NPort 6000-G2 Series User Manual

Version 1.0, October 2024

www.moxa.com/products



NPort 6000-G2 Series User Manual

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

Copyright Notice

© 2024 Moxa Inc. All rights reserved.

Trademarks

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

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no
 responsibility for its use, or for any infringements on the rights of third parties that may result from its
 use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1.	Introduction	6
	Overview	6
	Package Checklist	7
	NPort 6150-G2 and NPort 6250-G2	7
2.	Getting Started	8
	Panel Layout	8
	NPort 6150-G2	8
	NPort 6250-G2	9
	Connecting the Hardware	9
	Wiring Requirements	9
	Powering the NPort 6100-G2/6200-G2	10
	LED Indicators	11
	Pin Assignments of the Serial Ports	11
	Mounting Options	12
	Connecting to the Network	13
3.	First-time Setup	14
	Find the Device	14
	Search Device	15
	First-time login with Device Search Utility	15
	Unlock	17
	Assign IP	17
	COM Mapping	20
	Console	21
	Locate	21
	First Time Login Process	21
4.	Mapping COM Ports	25
	Mapping COM Ports on Windows Platforms	25
	Mapping COM Ports With Real COM Mode	25
	Mapping COM Ports with Reverse Real COM Mode	27
	Mapping COM Ports on Linux Platforms	28
	Mapping TTY Ports	29
	Removing Mapped TTY Ports	29
	Removing Linux Driver Files	29
	Mapping COM Ports on macOS Platforms	30
	Installing macOS TTY Driver Files	30
	Mapping macOS TTY Port	33
	Uninstalling the macOS Driver	35
	Mapping COM Ports on UNIX-Like Platforms	36
	Installing the UNIX Fixed TTY Driver	36
_	Configuring the UNIX Driver	37
5.	Cybersecurity Considerations	38
		38
	Turn Off Unused Service and Ports	38
	Turn On Services That Are Necessary	39
		40
	Account and Password	40
	System Log	40
	Testing the Coswity Environment	
6	Management Consoles	41 43
0.	Configuration Ontions	
	Device Search Iltility	ر بالمنا ۲۵
	Web Console	ر ب د ۸
	Serial Console	ر ب د ۱
7.	Configuration with the Web Console	
	Factory Default IP Address	
	Using Your Web Browser	
	Opening the Web Console	45

	Web Console Navigation	47
	Dashboard Introduction	48
	System Settings	49
	General	49
	Notification	51
	SNMP Agent	56
	Network Settings	58
	IP Address	58
	Routing Table	61
	Hosts & WINS	63
	Serial Port Settings	64
	Operation Modes	
	Serial Darameters	110
	Serial Falameters	122
		124
	Security	. 124
		. 126
		. 126
	Login Settings	. 128
	Account Management	. 129
	Accounts	. 129
	Groups	. 131
	Password Policy	. 134
	Authentication Server	. 135
	Maintenance	. 136
	Config. Import/Export	. 136
	Firmware Upgrade	. 137
	Reset to Default	. 139
	Restart	. 139
	Diagnostics	. 139
	Support	. 140
	System Log	. 142
	Operation Mode Statistics	. 145
	Network Monitor	148
	Ping	149
	Traffic Monitor	149
8	Mass Denloyment/Maintenance	151
0.	Mass Configuration With GUI Tool: Device Search Utility v3.0 or Newer	151
	Import/Export Configuration	151
	Import / Export Configuration	152
	Firmware Ungrade	152
	Firmware Opyrade	. 155
	Mass Configuration with CLI tool: MCC 1001	. 153
	Import/Export Configuration	. 153
	Firmware Upgrade	. 155
•	Change Password	. 155
9.	Advanced Settings of NPort windows Driver Manager	.15/
	Configure the mapped COM ports	. 15/
	Change the number of a mapped COM port	. 15/
	COM Splitting	. 158
	Advanced Setting	. 160
	Security	. 162
	Importing/Exporting COM mapping	. 163
	Port Sniffer Wizard	. 164
10.	Frequently Asked Questions	.172
	Q1. If I disable the Web console, how can I change the settings?	. 172
	Q2. Can different users use the same account to log in to the device server?	. 172
	Q3. Why Device Search Utility v3.0 and later cannot be executed on my Windows 7 or Windows 2008 R2?	. 172
	Q4. How can I check the CRC value of the runtime settings?	. 173
	Q5. Is there an easier way to copy the settings of a NPort 6000 device server to a NPort 6000-G2?	. 173
	Q6. If there is a power outage during a firmware upgrade, how can I recover the device?	. 173
	Q7. Before calling Moxa customer service, is there anything I can prepare to save both of us time?	. 173

Α.	Pinouts and Cable Wiring	
	Cable Wiring Diagrams	
	Ethernet Cables	
	Serial Cables	
в.	Accessory Introduction	
	Convert the DB9 Connector to Other Connectors	
	Selecting Suitable Power Adapter Depends on the Environment	
C.	Well-known Port Numbers	
D.	SNMP MIB List	
	RFC1213 MIB-II Supported SNMP Variables	
	RFC1317 RS-232 Like Groups	
	Moxa-NP6000-G2-MIB	
Е.	Event List	
F.	Command List of the Serial Console	
G.	How to Become a Registered User	

By leveraging the IEC 62443-4-1 secure development life-cycle process, Moxa has created a new line of secure terminal servers. The NPort 6000-G2 Series secure terminal servers follow the IEC 62443-4-2 design and guidelines to connect your legacy serial devices to industrial networks securely. Furthermore, Moxa's 35 years of experience in serial-connectivity contributes to an enhanced user experience with flexible installation options and a convenient troubleshooting tool for maintenance.

The NPort 6000-G2 Series of secure serial device servers has many exceptional features. The NPort 6000-G2 Series includes a lineup of over 20 models. What distinguishes the models apart are the number of ports and the type of network connection they employ. The NPort 6000-G2 Series shares the same instructions and information across all its models. We will specify any variations between models. To learn more about the variations between models in the series, please refer to the Product Selection Chart section in this chapter.

Overview

The NPort 6000-G2 enables connection of serial devices to Ethernet networks and supports multiple operation modes. In particular, the NPort 6000-G2 has support for Secure Real COM, Secure TCP Server, Secure TCP Client, and Secure Pair Connection modes. This makes it ideal for security-critical applications like banking, telecom, access control, and remote site management. With these secure operation modes, you'll have access to supported protocols, authentication control, advanced data encryption, and more.

The NPort 6000-G2's Any Baudrate feature, which is based on Moxa's UART IC, allows the use of nonstandard baudrates. For example, some special applications may require a baudrate of 500 kbps. Most device servers can only support a baudrate of 460.8 kbps, leading to an error rate of 7.84%. The margin of error allowed for serial communication is just 3%. With the NPort 6000-G2, you can configure the baudrate more precisely and transmit serial data at a rate of 491.5 kbps. This is only a 1.7% margin of error, which is well within the acceptable margin for serial data.

Even when communication is disrupted, reliable data delivery is crucial for certain applications. The NPort 6000-G2 has an exceptional feature that buffers data in case of communication failure. In case of a communication failure, the NPort 6000-G2 stores the data. Upon resumption of communication, the buffered data will be sent to the destination. Each port has a default buffer size of 64 KB. Users can expand the buffer size for the NPort 6250-G2 with an external SD card.

Package Checklist

Each NPort 6000-G2 serial device server is packaged individually with various standard accessories. When you receive your shipment, please check the contents of the box carefully and notify your Moxa sales representative if any of the items are missing or appear to be damaged.

NPort 6150-G2 and NPort 6250-G2

The supported models of NPort 6150-G2 and NPort 6250-G2:

Model Name	No. of Ethernet Ports	No. of Serial Ports	SD Card Support	Power Supply Included	Operating Temperature
NPort 6150-G2	1	1	-	\checkmark	-10 to 60°C
NPort 6150-G2-T	1	1	-	-	-40 to 75°C
NPort 6250-G2	1	2	Up to 2 TB (high speed, 25 MB/s)	\checkmark	-10 to 60°C
NPort 6250-G2-T	1	2	Up to 2 TB (high speed, 25 MB/s)	-	-40 to 75°C

Standard Accessories for the NPort 6150-G2 and NPort 6250-G2

- Quick installation guide (printed)
- Power adapter (standard temp. models only)
- 1 wall-mounting kit (WK-35-02)

This chapter covers the hardware installation of the NPort 6000-G2. The software installation is covered in the following chapters.

Panel Layout

NPort 6150-G2

Unit: mm (inch)













NPort 6250-G2

Unit: mm (inch)







Connecting the Hardware

This section describes how to connect the power supply to the NPort 6000-G2.

Wiring Requirements

ATTENTION

Disconnect the power before installing and wiring

Disconnect the power cord before installing and/or wiring your NPort 6000-G2.

Do not exceed the maximum current for the wiring

Determine the maximum possible current for each power wire and common wire. Adhere to electrical codes that dictate the maximum current allowed for each wire size.

If the current exceeds the maximum rating, the wiring could overheat, causing serious damage to your equipment.

Server may get hot; use caution when handling

Exercise caution when handling the NPort 6000-G2 after it has been plugged in. The internal components generate heat, and the casing may get too hot to touch.

You should also heed the following guidelines:

• 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.

- The type of signal transmitted through a wire should determine which wires should be kept separate. The rule of thumb is that wires sharing similar electrical characteristics may be bundled together.
- Keep input wiring and output wiring separately.
- It is good practice to label the wiring to all devices in the system.

Powering the NPort 6100-G2/6200-G2

Unbox the device server and power it up using the power adapter provided in the box. The position of the DC outlet on the device server is shown in the following figures:



NPort 6250-G2



If you are connecting the DC outlet to a DIN-rail power supply, you will need a separate power cable, CBL-PJ21NOPEN-BK-30 w/Nut, to convert the terminal block output to the DC outlet on the NPort 6100-G2/6200-G2.



The power cable CBL-PJ21NOPEN-BK-30

If you use a DIN-rail power supply or another vendor's power adapter, please make sure the ground pin is properly connected. The ground pin must be connected with the chassis ground of the rack or the system.

The Power (PWR) LED will change to green once the device is powered up. In a matter of seconds, the Ready LED will switch to green and a beep will sound, signifying that the device is ready. The behavior of the LED indicators is outlined below.

NPort 6150-G2





LED Indicators

LED Name LED Color LED Fu		LED Function
PWR	Green	Power is being supplied to the power input.
		Steady on: Power is on, and the NPort 6000-G2 is booting up.
	Red	Blinking: Showed an IP conflict occurs, or the DHCP or BOOTP server does not
Roady		respond properly.
Reduy	Croop	Steady on: Power is on, and the NPort 6000-G2 is functioning normally.
	Green	Blinking: The device server has been located by the NPort Search Utility.
	Off	Power is off, or there is a power error condition.
	Yellow	The serial port is receiving data.
P1, P2	Green	The serial port is transmitting data.
	Off	No data is being transmitted or received through the serial port.

The LED indicators on the front panel of the NPort 6000-G2 are described in the following table.

