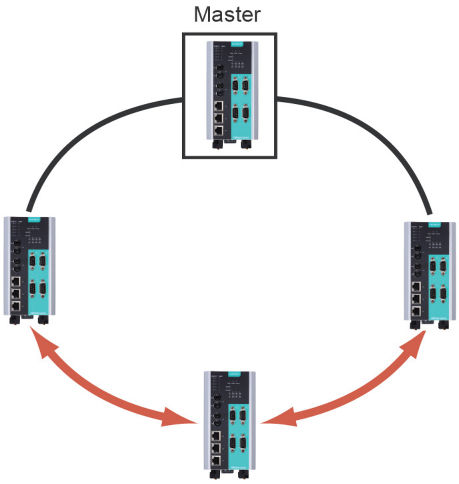
1. For each NPort S9000 in the ring, select any two ports as the redundant ports.
2. Connect redundant ports on neighboring NPort S9000 or switches to form the redundant ring.

The user does not need to configure any of the NPort S9000 or switches as the master to use Turbo Ring or Turbo Ring V2. If none of the NPort S9000 switches in the ring is configured as the master, then the protocol will automatically assign master status to one of the switches. In fact, the master is only used to identify which segment in the redundant ring acts as the backup path. In the following subsections, we explain how the redundant path is selected for rings configured for Turbo Ring and Turbo Ring V2.

Determining the Redundant Path of a "Turbo Ring" Ring

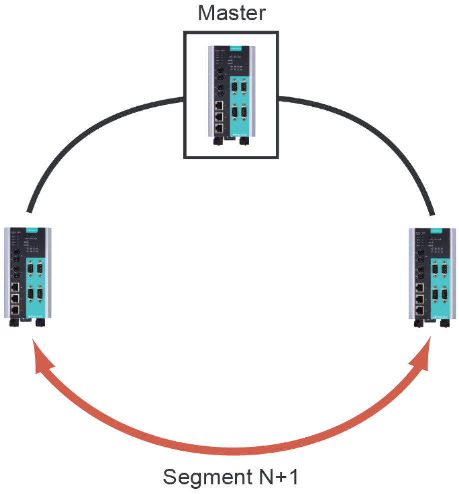
In this case, the redundant segment (i.e., the segment that will be blocked during normal operation) is determined by the number of NPort S9000 gateways that make up the ring and where the ring master is located.

"Turbo Ring" rings with an even number of NPort S9000



If there are 2N NPort S9000 (an even number) in the "Turbo Ring" ring, then the backup segment is one of the two segments connected to the (N+1) NPort S9000 (i.e., the NPort S9000 unit directly opposite the master).

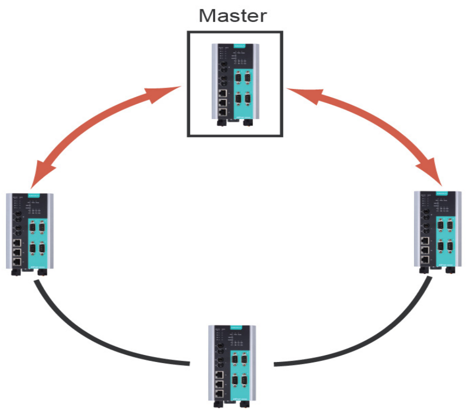
"Turbo Ring" rings with an odd number of NPort S9000



If there are 2N+1 NPort S9000 (an odd number) in the "Turbo Ring" ring, with the NPort S9000 and segments labeled counterclockwise, then segment N+1 will serve as the backup path.

For the example shown here, N=1, so that N+1=2.

Determining the Redundant Path of a "Turbo Ring V2" Ring



For a "Turbo Ring V2" ring, the backup segment is the segment connected to the second redundant port on the master.

See Configuring "Turbo Ring V2" in the Configuring "Turbo Ring" and "Turbo Ring V2" section below.

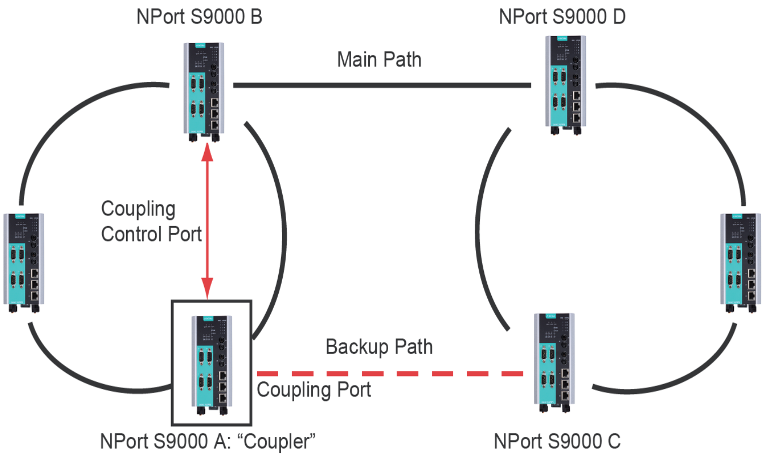
Ring Coupling Configuration

For some systems, it may not be convenient to connect all devices in the system to create one BIG redundant ring as some devices could be located in a remote area. For these systems, "Ring Coupling" can be used to separate the devices into different smaller redundant rings, but in such a way that they can still communicate with each other.

ATTENTION

In a VLAN environment, the user must set **Redundant Port**, **Coupling Port**, and **Coupling Control Port** to join all VLANs, since these ports act as the backbone to transmit all packets of different VLANs to different NPort S9000 gateways.

Ring Coupling for a "Turbo Ring" Ring

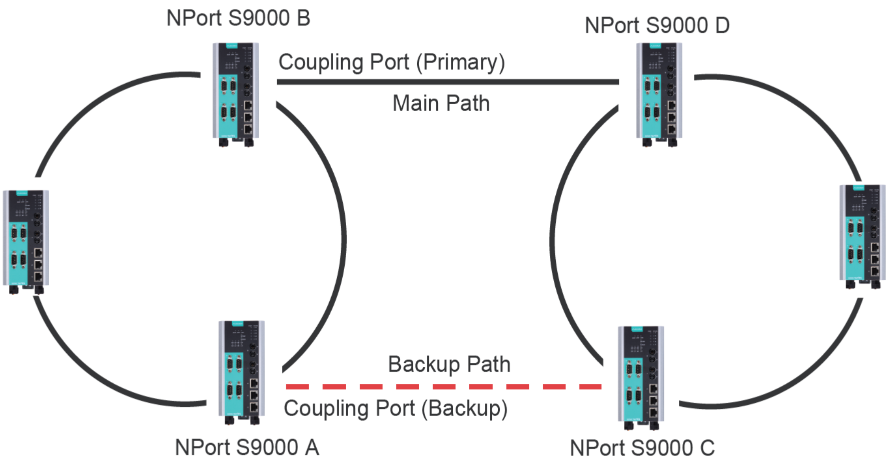


To configure the Ring Coupling function for a "Turbo Ring" ring, select two NPort S9000 devices (e.g., Device A and B in the above figure) in the ring, and another two NPort S9000 devivces in the adjacent ring (e.g., Device C and D).

Decide which two ports in each switch are appropriate to be used as coupling ports, and then link them together. Next, assign one switch (e.g., Device A) to be the "coupler," and connect the coupler's coupling control port with Device B (for this example).

The coupler switch (i.e., Device A) will monitor Device B through the coupling control port to determine whether or not the coupling port's backup path should be recovered.

Ring Coupling for a "Turbo Ring V2" Ring



Note that the ring coupling settings for a "Turbo Ring V2" ring are different from a "Turbo Ring" ring. For Turbo Ring V2, Ring Coupling is enabled by configuring the **Coupling Port (Primary)** on Switch B, and the **Coupling Port (Backup)** on Switch A only. You do not need to set up a coupling control port, so that a "Turbo Ring V2" ring does not use a coupling control line.

The Coupling Port (Backup) on Switch A is used for the backup path and connects directly to an extra network port on Switch C. The Coupling Port (Primary) on Switch B monitors the status of the main path and connects directly to an extra network port on Switch D. With ring coupling established, Switch A can activate the backup path as soon as it detects a problem with the main path.

ATTENTION

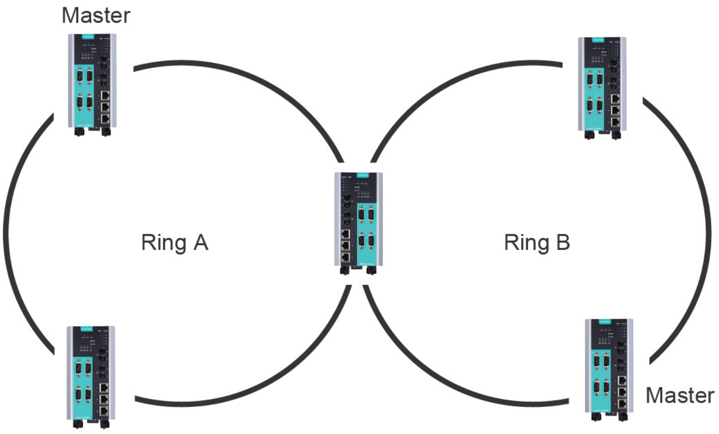
Ring Coupling only needs to be enabled on one of the switches serving as the Ring Coupler. The Coupler must designate different ports as the two Turbo Ring ports and the coupling port.

NOTE You do not need to use the same NPort S9000 unit for both Ring Coupling and Ring Master.

Dual-Ring Configuration (applies only to "Turbo Ring V2")

The "dual-ring" option provides another ring coupling configuration, in which two adjacent rings share one switch. This type of configuration is ideal for applications that have inherent cabling difficulties.

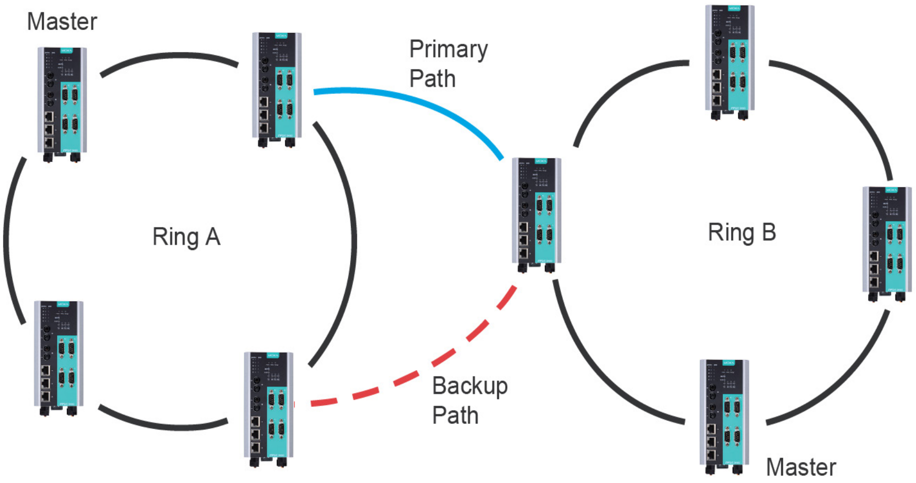
Dual-Ring for a "Turbo Ring V2" Ring



Dual-Homing Configuration (applies only to "Turbo Ring V2")

The "dual-homing" option uses a single Ethernet switch to connect two networks. The primary path is the operating connection, and the backup path is a backup connection that is activated in the event that the primary path connection fails.

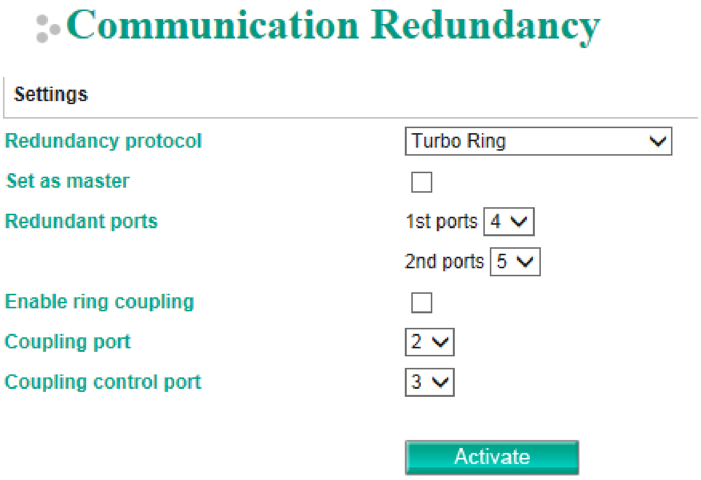
Dual-Homing for a "Turbo Ring V2" Ring



Configuring "Turbo Ring" and "Turbo Ring V2"

Use the **Communication Redundancy** page to configure the "Turbo Ring" or "Turbo Ring V2." Note that configuration pages for these two protocols are different.

Configuring "Turbo Ring"



Communication Redundancy

Settings

Redundancy protocol	Turbo Ring
Set as master	□
Redundant ports	1st ports 4
	2nd ports 5
Enable ring coupling	□
Coupling port	2
Coupling control port	3

NOTE The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the NPort S9000 in the ring. The master is only used to determine which segment serves as the backup path.

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	Turbo Ring V2
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	

Set as Master

Setting	Description	Factory Default
Enabled	Select this NPort S9000 as Master	Not checked
Disabled	Do not select this NPort S9000 as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the NPort S9000 to be one of the redundant ports.	Port 4
2nd Port	Select any port of the NPort S9000 to be one of the redundant ports.	Port 5

Enable Ring Coupling

Setting	Description	Factory Default
Enable	Select this NPort S9000 as Coupler	Not checked
Disable	Do not select this NPort S9000 as Coupler	

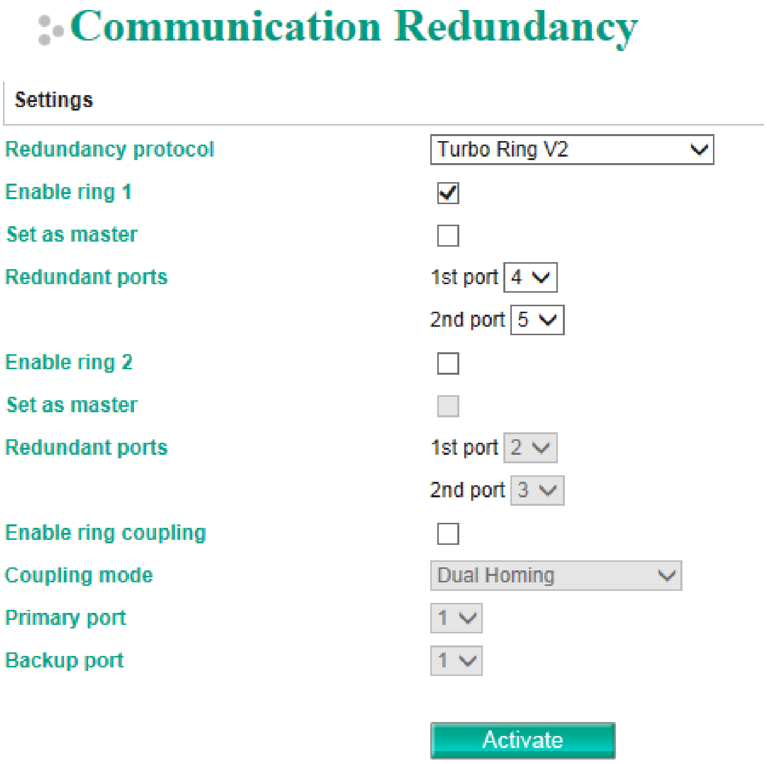
Coupling Port

Setting	Description	Factory Default
Coupling Port	Select any port of the NPort S9000 to be the coupling port	port 2

Coupling Control Port

Setting	Description	Factory Default
Coupling Control Port	Select any port of the NPort S9000 to be the coupling control port	port 3

Configuring "Turbo Ring V2"



Communication Redundancy

Settings

Redundancy protocol	Turbo Ring V2
Enable ring 1	☑
Set as master	□
Redundant ports	1st port 4 2nd port 5
Enable ring 2	□
Set as master	□
Redundant ports	1st port 2 2nd port 3
Enable ring coupling	□
Coupling mode	Dual Homing
Primary port	1
Backup port	1

NOTE When using the Dual-Ring architecture, users must configure settings for both Ring 1 and Ring 2. In this case, the status of both rings will appear under **Current Status**.

NOTE The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the NPort S9000 in the ring. The master is only used to determine which segment serves as the backup path.

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	RSTP
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	

Enable Ring 1

Setting	Description	Factory Default
Enabled	Enable the Ring 1 settings	Not checked
Disabled	Disable the Ring 1 settings	

Enable Ring 2*

Setting	Description	Factory Default
Enabled	Enable the Ring 2 settings	Not checked
Disabled	Disable the Ring 2 settings	

*You should enable both Ring 1 and Ring 2 when using the Dual-Ring architecture.

Set as Master

Setting	Description	Factory Default
Enabled	Select this NPort S9000 as the master	Not checked
Disabled	Do not select this NPort S9000 as the master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the NPort S9000 to be one of the redundant ports.	Ring 1: port 4 Ring 2: port 5
2nd Port	Select any port of the NPort S9000 to be one of the redundant ports.	Ring 1: port 2 Ring 2: port 3

Enable Ring Coupling

Setting	Description	Factory Default
Enable	Select this NPort S9000 as Coupler	Not checked
Disable	Do not select this NPort S9000 as Coupler	

Coupling Mode

Setting	Description	Factory Default
Dual Homing	Select this item to change to the Dual Homing configuration page	Primary Port: port 2 Backup Port: port 3
Ring Coupling (backup)	Select this item to change to the Ring Coupling (backup) configuration page	Coupling Port : Port 2
Ring Coupling (primary)	Select this item to change to the Ring Coupling (primary) configuration page	Coupling Port : Port 2

Primary/Backup Port

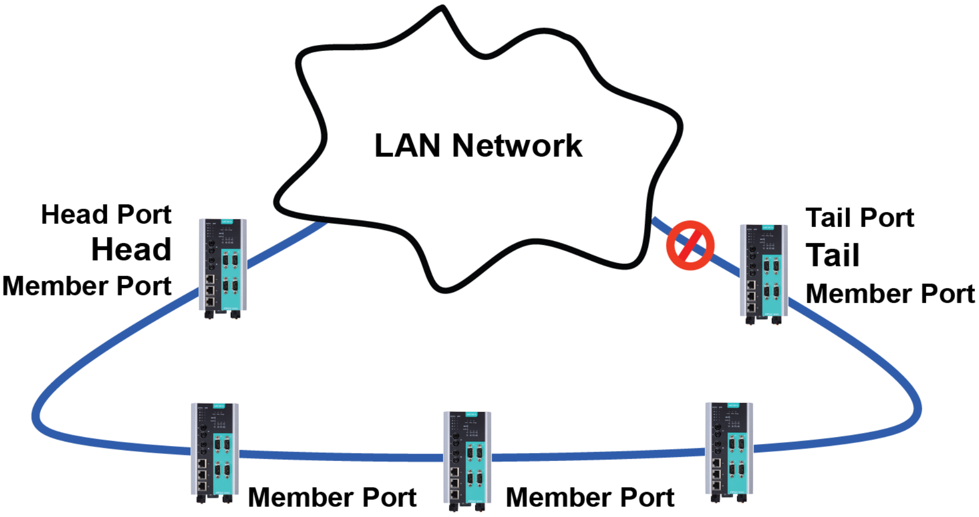
Setting	Description	Factory Default
Primary Port	Select any port of the NPort S9000 to be the primary port.	port 2
Backup Port	Select any port of the NPort S9000 to be the backup port.	port 3

The Turbo Chain Concept

Moxa’s Turbo Chain is an advanced software technology that gives network administrators the flexibility of constructing any type of redundant network topology. When using the chain concept, you first connect the Ethernet switches in a chain and then simply link the two ends of the chain to an Ethernet network, as illustrated in the following figure.

Turbo Chain can be used on industrial networks that have a complex topology. If the industrial network uses a multiring architecture, Turbo Chain can be used to create flexible and scalable topologies with a fast media-recovery time.

Setting up Turbo Chain

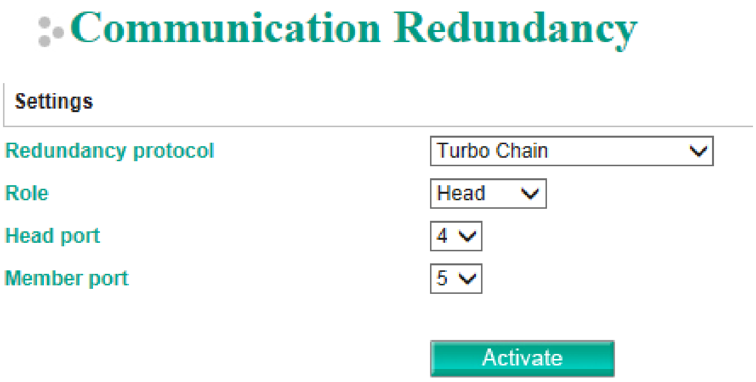


1. Select the Head, Tail, and Member switches.
2. Configure one port as the Head port and one port as the Member port in the Head switch; configure one port as the Tail port and one port as the Member port in the Tail switch; and configure two ports as Member ports in each of the Member switches.
3. Connect the Head, Tail, and Member switches as shown in the diagram.

The path connecting to the Head port is the main path, and the path connecting to the Tail port is the backup path of the Turbo Chain. Under normal conditions, packets are transmitted through the Head Port to the LAN Network. If any Turbo Chain path is disconnected, the Tail Port will be activated to continue packet transmission.

Configuring "Turbo Chain"

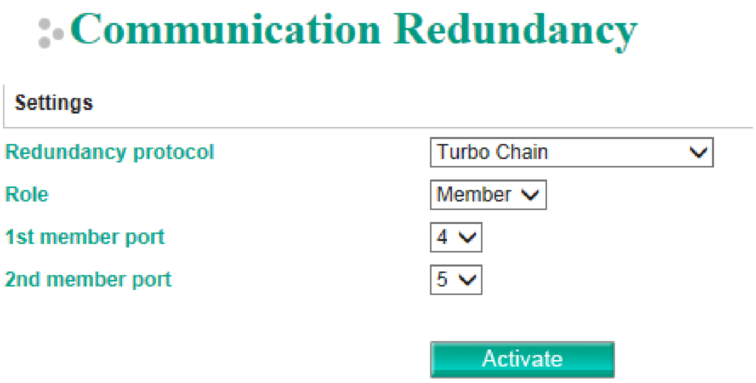
Head Switch Configuration


Communication Redundancy

Settings

Redundancy protocol	Turbo Chain
Role	Head
Head port	4
Member port	5

Member Switch Configuration



Communication Redundancy

Settings

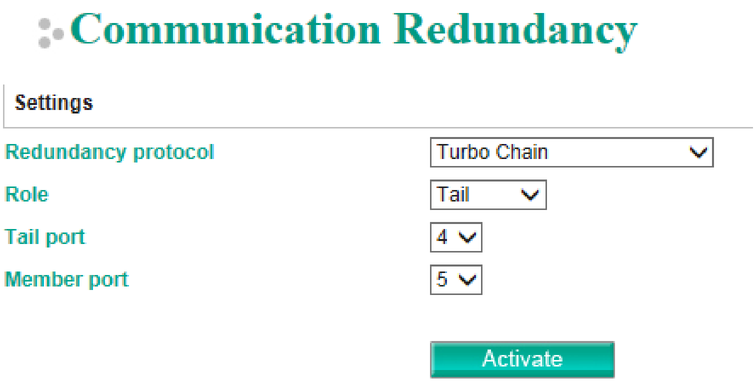
Redundancy protocol: Turbo Chain

Role: Member

1st member port: 4

2nd member port: 5

Tail Switch Configuration



Communication Redundancy

Settings

Redundancy protocol: Turbo Chain

Role: Tail

Tail port: 4

Member port: 5

Current Status

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **RSTP**, **Turbo Chain** or **None**.

The "Ports Status" indicators show ***Forwarding*** for normal transmission, ***Blocked*** if this port is connected to the Tail port as a backup path and the path is blocked, and ***Link down*** if there is no connection.

Settings

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Role

Setting	Description	Factory Default
Head	Select this device server as Head Switch	Member
Member	Select this device server as Member Switch	
Tail	Select this device server as Tail Switch	

Head Role

Setting	Description	Factory Default
Head Port	Select any port of the device server to be the head port.	port 4
Member Port	Select any port of the device server to be the member port.	port 5

Member Role

Setting	Description	Factory Default
1st Member port	Select any port of the device server to be the 1st member port	port 4
2nd Member port	Select any port of the device server to be the 2nd member port	port 5

Tail Role

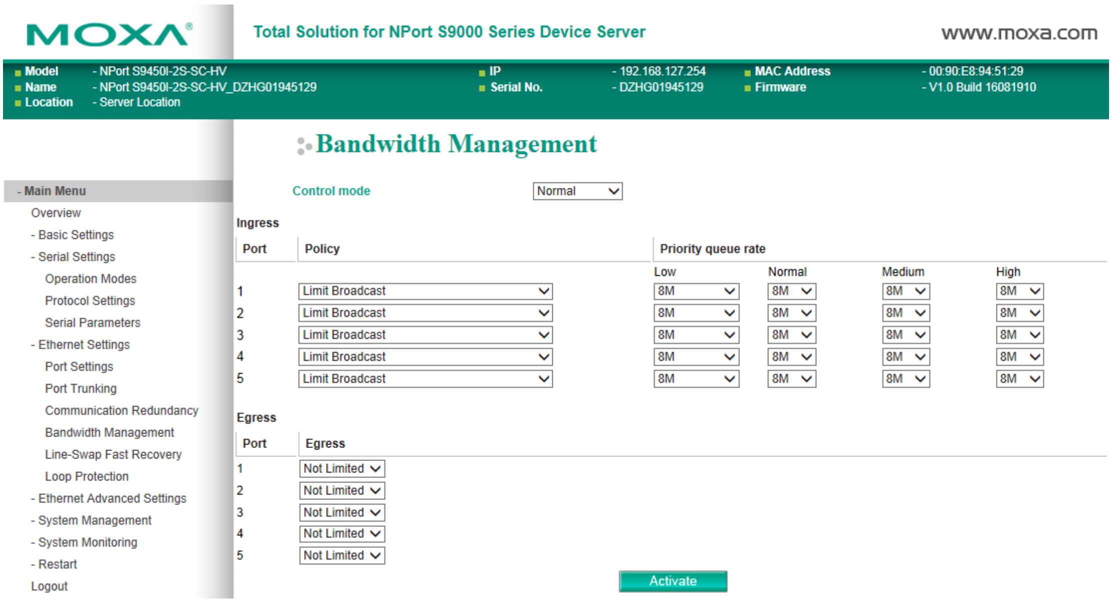
Setting	Description	Factory Default
Tail Port	Select any port of the device server to be the tail port.	port 4
Member Port	Select any port of the device server to be the member port.	port 5

Bandwidth Management

Using Bandwidth Management

In general, one host should not be allowed to occupy unlimited bandwidth, particularly when the device malfunctions. For example, so-called "broadcast storms" could be caused by an incorrectly configured topology, or a malfunctioning device. The NPort S9000 not only prevents broadcast storms, but can also be configured to a different ingress rate for all packets, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

Configuring Bandwidth Management



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

Bandwidth Management

Control mode: Normal

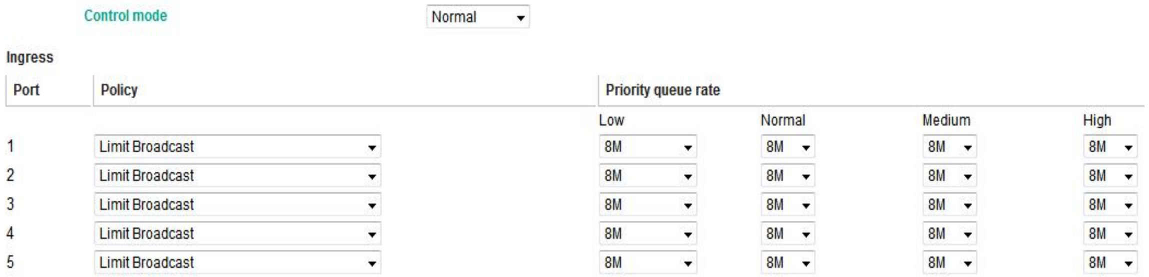
Ingress

Port	Policy	Priority queue rate			
		Low	Normal	Medium	High
1	Limit Broadcast	8M	8M	8M	8M
2	Limit Broadcast	8M	8M	8M	8M
3	Limit Broadcast	8M	8M	8M	8M
4	Limit Broadcast	8M	8M	8M	8M
5	Limit Broadcast	8M	8M	8M	8M

Egress

Port	Egress
1	Not Limited
2	Not Limited
3	Not Limited
4	Not Limited
5	Not Limited

Traffic Rate Limiting Settings



Control mode: Normal

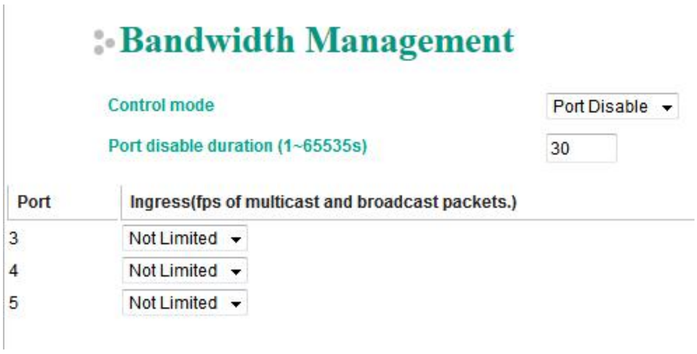
Ingress

Port	Policy	Priority queue rate			
		Low	Normal	Medium	High
1	Limit Broadcast	8M	8M	8M	8M
2	Limit Broadcast	8M	8M	8M	8M
3	Limit Broadcast	8M	8M	8M	8M
4	Limit Broadcast	8M	8M	8M	8M
5	Limit Broadcast	8M	8M	8M	8M

Control Mode	Description	Factory Default
Normal	Set the max. ingress rate limit for different packet types	Normal
Port Disable	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for a certain period. During this period, all packets from this port will be discarded.	