When the device is ready, connect an Ethernet cable to the NPort 6100-G2/6200-G2 directly with computer's Ethernet port or an Ethernet port of a switch.

To connect the serial device to the serial port of the NPort 6100-G2/6200-G2, follow the pin assignment below.

Pin Assignments of the Serial Ports

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

RS-232/422/485 pin assignment (male DB9):

The serial cables needed to connect the NPort 6100-G2/6200-G2 to a serial device can be purchased separately. Please refer to <u>Appendix A</u>.

Mounting Options

The NPort 6100-G2/6200-G2 device servers come with wall-mount kit, which can be used to mount the NPort to a wall or the inside of a cabinet. There are options to order a DIN-rail kit or side-mount kit separately for different placement.

The NPort 6100-G2/6200-G2 can be placed flat on a desktop or other horizontal surface. In addition, you may use the DIN-rail mount, wall-mount, or side-mount options (DIN-rail and side-mounting kits need to be ordered separately), as illustrated in the following diagrams.





Side Mounting



DIN-rail Mounting (metal) With Side-mounting Kit



The mounting kit packages include screws. However, if you prefer to buy your own, refer to the dimensions below:

- Wall-mounting kit screws: FMS M3 x 6 mm
- DIN-rail mounting kit screws: FTS M3 x 10.5 mm
- Side-mounting kit screws: FMS M3 x 6 mm
- Metal DIN-rail kit screws (on side-mount kit): FMS M3 x 5 mm

For attaching the device server to a wall or the inside of a cabinet, we recommend using a M3 screw with the following specifications:

- The head of the screw should be between 4 to 6.5 mm in diameter.
- The shaft should be 3.5 mm in diameter.
- The length should be longer than 5 mm.



Connecting to the Network

Connect one end of the Ethernet cable to the NPort 6000-G2's 10/100M Ethernet port and the other end of the cable to the Ethernet network.

If the cable is properly connected, the NPort 6000-G2 will show a valid connection to the Ethernet:

- The Ethernet LED glows solid green when connected to a 100 Mbps Ethernet network.
- The Ethernet LED glows solid orange when connected to a 10 Mbps Ethernet network.
- The Ethernet LED flashes when Ethernet packets are being transmitted or received.

LED Name	LED Color	LED Function
High speed of the D145	Croon	Steady on: The 100 Mbps Ethernet is connected
connector	Green	Blinking: The Ethernet packets are being transmitted or received
	Off	The 100 Mbps Ethernet is disconnected
Low around of the D14E	Vallaw	Steady on: The 10 Mbps Ethernet is connected
Low speed of the RJ45	renow	Blinking: The Ethernet packets are being transmitted or received
connector	Off	The 10 Mbps Ethernet is disconnected

The NPort 6000-G2 device server allows IP access to traditional serial devices (RS-232/422/485). The device server is a small computer with a CPU and TCP/IP protocols that can convert data between serial and Ethernet formats in both directions. With your computer, you can remotely control, manage, and configure facilities and equipment from any location in the world using the Internet.

Traditional SCADA and data collection systems rely on serial ports to collect data from various kinds of instruments. With the NPort 6000-G2, your SCADA and data collection system can access all instruments on a standard TCP/IP network, whether they are used locally or remotely, thanks to its compatibility with RS-232, RS-422, and RS-485 communication ports.

The NPort 6000-G2 is an external network device that adds more serial ports to a host computer as needed. If your host computer is TCP/IP protocol compatible, you won't be restricted by bus limitations or lack of drivers for a variety of operating systems.

To combat the rising number and complexity of cyberattacks, network device vendors are including protective functions to secure sensitive business and personal information. Thanks to our dedicated efforts, all Moxa products meet the security standard, allowing customers to use them worry-free.

To accomplish this, the services will be disabled until you set up the first username and password for the unit. The unit can only be configured and made functional using a web console (HTTPS) or Moxa service.

Find the Device

The default IP address of each NPort 6000-G2 Series is https://192.168.127.254. Directly input the IP address at the address bar of a browser to open the web console to set up the first username and password. Or download the **Device Search Utility (DSU) v3.0** and search for the device to access its web console.

	evice Search U	tility					G	D 🌣
Search Dev	ice 🗸				c 2 ~	© ~	P ~	
Please click s	earch device butt	ton					귶	: :
Seq.		Model	Lan1 IPv4	Lan1 MAC	Firmware Version			
No Devices								
				Items	per page: 10 👻 0 of 0	<	$\langle \rangle$	>1

DSU is a handy tool for easily finding NPort device servers and deploying single or multiple devices. DSU v3.0 functions as a web-based application that works on Chrome, Firefox and (Microsoft) Edge.

To use the web-based application DSU v3.0, your browser version and operating system must meet certain minimum requirements:

- Chrome:
 - > For Windows 7, 8/8.1, Server 2012 and Server 2012 R2: Chrome 109 and newer
 - > For Windows 10 and newer, Server 2016 and newer: All Chrome versions
- Firefox:

> For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions

- Edge:
 - > For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions

NOTE

For detailed instruction of how to use **DSU**, please download the user manual from moxa.com.

Search Device



When connecting the NPort device server to the network, the DSU's **Search Device** function for him to find the target NPort device server. Searching can be done in three different ways. To see the options, click on the pull-down menu:

Search	Default button action. It will search the devices by multicasting.
Search by IP	Search the device by a specific IP
Search by IP range	Search the device in a certain IP range; the search results will only display the corresponding IP type. For example, if you search by IPv4, only IPv4 values will be displayed.

Search Device	~			
Searching ••• Devic	e(s) found, or y	ou can press	STOP	to abort.

It's possible to stop the search at any stage of the process. A **STOP** button appears on top of the table; click it to halt the search and keep the already searched devices on the list.

The default search time is 10 seconds. DSU will continue searching until time runs out. If your device(s) does not appear, you may change the search timeout limit in **Preferences > Device Search > Timeout limit for device searching**, to give the network a bit more time to respond.

First-time login with Device Search Utility

To address cybersecurity concerns, the NPort device server found through DSU will prompt for an account name and password during the first login.

MOXA [®] Device Set	arch Utility			
Search Device 🗸				2 🖸
Please select device(s)				
🗆 No. 🔒	Device Name	Model Name	Lan1 IPv4	Lan1 MAC
🗆 1 🔒	NP54501_4850	NPort 5450I	192.168.1.222	00:90:E8:9A:E0:BF
🗆 2 1 🔂	NP6250_15731	NPort 6250	192.168.127.254	00:90:E8:7D:8D:AD
🗆 з 🛕	NP6150_15012	NPort 6150	192.168.127.254	00:90:E8:61:50:12
				Items per page: 10 💌

Please select the target device $\hat{\mathbf{0}}$ and click the unlock button $\hat{\mathbf{c}}$. The login window will remind you to set up the account name and password, and it will show the password minimum requirements as tips below the password field.

device, ne and pass	rst time to unlock the new eed to setup the account word.
Account	
moxa	
New Password	С С
Confirm Passwo	ord

Once you configure the first account and password successfully, the device may restart. After completing a new search, the lock icon will change to **Advance** type:

Please sele	ect device(s)					
No.	ê	Device Name	Model Name	Lan1 IPv4	Lan1 MAC	Firmw
1	Â	NP5450I_4850	NPort 5450I	192.168.1.222	00:90:E8:9A:E0:BF	3.14
2	Â	NP6150_15012	NPort 6150	192.168.127.254	00:90:E8:61:50:12	2.2
3	Â	NP6250_15731	NPort 6250	192.168.127.254	00:90:E8:7D:8D:AD	2.2.2

If there is an error during the unlocking process, like entering the wrong password, you will be notified with an error message at the bottom right of the screen.



Unlock



When selecting one or multiple NPort device servers, use can click the **Unlock** button to unlock them. Because of different product series, there are four types of the login permission types:

	Login Permission Type	Definition
	Dofault	The device has not completed the first-time login process, which
D	Delault	requires setting the first account name and password.
_	Bacic	The device only has password protection; the login requires to input
В	Dasic	the password only.
_	Advance	The device has username and password protection; the login
Α	Auvance	requires inputting both account name and password.
÷	Legacy/Unlocked	The device is unlocked, or not requiring any protection to log in.

To unlock multiple devices at once, they must be of the same model name.

NOTE

The DSU solely facilitates unlocking the device; for account name or password changes, you must access the web console and find the Account Management function.

Assign IP



The device(s) needs to be unlocked before the Assign IP function can be used.

Assign IPv4 or IPv6 (if supported) for the device. Clicking the button will show you all the options under **Assign IP**:

- Assign IPv4
- Assign IPv6
- Assign IPv4 & IPv6

If your device does not support certain options, they will be disabled.

Assign IPv4

Mode: Static or DHCP

Click on the field of IP Address, Subnet Mask, Default Gateway - opt, to manually key in the values.

If you have selected multiple devices and the specific IP is not required for each device, you may consider using **ASSIGN IP SEQUENTIALLY** to quickly set up an IP. The function increments the IP address based on the IP value of the first device in the list.

3 Dev	rice(s)			ASSIGN IP SEQUENTIALLY
No.	Model Name & Mac	IP Address	Subnet Mask	Default Gateway - opt.
1	NPort 5450I 00:90:E8:9A:E0:BF	192.168.1.222	255.255.255.0	· · ·
2	NPort 5210A 00:90:E8:AD:45:6A	192.168.1.223	255.255.255.0	
3	NPort 5210A 00:90:E8:AD:45:10	192.168.1.224	255.255.255.0	

Clone "Network Mask" / "Default Gateway" to All Devices

This is a quick way to copy and paste Netmask or gateway values to all the selected devices. Edit **Subnet Mask** and **Default Gateway – Opt** of any device first, and find the options in the menu icon at the end of the list and apply:

No.	Model Name & Mac	IP Address	Subnet Mask	Default Gateway - opt.
1	NPort 54501 00:90:E8:9A:E0:BF	192.168.1.222	255.255.255.0	I
2	NPort 5210A	192.168.127.254	255.255.255.0	Clone "Network Mask" to all devices Clone "Default Gateway" to all devices
				KI.

Assign IPv6

Mode: Static or DHCP

Click on the field of **IP Address, Prefix, Default Gateway – opt**, to manually key in the values.

If you have selected multiple devices and specific IP is not required for each device, you may consider using **ASSIGN IP SEQUENTIALLY** to quickly set up an IP. The function increments the IP address based on the IP value of the first device in the list .

	IPv4	IPv6		
ode				
atic				
2 Dev	vice(s)			ASSIGN IP SEQUENTIALLY
No.	Model Name & Mac	IP Address	Prefix	Default Gateway - opt.
1	NPort 6150 00:90:E8:61:50:12	fe80::290:e8ff:fe61:5012	64	
	NPort 6250	fe80::290:e8ff:fe61:5013	64	

Clone "Network Mask" / "Default Gateway" to all devices

This is a quick way to copy and paste Prefix or gateway value to all the selected devices. Edit **Prefix** and **Default Gateway – Opt** of any device first, and find the options in the menu icon at the end of the list and apply:

	IPv4	IPv6		
ode				
atic				
2 Dev	vice(s)			ASSIGN IP SEQUENTIALLY
No.	Model Name & Mac	IP Address	Prefix	Default Gateway - opt.
1	NPort 6150 00:90:E8:61:50:12	fe80::290:e8ff:fe61:5012	64	
2	NPort 6250 00:90:E8:7D:8D:AD	fe80::290:e8ff:fe61:5013	64	Clone "Prefix" to all devices
				Clone "Default Gateway" to all devices

Apply the changes

After you have set everything, click **ASSIGN & RESTART** to restart your device(s) and set a new IP. DSU should display the result, whether it is successful or failed, in the **Status & Message** columns of each device.

Info: It may take a whil to end before performin	e to execute this process, plea ng other actions.	se wait for it		
Assigning IP and restart	ting for 3 device(s)			
Device Name	Model Name	Status	Message	Last Updated Time
NP54501_4850	NPort 5450I	C Progressing	Processing	Feb 06, 2024 14:41:35
NP5210A_8295	NPort 5210A	8 Failed	Session timeout. Please retry.	Feb 06, 2024 14:41:35
NP5210A_8205	NPort 5210A	 Success 	Success.	Feb 06, 2024 14:41:35
			Items per page	= 10 ▼ 1 - 3 of 3 <

COM Mapping

MOXA [®] De	vice Searc	h Utility					(i) 🌣
Search Device	2 V				c D	- ~	◊ · ℙ · Ⅲ
Please click sea	arc <mark>h</mark> device	button				(*)	Firmware Upgrade
Seq.	6	Model	Lan1 IPv4	Lan1 MAC	Firmware	Ś	Import Configuration
						è	Export Configuration
No Devices						Ģ	Import Certificate
				Items per page: 10	▼ 0 c	E	Allowlist
						IJ	Restart
						¢	Reset
							COM Mapping

After etting up the first user account, password and IP address, if the software to communicate with the

serial devices by opening a COM port/TTY port, you can click the **More functions** to find **COM Mapping** function for next step. Please refer to the <u>Chapter 4 Mapping COM Ports</u> for more information.

Console



When user wants to configure more detail settings, please click the **Console** button $\square \vee$ to connect to the HTTPS console of the NPort 6000-G2 Series.

For how to use web console for configuration, please refer to Chapter 7. Configuration with the Web Console

Locate

Device Search Utility			() ¢
Search Device V	o D	~ 📀 🗸	P ~	

You need to unlock the device before you can use the Locate function.

This is to locate the device by triggering the buzzer to help the user to find the target device server easily. Clicking the button would show all options of **Locate**. If your device does not support certain options, they will be disabled:

- Locate (IPv4)
- Locate (IPv6)

First Time Login Process

When user clicks the Console button at Device Search Utility or he inputs the default IP address, 192.168.127.254 to first time login to the web console of an NPort 6000-G2 series, there will be a first-time login wizard to guide him/her to initialize the device with setting up the first administrator and the network settings of this device.

When seeing this page, click on the **START** button to start the process.



If the user had an existing configuration file of an NPort 6000 or NPort 6000-G2, he/she can select the file and import it at the first step. Then the NPort 6000-G2 will be configured as the old unit he/she has and the wizard will directly jump to step 5 for the user to confirm if the settings are correct?



If the user doesn't have an existing configuration file, please click **SKIP** to skip this step.

The default IP address of NPort 6000-G2 series is 192.168.127.254/255.255.255.0. User can base on his network topology to modify it to DHCP or a different IP address. Please click **NEXT** to next step.

ΜΟΧΛ	IPv4 Settings
Import Configuration Optional	Configure the IPv4 settings of the device.
2 IPv4 Settings	IPv4 Address 192.168.127.254
3 IPv6 Settings Optional	Subnet Mask 255.255.255.0
(4) Create Account	IPv4 Gateway - optional
5 Confirmation	Customize IPv4 DNS Server
	< BACK NEXT >

The NPort 6000-G2 Series supports IPv6 networks. If your network environment uses IPv6, configure it at this step. If not, click **SKIP**.



As there is no default username/password for NPort 6000-G2 devices, please set up the first account of this unit. The first user of the device will have full privilege through this account. Keep the account name and password protected. A minimum of 8 characters is required for the default password complexity. The Password Policy function in the Account Management category allows you to change it.

ΜΟΧΛ	Create Account	
Import 1 Configuration	Create the first account of the device.	
Optional	Account Name admin	
✓ IPv4 Settings	Password •••••••	Ø
3 IPv6 Settings Optional	✓ Contains at least 8 characters	
4 Create Account	Confirm Password	Ś
	The value is required.	
5 Confirmation		
	< BACK	NEXT >

Double-check the network settings at the "Confirmation" step. If everything is OK, click the **SUBMIT** button and the unit will reboot, affecting the above settings.

ΜΟΧΛ	Confirmation
Import Configuration Optional	Please confirm your initial settings.
V IPv4 Settings	If you imported the configuration file or modified the network settings, the system will restart automatically.
IPv6 Settings	IPv4 Settings 🗸
Optional	
Create Account	
5 Confirmation	
	< BACK SUBMIT

Once you complete the initial login, you'll have various next steps to choose from:

- 1. Read <u>Chapter 5 Cybersecurity Considerations</u> for the recommendations from Moxa to securely using the NPort 6000-G2 device server.
- 2. For using Real COM mode users, refer to <u>Chapter 4 Mapping COM Ports</u> for more information.
- 3. For other operation mode users, refer to <u>Chapter 7 Configuration with Web Console</u> > <u>Operation Modes</u> for more introductions.
- 4. For other advanced settings, refer to <u>Chapter 7 Configuration with web Console</u> for more details.

A device server connects devices with RS-232, RS-422, or RS-485 serial interfaces to a local area network, allowing for serial data transmission over Ethernet. Device servers provide network access to connected devices by bridging a physically wired Ethernet network connection on one side and one or more serial ports on the other side, making them appear as if they were directly connected to the serial port. To achieve this, you may have to map a COM port on Windows or a Fixed TTY port on UNIX-like platforms. Once you've configured the IP address using the First-time Login Wizard (introduced in Chapter 3) and mapped the COM port settings, the device server is ready for use. This chapter provides instructions on how to install the driver and map a COM port.

Mapping COM Ports on Windows Platforms

Mapping COM Ports With Real COM Mode

Refer to the "<u>COM Mapping</u>" section in Chapter 3 function triggers the NPort Windows Driver Manager when clicked. Once the software is installed, you can immediately run the NPort Windows Driver Manager.



NOTE

Install Microsoft Visual C++ 2022 Redistributable to use COM mapping in NPort Windows Driver Manager.

<u>File</u>	<u>C</u> OM Mapping C <u>o</u>	nfiguration <u>V</u> iew <u>H</u> elp		
Exit	Add Rei	move Apply Undo Setting		
٩o	COM Port /	Address 1	Address 2	

1. Click the **Add** icon.

😵 NPort Windows Driver Manager	_	×
File COM Mapping Configuration View Help		
III IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		

 Click the Search button to search for NPort device servers. Select the server from the list to map the COM ports before clicking OK. When you enable the Mapping IPv6 COM Port option, the default IPv4 address will be replaced with an IPv6 address.

elect	Mapping IPv6 COM Port		Search	Select All	Clear All
No	Model	MAC 1	Address 1	MAC 2	Address 2

 Alternatively, you can select Input Manually and then manually enter the NPort IP Address, first Data Port, first Command Port, and Total Ports to which COM ports will be mapped. Click OK to proceed to the next step. Note the Add NPort page will automatically fill in the IP address field if a Fully Qualified Domain Name (FQDN) is used.

Mapping IPv6 COM Port			Search Select All Clear All			
No	Model	MAC 1	Address 1	MAC 2	Address 2	
-						
	Manually					
nput	rianaanj					
Rea	I COM Redundant COM	Reverse Real COM				
Rea	I COM Redundant COM	Reverse Real COM	First Mapp	ing Port		
Rea N	I COM Redundant COM	Reverse Real COM	First Mapp Data Port	ing Port 950		
Input Rea N	I COM Redundant COM	Reverse Real COM	First Mapp Data Port Command	ing Port 950 Port 966		

- 4. 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 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.
- 5. Activated ports will be displayed in black.

🐝 NF	😵 NPort Windows Driver Manager –						×	
<u>F</u> ile	<u>C</u> OM Mapping	Configuration <u>V</u> iew <u>H</u> elp)					
Exi	t Add	Remove Apply Undo	Setting					
No	COM Port	Δ	Address 1			Address 2		
1	COM9		192.168.1.222	950:966	(Port1)			
2	COM10		192.168.1.222	951:967	(Port2)			
3	COM11		192.168.1.222	952:968	(Port3)			
4	COM27		192.168.1.222	953:969	(Port4)			
5	COM28		192.168.1.201	950:966	(Port1)			
6	COM50		192.168.1.201	951:967	(Port2)			
7	COM51		192.168.127.254	950:966	(Port1)			
8	COM52		192.168.127.254	951:967	(Port2)			
9	COM53		00:90:e8:12:fa:42	(Port1)	. ,			

Mapping COM Ports with Reverse Real COM Mode

1. Click the **Add** icon.



2. Select the **Input Manually** checkbox and switch to the **Reverse Real COM** tab. Enter the NPort MAC Address, 1st Mapping Port Index, and Total Ports manually. Proceed to the next step by clicking **OK**.

MAC Address of NPort	
Total Ports 1	
,	
(The "Port Index" means the NPort serial port index. E.g., for a 32-port NPort, the port index should be 1~32.) (If your NPort is a dual-LAN model, please input the MAC address of LAN1.)	

Depending on your application, maybe only some ports will be set up for Reverse Real COM mode. Assign which ports of which NPorts will be mapped in Reverse RealCOM mode.

For example: If you want to map port 2 only for an NPort 6250-G2, the configuration will be as follows:

MAC Address of NPort	The MAC address of the NPort 6250-G2 for identification	00:90:E8:E8:F1:36
First Mapping Port Index	Index port 15	15
Total Ports	Only port 15 will be mapped, and the total number of ports should be 1	1

For example: If you want to map both port 1 and port 2 for an NPort 6250-G2, the configuration will be as follows:

MAC Address of NPort	The MAC address of the NPort 6250-G2 for identification	00:90:E8:E8:F1:36
First Mapping Port Index	Index port 1	1
Total Ports	The total number of ports should be 2	2

3. Activated ports t will be displayed in black.

🐝 NP	😻 NPort Windows Driver Manager						_	×
<u>F</u> ile	<u>C</u> OM Mapping	C <u>o</u> nfiguration <u>V</u> iew <u>H</u> el	p					
Exit	din Add	Remove Apply Undo	Setting					
No	COM Port	Δ	Address 1			Address 2		
1	COM9		192.168.1.222	950:966	(Port1)			
2	COM10		192.168.1.222	951:967	(Port2)			
3	COM11		192.168.1.222	952:968	(Port3)			
4	COM27		192.168.1.222	953:969	(Port4)			
5	COM28		192.168.1.201	950:966	(Port1)			
6	COM50		192.168.1.201	951:967	(Port2)			
7	COM51		192.168.127.254	950:966	(Port1)			
8	COM52		192 168 127 254	951-967	(Port2)			
9	COM53		00:90:e8:12:fa:42	(Port1)	` '			

4. For Reverse Real COM mode, assign the TCP port number for the Remote Host/Server. Click the Configuration tab to change the port number.