Ingress Rate Limit—Normal

Policy	Description	Factory Default
Limit All	Select the ingress rate limit for different packet types from the following options: Unlimited, 128K, 256K, 512K, 1M, 2M, 4M, 8M	Limit Broadcast 8M
Limit Broadcast, Multicast, Flooded Unicast		
Limit Broadcast, Multicast		
Limit Broadcast		



Bandwidth Management

Control mode: Port Disable

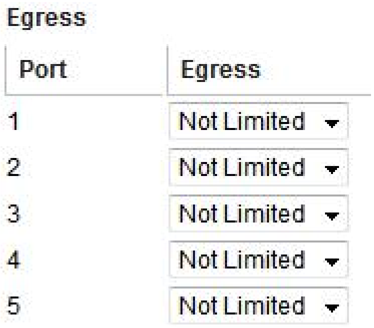
Port disable duration (1~65535s): 30

Port	Ingress(fps of multicast and broadcast packets.)
3	Not Limited
4	Not Limited
5	Not Limited

Ingress Rate Limit—Port Disable

Setting	Description	Factory Default
Port disable duration (1-65535 seconds)	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for this period of time. During this time, all packets from this port will be discarded.	30 seconds
Ingress (frames per second)	Select the ingress rate (fps) limit for all packets from the following options: Not Limited, 4464, 7441, 14881, 22322, 37203, 52084, 74405	Unlimited

Egress Rate Limit



Egress

Port	Egress
1	Not Limited ▾
2	Not Limited ▾
3	Not Limited ▾
4	Not Limited ▾
5	Not Limited ▾

Setting	Description	Factory Default
Egress rate (% of max. throughput)	Select the egress rate limit (% of max. throughput) for all packets from the following options: Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Unlimited

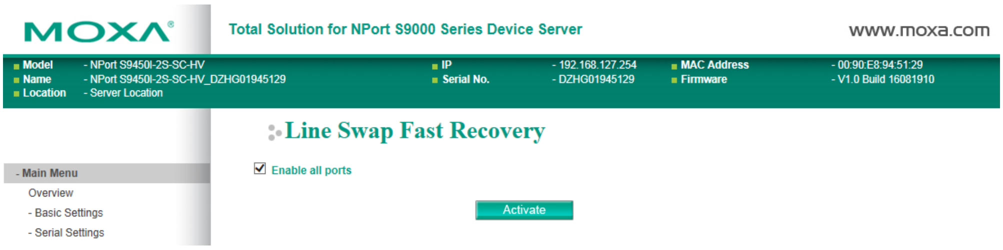
Line Swap Fast Recovery

Using Line-Swap-Fast-Recovery

The Line-Swap Fast Recovery function, which is enabled by default, allows the NPort S9000 to return to normal operation extremely quickly after devices are unplugged and then replugged into different ports. The recovery time is on the order of a few milliseconds (compare this with standard commercial switches for which the recovery time could be on the order of several minutes).

Configuring Line-Swap Fast Recovery

To disable the Line-Swap Fast Recovery function, or to reenable the function after it has already been disabled, access either the Console utility's **Line-Swap recovery** page, or the Web Browser interface's **Line-Swap fast recovery** page, as the following figure shows:



Total Solution for NPort S9000 Series Device Server

www.moxa.com

Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

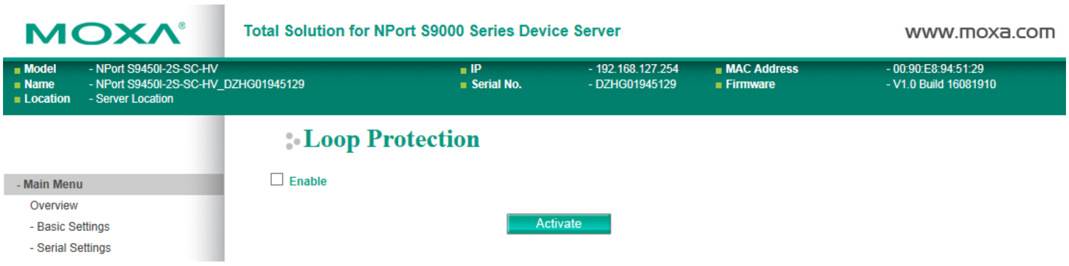
Line Swap Fast Recovery

☑ Enable all ports

Enable Line-Swap-Fast Recovery

Setting	Description	Factory Default
Enable/Disable	Select this option to enable the Line-Swap-Fast-Recovery function	Enable

Loop Protection



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

Loop Protection

□ Enable

Enable Loop Protection

Setting	**Description**	**Factory Default**
Enable	Select the Enable checkbox to enable the loop protection function.	Disable
Disable	Deselect the Enable checkbox to disable the loop protection function.	

Ethernet Advanced Settings

Ethernet Traffic Prioritization

Using Traffic Prioritization

The NPort S9000's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high-priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The NPort S9000 can inspect both IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information to provide consistent classification of the entire network. The NPort S9000's QoS capability improves the performance and determinism of industrial networks for mission-critical applications.

The Traffic Prioritization Concept

What is Traffic Prioritization?

Traffic prioritization allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- Improve network performance by controlling a wide variety of traffic and managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or business-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP (VoIP), and minimize traffic delay and jitter.
- Improve network performance as the amount of traffic grows. This will save costs by reducing the need to keep adding bandwidth to the network.

How Traffic Prioritization Works

Traffic prioritization uses the four traffic queues that are present in your NPort S9000 to ensure that high-priority traffic is forwarded on a different queue from lower priority traffic. This is what provides Quality of Service (QoS) to your network.

NPort S9000 traffic prioritization depends on two industry-standard methods:

- IEEE 802.1D—a layer 2 marking scheme.
- Differentiated Services (DiffServ)—a layer 3 marking scheme.

IEEE 802.1D Traffic Marking

The IEEE Std 802.1D, 1998 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. The 4-byte tag immediately follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D, 1998 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame. This determines the level of service that that type of traffic should receive. Refer to the table below for an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority Level	**IEEE 802.1D Traffic Type**
0	Best Effort (default)
1	Background
2	Standard (spare)
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (interactive media); less than 100 milliseconds of latency and jitter
6	Voice (interactive voice); less than 10 milliseconds of latency and jitter
7	Network Control Reserved traffic

Even though the IEEE 802.1D standard is the most widely used prioritization scheme in the LAN environment, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional in Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.

It is only supported on a LAN and not routed across WAN links, since the IEEE 802.1Q tags are removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to store the packet priority information. DSCP is an advanced intelligent method of traffic marking as you can choose how your network prioritizes different types of traffic. DSCP uses 64 values that map to user-defined service levels, allowing you to establish more control over network traffic.

Advantages of DiffServ over IEEE 802.1D are:

- Configure how you want your switch to treat selected applications and types of traffic by assigning various grades of network service to them.
- No extra tags are required in the packet.
- DSCP uses the IP header of a packet and, therefore, priority is preserved across the Internet.
- DSCP is backward compatible with IPV4 TOS, which allows operation with existing devices that use a layer 3 TOS enabled prioritization scheme.

Traffic Prioritization

The NPort S9000 classifies traffic based on layer 2 of the OSI 7 layer model, and the switch prioritizes received traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1D frame and is assigned to the appropriate priority queue based on the IEEE 802.1p service-level value defined in that packet. Service-level markings (values) are defined in the IEEE 802.1Q 4-byte tag, and consequently traffic will only contain 802.1p priority markings if the network is configured with VLANs and VLAN tagging. The traffic flow through the switch is as follows:

1. A packet received by the NPort S9000 may or may not have an 802.1p tag associated with it. If it does not, then it is given a default 802.1p tag (which is usually 0). Alternatively, the packet may be marked with a new 802.1p value, which will result in all knowledge of the old 802.1p tag being lost.
2. As the 802.1p priority levels are fixed to the traffic queues, the packet will be placed in the appropriate priority queue, ready for transmission through the appropriate egress port. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port is tagged for that VLAN. If it is, then the new 802.1p tag is used in the extended 802.1D header.

The NPort S9000 will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based upon the IEEE 802.1p value (service levels) in that tag. It is this 802.1p value that determines to which traffic queue the packet is mapped.

Traffic Queues

The NPort S9000 hardware has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the NPort S9000 without being delayed by lower priority traffic. As each packet arrives in the NPort S9000, it passes through any ingress processing (which includes classification, marking/remarking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue.

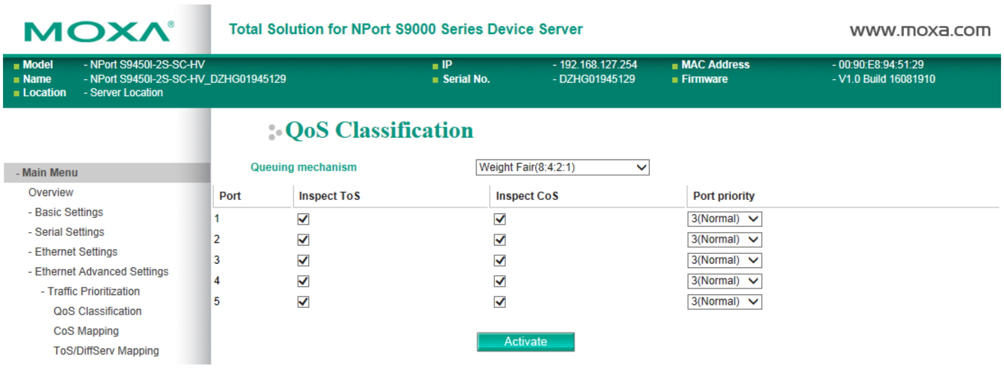
The NPort S9000 supports two different queuing mechanisms:

- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, this method gives high-priority precedence over low-priority, but in the event that high-priority traffic exceeds the link capacity, lower priority traffic is not blocked.
- **Strict:** This method services high-traffic queues first; low-priority queues are delayed until no more high-priority data needs to be sent. This method always gives precedence to high-priority over low-priority.

Configuring Ethernet Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization capability to ensure that important data is delivered consistently and predictably. The NPort S9000 can inspect IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information, to provide a consistent classification of the entire network. The NPort S9000's QoS capability improves your industrial network's performance and determinism for mission-critical applications.

QoS Classification



Total Solution for NPort S9000 Series Device Server

www.moxa.com

Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

QoS Classification

Queuing mechanism: Weight Fair(8:4:2:1)

Port	Inspect ToS	Inspect CoS	Port priority
1	☑	☑	3(Normal)
2	☑	☑	3(Normal)
3	☑	☑	3(Normal)
4	☑	☑	3(Normal)
5	☑	☑	3(Normal)

The NPort S9000 supports inspection of layer 3 TOS and/or layer 2 CoS tag information to determine how to classify traffic packets.

Queuing Mechanism

Setting	Description	Factory Default
Weighted Fair	The NPort S9000 has four priority queues. In the weighted fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower-priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures all high-priority frames to egress the switch as soon as possible.	

Inspect TOS

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the NPort S9000 to inspect the Type of Service (TOS) bits in IPV4 frame to determine the priority of each frame.	Enable

Inspect COS

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the NPort S9000 to inspect the 802.1p COS tag in the MAC frame to determine the priority of each frame.	Enable

Port Priority

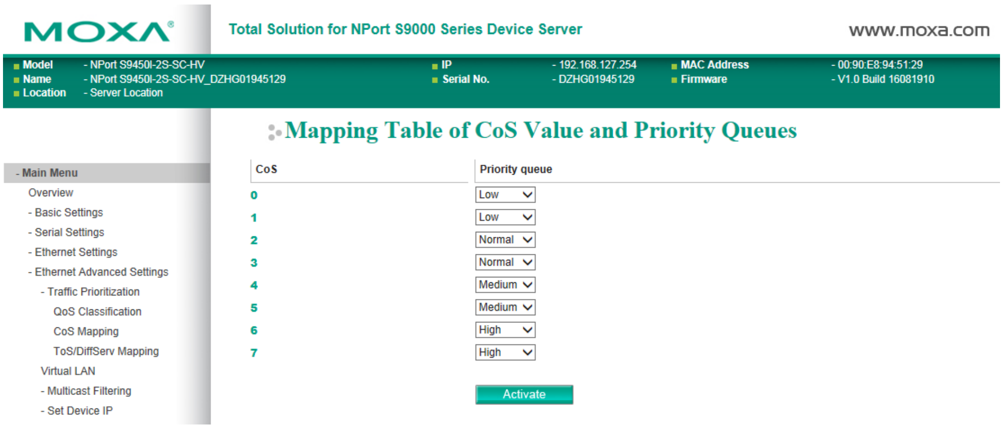
Setting	Description	Factory Default
Numerical value selected by user (from 0 to 7)	Increase this port's priority as a node on the 802.1d priority queue. The higher number the higher priority.	3

NOTE The priority of an ingress frame is determined in order by:

1. Inspect TOS
2. Inspect CoS
3. Port Highest Priority

NOTE The designer can enable these classifications individually or in combination. For instance, if a 'hot,' higher priority port is required for a network design, "Inspect TOS" and "Inspect CoS" can be disabled. This setting leaves only port default priority active, which results in all ingress frames being assigned the same priority on that port.

CoS Mapping



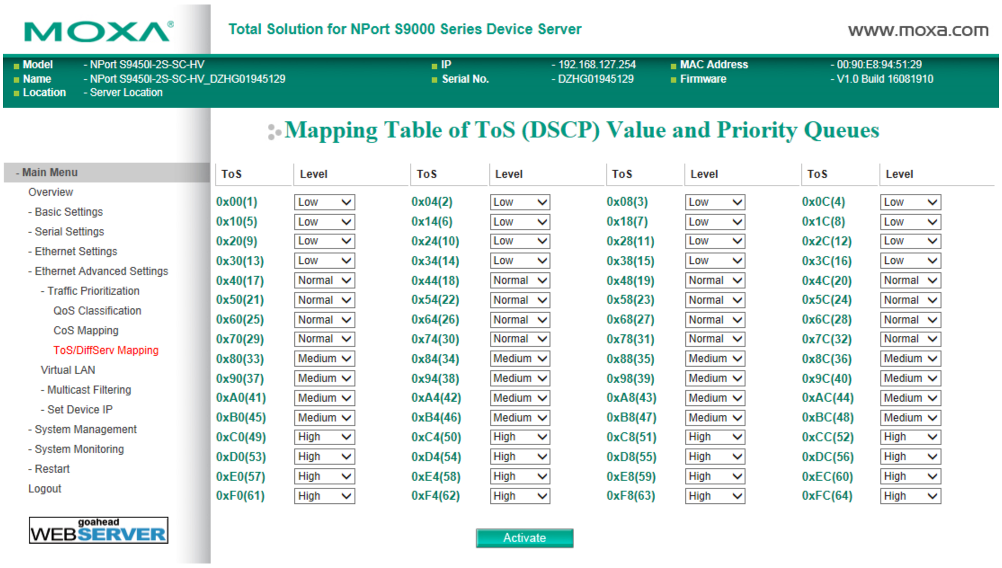
Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

Mapping Table of CoS Value and Priority Queues

CoS	Priority queue
0	Low
1	Low
2	Normal
3	Normal
4	Medium
5	Medium
6	High
7	High

Setting	Description	Factory
Low Normal Medium High	Set the mapping table of different CoS values to four different egress queues.	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

ToS/DiffServ Mapping



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

Mapping Table of ToS (DSCP) Value and Priority Queues

ToS	Level	ToS	Level	ToS	Level	ToS	Level
0x00(1)	Low	0x04(2)	Low	0x08(3)	Low	0x0C(4)	Low
0x10(5)	Low	0x14(6)	Low	0x18(7)	Low	0x1C(8)	Low
0x20(9)	Low	0x24(10)	Low	0x28(11)	Low	0x2C(12)	Low
0x30(13)	Low	0x34(14)	Low	0x38(15)	Low	0x3C(16)	Low
0x40(17)	Normal	0x44(18)	Normal	0x48(19)	Normal	0x4C(20)	Normal
0x50(21)	Normal	0x54(22)	Normal	0x58(23)	Normal	0x5C(24)	Normal
0x60(25)	Normal	0x64(26)	Normal	0x68(27)	Normal	0x6C(28)	Normal
0x70(29)	Normal	0x74(30)	Normal	0x78(31)	Normal	0x7C(32)	Normal
0x80(33)	Medium	0x84(34)	Medium	0x88(35)	Medium	0x8C(36)	Medium
0x90(37)	Medium	0x94(38)	Medium	0x98(39)	Medium	0x9C(40)	Medium
0xA0(41)	Medium	0xA4(42)	Medium	0xA8(43)	Medium	0xAC(44)	Medium
0xB0(45)	Medium	0xB4(46)	Medium	0xB8(47)	Medium	0xBC(48)	Medium
0xC0(49)	High	0xC4(50)	High	0xC8(51)	High	0xCC(52)	High
0xD0(53)	High	0xD4(54)	High	0xD8(55)	High	0xDC(56)	High
0xE0(57)	High	0xE4(58)	High	0xE8(59)	High	0xEC(60)	High
0xF0(61)	High	0xF4(62)	High	0xF8(63)	High	0xFC(64)	High

Setting	Description	Factory Default
Low Normal Medium High	Set the mapping table of different TOS values to four different egress queues.	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

Virtual LAN

Using Virtual LAN

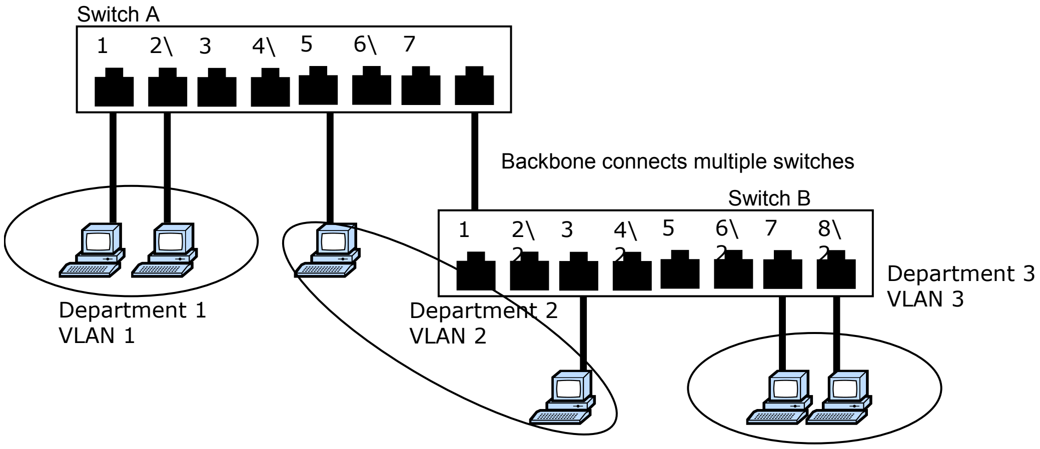
Setting up Virtual LANs (VLANs) on your NPort S9000 increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

The Virtual LAN (VLAN) Concept

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. As an example, with VLANs you can segment your network according to:

- **Departmental groups**—You could have one VLAN for the Marketing department, another for the Finance department, and another for the Development department.
- **Hierarchical groups**—You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—You could have one VLAN for e-mail users and another for multimedia users.



Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend most of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host on VLAN Marketing, for example, is moved to a port in another part of the network, and retains its original subnet membership, you only need to specify that the new port is on VLAN Marketing. You do not need to carry out any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on VLAN Marketing needs to communicate with devices on VLAN Finance, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs and Moxa EtherDevice Switch

Your NPort S9000 provides support for VLANs using IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-1998 standard allows each port on your NPort S9000 to be placed in:

- Any one VLAN defined on the NPort S9000.
- Several VLANs at the same time using 802.1Q tagging.

The standard requires that you define the *802.1Q VLAN ID* for each VLAN on your NPort S9000 before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized NPort S9000 contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- *VLAN Name*—Management VLAN
- *802.1Q VLAN ID*—1 (if tagging is required)

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the NPort S9000 over the network.

Communication Between VLANs

If devices connected to a VLAN need to communicate to devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

The NPort S9000 supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical (backbone, trunk) link. When setting up VLANs, you need to understand when to use untagged and tagged membership of VLANs. Simply put, if a port is on a single VLAN, it can be an untagged member, but if the port needs to be a member of multiple VLANs, tagged membership must be defined.

A typical host (e.g., clients) will be untagged members of one VLAN, defined as "Access Port" in the NPort S9000, while inter-switch connections will be tagged members of all VLANs, defined as "Trunk Port" in the NPort S9000.

The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs. If a frame is carrying the additional information, it is known as a *tagged* frame.

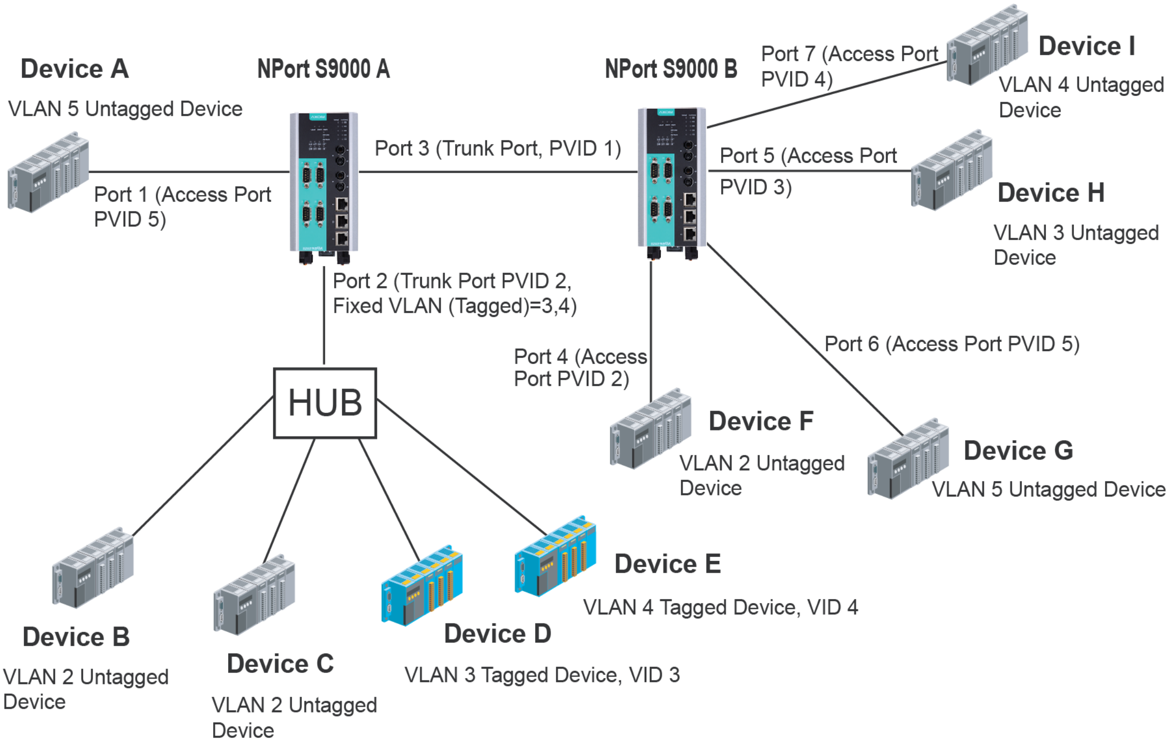
To carry multiple VLANs across a single physical (backbone, trunk) link, each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong to which VLAN. To communicate between VLANs, a router must be used.

The NPort S9000 supports two types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that determines to which VLAN the device belongs. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the NPort S9000 will insert this PVID into this packet to help the next 802.1Q VLAN switch recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices/tagged devices and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the port default PVID as its VID.

The following section illustrates how to use these ports to set up different applications.

Sample Applications of VLANs using the NPort S9000


Device A
VLAN 5 Untagged Device
NPort S9000 A
NPort S9000 B
Port 7 (Access Port PVID 4)
Device I
VLAN 4 Untagged Device
Port 3 (Trunk Port, PVID 1)
Port 5 (Access Port PVID 3)
Port 1 (Access Port PVID 5)
Device H
VLAN 3 Untagged Device
Port 2 (Trunk Port PVID 2, Fixed VLAN (Tagged)=3,4)
Port 6 (Access Port PVID 5)
Port 4 (Access Port PVID 2)
HUB
Device F
VLAN 2 Untagged Device
Device G
VLAN 5 Untagged Device
Device E
VLAN 4 Tagged Device, VID 4
Device B
VLAN 2 Untagged Device
Device C
VLAN 2 Untagged Device
Device D
VLAN 3 Tagged Device, VID 3

In this application:

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as "Access Port" with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as "Trunk Port" with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port can only belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as "Trunk Port." GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as "Access Port" with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as "Access Port" with PVID 3.
- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as "Access Port" with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as "Access Port" with PVID 4.

After proper configuration:

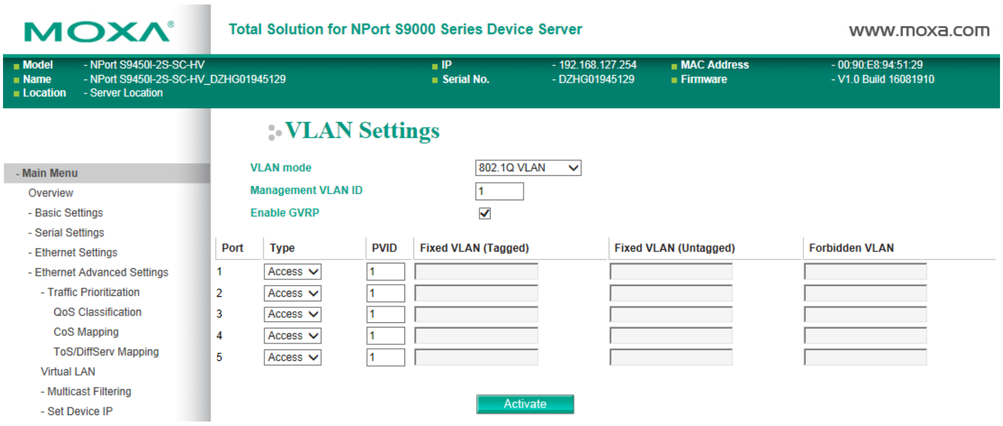
- Packets from device A will travel through "Trunk Port 3" with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by device G and vice versa.
- Packets from device B and C will travel through "Trunk Port 3" with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by device F and vice versa.
- Packets from device D will travel through "Trunk Port 3" with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by device H. Packets from device H will travel through "Trunk Port 3" with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device D.