	😵 NPort Windows Driver Manager				_	- 🗆	×
	<u>F</u> ile <u>C</u> i	OM Mapping	Configuration View Help				
ľ	<u>i</u> ,	d.	Reverse Real COM	B			
	Exit Add Remove Apply Undo Setting						
	No	COM Port	Δ	Address 1	Address 2		

This is the TCP port number assignment for the remote host/server. It is the port number that the serial port of the NPort 6000 uses to establish the connections with Remote Host/Server. To avoid conflicts with well-known TCP ports, the default is set to 60950. Configure the mapped COM port.

Reverse Real COM Settings	×
Settings Please CLOSE all Reverse Real COM ports before modifing Otherwise, the setting will not be applied.	the value.
Listening Data Port 60950 (defa	ult:60950)
Listening Command Port 60966 (defa	ult:60966)
Apply the Settings	Cancel

Mapping COM Ports on Linux Platforms

Download the Real TTY Linux driver on Moxa website and install it. Remember to check the kernel version that is suitable for your host PC. Before installing it, make sure you've already configured the device server properly:

- The IP address of the device server must comply with the network topology. The default IP address of the NPort 6000-G2 Series is https://192.168.127.254. Please log in to the device and change its location to the same subnet of the host PC.
- Make sure the Operation Mode is Real COM mode. Once the first administration user is set up, the default Operation Mode is Real COM mode. You may not need to change this. If you have a device server that has been modified by others, it's a good idea to double-check it.

When the IP address and Operation Mode settings are confirmed:

- 1. Get the driver file from Moxa's website, [waiting for support address]
- 2. Log in to the console of the host PC 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 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)

You are ready to map the NPort serial ports to the system tty port

Mapping TTY Ports

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 command **mxaddsvr** is as follows:

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

The mxaddsvr command will perform the following actions:

- 1. Change npreal2d.cf.
- The **npreal2d.cf** is the configuration file of the driver.
- 2. Create tty ports in directory /dev with major & minor number configured in npreal2d.cf.
- 3. Restart the driver.

To map the tty ports with default settings, execute **mxaddsvr** with the IP address and the number of ports, as in the following example:

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

This example involves adding 16 tty ports, each with IP 192.168.3.4. The data ports will span from 950 to 965, while the command ports will go from 966 to 981.

To map the tty ports with preferred data ports and command ports, execute **mxaddsvr** with the following example:

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

This example involves adding 16 tty ports, each with IP 192.168.3.4. The data ports will span from 4001 to 4016, while the command ports will go from 966 to 981.

Removing Mapped TTY Ports

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. Change npreal2d.cf.
- 2. Remove the relevant tty ports in directory /dev.
- 3. Restart the driver.

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

Removing Linux Driver Files

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

- Unload the driver.
- Delete all files and directories in /usr/lib/npreal2
- Delete directory /usr/lib/npreal2
- Change the system initializing script file.

Mapping COM Ports on macOS Platforms

To map an NPort 6000-G2 serial port to a Mac host's tty port, follow these instructions:

- 1. Download the macOS driver from Moxa website and install the Mac driver files on the host.
- 2. Set up the NPort 6000-G2. Verify the IP configuration works by using ping, telnet, etc.
- 3. Search or manually input the IP address of the NPort to set up a virtual COM port.

Installing macOS TTY Driver Files



NOTE

For the newest information, please refer to readme.txt on Mac TTY Driver. Resources location of product information, release note, and readme file: /usr/local/share/NportConnect.

1. Get the driver file from Moxa's website, at https://www.moxa.com. It is in the Resource section under the product page.

• • •	😺 Install NPortConnect	
	Welcome to the NPortConnect Installer	
 Introduction License Destination Select Installation Type Installation Summary 	This will install NPortConnect pseudo-tty driver Ver 1.0 for NPort series on your Mac. You will be guided through the steps necessary to install this software. Click "Continue" to continue the setup	
ΜΟΧΛ	Go Back Continue	

2. Execute the installer package 'moxa-macOS-tty-drivers-for-macOS-10.12-or-later-v1.0.pkg'.



3. Press Continue when the Introduction window opens to proceed with installation.



4. Press **Continue** in the **Destination Select** window.

• • •	🥪 Install NPortConnect	
	Select a Destination	
 Introduction License 	How do you want to install this software?	
Destination SelectInstallation Type	Install for all users of this computer	
InstallationSummary		
	Installing this software requires 3.4 MB of space.	
MOXV	this computer.	
	Go Back Conti	nue

5. Click **Install** to start the installation in the default directory or select an alternative location.

	🔯 Install NPortConnect	
	Standard Install on "FPCMBP"	
 Introduction License Destination Select Installation Type Installation Summary 	This will take 3.4 MB of space on your computer. Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.	
ΜΟΧΛ	Change Install Location Go Back Install	

6. Key in your system login username and password to confirm the authentication.

	🥪 Install NPortConnect
	Standard Install on "FPCMBP"
 Introducti License Destinatio Installatio Summary 	Installer is trying to install new software. Enter your password to allow this. User Name: moxa Password: ••••• Cancel Install Software
мохл	Change Install Location Go Back Install

7. The installation window reports the progress of the installation.

0 0	🥪 Install NPortConnect	
	Installing NPortConnect	
 Introduction License Destination Select Installation Type Installation Summary 	Optimizing system for installed software	
ΜΟΧΛ	Go Back Continue	

8. Click **Close** to complete the installation of the NPort macOS tty driver.

0 0	🥪 Install NPortConnect	
 Introduction License Destination Select Installation Type Installation Summary 	 Install NPortConnect The installation was completed successfully. NPortConnect pseudo-tty driver for NPort series Thank you for installation. Now you can find and launch the NPortConnect service on Apple Status Bar near the upper right corner. Resources Location of product information, release note, and readme file: /usr/local/share/NPortConnect Go through following links for additional information. Moxa Inc. Uninstall NPortConnect pseudo-tty driver Run the following command to uninstall driver. 	
MOXA	<pre>\$ sudo bash /usr/local/share/NPortConnect/uninstall.sh Go Back Close</pre>	

Mapping macOS TTY Port

1. In the menu bar, a NPortConnect icon will appear after the installation is completed.

🚱 🔽 🕴 85% [≁] 奈 ◀))) 🛄 ∪.s. Thu Sep 10 10:08

2. Click on the **NPortConnect** icon and select **NPort Mapping** for the port mapping function.



3. Click on + Add to enter the tty port setup.

• •	0	NPortConnect	
+ Ada	d Remove		Apply
٩o	Name	Address	Port

4. Click Search to find the NPort already set up in the Hardware Setup procedure. The Search function broadcasts a search to locate NPort units on the LAN that are connected to your Mac. The Broadcast Search function searches by MAC address and not IP address. The location of all NPort units connected to the LAN will be determined, regardless of their subnet. Alternatively, you can manually enter the IP address to locate the specific NPort.

		Windo	W	
O Se	lect From List	Search	Select All	Clear All
No Model		MAC	Address	
	out Manually		First Mappi	ng Port
NPo	rt IP Address	192.168.127.254	Data Port	950
			Total Ports	1
			-	

5. Once the search is completed, all the NPort found will appear on the list.

 Se 	lect From List	Search	Select	All	Clear All
٧o	Model	MAC		Address	
1	NPort 5110A NPort 5450	A 00:90:E8: 00:90:E8:	51:72:90 48:F3:30	192.168 192.168	.127.254 .127.254
	out Manually		Fi	rst Mappin	g Port

6. Select the model types that are for the tty port mapping and click **OK**.

O Se	lect From List	Search	Select A	MI	Clear All
No	Model	MAC		Addres	5
1	NPort 5110	A 00:90:E8	51:72:90	192.16	8.127.254
1 2	NPort 5450	00:90:E8	48:F3:30	192.16	8.127.254
	out Manually		-		ing Deat
	out Manually	102 168 127 254	Fir	st Mapp Ita Port	ing Port
	out Manually rt IP Address	192.168.127.254	Fir Da	st Mapp Ita Port	ing Port 950
O Ing	out Manually rt IP Address	192.168.127.254	Fir Da To	st Mapp Ita Port tal Ports	ing Port 950

7. NPortConnect auto assigns the tty name and corresponding port number to the IP address of the selected NPort.

• •		NPortConnect	
+ Ade	d Remove		Apply
No	Name	Address	Port
1	ttys001	192.168.127.254	950
2	ttys002	192.168.127.254	951
3	ttys003	192.168.127.254	952
4	ttys004	192.168.127.254	953

8. The tty name and port number are editable. Note these changed values are only for mapping configuration and would not change the values in the NPort settings.

Add	i Remove		Apply
No	Name	Address	Port
1	ttys001_Moxa	192.168.127.254	950
2	ttys002	192.168.127.254	951
3	ttys003	192.168.127.254	952
4	ttys004	192.168.127.254	953

9. When everything is set, click **Apply** to save the configuration.

		NPortConnect	
+ Ad	d Remove		Apply
No	Name	Address	Port
1	ttys001	192.168.127.254	950
2	ttys002	192.168.127.254	951
3	ttys003	192.168.127.254	952
4	ttys004	192.168.127.254	953

Uninstalling the macOS Driver

Run the following command to uninstall driver:

\$ sudo bash /usr/local/share/NPortConnect/uninstall.sh

Mapping COM Ports on UNIX-Like Platforms

NOTE

For the newest information, please refer to readme.txt on Fixed TTY Driver.

Installing the UNIX Fixed TTY Driver

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

mkdir -p /usr/etc

 Copy moxattyd.tar to the directory you created. If you created the /usr/etc directory above, 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

Change 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**. Use **vi** or any text editor to change 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.



ΝΟΤΕ

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

- Change the text file **moxattyd.cf** to add an additional server. Use **vi** or any text editor to change the file. For more configuration information, refer to 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 adding an additional server.

As cyberattacks increase and become more sophisticated, network device vendors are incorporating features to safeguard sensitive information. Moxa has made it a priority to develop measures that ensure all products meet security standards, so customers can use them with peace of mind. There are certain details that Moxa cannot do alone; customers and Moxa need to work together to build up a much-secured environment to defend against all kinds of cyberthreats. This chapter introduces the essential steps to enhance the cybersecurity of Moxa's products. Customers may need to refer to other sections in the user manual for the exact settings or commands.

Updating Firmware

Customers who buy products from Moxa or a reseller should be aware that Moxa might have already launched a newer firmware version with enhanced security features. Please check with Moxa's support website to see if there is a newer version of firmware. If so, we recommend upgrading the firmware to the newest.

Turn Off Unused Service and Ports

Imagine living in a house that has many entrances. If all the doors and windows are left unlocked or even open, it sends a message of welcoming to intruders out there. We always recommend turning off services and ports that are not in use to reduce the chances of being attacked.

Refer to the table below for all the ports, protocols and services that are provided to communicate between the NPort 6000-G2 Series and other devices.

Service Name	Option	Default Settings	Туре	Port Number	Description
Moxa services	Enable/ Disable	Enable	TCP UDP	443	For Moxa utility communication
DNS_wins	Enable	Enable	UDP	53, 137, 949	Processing DNS and WINS (client) data
SNMP agent	Enable/ Disable	Disable	UDP	161	SNMP handling routine
RIPD_PORT	Enable/ Disable	Disable	UDP	520, 521	Processing RIP routing data
HTTPS server	Enable/ Disable	Enable	ТСР	443	Secured web console
RADIUS	Enable/ Disable	Disable	UDP	1645 or 1812	Authentication server, the UDP port can be changed by user
TACACS+	Enable/ Disable	Disable	ТСР	49	Authentication server
DHCP client	Enable/ Disable	Disable	UDP	68	The DHCP client needs to get the system IP address from the DHCP server
SNTP	Enable/ Disable	Disable	UDP	Random port	Synchronize the time settings with a time server
Remote System Log	Enable/ Disable	Disable	UDP	Random port	Send the event log to a remote log server

Operation Mode	Option	Default Settings	Туре	Port Number
Real COM mode	Enable/ Disable	Disable (Changed to Enable after user set username/password)	тср	949 + (serial port number) 965 + (serial port number)
RFC2217 mode	Enable/ Disable	Disable	ТСР	4000 + (serial port number)
TCP Server mode	Enable/ Disable	Disable	ТСР	4000 + (serial port number) 965 + (serial port number)
UDP mode	Enable/ Disable	Disable	UDP	4000 + (serial port number)
Pair Connection Server mode	Enable/ Disable	Disable	тср	4000 + (serial port number)
Reverse Terminal – Telnet	Enable/ Disable	Disable	ТСР	4000 + (serial port number)
Reverse Terminal – SSH	Enable/ Disable	Disable	тср	4000 + (serial port number)
Disable mode	Enable/ Disable	Disable	N/A	N/A

Turn On Services That Are Necessary

Some services are recommended to be enabled because they are the key functions of the NPort 6000-G2, and they face cybersecurity threats. The communication of these services are encrypted on the Ethernet network.

- Web console (HTTPS): This is the major management console of the NPort 6000-G2 for configuring all the settings, and it also provides some diagnostic tools for an engineer to troubleshoot a problem.
- SNMPv3: The Simple Network Management Protocol is a popular tool for remote device monitoring and management. Enable SNMPv3 to encrypt communication data if needed.
- Moxa services (HTTPS): The Device Search Utility v3.0 is a good tool for first-time installation on the NPort 6000-G2 Series, and the Moxa MXview can easily monitor all the NPorts in a network. All these tools work with the Moxa services.
- Remote Syslog service: The system log is an important message for an engineer to analyze a problem. If the system has a central Log server, the NPort 6000-G2 supports syslog-ng to send the logs to the server securely.

ΝΟΤΕ

If all HTTP/HTTPS/Serial consoles are turned off, then there is no other route to access the product. The only way to recover it is to reset the device and start from the beginning. For guidance on resetting the device, refer to the user manual.

Limited IP Access

Limiting the number of IP addresses that can access the product is one of the most effective ways of blocking unwanted intruders. If the product is accessed by a limited number of desktop/notebook/mobile devices, provide access to those IPs.

The NPort 6000-G2 has the Allowlist function to grant an IP address or a range of devices to access the device server. You can **ADD RULE** for those granted IP addresses and then enable the Allowlist function to limit access to the specific NPort 6000-G2 only to those IP addresses.

Home > Security > Allowlist			
Allowlist			
Info All communications are only allowed for the enabled IPs o	n the list after enabling this allowlist.		
Allowlist			
lpv4 (0) lpv6 (0)			
			ADD RULE
No. IPv4 Address	Subnet Mask	Status	
No data to display. Click ADD RULE button to create	the first data.		

Account and Password

- There is no default username and password for NPort 6000-G2 devices. You may need to follow up the first-time login process to set the username and password for the first user (who will also be the admin user) of this device to enhance the device's security.
- Use strong passwords. The devices support a function called **Password Policy** to check if passwords are strong enough. Enable the function to help you check whether the passwords are strong enough.
- Use the account login failure lockout feature to prevent unwelcome access (Security > Login Settings > Login Lockout).
- For central management purposes, set up an authentication server in the network. The NPort 6000-G2 Series supports RADIUS and TACACS+ servers. Using an authentication server for account management can ease administrators' loads of repeatedly inputting the same account/password on multiple devices. Refer to Account Management > Authentication Server for more information.

System Log

The system log usually records all kinds of activities that are happening on your NPort, such as Login Fail, IP Changed, Password Changed, Config Changed, etc. Check the log regularly to examine any abnormal behavior.

For central management purposes, set up a log server in the network to collect all the logs from different devices. The NPort 6000-G2 Series supports syslog-ng protocol to deliver the logs securely to the log server. The events will be sent with the format defined by RFC3164 for the analyzer to read/analyze. Refer to **System Settings > Notifications > Channels Settings** for more information.

Deployment of the Device

Deploy the NPort 6000-G2 Series behind a secure firewall network that has sufficient security features in place to ensure that networks are safe from internal and external threats.

Make sure that the physical protection of the NPort devices and/or the system meets the security needs of your application. Depending on the environment and the threat situation, the form of protection can vary significantly.



Testing the Security Environment

Besides these devices that support these protective functions, network managers can follow several recommendations to protect their network and devices.

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

- Testing tools for cybersecurity environment checks are available. Some may provide limited free use, for example, Nessus. These tools help identify probable security leaks in the environment.
- The device should be operated inside a secure network, protected by a firewall or router that blocks attacks via the Internet.
- Control access to the serial console as with any physical access to the device.
- Avoid using insecure services such as SNMPv1 or v2; the best way is to disable them completely.
- Limit the number of simultaneous web server sessions allowed. Periodically, change the passwords.
- Back up the configuration files periodically and check the CRC value of the run time settings 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 that you had already backed up the current configuration before returning it.



NOTE

DISCLAIMER: Please note that the above information and guide (the "information") are for your reference only. We do not guarantee a cyberthreat-free environment. These guidelines are to increase the security level to defend against cyberintrusions and do not guarantee that the above information will meet your specific requirements. The above information is provided "as-is", and we make no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance. If you' are looking to open COM port applications, you can follow the steps in the **First-time Setup** and **Mapping COM Port** chapters to complete the basic settings. The NPort 6000-G2 will work properly at the actual site. If you want to configure more advanced settings, like **Security** or **Account Management**, access the device with the different management consoles introduced in this chapter.

If you use other applications, finish the account and IP settings by **First-time Setup** process. There are more settings waiting for you. Access the device with different management consoles introduced in this chapter to complete the configuration.

Configuration Options

Device Search Utility

Configure your NPort 6000-G2 with the bundled Device Search Utility (DSU) v3.0 and above for Windows. When you find the NPort 6000-G2 with the default IP address 192.168.127.254 on DSU, set the username and password for the first user (it will also be the admin user) of this device to enhance the device security. Then **right-click** on the device to change the IP address for your network. Or, you can **double-click** on the device to directly open the Web console of the device for configuration.

Web Console

Configure your NPort 6000-G2 using a standard web browser. The web console is the default management console of the device we recommend. Besides special reasons, we suggest keeping it enabled—not only for the first-time installation but also for maintenance and troubleshooting.

Serial Console

The NPort 6000-G2 supports the serial console as the local access point through serial port 1 if there is no dedicated serial console port. The serial console port only supports basic settings like network settings to change the IP address or when the Ethernet LAN port cannot be logged in.

The following instructions and screenshots show how to enter the serial console using PComm Terminal Emulator, which is available free 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. Turn off the power to the NPort 6000-G2. Use a serial cable to connect the NPort 6000-G2's serial console port to your computer's male RS-232 serial port.
- 2. From the Windows desktop, select **Start > All Programs > PComm Lite > Terminal Emulator**.
- 3. The PComm Terminal Emulator window will appear. From the Port Manager menu, select **Open**, or simply click the **Open** icon as shown below:

🔁 PComm Terminal Emulator						
Profile Port Manager <u>H</u> elp						

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

- COM Options	
Ports :	COM1
Baud Rate :	19200 💌
Data Bits :	8
Parity :	None
Stop Bits :	1
- Flow Control	- Output State
RTS/CTS	DTR C ON C OFF
	RTS ON C OFF

- 5. From the Property window's Terminal page, select **ANSI** or **VT100** for **Terminal Type** and click **OK**.
- If you are using the NPort 6150-G2 or 6250-G2, hold down the grave accent key (`) while powering it up, as shown below. Note the grave accent key (sometimes called backwards apostrophe) is NOT the apostrophe key—it is the key usually found next to the number 1 key.



The NPort 6000-G2 will then automatically switch from data mode to console mode.

7. When you see the "Login:" message, enter the username and password. You will be prompted to the command line mode.



8. The serial console is a Command-line Interface. You may need to input commands to view or change the settings. Please find the <u>Appendix F Command List of the Serial Console</u> section for more details.

7. Configuration with the Web Console

To configure the NPort 6000-G2, the web console is the easiest method to use. With a standard web browser, you can effortlessly navigate through all settings and options. Once you've completed the **First-time Setup** or used DSU-G2 to configure a new IP address for an NPort 6000-G2, enter the new IP address to access the web console. This chapter covers the introduction of the web console and explores its configuration options.

Factory Default IP Address

The NPort 6000-G2 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 cannot ping a device with a private IP address from an outside Internet connection.

Using Your Web Browser

Opening the Web Console

Open your web browser and enter the IP address you've changed in the website address line. Press **ENTER** to load the page.

ΜΟΧΛ	
Log in to NPort 6250-G2_3456	
Account Name	
Password 🗞	
Forgot password ?	
LOG IN	
© 2024 Moxa Inc. All rights reserved.	

You may find the "Not secure" icon on the website address line. Click it to add the NPort as a trusted device to remove the icon. For more information, refer to the **Security Hardening Guide**. Enter the account name and password you've set to access the device.



ATTENTION

In case of a forgotten password, the reset button must be used to configure the NPort 6000-G2 by resetting all settings and loading the factory defaults. Even if you disabled the reset button in your NPort 6000-G2 configuration, you can still use it to restore factory defaults within the first minute of powering on the NPort 6000-G2.

Remember to back up your configuration by exporting it to a file. Importing the file to the NPort 6000-G2 will quickly restore your configuration. This will save time if you have forgotten the password and need to reload the factory defaults.

The NPort 6000-G2's web console will appear after logging in and you may receive the history messages including the **Login Message** (can be configured at **Security > Login Settings > Login Message**) and account login history.