- Packets from device E will travel through "Trunk Port 3" with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by device I. Packets from device I will travel through "Trunk Port 3" with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device E.

Configuring Virtual LAN

VLAN Settings 802.1Q VLAN

To configure the NPort S9000's **802.1Q VLAN**, use the VLAN Setting page to configure the ports.



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

VLAN Settings

VLAN mode: 802.1Q VLAN
Management VLAN ID: 1
Enable GVRP: ☑

Port	Type	PVID	Fixed VLAN (Tagged)	Fixed VLAN (Untagged)	Forbidden VLAN
1	Access	1			
2	Access	1			
3	Access	1			
4	Access	1			
5	Access	1			

VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	

Management VLAN ID

Setting	Description	Factory Default
VLAN ID ranges from 1 to 4094	Set the management VLAN of this NPort S9000.	1

Port Type

Setting	Description	Factory Default
Access	This port type is used to connect single devices without tags.	Access
Trunk	Select "Trunk" port type to connect another 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs.	

ATTENTION

For communication redundancy in the VLAN environment, set **Redundant Port**, **Coupling Port**, and **Coupling Control Port** as **Trunk Port**, as these ports act as the "backbone" to transmit all packets of different VLANs to different NPort S9000 units.

Port PVID

Setting	Description	Factory Default
VID range from 1 to 4094	Set the port default VLAN ID for untagged devices that connect to the port.	1

Fixed VLAN List (Tagged)

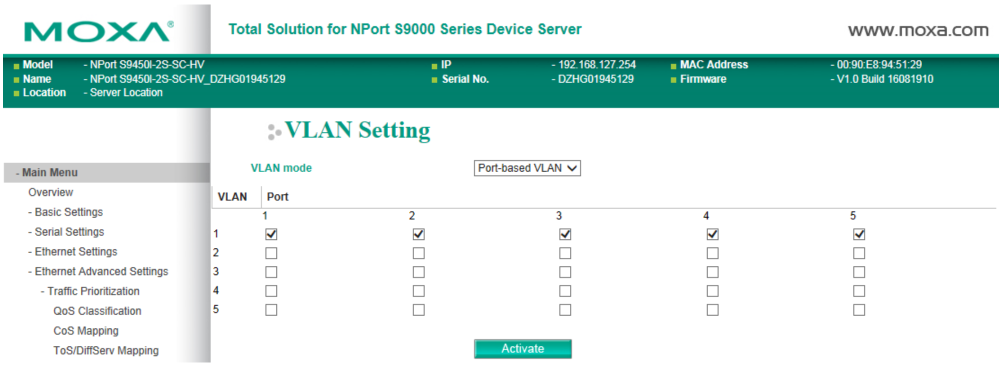
Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the "Trunk" port type. Set the other VLAN ID for tagged devices that connect to the "Trunk" port. Use commas to separate different VIDs.	None

Forbidden VLAN List

Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the "Trunk" port type. Set the VLAN IDs that will not be supported by this trunk port. Use commas to separate different VIDs.	None

Port-based VLAN

To configure the NPort S9000's **Port-based VLAN**, use the VLAN Setting page to configure the ports.



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

VLAN Setting

VLAN mode: Port-based VLAN

VLAN	Port 1	2	3	4	5
1	☑	☑	☑	☑	☑
2	□	□	□	□	□
3	□	□	□	□	□
4	□	□	□	□	□
5	□	□	□	□	□

VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	

Port

Setting	Description	Factory Default
Enable/Disable	Set port to specific VLAN Group.	Enable (all ports belong to VLAN1)

In 802.1Q VLAN table, you can review the VLAN groups that were created, Joined Access Ports and Trunk Ports, and in Port-based VLAN table, you can review the VLAN group and Joined port.

NOTE The physical network can have a maximum of 64 VLAN settings.

Multicast Filtering

Using Multicast Filtering

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your NPort S9000.

The Concept of Multicast Filtering

What is an IP Multicast?

A *multicast* is a packet sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. If the network is set up correctly, a multicast can only be sent to an end station or a subset of end stations on a LAN or VLAN that belong to the multicast group. Multicast group members can be distributed across multiple subnets, so that multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only *one* copy of the desired information across the network until the delivery path that reaches group members diverges. To make more efficient use of network bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

The benefits of using IP multicast are that it:

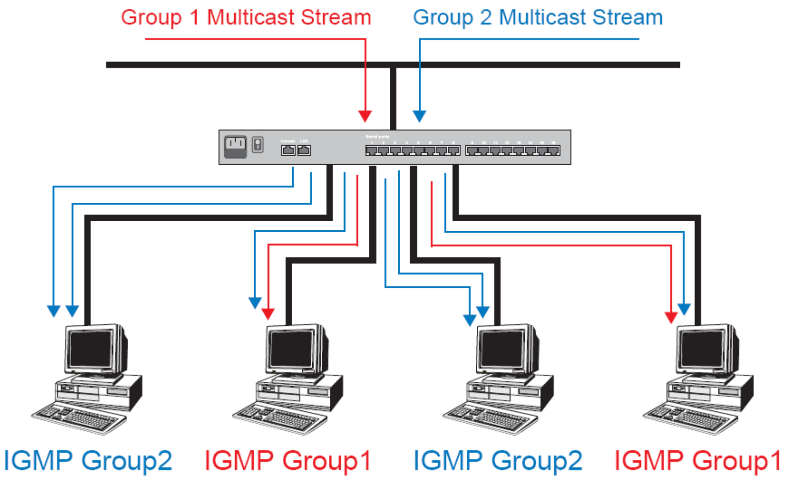
- Uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- Reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- Makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- Works with other IP protocols and services, such as Quality of Service (QoS).

Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end stations at the same time, but where broadcasting the traffic to all end stations would cause a substantial reduction in network performance. Furthermore, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use multicast. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

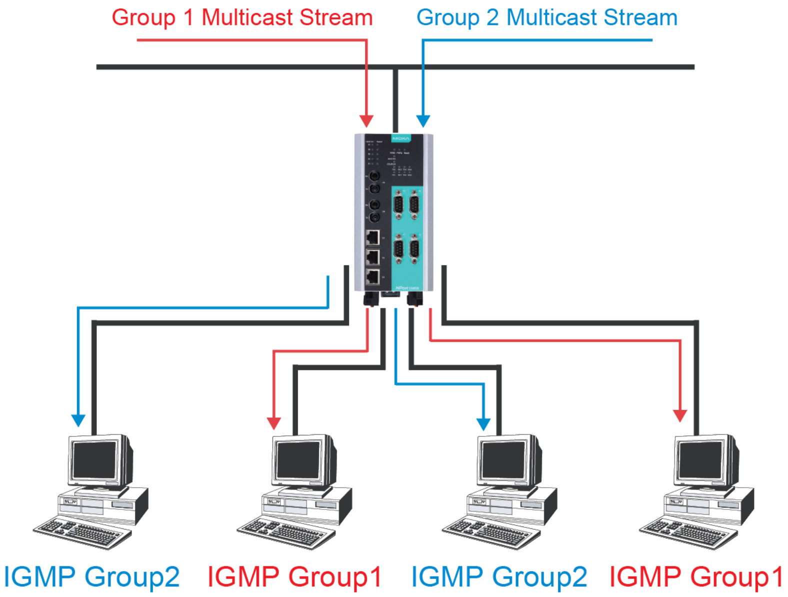
Multicast filtering ensures that only endstations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end stations. The following two figures illustrate how a network behaves without multicast filtering and with multicast filtering.

Network without multicast filtering



All hosts receive the multicast traffic, even if they don't need it.

Network with multicast filtering



The hosts only receive dedicated traffic from other hosts belonging to the same group.

Multicast Filtering and Moxa Switching Device Server

The NPort S9000 has three ways to achieve multicast filtering: IGMP (Internet Group Management Protocol) Snooping, GMRP (GARP Multicast Registration Protocol), and adding a static multicast MAC manually to filter multicast traffic automatically

IGMP Multicast Filtering

IGMP is used by IP-supporting network devices to register hosts with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router and on other network devices that support multicast filtering. IGMP works as follows:

The IP router (or querier) periodically sends *query* packets to all end stations on the LANs or VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with IP address lower than the IP address of any other IGMP queriers connected to the LAN or VLAN can become the IGMP querier.

When an IP host receives a query packet, it sends a *report* packet back that identifies the multicast group that the end station would like to join.

When the report packet arrives at a port on a switch with *IGMP Snooping* enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.

When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.

When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

IGMP (Internet Group Management Protocol)

Snooping Mode

Snooping Mode allows your switch to forward multicast packets only to the appropriate ports. The switch “snoops” on exchanges between hosts and an IGMP device, such as a router, to find those ports that want to join a multicast group, and then configures its filters accordingly.

Query Mode

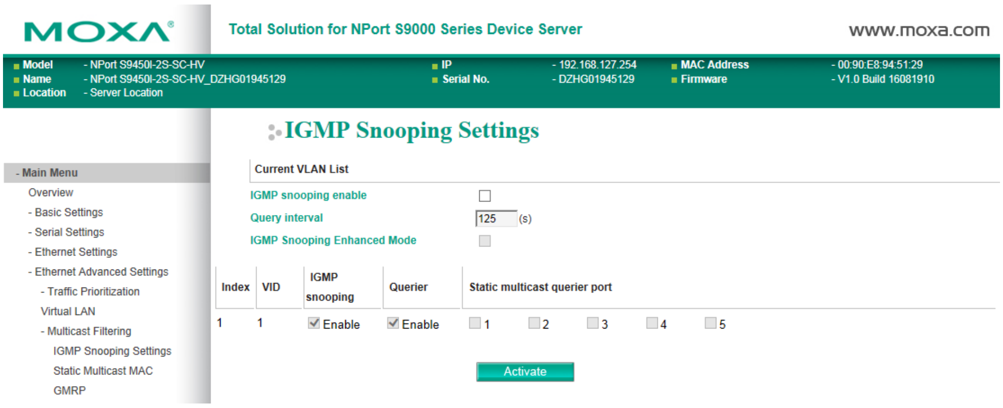
Query mode allows the NPort S9000 to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs. IGMP querying is enabled by default on the NPort S9000 to help prevent interoperability issues with some multicast routers that may not follow the lowest IP address election method. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers).

NOTE The NPort S9000 is compatible with any device that conforms to the IGMP v2 and IGMP v3 device protocol.

Configuring IGMP Snooping

IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.

IGMP Snooping Settings



Total Solution for NPort S9000 Series Device Server

Model	- NPort S9450I-2S-SC-HV	IP	- 192.168.127.254	MAC Address	- 00:90:E8:94:51:29
Name	- NPort S9450I-2S-SC-HV_DZHG01945129	Serial No.	- DZHG01945129	Firmware	- V1.0 Build 16081910
Location	- Server Location				

IGMP Snooping Settings

Current VLAN List

IGMP snooping enable □

Query interval 125 (s)

IGMP Snooping Enhanced Mode □

Index	VID	IGMP snooping	Querier	Static multicast querier port
1	1	☑ Enable	☑ Enable	□ 1 □ 2 □ 3 □ 4 □ 5

IGMP Snooping Enable

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the IGMP Snooping function globally.	Disabled

Query Interval

Setting	Description	Factory Default
Numerical value input by user	Set the query interval of the Querier function globally. Valid settings are from 20 to 600 seconds.	125 seconds

IGMP Snooping

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the IGMP Snooping function per VLAN.	Enabled if IGMP Snooping Enabled Globally

Querier

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the NPort S9000's querier function.	Enabled if IGMP Snooping is Enabled Globally

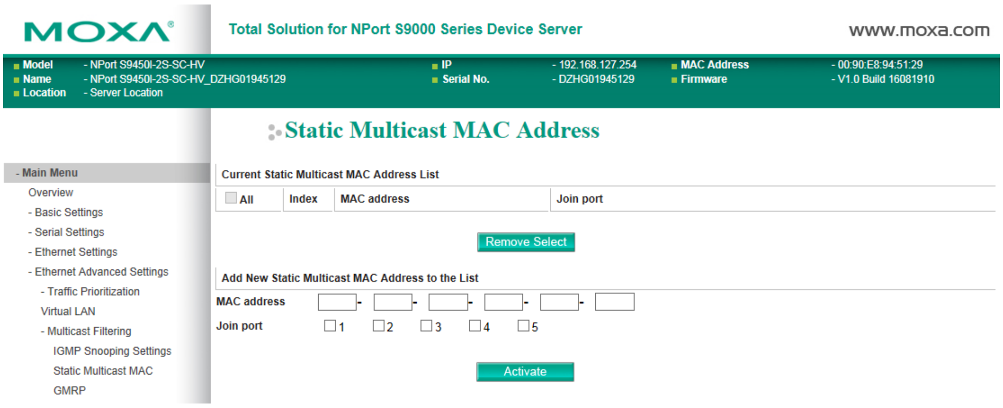
Static Multicast Router Port

Setting	Description	Factory Default
Select/Deselect	Select the option to select which ports will connect to the multicast routers. It's active only when IGMP Snooping is enabled.	Disabled

NOTE At least one switch must be designated the Querier or enable IGMP snooping and GMRP when enabling Turbo Ring and IGMP snooping simultaneously.

Static Multicast MAC

Some devices may only support multicast packets, but not support either IGMP Snooping or GMRP. The NPort S9000 supports adding multicast groups manually to enable multicast filtering.



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

Static Multicast MAC Address

Current Static Multicast MAC Address List

□ All	Index	MAC address	Join port

Add New Static Multicast MAC Address to the List

MAC address ____ - ____ - ____ - ____ - ____ - ____

Join port □1 □2 □3 □4 □5

Add New Static Multicast Address to the List

Setting	Description	Factory Default
MAC Address	Input the multicast MAC address of this host.	None

Join Port

Setting	Description	Factory Default
Select/Deselect	Select the appropriate options to select the join ports for this multicast group.	None

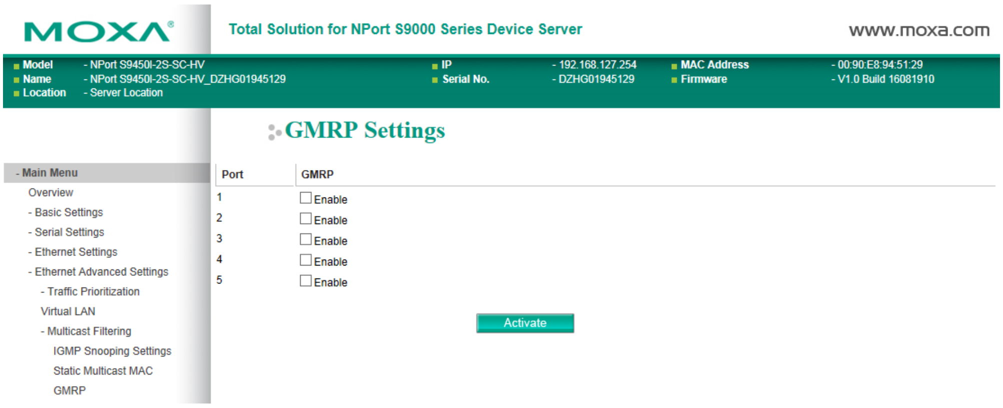
GMRP (GARP Multicast Registration Protocol)

The NPort S9000 supports IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol), which differs from IGMP (Internet Group Management Protocol). GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or deregister Group membership information dynamically. GMRP functions similarly to GVRP, except that GMRP registers multicast addresses on ports. When a port receives a ***GMRP-join*** message, it will register the multicast address to its database if the multicast address is not registered, and all the multicast packets with that multicast address are able to be forwarded from this port. When a port receives a ***GMRP-leave*** message, it will deregister the multicast address from its database, and all the multicast packets with this multicast address are not able to be forwarded from this port.

(Please refer to Chapter 8, "System Monitoring," *Ethernet Status for IGMP/GMRP Table*)

Configuring GMRP

GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or deregister Group membership information dynamically.



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

GMRP Settings

Port	GMRP
1	□ Enable
2	□ Enable
3	□ Enable
4	□ Enable
5	□ Enable

GMRP enable

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the GMRP function for the port listed in the Port column	Disable

Set Device IP

Using Set Device IP

To reduce the effort required to set up IP addresses, the NPort S9000 comes equipped with a DHCP/BOOTP server and RARP protocol to set up the IP addresses of Ethernet-enabled devices automatically.

When enabled, the **Set device IP** function allows The NPort S9000 to assign specific IP addresses automatically to connected devices that are equipped with *DHCP Client* or *RARP* protocol. In effect, the NPort S9000 acts as a DHCP server by assigning a connected device with a specific IP address stored in its internal memory. Each time the connected device is switched on or rebooted, the NPort S9000 sends the device the desired IP address.

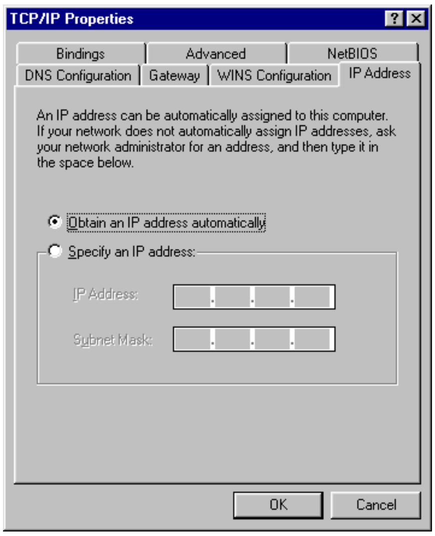
Perform the following steps to use the **Set device IP** function:

1. *Set up the connected devices*

Set up those Ethernet-enabled devices connected to the NPort S9000 for which you would like IP addresses to be assigned automatically. The devices must be configured to obtain their IP address automatically.

The devices' configuration utility should include a setup page that allows you to choose an option similar to obtain an IP address automatically.

For example, a Windows' TCP/IP Properties window is shown at the right. Although your device's configuration utility may look quite a bit different, this figure should give you some idea of what to look for.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

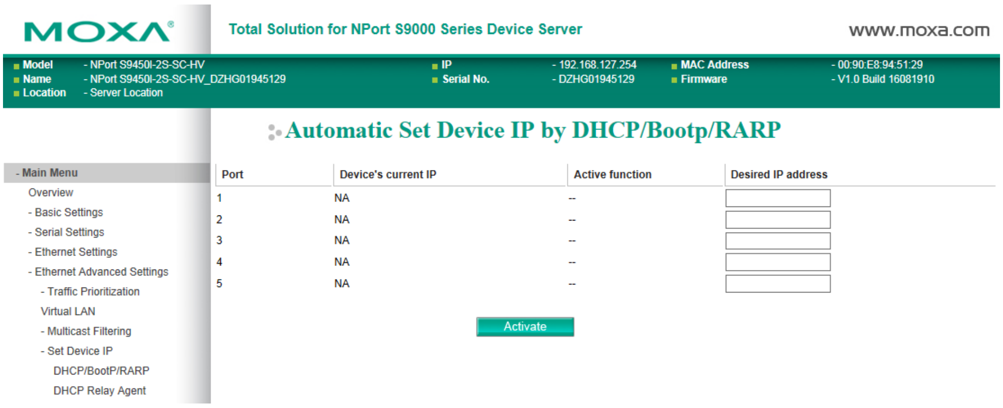
IP Address: . . .

Subnet Mask: . . .

You also need to decide to which of the NPort S9000's ports your Ethernet-enabled devices will be connected. You will need to set up each of these ports separately, as described in the following step.

2. Configure the NPort S9000's Set device IP function, either from the Console utility or from the Web Browser interface. In either case, you simply need to enter the Desired IP for each port that needs to be configured.
3. Be sure to activate your settings before exiting.
   - When using the Web Browser interface, activate by clicking **Activate**.
   - When using the Console utility, activate by first highlighting the **Activate** menu option, and then press **Enter**. You should receive the **Set device IP settings are now active! (Press any key to continue)** message.

Configuring Set Device IP



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

Automatic Set Device IP by DHCP/Bootp/RARP

Port	Device's current IP	Active function	Desired IP address
1	NA	--	
2	NA	--	
3	NA	--	
4	NA	--	
5	NA	--	

Desired IP Address

Setting	Description	Factory Default
IP Address	Set the desired IP of connected devices.	None

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

DHCP Relay Agent (Option 82)

Option 82 is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

When Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains two sub-options: Circuit ID and Remote ID, which define the relationship between end device IP and the DHCP Option 82 server. The “Circuit ID” is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID. The format of the “Circuit ID” is as described below:

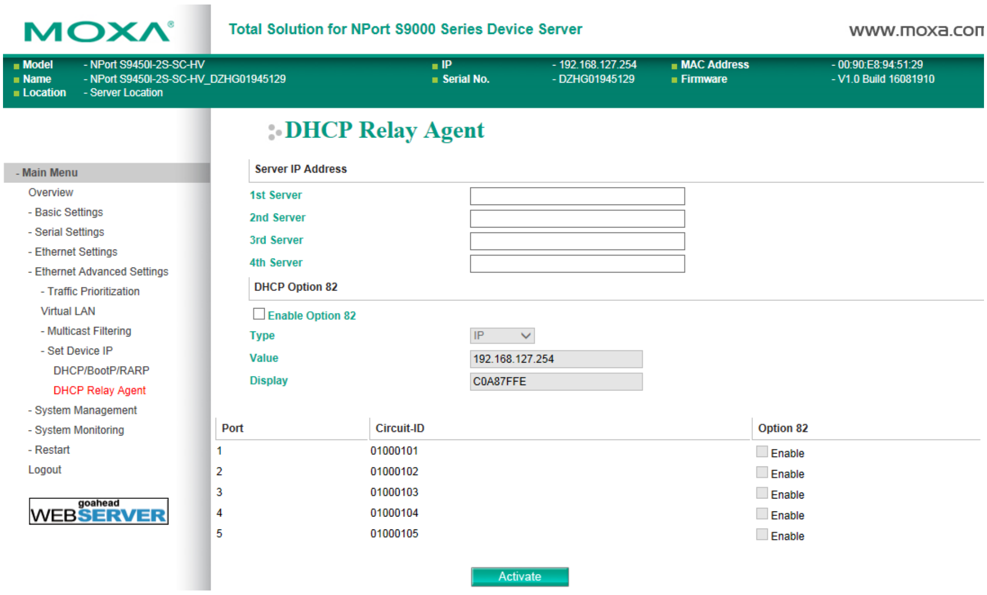
FF–VV–VV–PP

Where the first byte “FF” is fixed to “01”, the second and the third byte “VV-VV” is formed by the port VLAN ID in hex, and the last byte “PP” is formed by the port number in hex. For example,

01–00–0F–03 is the “Circuit ID” of port number 3 with port VLAN ID 15.

The “Remote ID” is to identify the relay agent itself, and it can be one of the following:

1. The IP address of the relay agent.
2. The MAC address of the relay agent.
3. A combination of IP address and MAC address of the relay agent.
4. A user-defined string.



Model - NPort S9450I-2S-SC-HV
Name - NPort S9450I-2S-SC-HV_DZHG01945129
Location - Server Location
IP - 192.168.127.254
Serial No. - DZHG01945129
MAC Address - 00:90:E8:94:51:29
Firmware - V1.0 Build 16081910

DHCP Relay Agent

Server IP Address

1st Server
2nd Server
3rd Server
4th Server

DHCP Option 82

☐ Enable Option 82
Type: IP
Value: 192.168.127.254
Display: C0A87FFE

Port	Circuit-ID	Option 82
1	01000101	☐ Enable
2	01000102	☐ Enable
3	01000103	☐ Enable
4	01000104	☐ Enable
5	01000105	☐ Enable

8

Management and Monitor Function

In this chapter, we use the Web Console interface to introduce the functions focus on the Management and Monitor Functions.

The following topics are covered in this chapter:

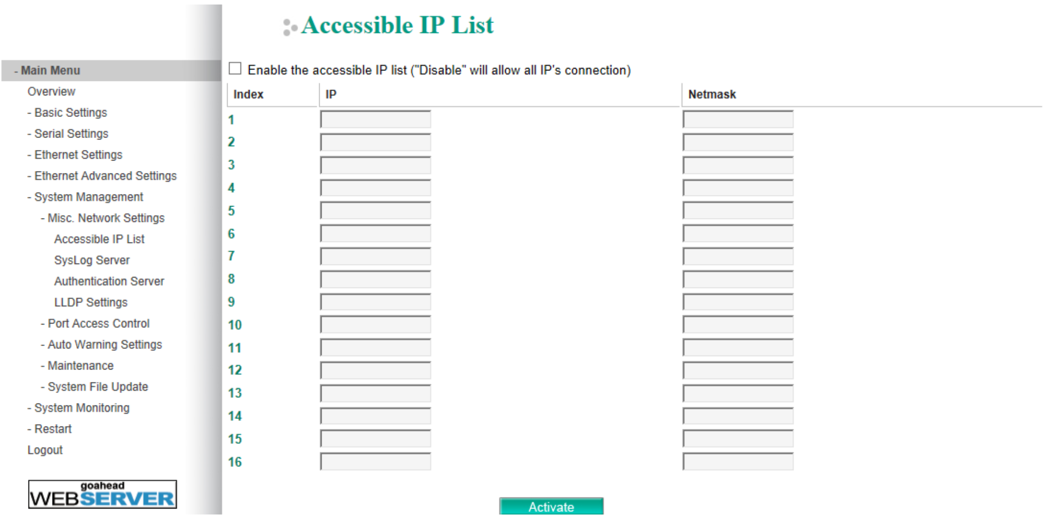
- **System Management**
  - Misc. Network Settings
- **Syslog Server**
  - Using Syslog
- **Authentication Server**
  - LLDP
- **Port Access Control**
  - Configuring Static Port Lock
  - Configuring IEEE 802.1X
  - Auto Warning Settings
- **Configuring E-Mail Alert**
- **Configuring SNMP**
  - SNMP Read/Write Settings
  - Trap Settings
  - E-mail Event Settings
  - SNMP Trap
  - Relay Alarm Settings
  - System Log Settings
- **Maintenance**
  - Console Settings
  - Ping
  - Load Factory Default
  - Mirror
  - Authentication Certificate
  - System File Update
  - FTP Settings
  - TFTP Settings
- **System Monitoring**
  - Serial Status
  - System Status
  - Ethernet Status
- **Restart**
  - Restart System
  - Restart Serial Port
  - Logout

System Management

Misc. Network Settings

Accessible IP List

The NPort S9000 uses an IP address-based filtering method to control access to NPort S9000 units.