E Dashboard	Home > Dashboard Dashboard								
> 3 ∰ System Settings									
> 👗 Network Settings	Device Information	System Operatio	ns	Network Operations					
> 🕅 Serial Port Settings	History Mossago			Device Address					
> 🦁 Security	Thistory Message	History Wessage							
> 🖻 Account Management	Hi admin I The latest successful login time is	Hi admin ! The latest successful login time is 2024-05-31 14:42:16 from 0.123.125.172.							
> 🚉 Maintenance	Mod 10.123.125.172.								
> 🙊 Diagnostics	Desc		CLOSE	LAN1 🗸 100MB FD					
	Serial Number SERIAL123456	Power Input1 🗸 🖡	ower on						
	MAC Address 00:90:E8:62:50:02 Firmware Version v1.0.0 Build 24053 102	SD Card O I	Undetected						
	System Log. Top 5 critical events within pas			VIEW MORE >					

Click the **CLOSE** button and the Dashboard page will be displayed.

	NPort 6250-G2		Header			Administrator admin
Dashboard	Home > Dashboard Dashboard					
> ﷺ System Settings						
> 🛔 Network Settings	Device Informatio	on	System Oper	rations	Network Operation	ons
➤ II Serial Port Settings			Time		Device Address	
> 🕑 Security		-	System Time 2 Uptime (2024-05-31T15:37:55) day 02h:41m:34s	IPv4 Address 10.123 IPv6 Address ::	.6.74
Account Management	100					
> 🚔 Maintenance	Model Name N Device Name N	Port 6250-G2 Port 6250-G2_3	System State		Running State	
> ® Diagnostics	45 Description Serial Number SE MAC Address 00 Firmware Version v1 10	56 ERIAL123456 0:90:E8:62:50:02 I.0.0 Build 24053 D2	CPU Usage Memory Usage Power Input1 SD Card	27% 8% ✓ Power on ○ Undetected	LANT 🗸 100MB FD	
Menu	System Log Top 5 cri	tical events within past	30 days	Main	\ \	/IEW MORE >
	Severity	Category	6	event Name	Timestamp	
	No critical events re	ecently.				
	Operation Mode	State			V	/IEW MORE >
	Port Operation	n Mode Conn	ection Status	Serial Parameters	Serial Error	rs (count)
	1 Real COM	vi ⊗Di	isconnected	RS-232, 19200, None, 8,	1 0	

The Header shows who is logged in to the device. Click the account to change your password or log out the web console.



Click the \equiv icon to hide or show the Navigation Panel.

≡	ΜΟΧΛ	NPort 6250-G2	≡	ΜΟΧΛ	١	NPort 6250-G2	
8	Home > Dashboard			Dashboard		Home > Dashboard	
> 류 > 聶	Device Informa	ition	> ::: : > 로 :	System Settings Network Settings		Device Informa	ation
> 🕡			> 01 s	Serial Port Settings			
> 🖗		and the second second	> 🔁 s	Security Account Management			
> 00	Model Name Device Name	NPort 6250-G2 NPort 6250-G2_3456	> 👘	Vaintenance		Model Name Device Name	NPort 6250-G2 NPort-6250-G2_3456
> 也	Serial Number MAC Address Firmware Version	SERIAL123456 00:90:E8:62:50:02 v1.0.0 Build 24053102	> - (Diagnostics		Description Serial Number MAC Address Firmware Version	 SERIAL123456 00:90:E8:62:50:44 v1.0.0 Build 24071808

How many categories you may see on the Navigation Panel depends on the privilege of the user group you belong to. The administrators will see all of them as in snapshot above.

Web Console Navigation

On the NPort 6000-G2 web console, the left panel is the navigation panel and contains an expandable menu tree for navigating among the various settings and categories. When you click on a menu item in the navigation panel, the main window will display the corresponding options for that item. Configuration changes can then be made in the main window.

Changes will take effect immediately except for the network-related settings. If users add or remove devices after the NPort is online, they would want the new settings to immediately take effect without needing to reboot the device. Support for this function is provided by the NPort 6000-G2 Series.

The IP address change for the NPort 6000-G2 is a separate issue. It may require notifying all network devices and updating their tables. To make the NPort 6000-G2 work after changing its IP address, a reboot is necessary.

Dashboard Introduction

NPort 6250-G2		Administrator admin
Home > Dashboard Dashboard		
Device Information	System Operations	Network Operations
Model NameNPort 6250-G2Device NameNPort 6250-G2DescriptionSerial NumberSERIAL123456MAC Address00:90:E8:62:50:02Firmware Versionv1.0.0 Build 2405102102	TimeSystem Time2024-05-31T15:37:55Uptime0 day 02h:41m:34sSystem StateCPU Usage2">2">2">2">2">2">2">2">2">2">2">2">2">	Device Address IPv4 Address 10.123.6.74 IPv6 Address ::
System Log Top 5 critical events with	in past 30 days	VIEW MORE >
Severity Catego	ory Event Name	Timestamp
No critical events recently.		
Operation Mode State		VIEW MORE >
Port Operation Mode	Connection Status Serial Parameters	Serial Errors (count)
1 Real COM	© Disconnected RS-232, 19200, None	e, 8, 1 0

When you access the web console of an NPort 6000-G2 device, it will take you to the Dashboard page to have an overview of the status of the unit. There are five sections:

Device Information: The section displays the basic/general information of the unit, including the Model Name, Serial Number, MAC address, and firmware version.

System Operations: This section displays some unique information about the unit, like when the device is powered up, the CPU, and memory usage.

Network Operations: In this section, it shows the network status of the unit. For example, the IP address and the Ethernet LAN speed.

System Log: You can check whether any critical events have happened since you last login to the device. It will remind if any abnormal events happened.

Operation Mode State: The key function of an NPort 6000-G2 device is to provide communication between serial port(s) and the Ethernet LAN port(s). You will find the Operation Modes of each serial port in this section, and you can check the status here to see if it works properly.

System Settings

The first category of the navigation panel is System Settings, which includes three parts. The General page has the Identity and Date & Time settings of the device. The Notification page has the system events, emails, and SNMP Trap/Inform settings. The SNMP Agent has the SNMP Agent settings, which will be needed if you want to get information or settings from the NPort 6000-G2 device via SNMP protocol.

General

Dashboard	Home > System Settings > General			
✓	Concrai			
• General	Identity Date & Time			
Notification	Device Name			
SNMP Agent	NPort-6250-G2_3456			
> 🛃 Network Settings	Description - optional			
> 🚺 Serial Port Settings				
> 😯 Security	<i>k</i>			
> 🖻 Account Management	SAVE			

Under the General page, the Identity tab provides the Device Name and Description column for you to identify which unit the NPort 6000-G2 is using.

Device Name: This is an optional free text field for your own use. It does not affect the operation of the NPort 6000-G2. It will be set as the Model Name of the device and the last 4 digits of the serial number. It helps differentiate one NPort 6000-G2 server from another.

Description: This is an optional free text field for your own use. It does not affect the operation of the NPort 6000-G2. It is useful for assigning or describing the location of an NPort 6000-G2. In a network environment of multiple servers, this can be a valuable aid when performing maintenance.

Home > System Sett	ngs ≯ General	
Identity	Date & Time	
Current Date 2024-07-2	And Time 2 11:16:56	EDIT
Time Zone (GMT+08:	00) Taipei	EDIT

The NPort 6000-G2 has a built-in Real-Time Clock for time calibration functions. To change the time, please switch to the Date & Time tab. Click the **EDIT** button to change the current date and time and the time zone.

The NPort 6000-G2 uses SNTP (RFC-1769) for auto time calibration. Enter a time server IP address or domain name in this optional field. Once the correct time server address is set, the NPort 6000-G2 will regularly request time information from the time server every 10 minutes.

Edit Date And 1	ime	
Mode Manual O Sy	nc with NTP server	
Date 07/22/2024		E
Hour 11	Minute : 17	Second : 29
		CANCEL SAVE

To change the time zone, please click the **EDIT** button and select the location of the device. It will adjust the time zone automatically.

Edit Time Zone		
Time Zone (GMT+08:00) Taipei		-
Enable daylight saving time by recurring		
	CANCEL	SAVE

If daylight saving time applies in the summer, enable the checkbox **Enable daylight saving time by recurring**.

0.00		10 001	ing time b	oy recu	rring			
offse 1	t (hour)							_
1								*
Sta	art/End	Date	9					
Fro	m							
Mo	onth		Week		Day		Hour	
Ja	n	•	First	•	Sun	•	0	•
То								
Mo	onth		Week		Day		Hour	
Ja	n	-	First	-	Sun	-	0	•

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

Offset		
Setting	Description	Factory Default
User adjustable hour	The clock should be set forward by the number of hours specified in the offset parameter.	1
Start Date		
Setting	Description	Factory Default
User adjustable date	The Start Date parameter allows users to enter the date that daylight saving time begins.	The Sunday of the First week of January
End Date		
Setting	Description	Factory Default
User adjustable date	The End Date parameter allows users to enter the date that daylight saving time ends.	The Sunday of the First week of January



ATTENTION

A risk of an explosion exists if the real-time clock battery is replaced with the wrong type!

The NPort 6000-G2's real-time clock is powered by a lithium battery. We strongly recommend that you do not attempt replacement of the lithium battery without help from a qualified Moxa support engineer. If you need to change the battery, please contact the Moxa RMA service team.

Notification

ome > System Settings > N	otification				
lotification					
elect the events and chan nd SNMP Trap/Inform is n	nels to receive not ecessary for it to f	tifications. Completing the function.	settings for Syslog	, Email,	
Events Settings 0 event(s) selected					EDIT
Channels Settings					
Syslog O Not configured	EDIT	Email ல Disabled	EDIT	SNMP Trap/Inform O Not configured	EDIT
> More Information		> More Information		> More Information	

Notification sSettings allow you to customize events that are logged by the NPort 6000-G2. Events are grouped into five categories, known as event groups. Select which groups or events you want to log on on the **Remote Log** server. An email or SNMP Trap/Inform can also notify the administrator immediately of some of the events.

By default, the NPort will enable the event severity as Notice, Warning, and Error under the Security category and save them on the local flash memory. For the local log settings, find the diagnostics section. If you have a central management log server, configure the relative settings under **System Settings** > **Notification**.

Local Log	Keep the log in the flash of NPort 6000-G2 up to 10,000 items.	
	Keep the log in the remote defined Log Server.	
Remote Log	You will need to assign a remote Log Server in the System Management/Misc.	
	Network Settings/Remote Log Settings if a remote log is checked.	

The Categories of Notifications

Category	Description	
System	The events related to the NPort itself, like firmware ready.	
Network	The events related to the Ethernet interface, for example, the Ethernet link up.	
Security The events which may be considered security related; the administrator may need to out why it happened. For example, a Login fail event.		
Maintenance The events which usually happen at maintenance process, for example, firmware upg		
Serial The events related to the serial interface(s), for example, Port connect.		

The Severity of Events

Based on RFC5424, the severity of different events is categorized according to the following priority and description.

Priority	Severity	Description
1	Error	Events that indicate problems, but in a category that does not require immediate attention.
2	Warning	Events that provide forewarning of potential problems and indicate that some further actions could result in a critical error.
3	Notice	Events that are not error conditions, but that may require special handling.
4	Informational Confirmation that the program works as expected.	

The logs are essential for troubleshooting in case of errors. Refer to Appendix E for a detailed event list.