☐ Enable the accessible IP list ("Disable" will allow all IP's connection)

Index	IP	Netmask
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		

Accessible IP Settings allows you to add or remove "Legal" remote host IP addresses to prevent unauthorized access. Access to the NPort S9000 is controlled by an IP address. If a host's IP address is in the accessible IP table, then the host will be allowed access to the NPort S9000. You can allow one of the following cases by setting this parameter:

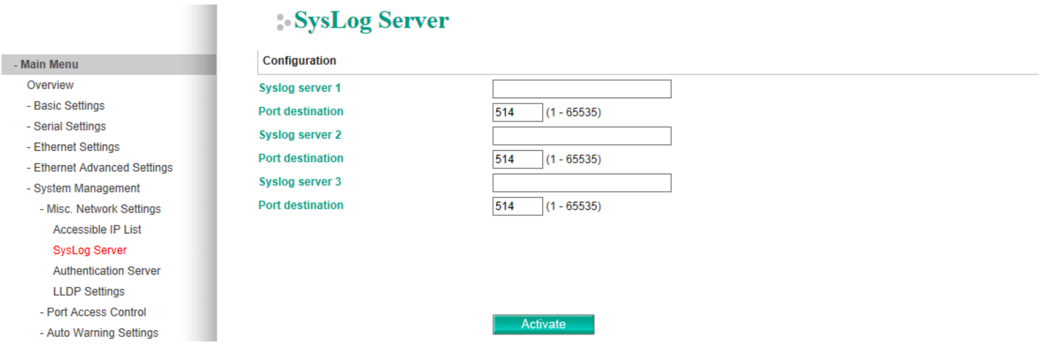
- **Only one host with the specified IP address can access the NPort S9000**
  E.g., enter "192.168.1.1/255.255.255.255" to allow access to just the IP address 192.168.1.1.
- **Any host on a specific subnetwork can access the NPort S9000**
  E.g., enter "192.168.1.0/255.255.255.0" to allow access to all IPs on the subnet defined by this IP address/subnet mask combination.
- **Any host can access the NPort S9000**
  Disable this function by deselecting the Enable the accessible IP list option. The following table shows additional configuration examples:

Allowable Hosts	Input format
Any host	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

Syslog Server

Using Syslog

This function provides the event logs for the syslog server. The function supports three configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a Syslog UDP packet to the specified syslog servers.



SysLog Server

Configuration

Syslog server 1	
Port destination	514 (1 - 65535)
Syslog server 2	
Port destination	514 (1 - 65535)
Syslog server 3	
Port destination	514 (1 - 65535)

Syslog Server 1

Setting	Description	Factory Default
IP Address	Enter the IP address of the first Syslog Server used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of the first Syslog Server.	514

Syslog Server 2

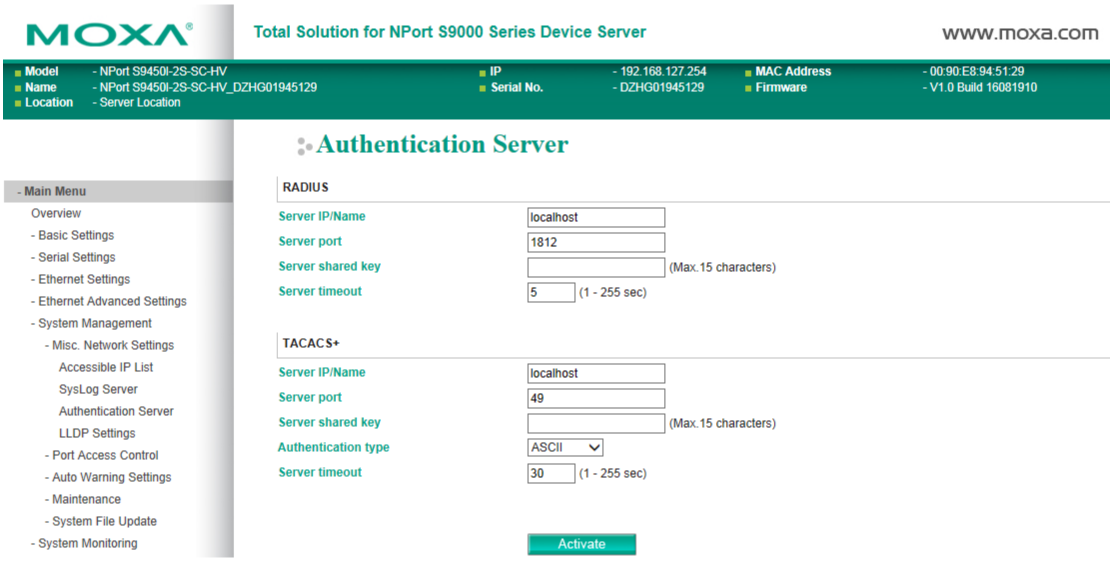
Setting	Description	Factory Default
IP Address	Enter the IP address of the second Syslog Server used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of the second Syslog Server.	514

Syslog Server 3

Setting	Description	Factory Default
IP Address	Enter the IP address of the third Syslog Server used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of the third Syslog Server.	514

NOTE The log events will be recorded, so please reference to the **System Log Settings** under **System Management --> Auto Warning Settings --> System Log Settings.**

Authentication Server



Model	- NPort S9450I-2S-SC-HV	IP	- 192.168.127.254	MAC Address	- 00:90:E8:94:51:29
Name	- NPort S9450I-2S-SC-HV_DZHG01945129	Serial No.	- DZHG01945129	Firmware	- V1.0 Build 16081910
Location	- Server Location				

Authentication Server

RADIUS

Server IP/Name	localhost
Server port	1812
Server shared key	(Max.15 characters)
Server timeout	5 (1 - 255 sec)

TACACS+

Server IP/Name	localhost
Server port	49
Server shared key	(Max.15 characters)
Authentication type	ASCII
Server timeout	30 (1 - 255 sec)

Radius

Setting	Description	Default
Server IP/Name	When using a RADIUS server for user authentication, enter its IP address here.	
Server port	When using a RADIUS server, enter the connected port here.	1812
Server shared key	When using a RADIUS server, enter the password here.	
Server timeout	When using a RADIUS server, enter the timeout time here for the communication packets.	5 sec.

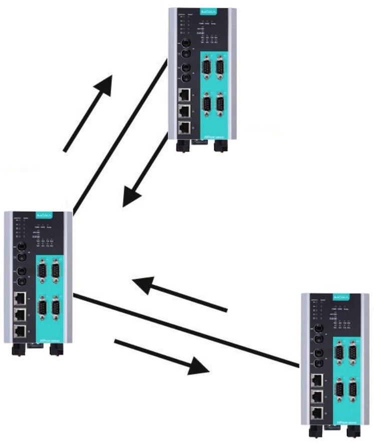
TACACS+

Setting	Description	Default
Server IP/Name	When using a TACACS+ server for user authentication, enter its IP address here.	
Server port	When using a TACACS+ server, enter the connected port here.	
Server shared key	When using a TACACS+ server, enter the password here.	
Authentication type	When using a TACACS+ server, select the authentication type here. It supports ASCII, PAP, CHAP and MSCHAP.	
Server timeout	When using a TACACS+ server, enter the timeout time here for the communication packets.	30 sec.

LLDP

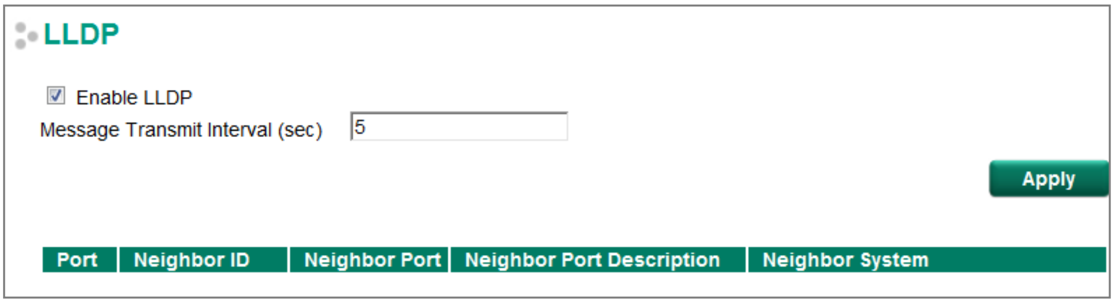
Overview

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a Moxa managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configuration, and with SNMP, this information can be transferred to Moxa's MXview for auto-topology and network visualization.



From the switch's web interface, you can enable or disable the LLDP, and set the LLDP transmit interval. In addition, you can view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows Moxa's MXview to automatically display the network's topology and system setup details, such as VLAN and Trunking, for the entire network.

Configuring LLDP Settings



LLDP

☑ Enable LLDP

Message Transmit Interval (sec) 5

Port	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System

General Settings

LLDP

Setting	Description	Factory Default
Enable or Disable	Enables or disables the LLDP function.	Enable

Message Transmit Interval

Setting	Description	Factory Default
5 to 32768 sec.	Sets the transmit interval of LLDP messages in seconds.	5 (seconds)

LLDP Table

The LLDP Table displays the following information:

Port The port number that connects to the neighbor device.

Neighbor ID A unique entity (typically the MAC address) that identifies a neighbor device.

Neighbor Port The port number of the neighbor device.

Neighbor Port Description A textual description of the neighbor device’s interface.

Neighbor System Hostname of the neighbor device.

Port Access Control

Using Port Access Control

The NPort S9000 provides two kinds of Port-Based Access Controls: one is Static Port Lock and the other is IEEE 802.1X.

Static Port Lock

The NPort S9000 can also be configured to protect static MAC addresses for a specific port. With the Port Lock function, these locked ports will not learn any additional addresses, but they only allow traffic from preset static MAC addresses, helping to block crackers and careless usage.

IEEE 802.1X

The IEEE 802.1X standard defines a protocol for client/server-based access control and authentication. The protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet, and which otherwise would be readily accessible. The purpose of the authentication server is to check each client that requests access to the port. The client is only allowed access to the port if the client’s permission is authenticated.

The IEEE 802.1X Concept

Three components are used to create an authentication mechanism based on 802.1X standards: Client/Supplicant, Authentication Server, and Authenticator.

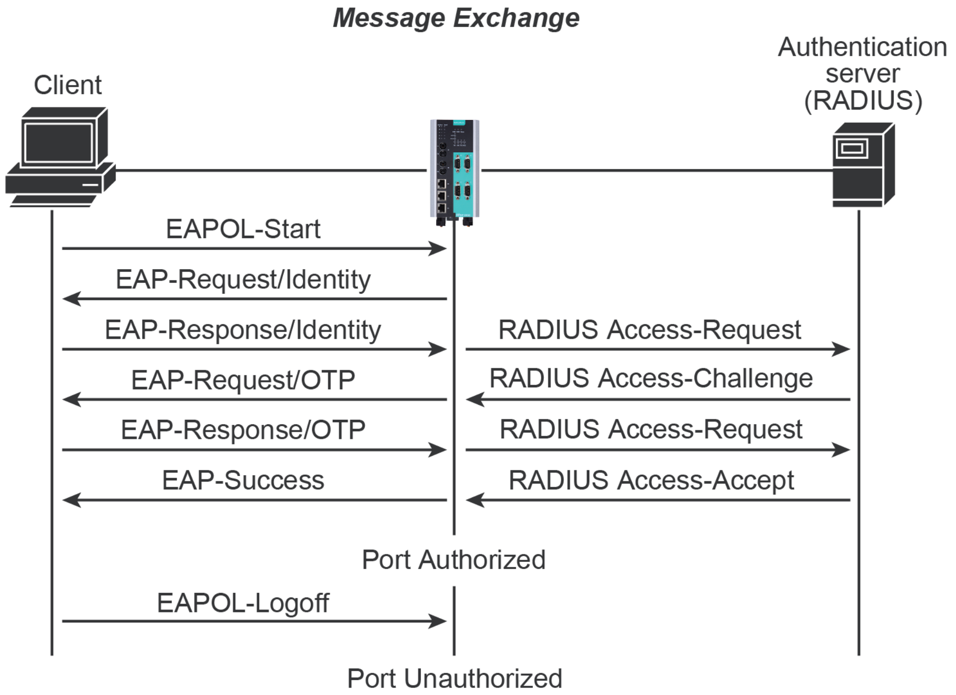
Supplicant: The end station that requests access to the LAN and switch services and responds to the requests from the switch.

Authentication server: The server that performs the actual authentication of the supplicant.

Authenticator: Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant.

The NPort S9000 acts as an authenticator in the 802.1X environment. A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server, or implement the authentication server in the NPort S9000 by using a Local User Database as the authentication look-up table. When we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames between each other.

Authentication can be initiated either by the supplicant or the authenticator. When the supplicant initiates the authentication process, it sends an "EAPOL-Start" frame to the authenticator. When the authenticator initiates the authentication process or when it receives an "EAPOL Start" frame, it sends an "EAP Request/Identity" frame to ask for the username of the supplicant. The following actions are described below:



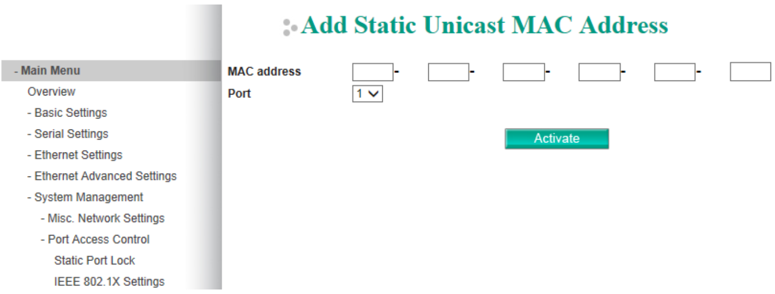
1. When the supplicant receives an "EAP Request/Identity" frame, it sends an "EAP Response/Identity" frame with its username back to the authenticator.
2. If the RADIUS server is used as the authentication server, the authenticator relays the "EAP Response/Identity" frame from the supplicant by encapsulating it into a "RADIUS Access-Request" frame and sends to the RADIUS server. When the authentication server receives the frame, it looks up its database to check if the username exists. If the username is not present, the authentication server replies with a "RADIUS Access-Reject" frame to the authenticator if the server is a RADIUS server or just indicates failure to the authenticator if the Local User Database is used. The authenticator sends an "EAP-Failure" frame to the supplicant.
3. The RADIUS server sends a "RADIUS Access-Challenge," which contains an "EAP Request" with an authentication type to the authenticator to ask for the password from the client. RFC 2284 defines several

EAP authentication types, such as "MD5-Challenge," "One-Time Password," and "Generic Token Card." Currently, only "MD5-Challenge" is supported. If the Local User Database is used, this step is skipped.

4. The authenticator sends an "EAP Request/MD5-Challenge" frame to the supplicant. If the RADIUS server is used, the "EAP Request/MD5-Challenge" frame is retrieved directly from the "RADIUS Access-Challenge" frame.
5. The supplicant responds to the "EAP Request/MD5-Challenge" by sending an "EAP Response/MD5-Challenge" frame that encapsulates the user's password using the MD5 hash algorithm.
6. If the RADIUS server is used as the authentication server, the authenticator relays the "EAP Response/MD5-Challenge" frame from the supplicant by encapsulating it into a "RADIUS Access-Request" frame along with a "Shared Secret," which must be the same within the authenticator and the RADIUS server, and sends the frame to the RADIUS server. The RADIUS server checks against the password with its database, and replies with "RADIUS Access-Accept" or "RADIUS Access-Reject" to the authenticator. If the Local User Database is used, the password is checked against its database and indicates success or failure to the authenticator.
7. The authenticator sends "EAP Success" or "EAP Failure" based on the reply from the authentication server.

Configuring Static Port Lock

The NPort S9000 supports adding unicast groups manually if required.



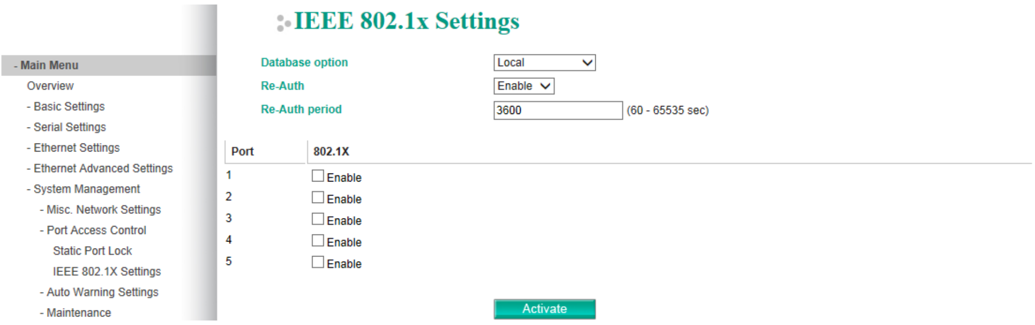
Add Static Unicast MAC Address

MAC address: [ ]-[ ]-[ ]-[ ]-[ ]-[ ]

Port: 1

Setting	Description	Factory Default
MAC Address	Add the static unicast MAC address into the address table.	None
Port	Fix the static address with a dedicated port.	1

Configuring IEEE 802.1X



IEEE 802.1x Settings

Database option: Local

Re-Auth: Enable

Re-Auth period: 3600 (60 - 65535 sec)

Port	802.1X
1	□ Enable
2	□ Enable
3	□ Enable
4	□ Enable
5	□ Enable

Database Option

Setting	Description	Factory Default
Local (Max. 32 users)	Select this option when setting the Local User Database as the authentication database.	Local
Radius	Select this option to set an external RADIUS server as the authentication database. The authentication mechanism is "EAP-MD5."	Local

Setting	Description	Factory Default
Radius, Local	Select this option to make an external RADIUS server as the authentication database with first priority. The authentication mechanism is "EAP-MD5." The second priority is to set the Local User Database as the authentication database.	Local

Re-Auth

Setting	Description	Factory Default
Enable/Disable	Select to require reauthentication of the client after a preset time period of no activity has elapsed.	Disable

Re-Auth Period

Setting	Description	Factory Default
Numerical (60-65535 sec.)	Specify how frequently the end stations need to reenter usernames and passwords in order to stay connected.	3600

802.1X

Setting	Description	Factory Default
Enable/Disable	Select the option under the 802.1X column to enable IEEE 802.1X for one or more ports. All end stations must enter usernames and passwords before access to these ports is allowed.	Disable

Auto Warning Settings

Using Auto Warning

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet switch that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The NPort S9000 supports different approaches to warn engineers automatically, such as by using email and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms using email and relay output.

On the Event Settings page, you may configure how administrators are notified of certain system, network, and configuration events. Depending on the event, different options for automatic notification are available, as shown above. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending an SNMP Trap.

Configuring E-Mail Alert

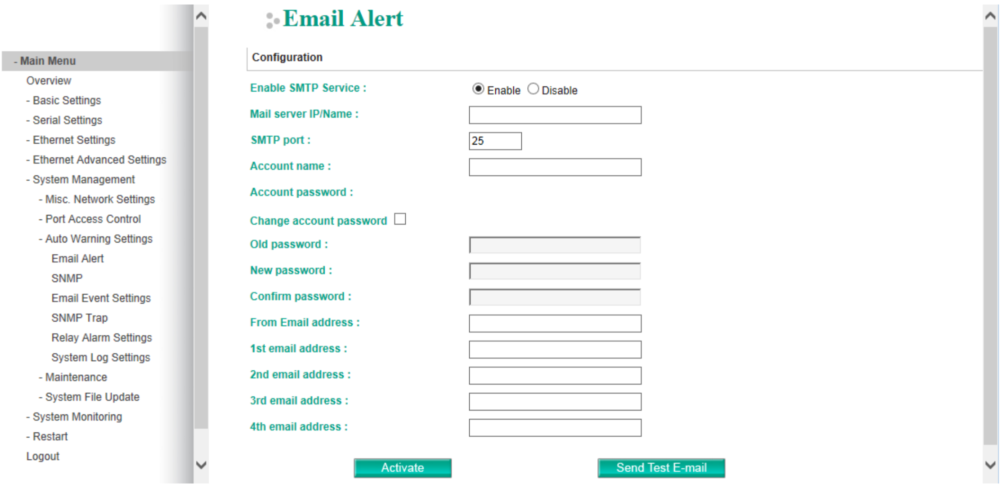
The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place.

Three basic steps are required to set up the Auto Warning function:

1. **Configuring Email Event Types**
   Select the desired Event types from the Console or Web Browser Event type page (a description of each event type is given later in the Email Alarm Events setting subsection).
2. **Configuring Email Settings**
   To configure the NPort S9000's email setup from the Console interface or browser interface, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address to which warning messages will be sent.

3. **Activate your settings and if necessary, test the email**

   After configuring and activating your NPort S9000's Event Types and Email Setup, you can use the Test Email function to see if your e-mail addresses and mail server address have been properly configured.



Email Alert

Configuration

Enable SMTP Service : ● Enable ○ Disable

Mail server IP/Name :

SMTP port : 25

Account name :

Account password :

Change account password □

Old password :

New password :

Confirm password :

From Email address :

1st email address :

2nd email address :

3rd email address :

4th email address :

Mail Server IP/Name

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

Account Name

Setting	Description	Factory Default
Max. 45 Characters	Your email account name (typically your user name)	None

Account Password

Setting	Description	Factory Default
Disable/Enable to change Password	To reset the password from the Web Browser interface, click the Change password checkbox, type the old password, type the new password, retype the new password, and then click Activate; Max. 45 Characters.	Disable
Old Password	Type the current password when changing the password	None
New Password	Type the new password when enabled to change password; Max. 45 Characters.	None
Confirm Password	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	None

Email Address

Setting	Description	Factory Default
Max. 30 characters	You can set up to 4 email addresses to receive alarm emails from the NPort S9000.	None

Send Test Email

After configuring the email settings, you should first click ***Activate*** to activate those settings, and then click ***Send Test Email*** to verify that the settings are correct.

NOTE Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PLAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism.

We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.

Configuring SNMP

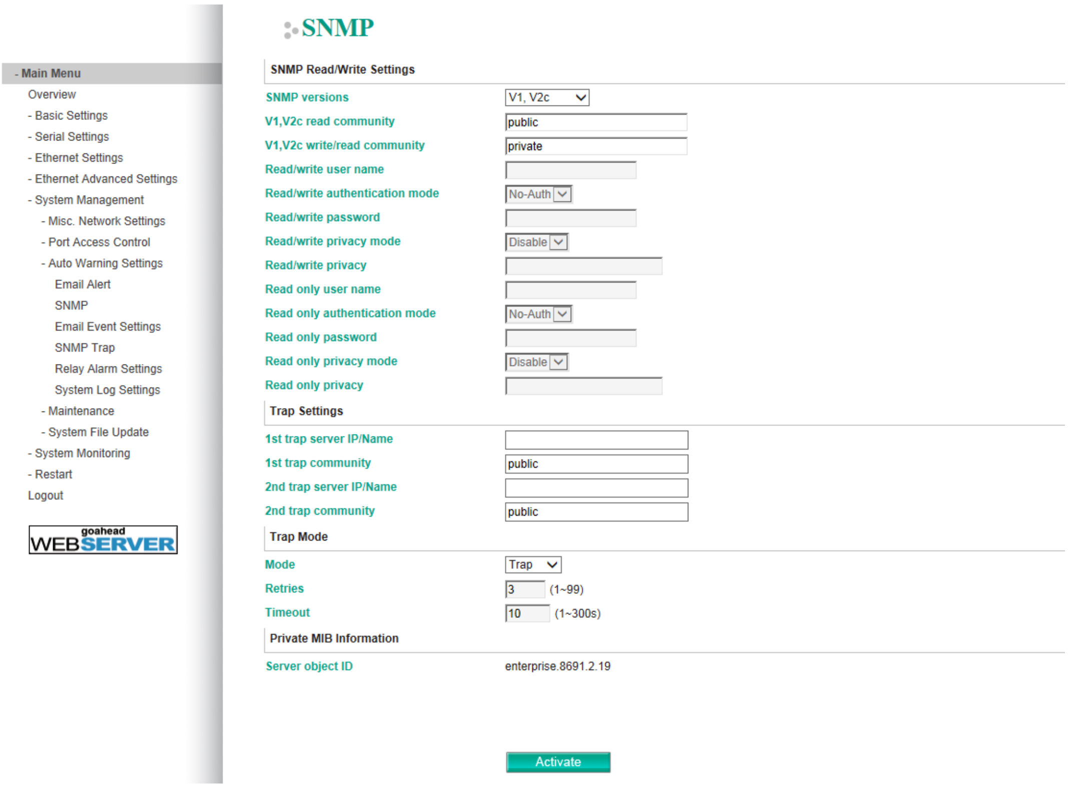
The NPort S9000 supports SNMP V1/V2c/V3. SNMP V1, and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions, using the community string *public/private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

SNMP security modes and security levels supported by the NPort S9000 are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	**UI Setting**	**Authentication Type**	**Data Encryption**	**Method**
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

These parameters are configured on the SNMP page. A more detailed explanation of each parameter follows.

SNMP Read/Write Settings



SNMP

SNMP Read/Write Settings

SNMP versions	V1, V2c
V1,V2c read community	public
V1,V2c write/read community	private
Read/write user name	
Read/write authentication mode	No-Auth
Read/write password	
Read/write privacy mode	Disable
Read/write privacy	
Read only user name	
Read only authentication mode	No-Auth
Read only password	
Read only privacy mode	Disable
Read only privacy	

Trap Settings

1st trap server IP/Name	
1st trap community	public
2nd trap server IP/Name	
2nd trap community	public

Trap Mode

Mode	Trap
Retries	3 (1~99)
Timeout	10 (1~300s)

Private MIB Information

Server object ID	enterprise.8691.2.19

SNMP agent version: The NPort S9000 supports SNMP V1, V2c, and V3.

V1, V2c Read community (default=public): This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.

V1, V2c Write/Read community (default=private): This is a text password mechanism that is used to weakly authenticate changes to agents of managed network devices.

Read/write User name: Use this optional field to identify the username for the specified level of access.

Read/write Authentication mode (default=No-Auth): Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication

Read/write Password: Use this field to set the password for the specified level of access.

Read/write Privacy mode (default=Disable): Use this field to enable and disable DES data encryption for the specified level of access.

Read/write Privacy: Use this field to define the encryption key for the specified level of access.

Read only: Read-only authentication mode allows you to configure the authentication mode for read/write access. For each level of access, you may configure the following:

Read/only User name: Use this optional field to identify the user name for the specified level of access.

Read/only Authentication mode (default=No-Auth): Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication.

Read/only Password: Use this field to set the password for the specified level of access.

Read/only Privacy mode (default=Disable): Use this field to enable and disable DES data encryption for the specified level of access.

Read/only Privacy: Use this field to define the encryption key for the specified level of access.

1st Trap Server IP/Name: Enter the IP address or the name of the first Trap Server used by your network.

1st Trap Community: Use a community string match for authentication (maximum of 30 characters).

2nd Trap Server IP/Name: Enter the IP address or the name of the second Trap Server used by your network.

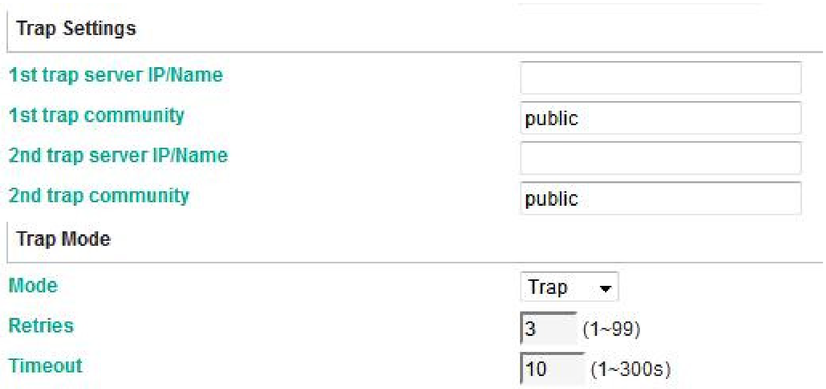
2nd Trap Community: Use a community string match for authentication (maximum of 30 characters).

Trap Settings

SNMP traps allow an SNMP agent to notify the NMS of a significant event. The switch supports two SNMP modes: **Trap** and Inform.

SNMP Trap Mode—Trap

In Trap mode, the SNMP agent sends an SNMPv1 trap PDU to the NMS. No acknowledgment is sent back from the NMS so the agent has no way of knowing if the trap reached the NMS.



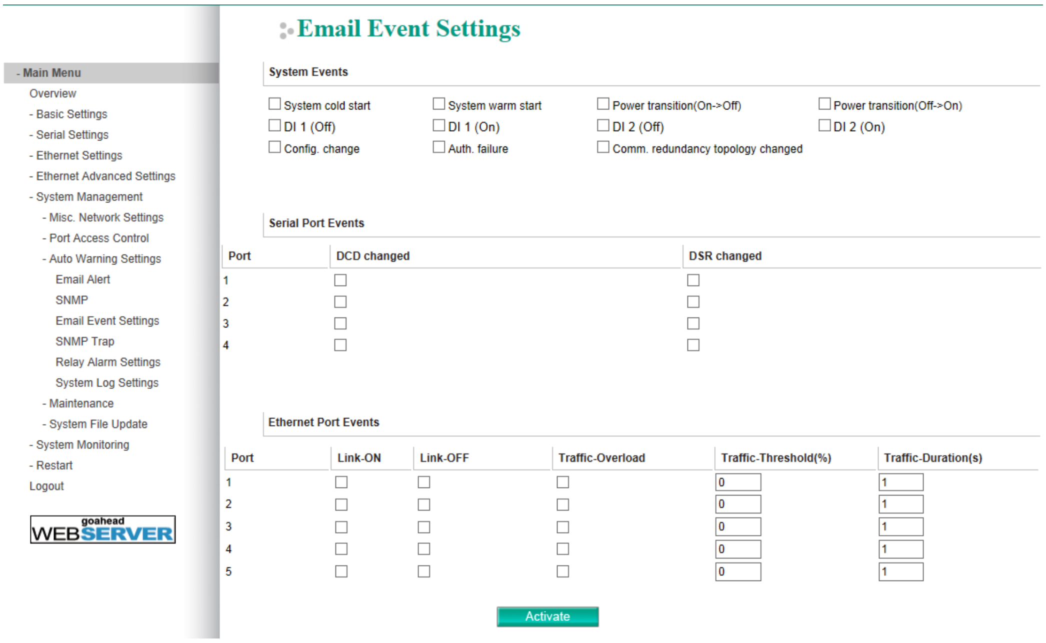
Trap Settings	
1st trap server IP/Name	
1st trap community	public
2nd trap server IP/Name	
2nd trap community	public
Trap Mode	
Mode	Trap
Retries	3 (1~99)
Timeout	10 (1~300s)

SNMP Trap Mode—Inform

SNMPv2 provides an inform mechanism. When an inform message is sent from the SNMP agent to the NMS, the receiver sends a response to the sender acknowledging receipt of the event. This behavior is similar to that of the get and set requests. If the SNMP agent does not receive a response from the NMS for a period of time, the agent will resend the trap to the NMS agent. The maximum timeout time is 300 sec (default is 1 sec), and the maximum number of retries is 99 times (default is 1 time). When the SNMP agent receives acknowledgement from the NMS, it will stop resending the inform messages.

E-mail Event Settings

Event Types can be divided into three basic groups: **System Events, Serial Port Events** and **Ethernet Port Events**.



Email Event Settings

System Events

□ System cold start □ System warm start □ Power transition(On->Off) □ Power transition(Off->On)
□ DI 1 (Off) □ DI 1 (On) □ DI 2 (Off) □ DI 2 (On)
□ Config. change □ Auth. failure □ Comm. redundancy topology changed

Serial Port Events

Port	DCD changed	DSR changed
1	□	□
2	□	□
3	□	□
4	□	□

Ethernet Port Events

Port	Link-ON	Link-OFF	Traffic-Overload	Traffic-Threshold(%)	Traffic-Duration(s)
1	□	□	□	0	1
2	□	□	□	0	1
3	□	□	□	0	1
4	□	□	□	0	1
5	□	□	□	0	1

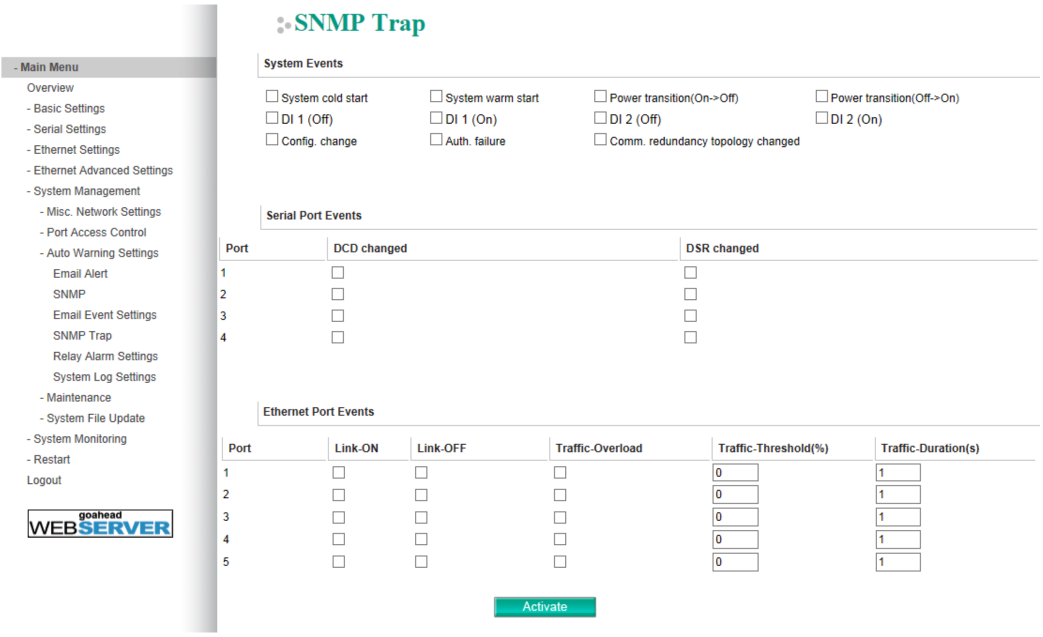
System Events	Warning e-mail is sent when...
System Cold Start	Power is cut off and then reconnected.
System Warm Start	The NPort S9000 is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	The NPort S9000 is powered down.
Power Transition (Off→On)	The NPort S9000 is powered up.
DI1 (On→Off)	Digital Input 1 is triggered by on to off transition
DI1 (Off→On)	Digital Input 1 is triggered by off to on transition
DI2 (On→Off)	Digital Input 2 is triggered by on to off transition
DI2 (Off→On)	Digital Input 2 is triggered by off to on transition
Configuration Change Activated	A configuration item has been changed.
Authentication Failure	An incorrect password is entered.
Comm. Redundancy Topology Changed	Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). The Master of the Turbo Ring has changed or the backup path is activated.

Serial Port Events	Warning e-mail is sent when...
DCD changed	A change in the DCD (Data Carrier Detect) signal indicates that the modem connection status has changed. For example, if the DCD signal changes to low, it indicates that the connection line is down. When the DCD signal changes to low, the NPort S9000 will automatically send a warning to the administrator as configured on the Serial Event Settings page.
DSR changed	A change in the DSR (Data Set Ready) signal indicates that the data communication equipment is powered off. For example, if the DSR signal changes to low, it indicates that the data communication equipment is powered down. When the DSR signal changes to low, the NPort S9000 will automatically send a warning to the administrator as configured on the Serial Event Settings page.

Ethernet Port Events	Warning e-mail is sent when…
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a non-zero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.

NOTE The default "Warning e-mail message" is empty in the sender field. It is recommended to set a message to help you to recognize the Warning e-mail message.

SNMP Trap



SNMP Trap

System Events

□ System cold start □ System warm start □ Power transition(On->Off) □ Power transition(Off->On)
□ DI 1 (Off) □ DI 1 (On) □ DI 2 (Off) □ DI 2 (On)
□ Config. change □ Auth. failure □ Comm. redundancy topology changed

Serial Port Events

Port	DCD changed	DSR changed
1	□	□
2	□	□
3	□	□
4	□	□

Ethernet Port Events

Port	Link-ON	Link-OFF	Traffic-Overload	Traffic-Threshold(%)	Traffic-Duration(s)
1	□	□	□	0	1
2	□	□	□	0	1
3	□	□	□	0	1
4	□	□	□	0	1
5	□	□	□	0	1

System Events	Warning e-mail is sent when…
System Cold Start	Power is cut off and then reconnected.
System Warm Start	The NPort S9000 is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	The NPort S9000 is powered down.
Power Transition (Off→On)	The NPort S9000 is powered up.
DI1 (On→Off)	Digital Input 1 is triggered by on to off transition
DI1 (Off→On)	Digital Input 1 is triggered by off to on transition
DI2 (On→Off)	Digital Input 2 is triggered by on to off transition
DI2 (Off→On)	Digital Input 2 is triggered by off to on transition
Configuration Change Activated	A configuration item has been changed.
Authentication Failure	An incorrect password has been entered.
Comm. Redundancy Topology Changed	Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). The Master of the Turbo Ring has changed or the backup path is activated.

Serial Port Events	Warning e-mail is sent when…
DCD changed	A change in the DCD (Data Carrier Detect) signal indicates that the modem connection status has changed. For example, if the DCD signal changes to low, it indicates that the connection line is down. When the DCD signal changes to low, the NPort S9000 will automatically send a warning to the administrator as configured on the Serial Event Settings page.
DSR changed	A change in the DSR (Data Set Ready) signal indicates that the data communication equipment is powered off. For example, if the DSR signal changes to low, it indicates that the data communication equipment is powered down. When the DSR signal changes to low, the NPort S9000 will automatically send a warning to the administrator as configured on the Serial Event Settings page.

Ethernet Port Events	Warning e-mail is sent when…
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port’s traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a non-zero number if the port’s Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.

NOTE The default “Warning e-mail message” is empty in the sender field. It is recommended to set a message to help you to recognize the Warning e-mail message.

Relay Alarm Settings

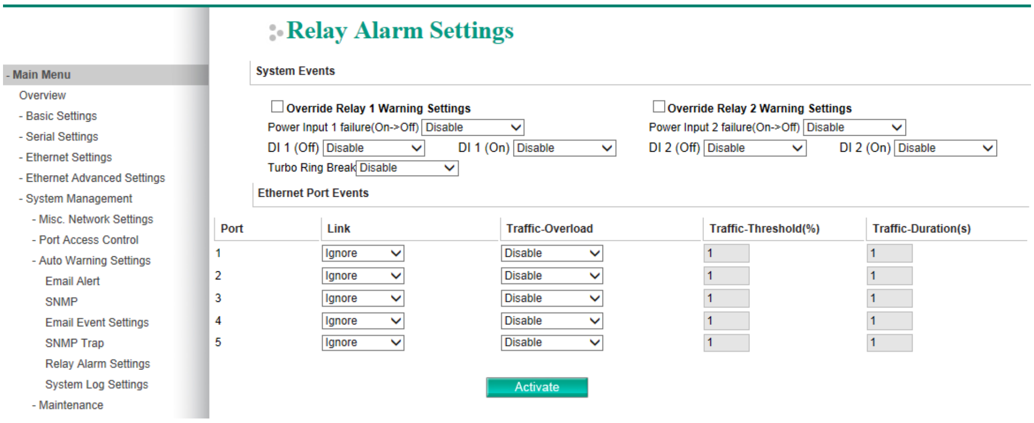
Configuring Relay Warning

The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

1. **Configuring Relay Event Types**
   Select the desired Event types from the Console or Web Browser Event type page (a description of each event type is given later in the Relay Alarm Events setting subsection).

2. **Activate your settings**

   After completing the configuration procedure, you will need to activate your NPort S9000's Relay Event Types.



Relay Alarm Settings

System Events

□ Override Relay 1 Warning Settings

Power Input 1 failure(On->Off) Disable

DI 1 (Off) Disable DI 1 (On) Disable

Turbo Ring Break Disable

□ Override Relay 2 Warning Settings

Power Input 2 failure(On->Off) Disable

DI 2 (Off) Disable DI 2 (On) Disable

Ethernet Port Events

Port	Link	Traffic-Overload	Traffic-Threshold(%)	Traffic-Duration(s)
1	Ignore	Disable	1	1
2	Ignore	Disable	1	1
3	Ignore	Disable	1	1
4	Ignore	Disable	1	1
5	Ignore	Disable	1	1

Event Types can be divided into two basic groups: **System Events** and **Ethernet Port Events**. System Events are related to the overall function of the NPort S9000, whereas Ethernet Port Events are related to the activity of a specific port.

The NPort S9000 supports two relay outputs. You can configure which relay output is related to which events. This helps administrators identify the importance of the different events.

Override relay alarm settings

Select this option to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition.

System Events	**Factory Default**
Override relay 1 Warning settings	Non-check
Override relay 2 Warning settings	Non-check

System Events	**Warning Relay output is triggered when…**	
Power Input 1 failure (On→Off)	Disable	Default
	Relay 1	Relay 1 is triggered by on to off transition
	Relay 2	Relay 2 is triggered by on to off transition
Power Input 2 failure (On→Off)	Disable	Default
	Relay 1	Relay 1 is triggered by on to off transition
	Relay 2	Relay 2 is triggered by on to off transition
DI1 (On→Off)	Disable	Default
	Relay 1	Digital Input 1 is triggered by on to off transition and enable Relay 1
	Relay 2	Digital Input 1 is triggered by on to off transition and enable Relay 2.
DI1 (Off→On)	Disable	Default
	Relay 1	Digital Input 1 is triggered by off to on transition and enable Relay 1
	Relay 2	Digital Input 1 is triggered by off to on transition and enable Relay 2.
DI2 (On→Off)	Disable	Default
	Relay 1	Digital Input 2 is triggered by on to off transition and enable Relay 1

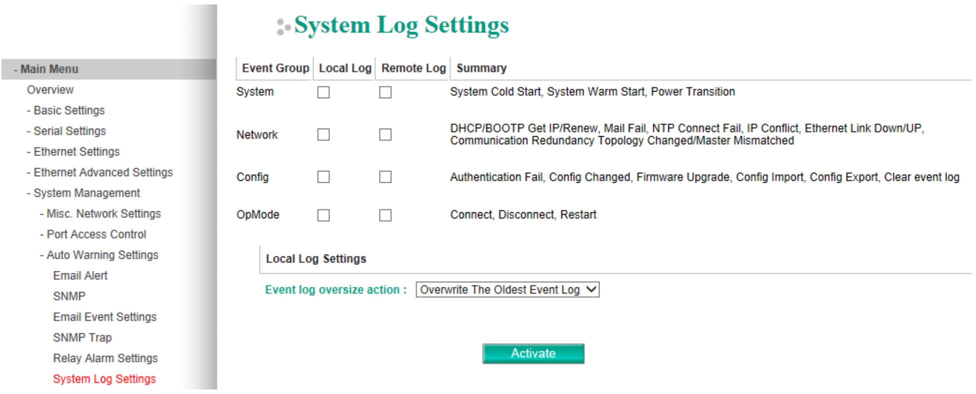
System Events	Warning Relay output is triggered when…	
	Relay 2	Digital Input 2 is triggered by on to off transition and enable Relay 2.
DI2 (Off→On)	Disable	Default
	Relay 1	Digital Input 2 is triggered by off to on transition and enable Relay 1
	Relay 2	Digital Input 2 is triggered by off to on transition and enable Relay 2.

Port Events	Warning Relay output is triggered when…
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port’s traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a non-zero number if the port’s Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.

NOTE The **Traffic-Overload, Traffic-Threshold (%)**, and **Traffic-Duration (sec)** Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a non-zero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

System Log Settings

System Log Settings allow the administrator to customize which network events are logged by the NPort S9000. Events are grouped into four categories, known as event groups, and the administrator selects which groups to log under Local Log. The actual system events that would be logged for each system group are listed under summary. For example, if **System** was enabled, then System Cold Start events and System Warm Start events would be logged.



System Log Settings

Event Group	Local Log	Remote Log	Summary
System	□	□	System Cold Start, System Warm Start, Power Transition
Network	□	□	DHCP/BOOTP Get IP/Renew, Mail Fail, NTP Connect Fail, IP Conflict, Ethernet Link Down/UP, Communication Redundancy Topology Changed/Master Mismatched
Config	□	□	Authentication Fail, Config Changed, Firmware Upgrade, Config Import, Config Export, Clear event log
OpMode	□	□	Connect, Disconnect, Restart

Local Log Settings

Event log oversize action : Overwrite The Oldest Event Log

Local Log Settings

When the local logs reaches 1,000 items, you may select **Overwrite The Oldest Event Log** or **Stop Recording Event Log** for the device server to handle the new event.

Local Log	Keep the log in to the flash of NPort S9000 up to 1000 items.
Remote Log	Keep the log in to the remote defined Log Server. You will need to assign a remote Log Server in the System Management / Misc. Network Settings / Remote Log Settings if remote log is checked.

System

System Cold Start	NPort S9000 cold start.
System Warm Start	NPort S9000 warm start.
Power Transition	The NPort S9000 is powered up or down.
DI On/Off	Digital Input 1 is triggered

Network

DHCP/BOOTP/Get IP/Renew	IP of the NPort S9000 is refreshed.
Mail Fail	Failed to deliver the E-mail.
NTP Connect Fail	The NPort S9455I-MM-SC failed to connect to the NTP Server.
IP Conflict	There is an IP conflict on the local network.
Network Link Down/UP	LAN 1 Link is down.
Communication Redundancy Topology Changed/Master Mismatched	When the status of Ring is changed or Master device is mismatched

Config

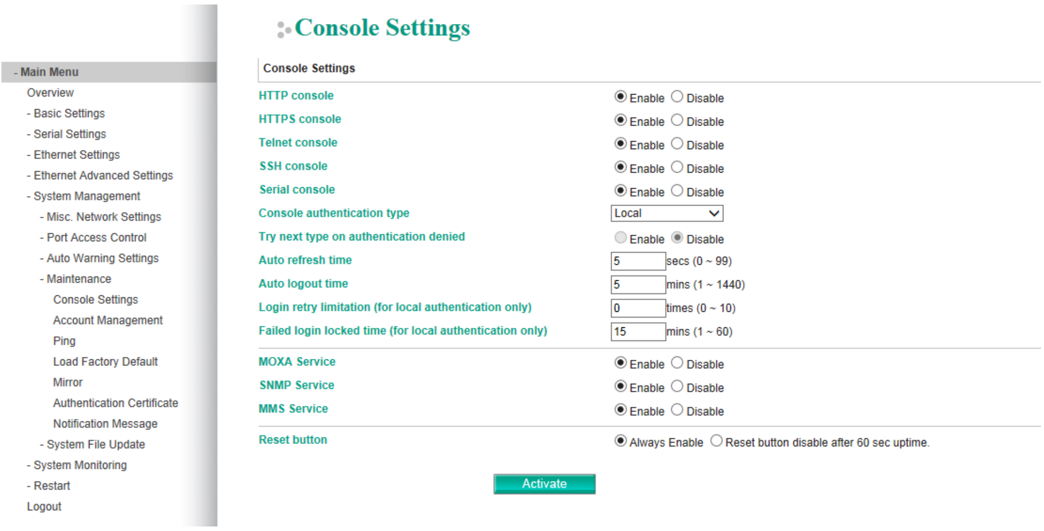
Authentication Success	
Authentication Fail	
IP Changed	Static IP address was changed.
Config Changed	The NPort S9000’s configuration was changed.
Firmware Upgrade	Firmware was upgraded.
Firmware Upgrade Failed	
Config Import	Config was imported.
Config Import Failed	Configuration file import failed by which user
Config Export	Config was exported.
Over the threshold of event log storage capacity	The event logs has been recorded over 1,000 items
Clear Log	It will record which user clear all the event logs

OpMode

Connect	Op Mode is In Use
Disconnect	Op Mode switched from In Use to Disconnect.
Restart	Serial port was restarted.

Maintenance

Console Settings



Console Settings

Console Settings	
HTTP console	● Enable ○ Disable
HTTPS console	● Enable ○ Disable
Telnet console	● Enable ○ Disable
SSH console	● Enable ○ Disable
Serial console	● Enable ○ Disable
Console authentication type	Local
Try next type on authentication denied	○ Enable ● Disable
Auto refresh time	5 secs (0 ~ 99)
Auto logout time	5 mins (1 ~ 1440)
Login retry limitation (for local authentication only)	0 times (0 ~ 10)
Failed login locked time (for local authentication only)	15 mins (1 ~ 60)
MOXA Service	● Enable ○ Disable
SNMP Service	● Enable ○ Disable
MMS Service	● Enable ○ Disable
Reset button	● Always Enable ○ Reset button disable after 60 sec uptime.

Config

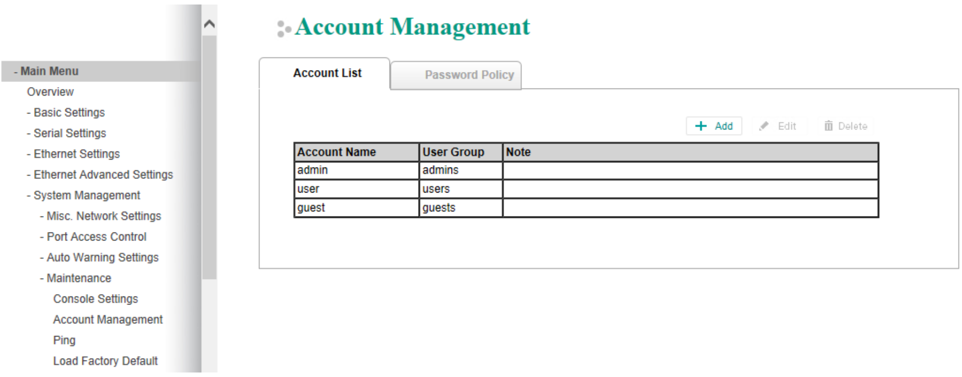
HTTP console	HTTP console enable/disable
HTTPS console	HTTPS console enable/disable
Telnet console	Telnet console enable/disable
SSH console	SSH console enable/disable
Serial console	Serial console enable/disable
Console authentication type	Set the console authentication type in the dropdown menu. NPort S9000 series supports, Local, RADIUS, RADIUS - Local, Local - RADIUS, TACACS+, TACACS+ - Local, and Local - TACACS+.
Try next type if authentication is denied	If a user selects more than one authentication server types, (RADIUS - Local, Local - RADIUS, TACACS+ - Local, Local - TACACS+), the NPort S9000 series will make attempts on the second authentication server if the first authentication server gets denied
Auto refresh time	Monitor page will auto refresh by this setting, default time is 5 seconds.
Auto logout time	The device server will enforce a user to logout without any movement by this setting, default is 5 minutes.
Login retry limitation (for local authentication only)	When a user login failed, the default is 0, which means users have unlimited retries.
Failed login locked time (for local authentication only)	When a user has failed to log in to the device server and reached the limitation set by the Login retry limitation setting, then the default time for blocking users is 15 minutes before they can retry again.
Moxa Service	Moxa service enable/disable, if you disable it, the Device Search Utility and NPort Windows Driver Manager will not work with this device server.
SNMP Service	SNMP Service enable/disable
MMS Service	MMS service enable/disable.
Reset button	Always Enable
	Reset button disable after 60 sec uptime
Auto refresh time	Monitor page refresh time

Account Management

Account management setting provides administrators the authority to add/delete/modify a user account, grant access to the device users for specified function groups, and manages password and login policy to ensure the device is used by an authorized set of people.

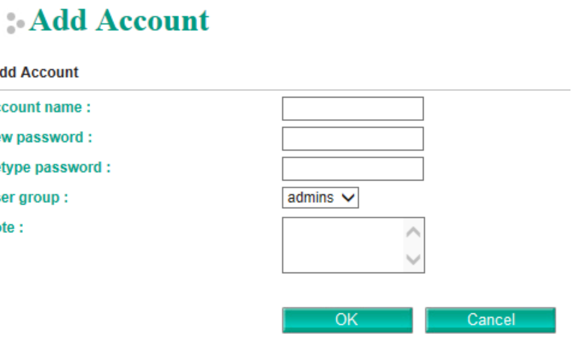
Account List

The Administrator is allowed to add user accounts to the device server by clicking the **Add** button on the **Account List** tab. You may also click the current user to Edit/Delete the selected account. There must be at least one account name in the User Group "admins". To have a secure user management, you may create a specific account name in admins, for example, John, then you can delete the default "admin" account in the admins group.



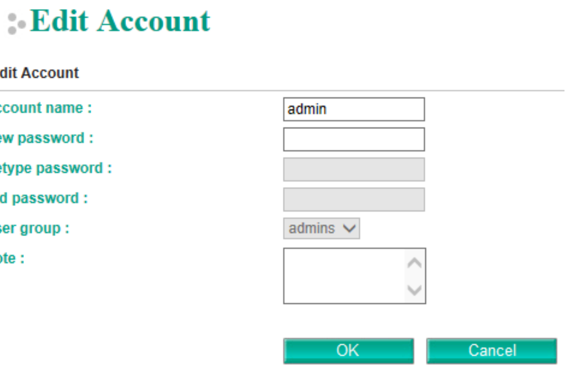
Account Name	User Group	Note
admin	admins	
user	users	
guest	guests	

The Add Account (Edit Account) page will show up for you to enter (modify) account information and assign a password to this user. Also, the Administrator(s) are allowed to assign a proper User Group to this user to limit his/her privileges of using the device server.



Add Account

Account name :	
New password :	
Retype password :	
User group :	admins
Note :	



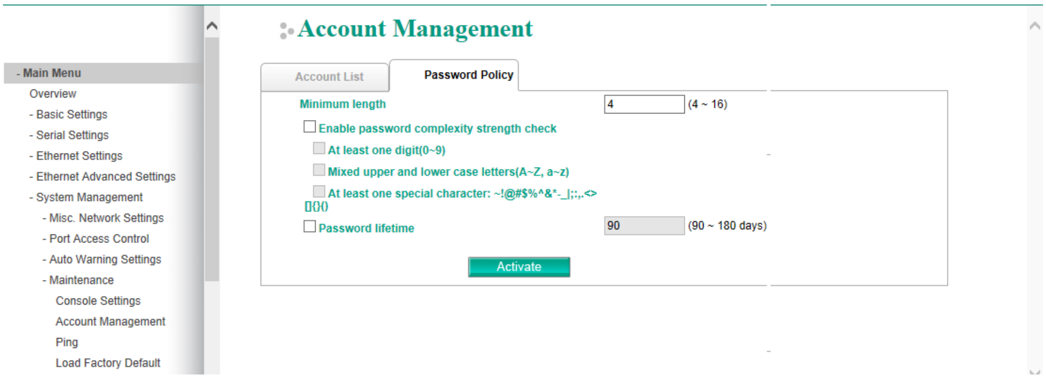
Edit Account

Account name :	admin
New password :	
Retype password :	
Old password :	
User group :	admins
Note :	

The privileges of different User Groups are defined as below:

User Group	Web/Telnet/Serial Console	Ethernet port authority for 802.1x authentication
Admin	User can modify all settings	Allow
User	User can view status via System monitoring page, and reset alarm/statistics	Allow
Guest	User can't change/view settings	Allow

Password Policy



Account Management

Minimum length 4 (4 ~ 16)

□ Enable password complexity strength check

□ At least one digit(0~9)

□ Mixed upper and lower case letters(A~Z, a~z)

□ At least one special character: ~!@#$%^&*-_|;:,.<> []{}()

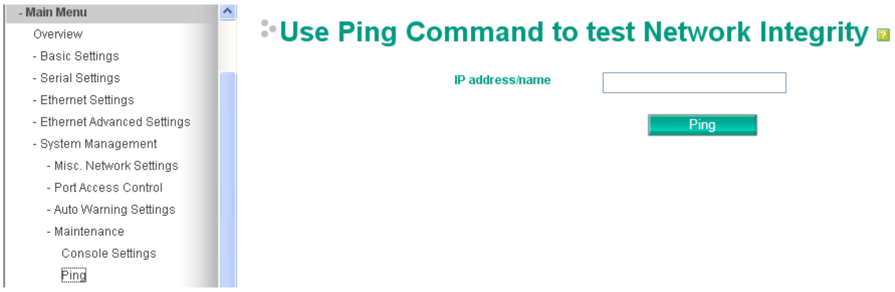
□ Password lifetime 90 (90 ~ 180 days)

Parameter	Setting	Default	Description
Password minimum length	4-16 characters	4	Define the minimum length of login password for NPort 9000
Password complexity strength check:	Enable/Disable	Disable	Enable password complexity strength check will enforce the password combination setting
• At least one digit (0-9)	Enable/Disable	Disable	The password must contain at least one number (0-9) when enabling this parameter
• Mixed upper and lower case letters (A~Z, a~z)	Enable/Disable	Disable	The password must contain an upper and a lower case letter when enabling this parameter
• At least one special characters (~!@#$%^&*-_|;:,.<>[]{}())	Enable/Disable	Disable	The password must contain at least one special character when enabling this parameter
Password Lifetime	0-180 days (0 for disable)	90 days	A password lifetime can be specified and a system notification message will show up to remind users to change the password if the option is enabled.