Event Settings

SEARCH
seray

When clicking the **EDIT** button of the **Events Settings** column, you will see the event list, separated into different categories. Click the checkbox to enable the event for Syslog, Email, SNMP Trap/Inform, or the Relay function. Only the enabled events will be recorded on the Syslog or trigger an email, SNMP Trap/Inform, or Relay output.

 System (13)	Network (7)	Security (15)	Mainte	nance (7)	Serial (8)	
Severity 🌲	Event Name		Syslog	Email	SNMP Trap/Inform	🗆 Relay
Informational	Ethernet link	up	~			
Notice	Ethernet link	down		\checkmark		

Channels Settings

Once you choose which events to record, set up the recording location and decide on email, SNMP Trap/Inform, or Relay for immediate notification.

Home > Systen ← Syste	n Settings > Notification > Syslog DG		
Syslog S	Add Server		+ ADD SERVER
There is no :	Port		
	Enable TLS authentication If TLS authentication is enabled, server auth import the CA certificate for server authentik Certificate for TLS	entication is required. Please ation.	
	Info For client authentication, please go to export the system certificate of the de permission for the page, please contac	Security > Certificate and vice. If your account has no tt your administrator.	
	CA Certificate No file	CHOOSE FILE	
		CANCEL SAVE	

Click the **EDIT** button at Syslog column. Input the remote log server's IP address and port to receive the events from the NPort. You can also enable the TLS authentication and import a CA certificate to secure the communication for the log recording.

Email

Home > System Settings > Notification > Email ← Email
Enable SMTP service
Sever Settings
Server Address
TCP Port 25
Enable secure connection Enable authentication
Contact Information
Sender Email (From)
Recipient Email (up to 4 Emails)
Recipient Email 1 (To)
+ Add Email
SAVE

Click the **EDIT** button in the Email column. You can enable the SMTP service so that the NPort will send an email if the selected events happen.

Server Settings

Setting	Description	Factory Default
Server Address	The IP address or domain name of the SMTP server.	N/A
TCP port	The TCP port to which the SMTP server receives SMTP	25
TCF port	messages.	25

Enable secure connection	
Secure Connection Type	_
TLS	
STARTTLS STARTTLS-None	

If the SMTP server requires a secure connection (encrypt the email), click **Enable secure connection**. There are three options.

Setting	Description	Factory Default
	Encrypts the entire communication channel between the	
TLS	client and the server from the beginning, ensuring that all	N/A
	data transmitted is secure.	
	It is possible to start the connection in plain text and then	
STARTTLS	switch to encrypted mode through STARTTLS. If the	N/A
	upgrade fails, the communication remains in plain text.	
	No encryption. STARTTLS-None as an option helps system	
STARTTLS-None	administrators clearly specify which connections should	N/A
	remain unencrypted.	

Enable authentication	
Username	
Password	
	Ø

If the SMTP server requires authentication verification, click **Enable authentication**, and input the username and password used to log into the SMTP server.

Setting	Description	Factory Default
Username	The name used to log into the SMTP server.	N/A
Password	The password used to log into the SMTP server.	N/A

Contact Information				
Setting	Description	Factory Default		
Sender Email (From)	The email address that the NPort will use to send the message. The user can easily figure out which NPort sends the message by this account.	N/A		
Recipient Email 1 (To)	The email address that the NPort will send the message to. It shall be the administrator/manager of the NPort who manages/monitors the status of the NPort or the serial device connected to the NPort. There are 4 recipient emails at most.	N/A		

SNMP Trap/Inform

Home > System S	ettings > Notification > SN P Trap/Inform				
SNMP Trap	/Inform Server				+ ADD SERVER
There is no St	IMP Trap/Inform server. (lick + ADD SERVER	button to cre	ate one.	
	Add Server				
	Server Settings	SNMP Settings			
	Server Address				
	UDP Port				
	162				
			CANCEL	SAVE	

Click the **EDIT** button at SNMP Trap/Inform column and click **ADD SERVER**. Set the Server Setting and the SNMP Settings.

Server Settings

Setting	Description	Factory Default
Server Address	The IP address or domain name of the SNMP server.	N/A
UDP port	The UDP port to which the SNMP server receives SMTP messages.	162

SNMP Settings

A	dd Server				
	Server Settings	SNMP Settings			
	SNMP Type Select One				•
	SNMP Version Select One				-
			C/	ANCEL	SAVE

SNMP Type	Description	Retry (Count)	Timeout (sec)	SNMP version
Trap	The NPort will send SNMP Trap and will not wait for acknowledgment	N/A	N/A	v1/v2c/v3
Inform	After sending an SNMP Inform, the NPort waits for the acknowledgment. The NPort will resend the Inform message until it gets a confirmation or times out.	Number of retries Default=3	The duration before a timeout occurs Default=5	v2c/v3

SNMP Inform messages requires acknowledgement of notifications. If you choose SNMP Inform as the SNMP type, you might have to specify the number of retries the NPort should attempt if it doesn't receive acknowledgments. Also, determine the time interval for the NPort to wait before sending the SNMP Inform message.

Ser	ver Settings	SNMP Settings	
SNN Info	ЛР Туре orm		•
	Retry (count) 3		
	Timeout (sec) 5		

SNMP Agent

Simple Network Management Protocol (SNMP) is a widely used protocol/tool for network administrators to manage and monitor network devices. To meet this requirement, the NPort 6000-G2 Series supports SNMPv1/v2c/v3 and includes a private MIB for device management and status monitoring of Ethernet or serial communication. For such purposes, enable the SNMP Agent service here (**System Settings > SNMP Agent**) and configure the proper settings introduced in the following sections.

Home > System Settings > S	SNMP Agent				
SNMP Agent servic	ce ect the SNMP version an	d fulfill the relev	ant configurations below.		
General SNMP v3					EDIT
Contact: Location:					
V3 Account V3 A	Account Protection				
					CREATE
Account Name	Authority	Status	Authentication Type	Privacy Type	
Set up at least one ac	count to make the servi	ice work. Click	CREATE button to create the a	account.	

Click the **EDIT** button under the General column. Select the SNMP Version and set the Device Details.

Setting	Description	Factory Default		
SNMP Vorsion	Select the SNMP Version.	v3		
SININF VEISION	Use only SNMP v3/Use only v1, v2c/Use v1, v2c, and v3.			
Contact - Ontional	This field usually includes an emergency contact name and	N/A		
	telephone or pager number.			
	Use this field to specify the location string for SNMP agents			
Location - Optional	such as the NPort 6000-G2. This string is usually set to the	N/A		
	street address where the NPort 6000-G2 is physically located.			

When using SNMP v3, you need to create a V3 Account first. Click the **CREATE** button at V3 Account column.

C	reate Account			×	
A	ccount Name				
A	uthority				
R	ead Only		•		
~	Enable account authentication				
	Authentication Type Select One		•		
	Authentication Password		Ø		
	Enable account privacy			1	
	Privacy Type Select One		•		,
		CANCEL	SAVE		
					-

Account Name: Use this field to identify the username for the specified level of access.

Authority: Select authentication parameters for two levels of access: Read Only(default) and Read/Write.

When enabling account authentication, select the Authentication Type and input the Authentication Password.

Authentication Type: Use this field to select MD5 or SHA as the method of password encryption.

Authentication Password: Use this field to set the password.

Privacy Type: Use this field to enable DES_CBC or AES_128 data encryption when you enable account privacy.

	V3 Account Protection
To enhance the and privacy pass	ecurity of the v3 accounts, set the minimum password length for authenticatio words.
Min. Password Le	ngth
To prevent hack v3 account prot	ers from repeatedly logging into your account to crack passwords, you can enal action and configure the settings accordingly.
Max. Auther	tication Failure Retry(times)
Enable i	eset login failure counter
Enable I The login recalcula reset per	eset login failure counter failure counter will reset and be ted according to your designated od.
Enable i The login recalcula reset per Reset P 10	eset login failure counter failure counter will reset and be ted according to your designated od. eriod(min)
Enable r The login recalcula reset per Reset P 10	eset login failure counter failure counter will reset and be ted according to your designated od. eriod(min) e (min)

Click the V3 Account Protection to set the minimum password length for authentication and privacy passwords. Enable v3 account protection can set the maximum authentication failure times and lockout time. Additionally, you can enable the reset login failure counter to automatically reset and recalculate it within your designated reset period.

Network Settings

The second category of the Navigation Panel is Network Settings, which also includes three parts. The IP Address page is where you assign the NPort 6000-G2 IP address, netmask, gateway, and other IP parameters. The Routing Table page allows you to configure the NPort 6000-G2's connection to an external network. The Hosts & amp; WINS page can make entering IP addresses on the NPort 6000-G2 console easier by assigning a Host Name to an IP Address.

IP Address

A network device will need an IP address to communicate with other network devices. The IP address should have already been set up during the first-time login process. When accessing the Network Settings category, you may want to configure the advanced settings or change the existing IP address.

	NPort 6250-G2
Dashboard	Home > Network Settings > IP Address
> ﷺ System Settings	
🗸 🛔 Network Settings	IPv4 and IPv6
IP Address	IPv4 Address
Routing Table	Get IP from
Hosts & WINS	Manual 👻
> 🐧 Serial Port Settings	IPv4 Address
> 😯 Security	10.90.60.63
> 🖻 Account Management	Subnet Mask
> 🚉 Maintenance	255.255.254.0
> 🛞 Diagnostics	IPv4 Gateway - Optional
	10.90.60.1

Network Configuration

Network Configuration	
IPv4	-
IPv4	
IPv4 and IPv6	

IPv6 Address

The abbreviation IPv6 stands for Internet Protocol version 6. IPv6 is the second version of the Internet Protocol, introduced after IPv4. What distinguishes the two versions is the varying length of the IP address. IPv4 uses 32-bit IP addresses; IPv6 uses 128-bit IP addresses. IPv4 is still the most widely used protocol on the Internet. If your devices and network infrastructure are limited to IPv4 compatibility, opt for IPv4 only. However, if you have already deployed IPv6 and need a large number of IP addresses, then select IPv4 and IPv6.

IPv4 Address

Get IP From: DHCP or Manual. If there is a DHCP server in the network assigns the IP address automatically, then select **DHCP**. If not, select **Manual** and input the IPv4 address, subnet mask, and IPv4 gateway.

IPv4	Address
Get	IP From
Ma	nual 👻
DH	СР
Ma	nual
-	10.90.60.63
	Subnet Mask
	255.255.254.0
	IPv4 Gateway - optional
	10.90.60.1

IPv4 Address (default=192.168.127.254): Enter the IP address that will be assigned to your NPort 6000-G2. All ports on the NPort 6000-G2 will share this IP address. An IP address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IP address to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your network environment.

Subnet Mask (default=255.255.255.0): Enter the subnet mask. A subnet mask represents all the network hosts at one geographic location, in one building, or on the same local area network. When a packet is sent out over the network, the NPort 6000-G2 will use the subnet mask to check if 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 6000-G2, the NPort 6000 establishes a connection directly. Otherwise, the connection is established through the default gateway.