Ping

The **Ping** function uses the *ping* command to give users a simple but powerful tool for troubleshooting network problems. The function’s most unique feature is that even though the ping command is entered from the user’s PC keyboard, the actual ping command originates from NPort S9000 itself. In this way, the user can essentially control the NPort S9000 and send ping commands out through its ports.

To use the Ping function, type in the desired IP address, and then press **Enter** from the Console utility, or click **Ping** when using the Web Browser interface.



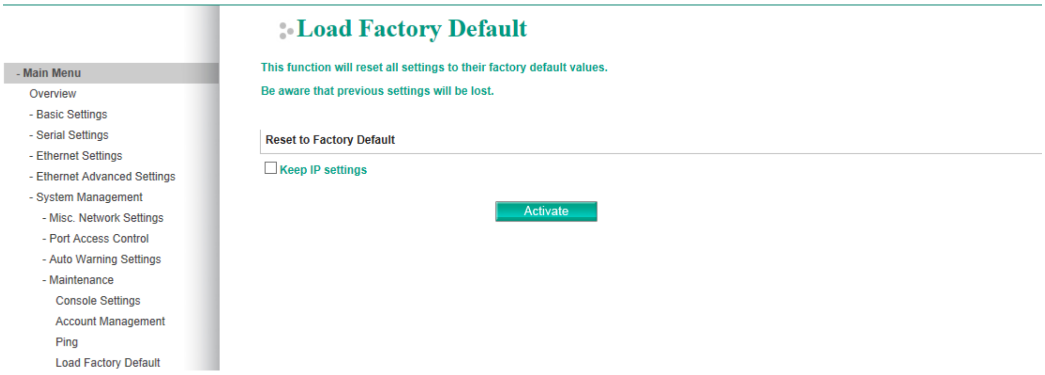
Use Ping Command to test Network Integrity

IP address/name

Load Factory Default

This function will reset all of the NPort S9000's settings to the factory default values. All previous settings including the console password will be lost. If you wish to keep the NPort S9000 IP address, netmask, and other IP settings, make sure **Keep IP settings** is checked off before loading the factory defaults.

The Factory Default function is included to give users a quick way of restoring the NPort S9000's configuration settings to their factory default values. This function is available in the Console utility (serial or Telnet), and Web Browser interface.



Load Factory Default

This function will reset all settings to their factory default values.

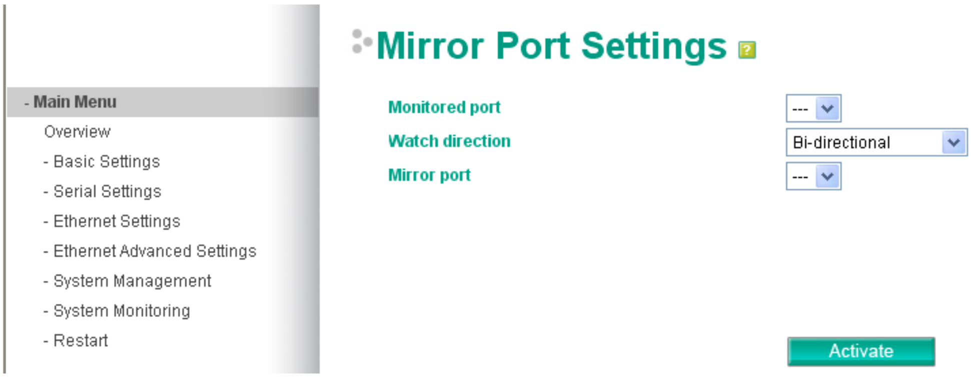
Be aware that previous settings will be lost.

Reset to Factory Default

☐ Keep IP settings

NOTE After activating the Factory Default function, you will need to use the default network settings to re-establish a web-browser or Telnet connection with your NPort S9000.

Mirror



Mirror Port Settings

Monitored port	---
Watch direction	Bi-directional
Mirror port	---

The **Mirror port** function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. This allows the network administrator to "sniff" the observed port and thus keep tabs on network activity.

Perform the following steps to set up the **Mirror Port** function:

1. Configure the NPort 9000's Mirror Port function from either the Console utility or Web Browser interface. You will need to configure three settings:

   Monitored Port Select the port number of the port whose network activity will be monitored.

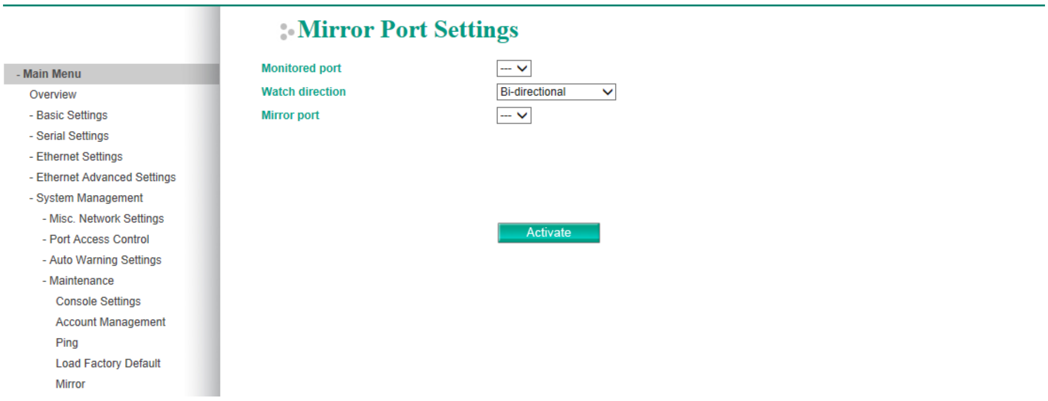
   Mirror Port Select the port number of the port that will be used to monitor the activity of the monitored port.

   Watch Direction Select one of the following three watch direction options:

   - **Input data stream**
     Select this option to monitor only those data packets coming *in through* the NPort 9000's port.
   - **Output data stream**
     Select this option to monitor only those data packets being sent *out through* the NPort 9000's port.
   - **Bi-directional**
     Select this option to monitor data packets both coming *into*, and being sent *out through*, the NPort 9000's port.

2. Be sure to activate your settings before exiting.
   - When using the Web Browser interface, activate by clicking **Activate**.
   - When using the Console utility, activate by first highlighting the Activate menu option, and then press Enter. You should receive the **Mirror port settings are now active! (Press any key to continue)** message.

Authentication Certificate



Mirror Port Settings

Monitored port: ---

Watch direction: Bi-directional

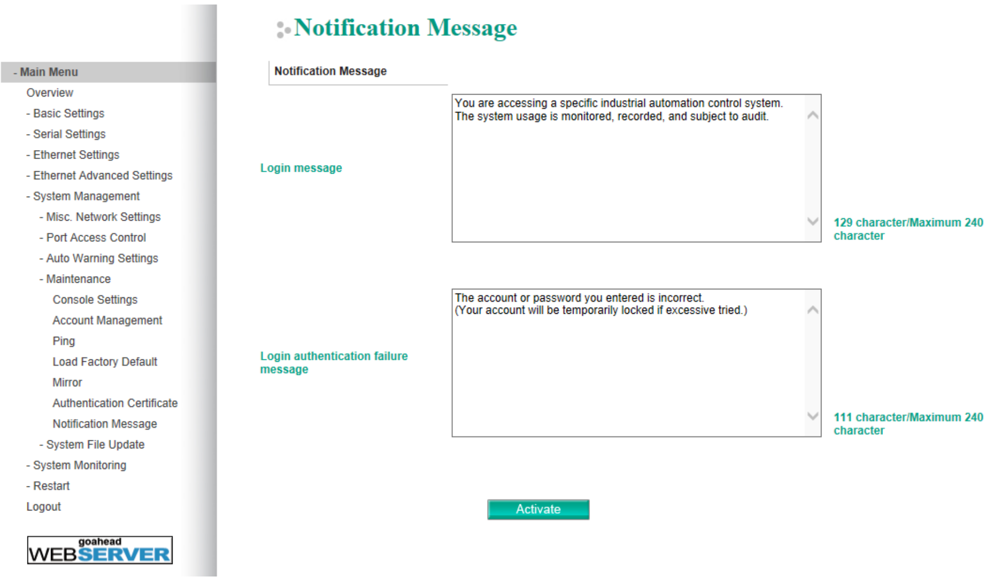
Mirror port: ---

For a secure network communication, you can set the relative settings in this page.

Setting	Description
CA Name	The CA Name of the SSL certificate. The device server will use a certificate generated by itself, so the default CA Name is Moxa Inc.
Expire Date	When the SSL certificate will be expired.
Select SSL certificate file	The browser will check if the device server is the one you're going to connect by the SSL certificate, so you may use this function to import a third party's certificate for verifying it.
Re-generate SSL Certificate	If you want the device server to generate a new SSL certificate, for example, when the old one is expired, you may use this function.
Re-generate SSH Key	When trying to establish a secure connection, for example HTTPS or SSH, the SSH Key is using to encrypt the data between the host and the device server. You may use this function to re-generate it.

Notification Message

As an administrator, you are allowed to customize your **Login Message** and the **Login Authentication Failure Message** to notify users with information you would like to provide.



Notification Message

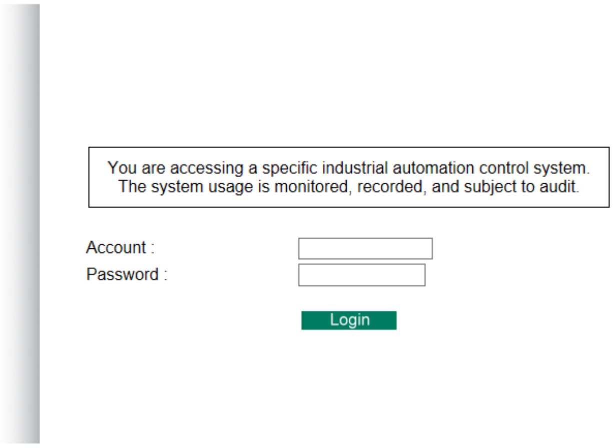
Login message: You are accessing a specific industrial automation control system. The system usage is monitored, recorded, and subject to audit.

129 character/Maximum 240 character

Login authentication failure message: The account or password you entered is incorrect. (Your account will be temporarily locked if excessive tried.)

111 character/Maximum 240 character

The message will appear when a user opens the log in to page of the device server.



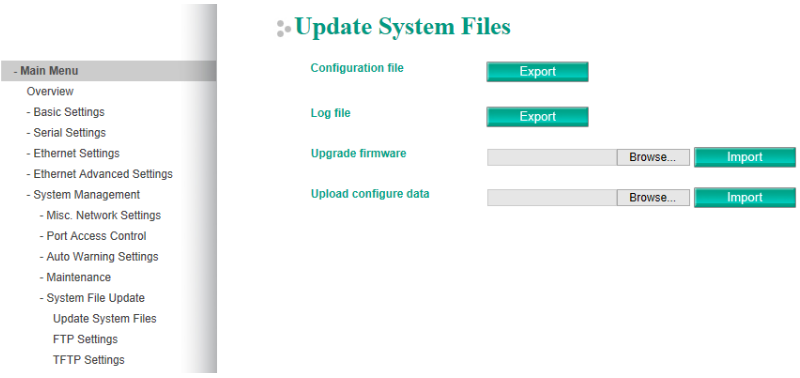
You are accessing a specific industrial automation control system.
The system usage is monitored, recorded, and subject to audit.

System File Update

The NPort S9000 can share or back up its configuration by exporting all settings to a file, which can then be imported into another NPort S9000.

To import a configuration, go to **System Management → System File Update --> System File Update**. Enter the configuration file path/name and click **Import**. The NPort S9000’s configuration settings will be updated according to the configuration file.

To export a configuration, go to **System Management → Maintenance → System File Update --> System File Update** and click **Export**. A standard download window will appear, and you will be able to download the configuration into a file name and location of your choice.



Configuration File

To export the configuration file of this NPort S9000, click **Export** to save it to the local host.

Log File

To export the Log file of this NPort S9000, click **Export** and save it to the local host.

NOTE Some operating systems will open the configuration file and log file directly in the web page. In such cases, right-click **Export** to save as a file.

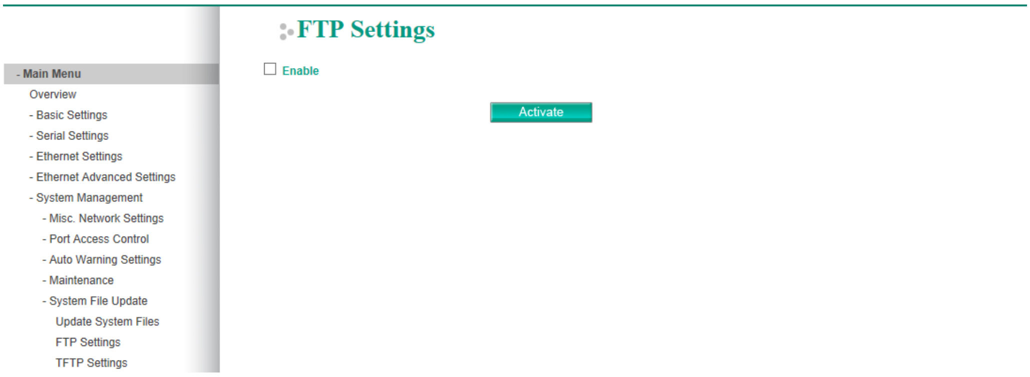
Upgrade Firmware

To import the firmware file of this NPort S9000, click **Browse** to select the firmware file already saved on your computer. The upgrade procedure will proceed automatically after clicking **Import**.

Upload Configuration Data

To import the configuration file of this NPort S9000, click **Browse** to select the configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking **Import**.

FTP Settings

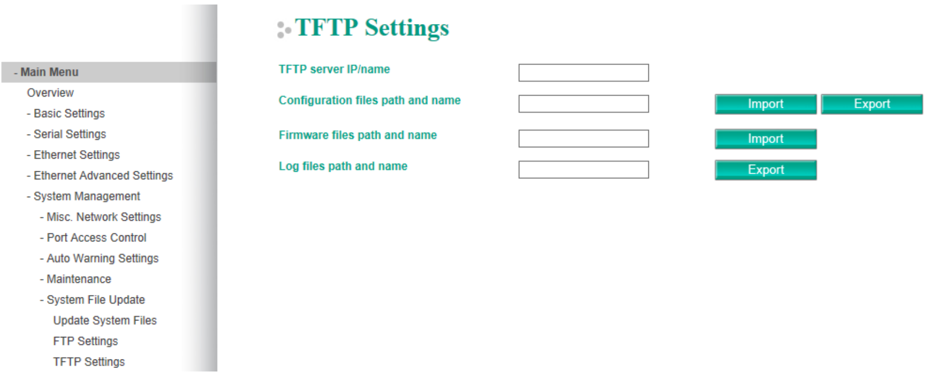


The NPort S9000 can be a FTP server to save configuration file or log files on it. You may enable it by checking the checkbox **Enable** and then click **Activate**.

TFTP Settings

System File Update—By Remote TFTP

The NPort S9000 supports saving your configuration file to a remote TFTP server or local host to allow other NPort S9000 switches to use the same configuration at a later time, or saving the Log file for future reference. Loading pre-saved firmware or a configuration file from the TFTP server or local host is also supported for easy upgrading or configuration of the NPort S9000.



TFTP Settings

TFTP server IP/name

Configuration files path and name

Firmware files path and name

Log files path and name

TFTP Server IP/Name

Setting	Description	Factory Default
IP Address of TFTP Server	The IP or name of the remote TFTP server. Must be set up before downloading or uploading files.	None

Configuration Files Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and file name of the NPort S9000's configuration file in the TFTP server.	None

Firmware Files Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and file name of the NPort S9000's firmware file.	None

Log Files Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and file name of the NPort S9000's log file	None

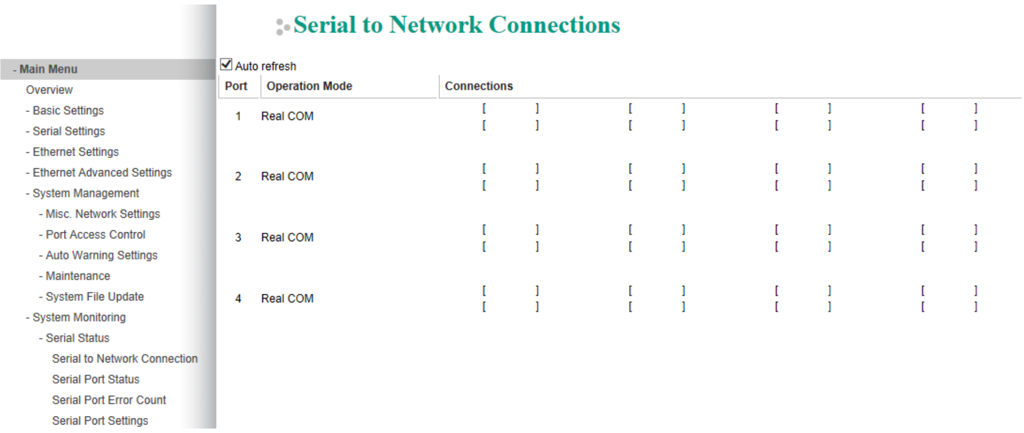
After setting up the desired path and file name, click **Activate** to save the setting, and then click **Download** to download the prepared file from the remote TFTP server, or click **Upload** to upload the desired file to the remote TFTP server.

System Monitoring

Serial Status

Serial to Network Connection

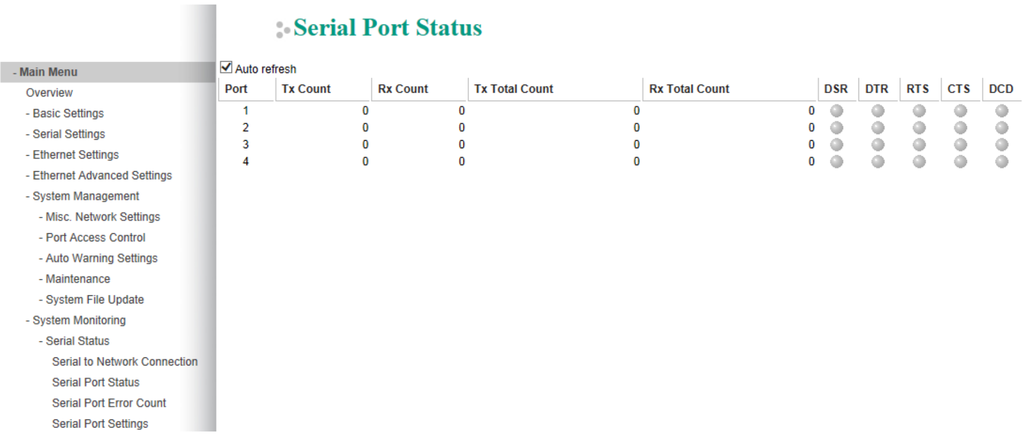
Go to **Serial to Network Connections** under **Serial Status** to view the operation mode and status of each connection, for each serial port. All monitor functions will refresh automatically every 5 seconds.



Port	Operation Mode	Connections
1	Real COM	[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
2	Real COM	[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
3	Real COM	[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
4	Real COM	[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

Serial Port Status

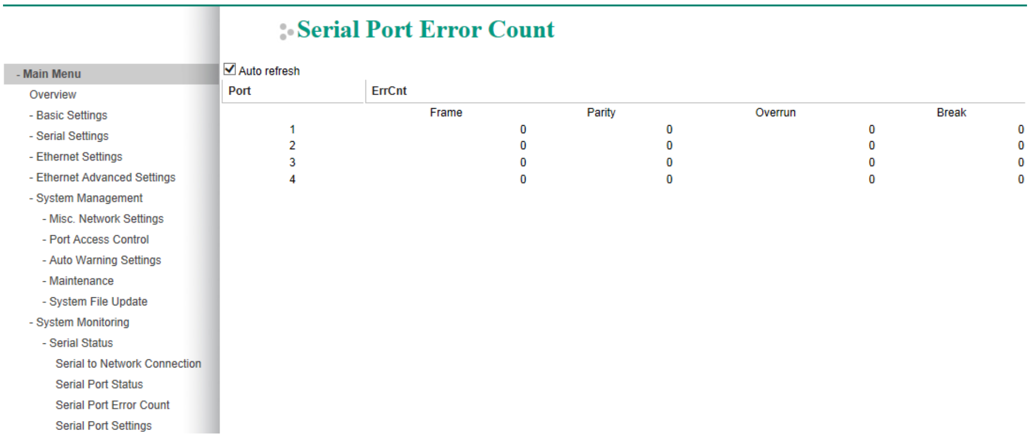
Go to **Serial Port Status** under **Serial Status** to view the current status of each serial port. **Serial Port Status → Buffering**.



Port	Tx Count	Rx Count	Tx Total Count	Rx Total Count	DSR	DTR	RTS	CTS	DCD
1	0	0	0	0	●	●	●	●	●
2	0	0	0	0	●	●	●	●	●
3	0	0	0	0	●	●	●	●	●
4	0	0	0	0	●	●	●	●	●

Serial Port Error Count

Go to **Serial Port Error Count** under **Serial Status** to view the error count for each serial port.



☑ Auto refresh

Port	ErrCnt			
	Frame	Parity	Overrun	Break
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0

Frame: Framing error indicates that the received character did not have a valid stop bit.

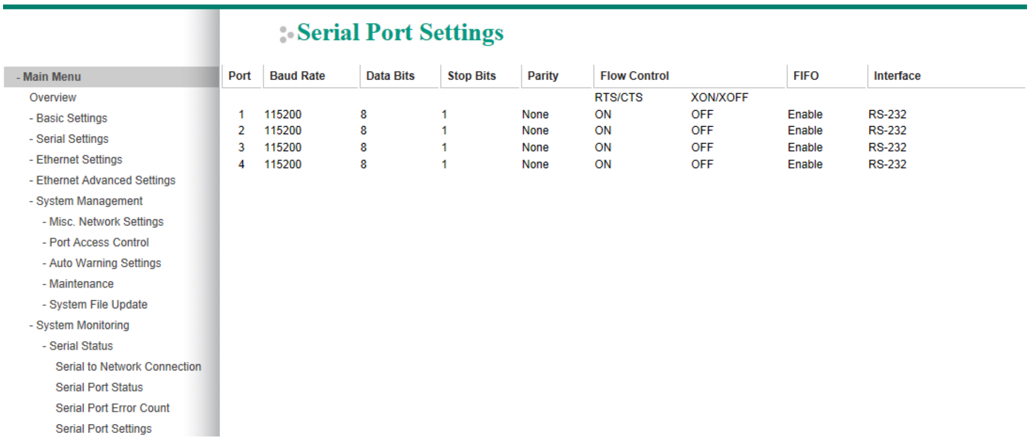
Parity: Parity error indicates that the received data character does not match the parity selected.

Overrun: The NPort is unable to hand received data to a hardware buffer because the input rate exceeds the NPort's ability to handle the data.

Break: Break interrupt indicates that the received data input was held low for longer than a full-word transmission time. A full-word transmission time is defined as the total time to transmit the start, data, parity, and stop bits.

Serial Port Settings

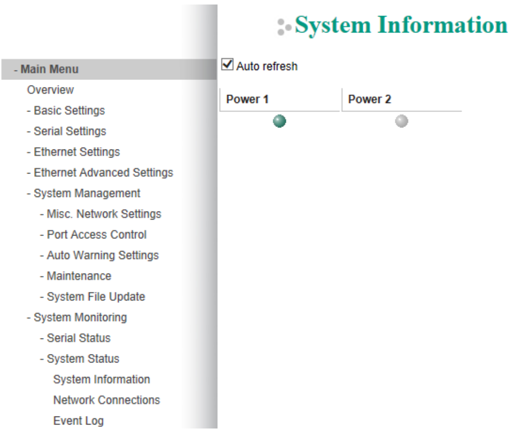
Go to **Serial Port Settings** under **Serial Status** to view a summary of the settings for each serial port.



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

System Status

System Information



System Information

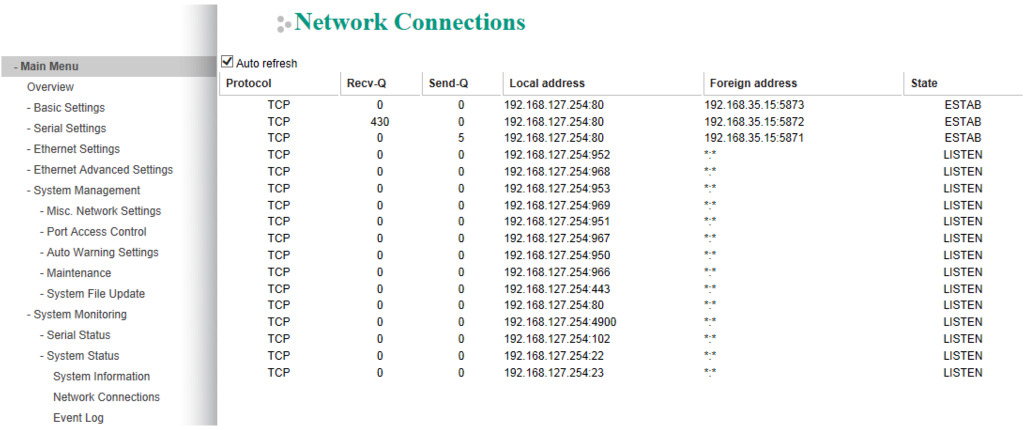
☑ Auto refresh

This page illustrate the status of system

Light	Status	Default
Power	Lighting when power is ON	blind

Network Connections

Go to **Network Connections** under System Status to view the network connection information.

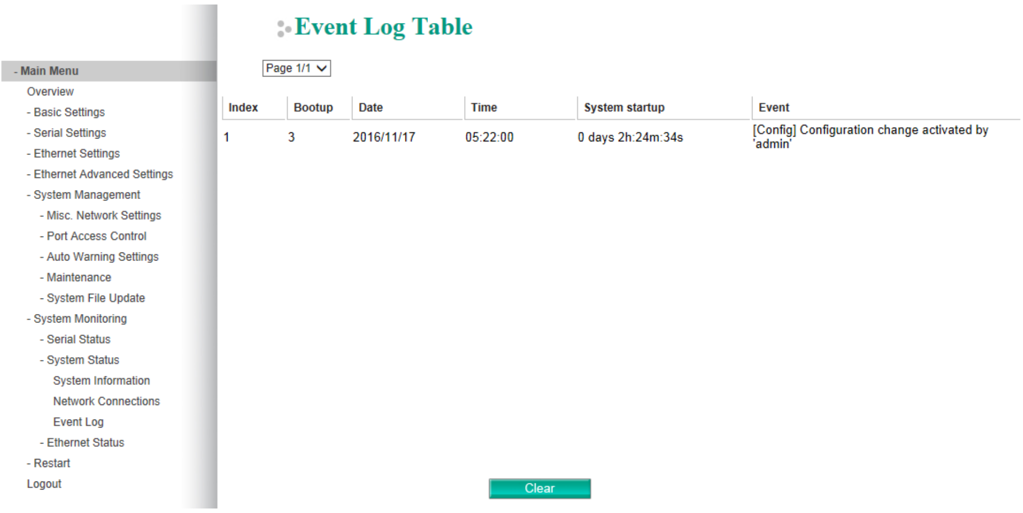


Network Connections

☑ Auto refresh

Protocol	Recv-Q	Send-Q	Local address	Foreign address	State
TCP	0	0	192.168.127.254:80	192.168.35.15:5873	ESTAB
TCP	430	0	192.168.127.254:80	192.168.35.15:5872	ESTAB
TCP	0	5	192.168.127.254:80	192.168.35.15:5871	ESTAB
TCP	0	0	192.168.127.254:952	*:*	LISTEN
TCP	0	0	192.168.127.254:968	*:*	LISTEN
TCP	0	0	192.168.127.254:953	*:*	LISTEN
TCP	0	0	192.168.127.254:969	*:*	LISTEN
TCP	0	0	192.168.127.254:951	*:*	LISTEN
TCP	0	0	192.168.127.254:967	*:*	LISTEN
TCP	0	0	192.168.127.254:950	*:*	LISTEN
TCP	0	0	192.168.127.254:966	*:*	LISTEN
TCP	0	0	192.168.127.254:443	*:*	LISTEN
TCP	0	0	192.168.127.254:80	*:*	LISTEN
TCP	0	0	192.168.127.254:4900	*:*	LISTEN
TCP	0	0	192.168.127.254:102	*:*	LISTEN
TCP	0	0	192.168.127.254:22	*:*	LISTEN
TCP	0	0	192.168.127.254:23	*:*	LISTEN

Event Log



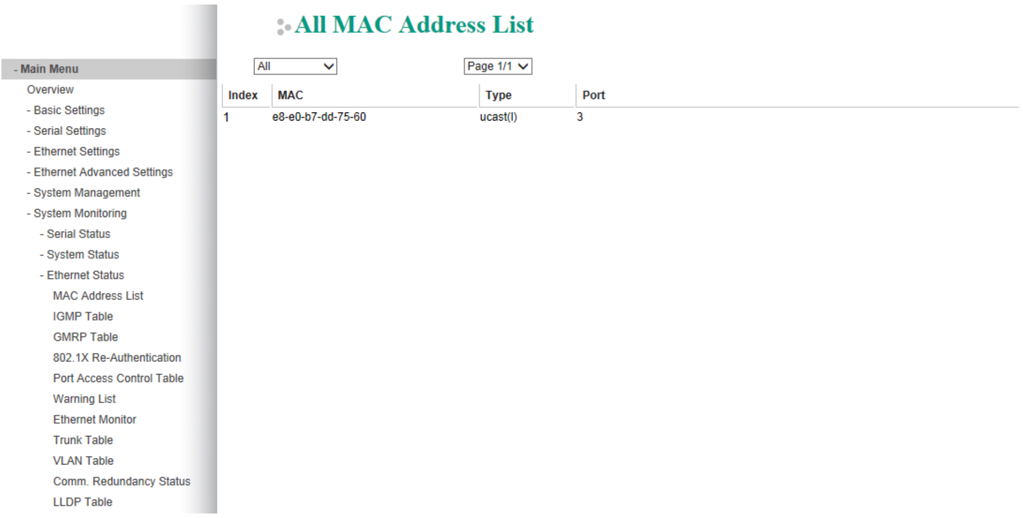
Index	Bootup	Date	Time	System startup	Event
1	3	2016/11/17	05:22:00	0 days 2h:24m:34s	[Config] Configuration change activated by 'admin'

Bootup	This field shows how many times the NPort S9000 has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the "Basic Setting" page.
Time	The time is updated based on how the current time is set in the "Basic Setting" page.
System Startup	The system startup time related to this event.
Events	Events that have occurred.

Ethernet Status

MAC Address List

This section explains the information provided by the NPort S9000's MAC address table.



Index	MAC	Type	Port
1	e8-e0-b7-dd-75-60	ucast(l)	3

The MAC Address table can be configured to display the following NPort S9000 MAC address groups.

ALL	Select this item to show all NPort S9000 MAC addresses
ALL Learned	Select this item to show all NPort S9000 Learned MAC addresses
ALL Static Lock	Select this item to show all NPort S9000 Static Lock MAC addresses
ALL Static	Select this item to show all NPort S9000 Static/Static Lock /Static Multicast MAC addresses
ALL Static Multicast	Select this item to show all NPort S9000 Static Multicast MAC addresses

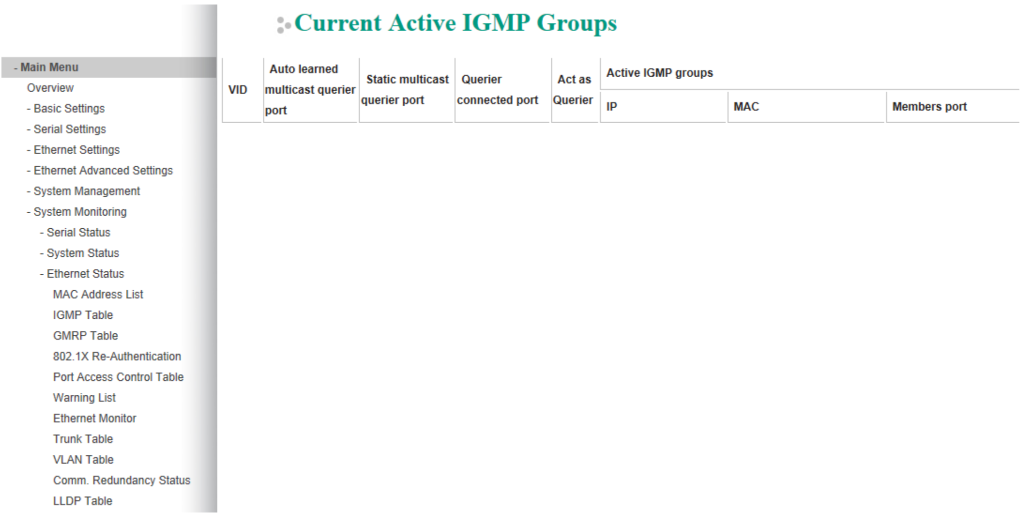
Port (1-5)	Select this item to show all MAC addresses of dedicated ports

The table will display the following information:

MAC	This field shows the MAC address
Type	This field shows the type of this MAC address
Port	This field shows the port that this MAC address belongs to

IGMP Table

The NPort S9000 displays the current active IGMP groups that were detected.

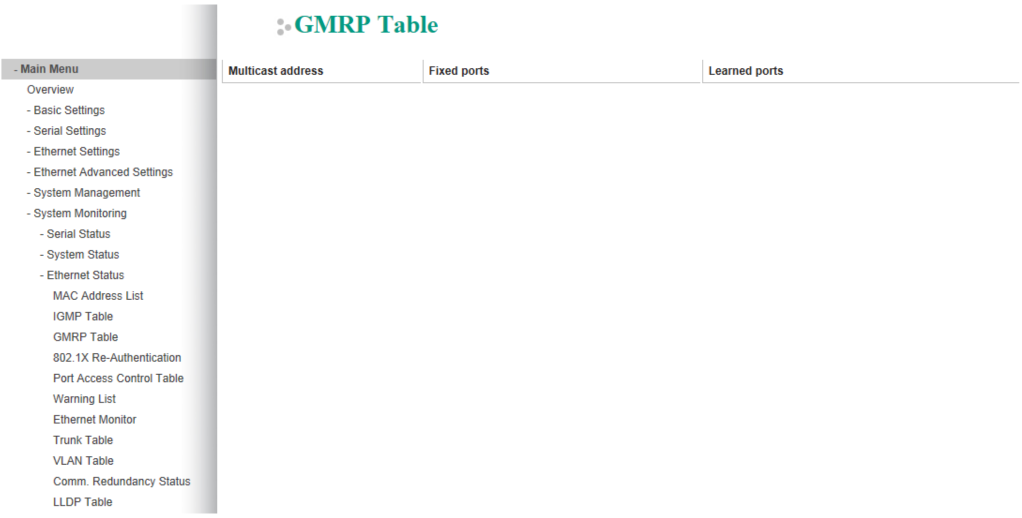


VID	Auto learned multicast querier port	Static multicast querier port	Querier connected port	Act as Querier	Active IGMP groups		
					IP	MAC	Members port

The information includes **VID**, **Auto-learned Multicast Router Port**, **Static Multicast Router Port**, **Querier Connected Port**, and the **IP** and **MAC** addresses of active IGMP groups.

GMRP Table

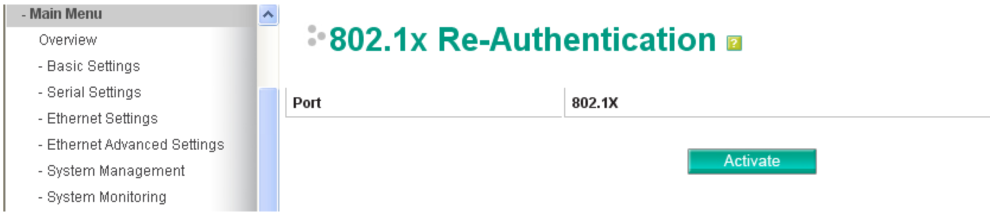
The NPort S9000 displays the current active GMRP groups that were detected.



Multicast address	Fixed ports	Learned ports

Setting	Description
Fixed Ports	This multicast address is defined by static multicast.
Learned Ports	This multicast address is learned by GMRP.

802.1X Reauth



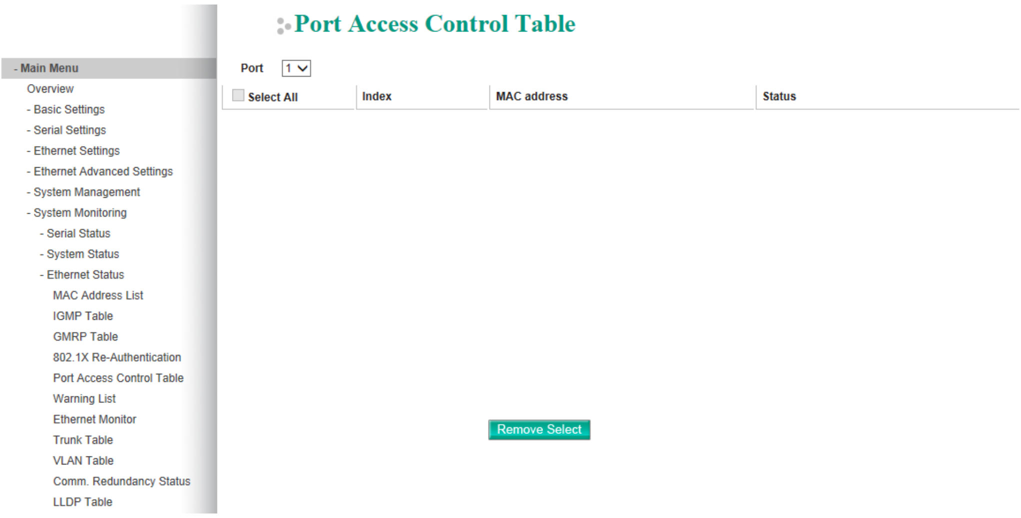
802.1x Re-Authentication

Port	802.1X

The NPort S9000 can force connected devices to be reauthorized manually.

Port Access Control Table

The port status will indicate whether the access is authorized or unauthorized.



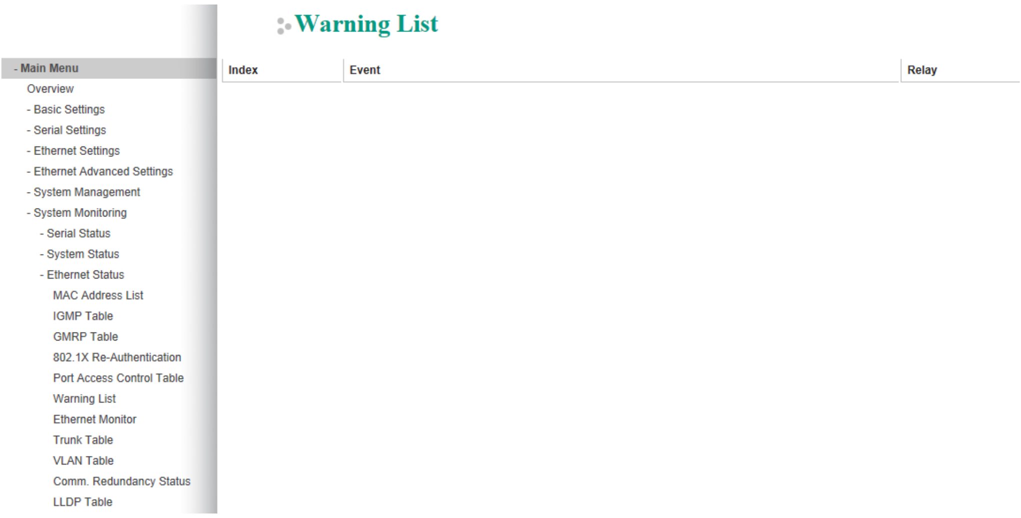
Port Access Control Table

Port 1

□ Select All	Index	MAC address	Status

Warning List

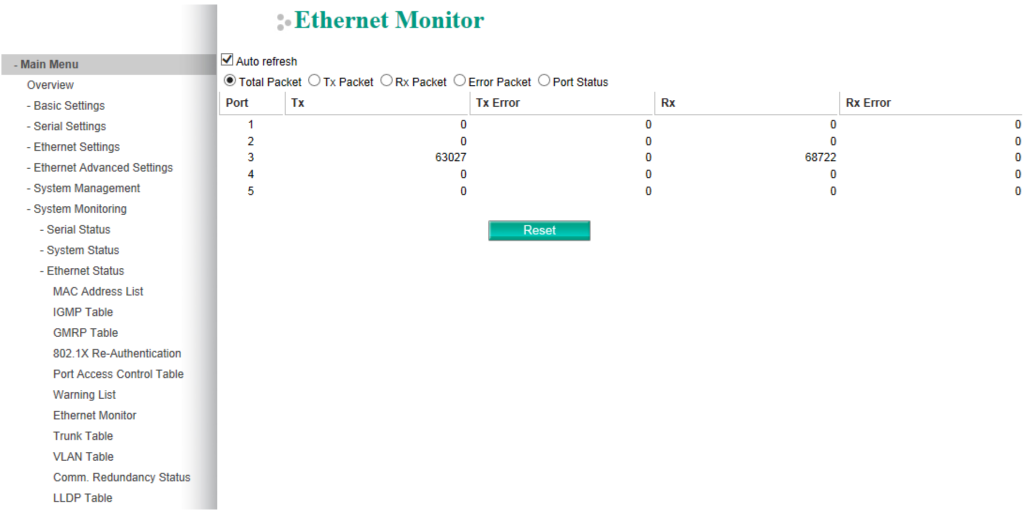
Use this table to see if any relay alarms have been issued.



Warning List

Index	Event	Relay

Ethernet Monitor



☑ Auto refresh

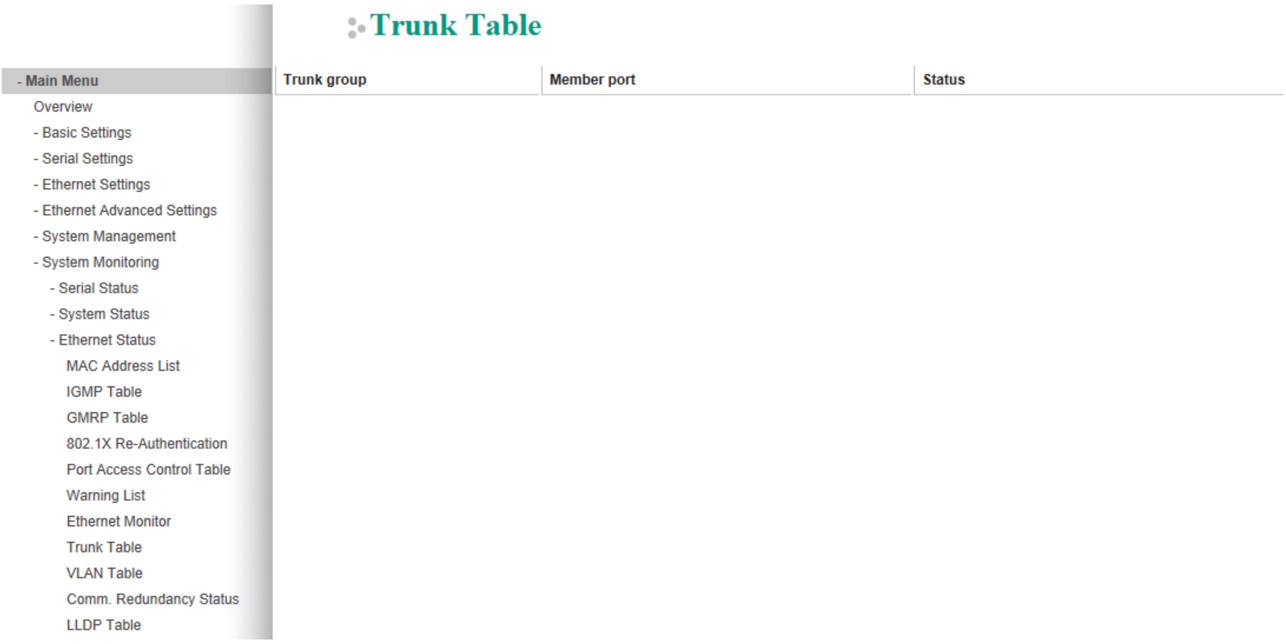
● Total Packet ○ Tx Packet ○ Rx Packet ○ Error Packet ○ Port Status

Port	Tx	Tx Error	Rx	Rx Error
1	0	0	0	0
2	0	0	0	0
3	63027	0	68722	0
4	0	0	0	0
5	0	0	0	0

This page illustrates the data transmission status of Ethernet. Check one of the four options, Total Packets, TX Packets, RX Packets, or Error Packets, to show the transmission activity of specific types of packets.

Check the Port Status to show the status of Ethernet port.

Trunk Table

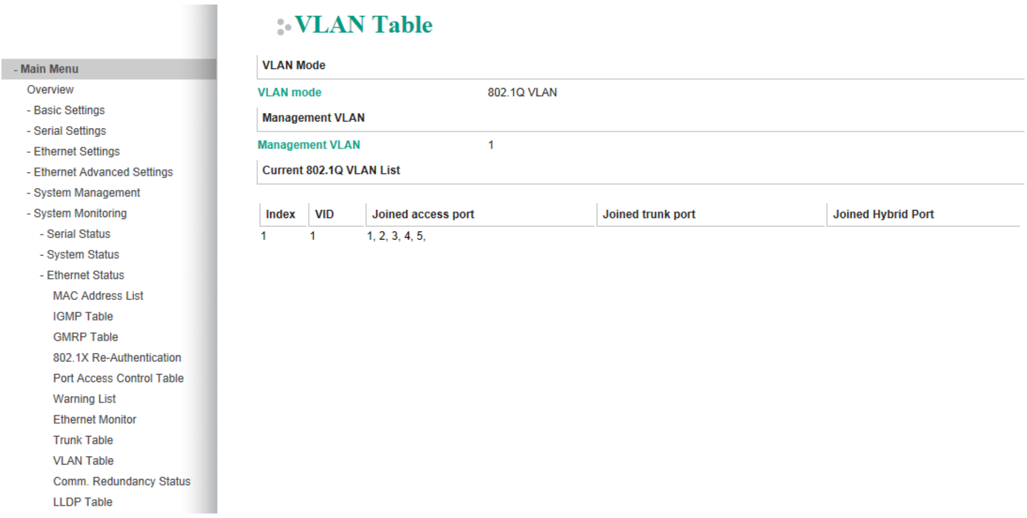


Trunk group	Member port	Status

Setting	Description
Trunk Group	Displays the Trunk Type and Trunk Group.
Member Port	Display which member ports belong to the trunk group.
Status	Success means port trunking is working properly. Fail means port trunking is not working properly. Standby means port trunking is working as a standby port. When there are more than eight ports trunked as a trunking group, the ninth port will be the standby port.

VLAN Table

In the 802.1Q VLAN table, you can review the VLAN groups that were created, Joined Access Ports, and Trunk Ports. In the Port-based VLAN table, you can review the VLAN group and Joined port



VLAN Table

VLAN Mode

VLAN mode 802.1Q VLAN

Management VLAN

Management VLAN 1

Current 802.1Q VLAN List

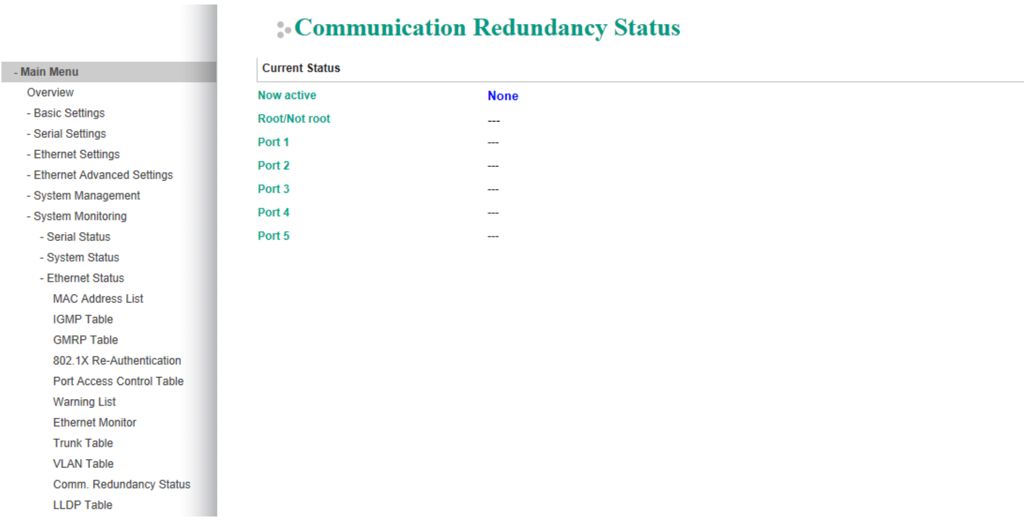
Index	VID	Joined access port	Joined trunk port	Joined Hybrid Port
1	1	1, 2, 3, 4, 5,		

NOTE The physical network can have a maximum of 64 VLAN settings.

Communication Redundancy Status

This page shows the status of communication redundancy.

RSTP



Communication Redundancy Status

Current Status

Now active	None
Root/Not root	---
Port 1	---
Port 2	---
Port 3	---
Port 4	---
Port 5	---

Explanation of "Current Status" Items

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **RSTP**

Ring 1/2—Status

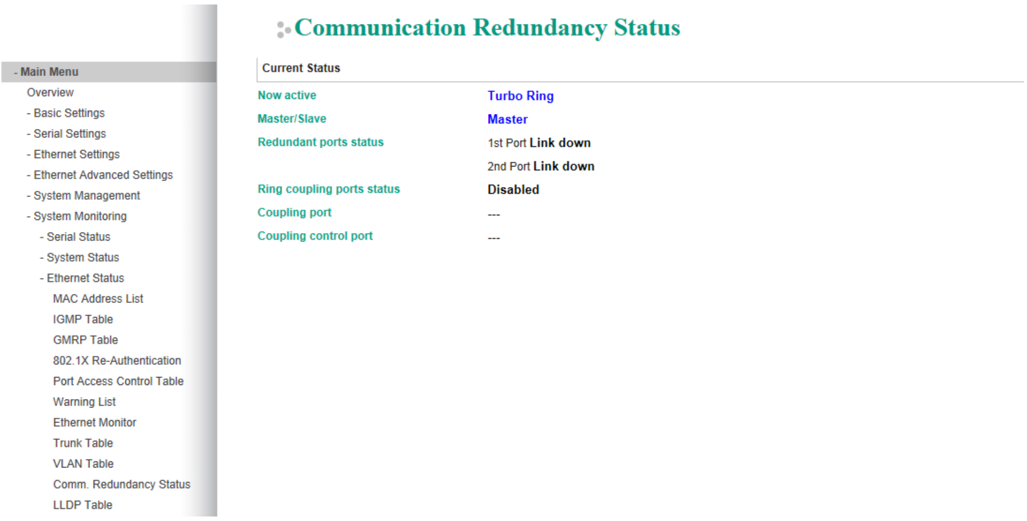
Shows **Healthy** if the ring is operating normally, and shows **Break** if the ring's backup link is active.

Ring 1/2—Master/Slave

Indicates whether or not this NPort S9000 is the Master of the Turbo Ring. (This field appears only when selected to operate in Turbo Ring or Turbo Ring V2 mode.)

Now active	Indicates the in-use communication protocol. It may be Turbo Ring, Turbo Ring V2, RSTP, or none.
Root/Not root	Available when Redundancy protocol is set to RSTP mode. Indicates the NPort S9000 is in the Root of the Spanning Tree. (The root is determined automatically).
Port 1 / Port 2 Port 3 / Port 4 Port 5	Indicates the current Spanning Tree status of these ports. “Forwarding” for normal transmission “Blocking” to block transmission.

Turbo Ring



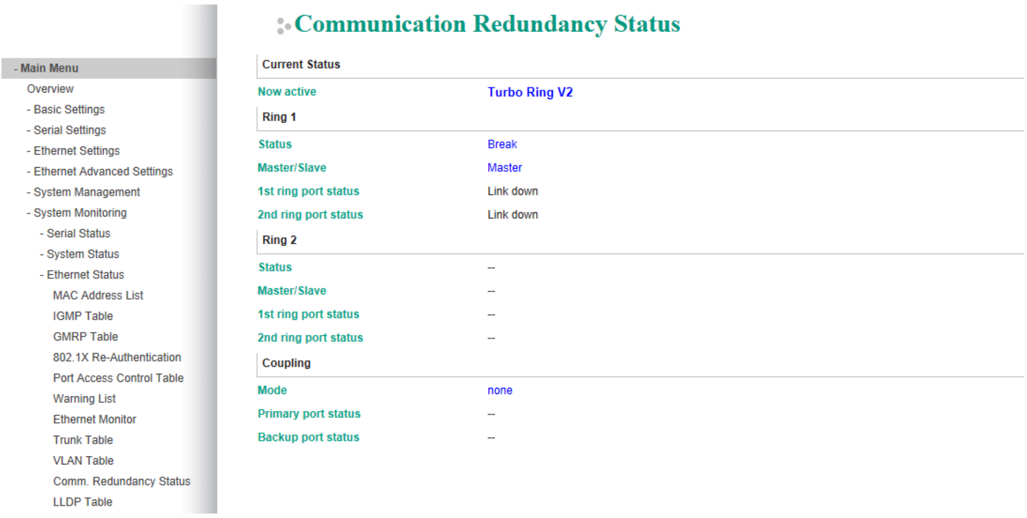
Communication Redundancy Status

Current Status

Now active	Turbo Ring
Master/Slave	Master
Redundant ports status	1st Port Link down 2nd Port Link down
Ring coupling ports status	Disabled
Coupling port	---
Coupling control port	---

Now active	Indicates the in-use- communication protocol. It may be Turbo Ring, Turbo Ring V2, RSTP, or none.	
Master/Slave	Indicates the NPort S9000 is in the Master mode or Slave mode of the Turbo Ring.	
Redundant Ports Status	Link down	No connection
	Blocked	This port is connected to a backup path and the path is blocked
	Forwarding	Normal transmission
	Learning	Learning
Ring Coupling Ports Status	Enable or disable	
Coupling Port	Indicates which port is used to be coupling port (port 1 to port 5). Available when Ring Coupling in communication redundancy setting page is enabled	
Coupling Control Port	Indicates which port is used to be coupling control port (port 1 to port 5). Available when Ring Coupling in communication redundancy setting page is enabled	

Turbo Ring 2

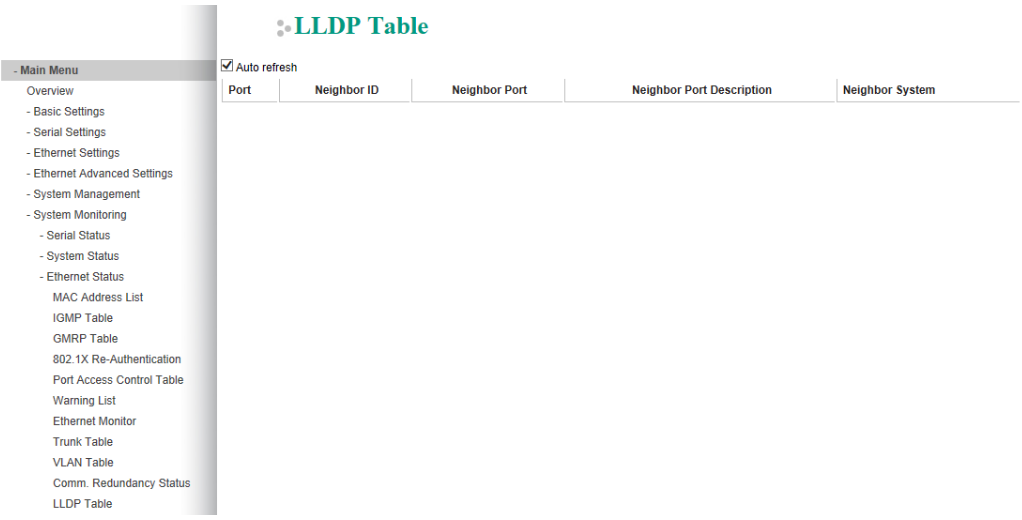


Communication Redundancy Status

Current Status	
Now active	Turbo Ring V2
Ring 1	
Status	Break
Master/Slave	Master
1st ring port status	Link down
2nd ring port status	Link down
Ring 2	
Status	--
Master/Slave	--
1st ring port status	--
2nd ring port status	--
Coupling	
Mode	none
Primary port status	--
Backup port status	--

Now Active	Indicates the in-use communication protocol. It may be Turbo Ring, Turbo Ring V2, RSTP, or none.	
Ring 1/2		
Status	Healthy	The ring is operating normally
	Break	The backup link is active in the Ring.
Master/Slave	Indicates the NPort S9000 is in the Master mode or Slave mode of the Turbo Ring 2.	
1st/2nd Ring Port Status	Link down	No connection
	Blocked	This port is connected to a backup path and the path is blocked
	Forwarding	Normal transmission
	Learning	Learning
Coupling Mode	Indicates current coupling mode It may be None, Dual Homing, or Ring Coupling.	
Coupling Port status	Indicates which port is used to be coupling port (port 1 to port 5). Available when Ring Coupling in communication redundancy setting page is enabled	

LLDP Table



LLDP Table

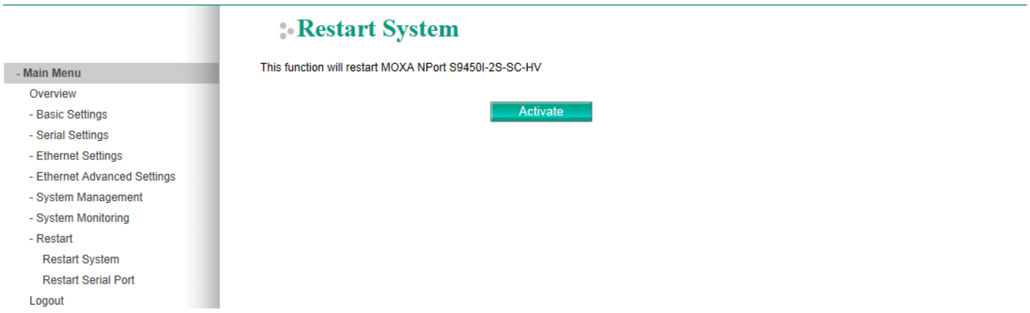
☑ Auto refresh

Port	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System

Restart

Restart System

Go to **Restart System** under **Restart** and then click **Restart** to restart the NPort S9000. Ensure that you save all your configuration changes before you restart the system or else these changes will be lost.

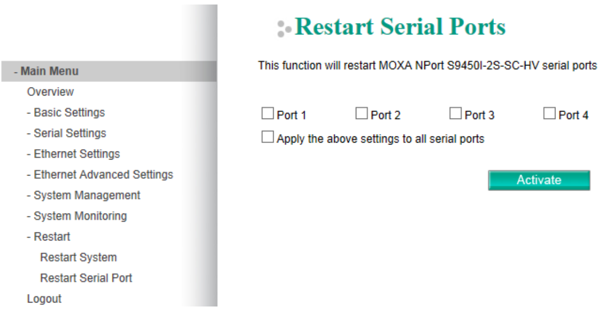


Restart System

This function will restart MOXA NPort S9450I-2S-SC-HV

Restart Serial Port

Go to **Restart Ports** under **Restart** and then select the ports to be restarted. Click **Select All** to select all the ports. Click **Submit** to restart the selected ports.



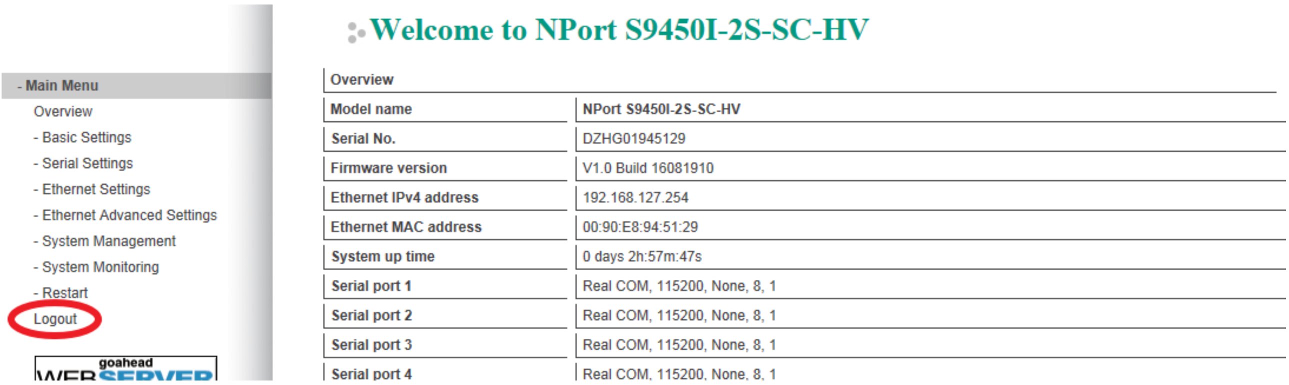
Restart Serial Ports

This function will restart MOXA NPort S9450I-2S-SC-HV serial ports

□ Port 1 □ Port 2 □ Port 3 □ Port 4

□ Apply the above settings to all serial ports

Logout



Welcome to NPort S9450I-2S-SC-HV

Overview	
Model name	NPort S9450I-2S-SC-HV
Serial No.	DZHG01945129
Firmware version	V1.0 Build 16081910
Ethernet IPv4 address	192.168.127.254
Ethernet MAC address	00:90:E8:94:51:29
System up time	0 days 2h:57m:47s
Serial port 1	Real COM, 115200, None, 8, 1
Serial port 2	Real COM, 115200, None, 8, 1
Serial port 3	Real COM, 115200, None, 8, 1
Serial port 4	Real COM, 115200, None, 8, 1

Click the Logout icon to terminate the session of current account. Be noted that any unsaved configuration changes will be discarded after logout.

A

Pinouts and Cable Wiring

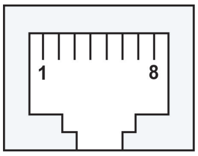
In this appendix, we cover the following topics.

- ❒ **Port Pinout Diagrams**
  - ➢ Ethernet Port Pinouts
  - ➢ Serial Port Pinouts
- ❒ **Cable Wiring Diagrams**
  - ➢ Ethernet Cables

Port Pinout Diagrams

Ethernet Port Pinouts

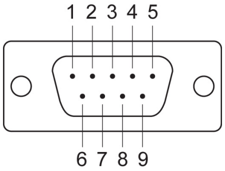
Pin	Signal
1	Tx+
2	Tx-
3	Rx+
6	Rx-



Serial Port Pinouts

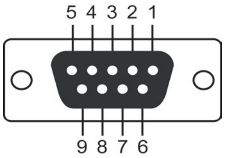
DB9 Male RS-232/422/485 Port Pinouts

Pin	RS-232	RS-422/485-4w	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	–	–



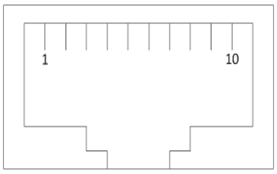
DB9 Female RS-232/422/485 Port Pinouts

Pin	RS-232	RS-422/485-4w	RS-485-2w
1	DCD	TxD-	–
2	TxD	RxD+	Data+
3	RxD	TxD+	–
4	DSR/+IRIG-B	DSR/+IRIG-B	DSR/+IRIG-B
5	GND	GND	GND
6	DTR	–	–
7	CTS	RxD-	DATA-
8	RTS	–	–



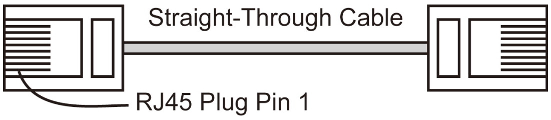
Serial Console Port Pinouts

Pin	RS-45
1	DCD
2	DSR
3	RTS
4	N.C.
5	Tx
6	Rx
7	GND
8	CTS
9	DTR
10	N.C.



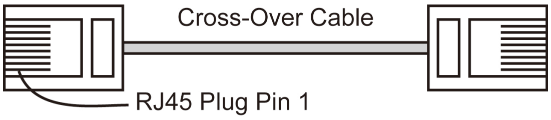
Cable Wiring Diagrams

Ethernet Cables



Cable Wiring

3	3
6	6
1	1
2	2



Cable Wiring

3	1
6	2
1	3
2	6

B

Well-Known Port Numbers

This appendix is for your reference about the well-known port numbers that may cause network problem if you set the NPort into the same port. Refer to RFC 1700 for well-known port numbers of refer to the following introduction from the IANA.

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

The Well-known Ports are those from 0 through 1023.

The Registered Ports are those from 1024 through 49151.

The Dynamic and/or Private Ports are those from 49152 through 65535.

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

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

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

C

SNMP Agents with MIB II & RS-232 Like Groups

The NPort S9000 has built-in SNMP (Simple Network Management Protocol) agent software. The following table lists the proprietary MIB-II group, as well as the variable implementation for the NPort S9000.

Moxa-NPort S9000-MIB

overview	basicSetting	portSetting	ethernetSetting
ModelName	generalSettings	opModeSetting	portSettings
SerialNumber	serverName	opMode	portTable
FirmwareVersion	serverLocation	opModePortTable	portEntry
MacAddress	serverDescription	opModePortEntry	portIndex_Eth
Uptime	maintainerContactInfo	portIndex	portEnable
ViewIpAddr	timeSetting	portMode	portDesc
	sysDateTime	application	portName
	daylightSaving	realcom	portSpeed
	startMonth	realComTable	portFDXFlowCtrl
	startWeek	realComEntry	portMDI
	startDay	realcomMaxConnection	
	startHour	realcomAllowDriverControl	portTrunking
	endMonth	realcomConnectionDownRTS	trunkSettingTable
	endWeek	realcomConnectionDownDTR	trunkSettingEntry
	endDay	rfc2217	trunkSettingIndex
	endHour	rfc2217Table	trunkType
	offsetHours	rfc2217Entry	trunkMemberPorts
	timeZone	rfc2217TcpPort	
	timeServer1	tcpServer	commRedundancy
	timeServer2	tcpServerTable	protocolOfRedundancySetup
	calibratePeriod	tcpServerEntry	spanningTree
	networkSettings	tcpServerInactivityTime	spanningTreeBridgePriority
	autoIPConfig	tcpServerMaxConnection	spanningTreeHelloTime
	serverIpAddr	tcpServerAllowDriverControl	spanningTreeMaxAge
	subMask	tcpServerTcpServerConnectionDownRTS	spanningTreeForwardingDelay
	gateway	tcpServerTcpServerConnectionDownDTR	spanningTreeTable
	dnsServer1IPAddr	tcpServerTcpPort	spanningTreeEntry
	dnsServer2IPAddr	tcpServerCmdPort	spanningTreeIndex
	tcpAliveChkTime	tcpClient	enableSpanningTree
		tcpClientTable	spanningTreePortPriority
		tcpClientEntry	spanningTreePortCost
		tcpClientInactivityTime	turboRing
		tcpClientDestinationAddress1	turboRingMasterSetup
		tcpClientDestinationPort1	turboRingRdntPort1

overview	basicSetting	portSetting	ethernetSetting
		tcpClientDestinationAddress2	turboRingRdntPort2
		tcpClientDestinationPort2	turboRingEnableCoupling
		tcpClientDestinationAddress3	turboRingCouplingPort
		tcpClientDestinationPort3	turboRingControlPort
		tcpClientDestinationAddress4	turboRingV2
		tcpClientDestinationPort4	turboRingV2Ring1
		tcpClientDesignatedLocalPort1	ringIndexRing1
		tcpClientDesignatedLocalPort2	ringEnableRing1
		tcpClientDesignatedLocalPort3	masterSetupRing1
		tcpClientDesignatedLocalPort4	rdnt1stPortRing1
		tcpClientConnectionControl	rdnt2ndPortRing1
		udp	turboRingV2Ring2
		udpTable	ringIndexRing2
		udpEntry	ringEnableRing2
		udpDestinationAddress1Begin	masterSetupRing2
		udpDestinationAddress1End	rdnt1stPortRing2
		udpDestinationPort1	rdnt2ndPortRing2
		udpDestinationAddress2Begin	turboRingV2Coupling
		udpDestinationAddress2End	couplingEnable
		udpDestinationPort2	couplingMode
		udpDestinationAddress3Begin	coupling1stPort
		udpDestinationAddress3End	coupling2ndPort
		udpDestinationPort3	
		udpDestinationAddress4Begin	rateLimiting
		udpDestinationAddress4End	rateLimitingTable
		udpDestinationPort4	rateLimitingEntry
		udpLocalListenPort	limitMode
		dataPacking	lowPriLimitRate
		dataPackingPortTable	normalPriLimitRate
		dataPackingPortEntry	mediumPriLimitRate
		portPacketLength	highPriLimitRate
		portDelimiter1Enable	
		portDelimiter1	lineSwapFastRecovery
		portDelimiter2Enable	lineSwapRecovery
		portDelimiter2	
		portDelimiterProcess	
		portForceTransmit	
		comParamSetting	
		comParamPortTable	
		comParamPortEntry	
		portAlias	
		portBaudRate	
		portDataBits	
		portStopBits	
		portParity	
		portFlowControl	
		portFIFO	
		portInterface	
		portBaudRateManual	
		serialTosSetting	

overview	basicSetting	portSetting	ethernetSetting
		serialTosTable	
		serialTosEntry	

ethernetAdvSetting	systemManagement
trafficPrioritization	miscNetwork
qosClassification	accessibleIP
queuingMechanism	enableAccessibleIP
qosPortTable	accessibleIpEntry
qosPortEntry	accessibleIpIndex
inspectTos	accessibleIpAddress
inspectCos	accessibleIpNetMask
portPriority	syslogSetting
cosMapping	syslogServer1
cosMappingTable	syslogServer1port
cosMappingEntry	syslogServer2
cosTag	syslogServer2port
cosMappedPriority	syslogServer3
tosMapping	syslogServer3port
tosMappingTable	portAccessControl
tosMappingEntry	staticPortLock
tosClass	staticPortLockAddress
tosMappedPriority	staticPortLockPort
vlan	staticPortLockStatus
vlanType	dot1x
managementVlanId	dataBaseOption
vlanPortSettingTable	radiusServer
vlanPortSettingEntry	radiusPort
portVlanType	radiusSharedKey
portDefaultVid	dot1xReauthEnable
portFixedVid	dot1xReauthPeriod
portForbiddenVid	dot1xSettingTable
portbaseVlanSettingEntry	dot1xSettingEntry
portbaseVlanSettingIndex	enableDot1X
portbaseVlanMemberPorts	autoWarming
multicastFiltering	emailAlert
igmpSnooping	emailWarningMailServer
enableGlobalIgmpSnooping	emailWarningFromEmail
querierQueryInterval	emailWarningFirstEmailAddr
igmpSnoopingSettingTable	emailWarningSecondEmailAddr
igmpSnoopingSettingEntry	emailWarningThirdEmailAddr
enableIgmpSnooping	emailWarningFourthEmailAddr
enableQuerier	snmpAgent
fixedMulticastQuerierPorts	snmpReadCommunity
staticMulticast	trapServerAddr1
staticMulticastTable	snmpTrapCommunity1
staticMulticastEntry	trap2ServerAddr
staticMulticastIndex	snmpTrap2Community
staticMulticastAddress	emailWarningEventType
staticMulticastPorts	emailWarningEventServerColdStart
staticMulticastStatus	emailWarningEventServerWarmStart
gmrp	emailWarningEventPowerOn2Off

ethernetAdvSetting	**systemManagement**
gmrpSettingTable	emailWarningEventPowerOff2On
gmrpSettingEntry	emailWarningEventDiTable
enableGMRP	emailWarningEventDiEntry
setDeviceIp	emailWarningEventDiInputOn2Off
setDevIpTable	emailWarningEventDiInputOff2On
setDevIpEntry	emailWarningEventConfigChange
setDevIpIndex	emailWarningEventAuthFail
setDevIpCurrentIpofDevice	emailWarningEventTopologyChanged
setDevIpPresentBy	emailWarningEventSerialPortTable
setDevIpDedicatedIp	emailWarningEventSerialPortEntry
	emailWarningEventSerailDCDChange
	emailWarningEventSerailDSRChange
	emailWarningEventEthernetPortTable
	emailWarningEventEthernetPortEntry
	emailWarningEventEthernetPortLinkOn
	emailWarningEventEthernetPortLinkOff
	emailWarningEventEthernetPortTrafficOverload
	emailWarningEventEthernetPortTrafficThreshold
	emailWarningEventEthernetPortTrafficDuration
	snmpWarningEventType
	snmpWarningEventServerColdStart
	snmpWarningEventServerWarmStart
	snmpWarningEventPowerOn2Off
	snmpWarningEventPowerOff2On
	snmpWarningEventDiTable
	snmpWarningEventDiEntry
	snmpWarningEventDiInputOn2Off
	snmpWarningEventDiInputOff2On
	snmpWarningEventConfigChange
	snmpWarningEventAuthFail
	snmpWarningEventTopologyChanged
	snmpWarningEventSerailPortTable
	snmpWarningEventSerailPortEntry
	snmpWarningEventSerailDCDchange
	snmpWarningEventSerailDSRchange
	snmpWarningEventEthernetPortTable
	snmpWarningEventEthernetPortEntry
	snmpWarningEventEthernetPortLinkOn
	snmpWarningEventEthernetPortLinkOff
	snmpWarningEventEthernetPortTrafficOverload
	snmpWarningEventEthernetPortTrafficThreshold
	snmpWarningEventEthernetPortTrafficDuration
	relayWarning
	relayWarningTable
	relayWarningEntry
	relayAlarmIndex
	relayWarningRelayContact
	overrideRelayWarningSetting
	relayWarningPower1Off
	relayWarningPower1OffStatus
	relayWarningPower2Off
	relayWarningPower2OffStatus

ethernetAdvSetting	systemManagement
	relayWarningTurboRingBreak
	relayWarningTurboRingBreakStatus
	portRelayWarningTable
	portRelayWarningEntry
	relayWarningLinkChanged
	relayWarningLinkChangedStatus
	relayWarningTrafficOverload
	relayWarningTrafficOverloadStatus
	relayWarningTrafficThreshold
	relayWarningTrafficDuration
	diRelayWarningTable
	diRelayWarningEntry
	relayWarningDiInputChanged
	relayWarningDiInputChangedStatus
	sysLogSettings
	sysLocalLog
	networkLocalLog
	configLocalLog
	opModeLocalLog
	sysRemoteLog
	networkRemoteLog
	configRemoteLog
	opModeRemoteLog
	maintenance
	consoleSetting
	webConsole
	httpConsole
	telnetConsole
	resetButtonFunction
	autoRefresh
	loadFactoryDefault
	loadFactoryDefaultSetting
	mirroring
	targetPort
	monitorDirection
	mirroringPort
	sysFileUpdate
	tftpServer
	confPathName
	firmwarePathName
	logPathName
	dipSwitchSetting
	dipSwitchEnableTurboRing
	dipSwitchTurboRingType

systemMonitoring	restart
serialStatus	restartSystem
s2eConnections	restartPortNumber
monitorRemoteIpTable	
monitorRemoteIpEntry	
remoteIpIndex	
monitorRemoteIp	

systemMonitoring	**restart**
serialPortStatus	
monitorSerialPortStatusTable	
monitorSerialPortStatusEntry	
monitorTxCount	
monitorRxCount	
monitorTxTotalCount	
monitorRxTotalCount	
monitorDSR	
monitorDTR	
monitorRTS	
monitorCTS	
monitorDCD	
serialPortErrorCount	
monitorSerialPortErrorCountTable	
monitorSerialPortErrorCountEntry	
monitorErrorCountFrame	
monitorErrorCountParity	
monitorErrorCountOverrun	
monitorErrorCountBreak	
serialPortSettings	
monitorSerialPortSettingsTable	
monitorSerialPortSettingsEntry	
monitorBaudRate	
monitorDataBits	
monitorStopBits	
monitorParity	
monitorRTSCTSFlowControl	
monitorXONXOFFFlowControl	
monitorFIFO	
monitorInterface	
systemStatus	
systemInfo	
power1InputStatus	
power2InputStatus	
monitorDiTable	
monitorDiEntry	
diIndex	
diInputStatus	
dipSwitchTurboRingPole	
dipSwitchRingCouplingPole	
dipSwitchRingMasterPole	
eventLog	
eventLogTable	
eventLogEntry	
eventListIndex	
eventListBootup	
eventListData	
eventListTime	
eventListSysUpTime	
eventListEvent	
eventListClear	
ethernetStatus	

systemMonitoring	restart
macAddressList	
igmpstatus	
igmpSnoopingMulticastGroupTable	
igmpSnoopingMulticastGroupEntry	
learnedMulticastQuerierPorts	
igmpSnoopingIpGroup	
igmpSnoopingMacGroup	
igmpSnoopingJoinedPorts	
gmrpStatus	
gmrpTable	
gmrpEntry	
gmrpMulticastGroup	
gmrpFixedPorts	
gmrpLearnedPorts	
dot1XReauth	
dot1xReauthTable	
dot1xReauthEntry	
dot1xReauthPortIndex	
dot1xReauth	
portAccessControlList	
portAccessControlTable	
portAccessControlEntry	
portAccessControlAddress	
portAccessControlPortNo	
portAccessControlAccessStatus	
portAccessControlStatus	
warningList	
warningListTable	
warningListEntry	
warningListIndex	
warningListEvent	
warningListRelay	
ethernetMonitor	
ethernetMonitorTable	
ethernetMonitorEntry	
ethernetMonitorTxTotal	
ethernetMonitorTxUicast	
ethernetMonitorTxMulticast	
ethernetMonitorTxBroadcast	
ethernetMonitorTxCollision	
ethernetMonitorRxTotal	
ethernetMonitorRxUicast	
ethernetMonitorRxMulticast	
ethernetMonitorRxBroadcast	
ethernetMonitorRxPause	
ethernetMonitorTxErr	
ethernetMonitorTxErrLate	
ethernetMonitorTxErrExcessive	
ethernetMonitorRxErr	
ethernetMonitorRxErrCRC	
ethernetMonitorRxErrDiscard	
ethernetMonitorRxErrUndersize	

systemMonitoring	restart
ethernetMonitorRxErrFragments	
ethernetMonitorRxErrOversize	
ethernetMonitorRxErrJabber	
ethernetMonitorReset	
monitorPortTable	
monitorPortEntry	
monitorLinkStatus	
monitorSpeed	
monitorFDXFlowCtrl	
monitorAutoMDI	
monitorConnectedIP	
monitorTraffic	
trunkTableList	
trunkTable	
trunkEntry	
trunkIndex	
trunkPort	
trunkStatus	
vlanList	
vlanTable	
vlanEntry	
vlanId	
joinedAccessPorts	
joinedTrunkPorts	
commRedStatus	
activeProtocolOfRedundancy	
spanningTreeStatus	
spanningTreeRoot	
spanningTreeStatusTable	
spanningTreeStatusEntry	
spanningTreePortStatus	
turboRingStatus	
turboRingMaster	
turboRingPortTable	
turboRingPortEntry	
turboRingPortIndex	
turboRingPortStatus	
turboRingPortDesignatedBridge	
turboRingPortDesignatedPort	
turboRingDesignatedMaster	
turboRingCouplingPortStatus	
turboRingControlPortStatus	
turboRingBrokenStatus	
turboRingV2Status	
turboRingV2Ring1Status	
masterStatusRing1	
designatedMasterRing1	
rdnt1stPortStatusRing1	
rdnt2ndPortStatusRing1	
brokenStatusRing1	
turboRingV2Ring2Status	
masterStatusRing2	

systemMonitoring	**restart**
designatedMasterRing2	
rdnt1stPortStatusRing2	
rdnt2ndPortStatusRing2	
brokenStatusRing2	
turboRingV2CouplingStatus	
coupling1stPortStatus	
coupling2ndPortStatus	

D

Switch MIB Groups

The NPort S9000 comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold/warm start trap, line up/down trap, and RFC 1213 MIB-II.

The standard MIB groups supported by the NPort S9000 are:

MIB II.1 – System Group

sysORTable

MIB II.2 – Interfaces Group

ifTable

MIB II.4 – IP Group

ipAddrTable
ipNetToMediaTable
IpGroup
IpBasicStatsGroup
IpStatsGroup

MIB II.5 – ICMP Group

IcmpGroup
IcmpInputStatus
IcmpOutputStats

MIB II.6 – TCP Group

tcpConnTable
TcpGroup
TcpStats

MIB II.7 – UDP Group

udpTable
UdpStats

MIB II.10 – Transmission Group

dot3
dot3StatsTable

MIB II.11 – SNMP Group

SnmpBasicGroup
SnmpInputStats
SnmpOutputStats

MIB II.17 – dot1dBridge Group

- dot1dBase
  - dot1dBasePortTable
- dot1dStp
  - dot1dStpPortTable
- dot1dTp
  - dot1dTpFdbTable
  - dot1dTpPortTable

- dot1dTpHCPortTable
- dot1dTpPortOverflowTable

pBridgeMIB

- dot1dExtBase
- dot1dPriority
- dot1dGarp

qBridgeMIB

- dot1qBase
- dot1qTp
  - dot1qFdbTable
  - dot1qTpPortTable
  - dot1qTpGroupTable
  - dot1qForwardUnregisteredTable
- dot1qStatic
  - dot1qStaticUnicastTable
  - dot1qStaticMulticastTable
- dot1qVlan
  - dot1qVlanCurrentTable
  - dot1qVlanStaticTable
  - dot1qPortVlanTable

The NPort S9000 also provides a private MIB file, located in the file "Moxa-NPort S9000-MIB.my" or "Moxa-NPort S9000-MIB.my" on the NPort S9000 series utility CD-ROM.

Public Traps:

1. Cold Start
2. Link Up
3. Link Down
4. Authentication Failure
5. dot1dBridge New Root
6. dot1dBridge Topology Changed

Private Traps:

1. Configuration Changed
2. Power On
3. Power Off
4. Traffic Overloaded
5. Turbo Ring Topology Changed
6. Turbo Ring Coupling Port Changed
7. Turbo Ring Master Mismatch

System Events

1. System cold start
2. System warm start
3. Power transition(On->Off
4. Power transition(Off->On)
5. DI 1 (Off)
6. DI 1 (On)
7. DI 2 (Off)
8. DI 2 (On)
9. Config. change
10. Auth. failure
11. Comm. redundancy topology changed

Serial Port Events

1. DCD changed
2. DSR changed

Ethernet Port Events

1. Link-ON
2. Link-OFF
3. Traffic-Overload
4. Traffic-Threshold(%)
5. Traffic-Duration(s)

E

Compliance Note

⚠ **CE Warming**

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take appropriate measures.

Federal Communications Commission Statement

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

⚠ **FCC Warming**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his or her own expense.