IPv4 Gateway: Enter the IP address of the gateway if applicable. A gateway is a network computer or device that acts as an entrance to another network. Usually, the devices that control traffic within the network or at the local Internet service provider are gateway nodes. The NPort 6000-G2 needs to know the IP address of the default gateway device to communicate with the hosts outside the local network environment. For correct gateway IP address information, consult the network administrator.

IPv6	Address
Get	IP From
Ma	nual 🔻
Au	to
Ma	inual
	Prefix
	ID-C Catavara anti-
	IPV6 Gateway - optional

IPv6 Address

Get IP From: You can choose from two possible IP configuration modes, Auto or Manual.

Option	Description
Auto	IPv6 router assigned prefix
	Step 1: The NPort generates the Link local address automatically
	Step 2: The NPort sends the "Router solicitation" to the router to apply for an IP address.
	2.1 Router assigns an IP address to NPort ->Step 4
	2.2 Router assigns the DHCPv6 Server to offer an IP address \rightarrow Step3
	2.3 Router has no response (e.g., router does not exist) \rightarrow Step 3

Option	Description					
	Step 3. The NPort applies for an IP address from the DHCPv6 Server					
	Step 4. Process closed					
Manual	User-defined IPv6 address, Prefix, IPv6 Gateway.					

IPv6 Address: Enter the IPv6 address that will be assigned to your NPort 6000-G2. All ports on the NPort 6000-G2 will share this IPv6 address. An IPv6 address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IPv6 address to identify and talk to each other over the network. Choose a proper IPv6 address that is unique and valid in your network environment.

Prefix: The prefix is the part of the address that shows the bits that have fixed values or are the bits of the subnet prefix. Prefixes for IPv6 subnets, routes, and address ranges are expressed in the same way as Classless Inter-Domain Routing (CIDR) notation for IPv4. An IPv6 prefix is written in address/prefix-length notation. For example, 21DA:D3::/48 and 21DA:D3:0:2F3B::/64 are IPv6 address prefixes.

DNS Server

DN:	DNS Server			
	Customize DNS server			
	DNS Server 1			
	DNS Server 2 - optional			

Domain Name System (DNS) is responsible for translating internet domain names into IP addresses. A domain name is an alphanumeric name, such as www.moxa.com, which is easier to remember than the numerical IP address. A DNS server is a host that translates this kind of text-based domain name into the actual IP address used to establish a TCP/IP connection. When a user wishes to access a specific website, their computer sends the domain name (e.g., moxa.com) to a DNS server to obtain the website's IP address. The user's computer connects to the website's web server using the IP address obtained from the DNS server.

The NPort 6000-G2 acts as a DNS client, actively querying the DNS server for domain name IP addresses. The following functions on the NPort 6000-G2 web console support the use of domain names in place of IP addresses: Time Server, Destination IP Address (in TCP Client mode), Mail Server, SNMP Trap Server, Destination Address (in Pair Connection mode), Primary/Secondary Host Address (in Terminal mode), RADIUS Server, TACACS+ Server and SMTP Server.

DNS server 1: Choose Customize DNS server to enter the DNS server's IP address in this field. This allows the NPort 6000-G2 to use domain names instead of IP addresses to access hosts.

DNS server 2: This is an optional field. The IP address of another DNS server can be entered in this field if DNS server 1 is unavailable.

Default Address Selection

Default Address Selection				
When resolving domains using custom DNS server settings or DHCP, this setting specifies the preferred IP version.				
Connection Priority				
● IPv6 first				
O IPv4 first				

Connection Priority: This function should work with the NPort 6000-G2 functions that use the domain name to get the IP address of the remote host/server. For this kind of application, the NPort 6000-G2 will ask for the IP address of the remote host/server through the DNS. The DNS will reply with both the IPv4 and IPv6 IP addresses if both exist simultaneously in the remote host/server. For this reason, you need to define which one has a higher priority, IPv6 first (RFC 3484) or IPv4 first.

Routing Table

If the NPort encounters an unknown IP address, it will check the routing table to determine the network interface for sending the Ethernet package. This is how network devices collaborate to ensure all Ethernet packets reach the target devices. The routing table in the NPort contains information about network routes and their associated metrics, for example, distances. The **routing table** also provides information about immediate network topology. You can configure the network connection for the NPort 6000-G2 to an outside network. Edit the route settings and view the current routing status on this page.

Home > Network Settings > Routing Table Routing Table									
Edit the route settings and view the current routing status in the table below. Refer to the definition of the flags.									
Route Settings									EDIT
Refresh every 10 sea	conds								
Destination 🌲	Subnet Mask	*	Gateway 🌲	Source Protocol	÷	Flags 🌲	Metrics ≑	Use 🌲	Interface 🌲

To edit route settings, click the **EDIT** button.

Route Settings-Static

← Ro	ute Settings				
Statio	Dynamic				
					CREATE
No	Destination 🌲	Subnet Mask 🌲	Gateway 🌲	Metric 🌻	Interface 🌲
No dat	ta to display.				

In the static page, click the **CREAT** button to create a routing entry. You must provide information on the Destination, Subnet Mask, Gateway, Metric, and Interface.

Create Routing Entry

Create Routing Entry	
Destination	
Subnet Mask	
Gateway	
Metric 10	
Interface	
Select One	•
	CANCEL SAVE

Destination: This is the target device's IP address of the route's destination.

Subnet Mask: This is the destination network's netmask.

Gateway: This is the IP address of the next-hop router.

Metric: You may use this optional field to enter the number of hops from the source to the destination. This allows the NPort 6000-G2 to prioritize the routing of data packets if more than one router is available.

Interface: This is the network interface to which the packet must be sent. Select the Ethernet or serial port (Only for dial-in/out mode).

Route Settings-Dynamic

Home > Network Settings > Routing Table > Route Settings ← Route Settings				
Static	Dynamic			
🗹 Enable dyn	amic routing pro	tocol		
Protocol Select One 🗸				
RIP 1 RIP 1 con S/ RIP 2	npatible			

On the Dynamic page, you can configure the routing protocol. Select **Enable dynamic routing protocol** to choose the protocol.

What is RIP?

Routing Information Protocol (RI) is a protocol used to manage routing information within a self-contained network, such as a corporate LAN (Local Area Network) or an interconnected group of such LANs. By using RIP, a gateway host with a router can send its entire routing table, which lists all the other hosts it knows about, to its closest host every 30 seconds. The closest host will pass this information on to its neighbor, and so on, until all the hosts within the network have the same routing path information. We call this state network convergence. RIP uses a hop count as a way of determining network distance. (Other protocols use more sophisticated algorithms that also include timing.) After receiving a packet headed for a specific destination, a network host with a router uses the routing table information to determine the next host to route the packet to.

RIP 1 is an effective solution for small homogeneous networks. For larger, more complicated networks, transmitting the entire routing table every 30 seconds can bog down the network with a lot of extra traffic.

RIP 2 is an extension of RIP. Its purpose is to expand the amount of useful information in RIP packets and to add security elements. RIP 2 has become the standard version of RIP, and the original RIP is no longer used.

RIP 1 compatible refers to RIP 2 running in a mode that is compatible with RIP 1, but with the limited functionality of RIP 1.

Hosts & WINS

It's hard for people to remember a lot of IP addresses to access different devices for different services. So, people tried to remember the popular devices with domain names, like www.google.com. A DNS server is a well-known service/device to translate the domain name and the IP address. In a small network, to build up a private DNS server may be too expensive. Another option is to configure the Host Table on all network devices, allowing users to access them by simply entering the domain name. The NPort 6000-G2 provides a Host Table to fulfill this need in a small network.

Hosts & WINS			
The application will first get th server and WINS.	ne IP address by domain name from t	the host table, then from the DNS	
Host Table WINS			
			CREATE
No.	Hostname	IP Address	
No data to display. Click	CREATE button to create the er	ntry.	

Host Table

The Host Table simplifies IP address entry on the NPort 6000-G2 console by assigning a host name to a host IP address. When you assign a host name to a host IP address, you use the host name for some fields on the console rather than entering the IP address.

Click the CREATE. Then fill in Hostname and IP Address to assign a host name to a host IP address.

Create Entry			
Hostname			
IP Address			
	CANCEL SAVE		

WINS

Basically, Windows Internet Name Service (WINS) is a legacy computer name registration and resolution service that maps computer NetBIOS names to IP addresses.

Hosts & WINS	
The application will first get the IP address by domain name from the host table, then from the DNS server and WINS.	
Host Table WINS	
Enable WINS to let the device self-respond to hostname queries and find IP addresses. The default mode is "broadcast", but it can be set to "hybrid" for initial unicast queries to a specified WINS server.	
WINS service	
WINS Mode Broadcast	EDIT

WINS service: Activate WINS service to allow the device to respond to host name queries and find IP addresses. The initial mode is "broadcast" by default, but it can be edited to "hybrid" for unicast queries to a specified WINS server.

Edi	t WINS Mode		
мо Ну	^{de} brid		•
	WINS Server		
		CANCEL	SAVE

WINS server: If a WINS Server is connected to the network, enter the WINS Server's IP address in this field. TCP/IP uses IP addresses to identify hosts, but users often use symbolic names, such as computer names. The WINS Server, which uses NetBIOS over TCP/IP, contains a dynamic database to map computer names to IP addresses.

Serial Port Settings

The third section of the Navigation Panel is Serial Port Settings which is grouped into three categories: Operation Modes, Serial Parameters, and Secure Connection. To configure the operation mode and settings for a port, expand Serial Port Configurations in the navigation panel; then, expand the category that you would like to configure.

Operation Modes

NPort 6000-G2 Series provides the capability to transfer the data from serial-to-Ethernet and vice versa. The setting of the Operation Modes sets the way how the data was packaged or how it is delivered on the Ethernet network. There are five popular applications: COM-based Control, Socket, Pair Connection, Connect Console and Connect Modem Application, They will be introduced one-by-one in the following sections.

- COM-based Control: For software using a COM port (Windows) or TTY port (Linux) to communicate with the serial device.
- Socket: For socket programs which communicate with NPort with IP address and TCP/UDP port.
- Pair Connection: To extend communication distance without changes to the host PC/HMI and serial device. This requires two NPort devices.
- Connect Console: For accessing a serial console via Telnet or SSH.
- Connect Modem: For accessing a serial modem.

Dashboard	Home >	Serial Port Sett	ings > Operation Modes			
	Ope	Operation Modes				
▶ 荘 System Settings	Select p	ort(s) and clic	k "CONFIGURE" to configure the operation r	mode settings.		
> 👗 Network Settings	Refer to the instructions for the operation modes.					
✓ ↓ Serial Port Settings						CONFIGURE
Operation Modes		_				
Serial Parameters		Port	Application	Operation Mode	Role	
Secure Connection	>	I 1	COM-based Control	Real COM	Server	:
> 🕑 Security	>	□ 2	COM-based Control	Real COM	Server	:
> 🖻 Account Management						
>P Maintenance						
> @ Diagnostics						

Select **Operation Modes** in the navigation panel to configure the mode for each serial port. For NPort 6000-G2 models with two or more serial ports, use the checkboxes of the Port to apply the settings to one or more ports. Then, click the **CONFIGURE** button.

 Serial Port Settings > Operation Configure Port(s) 	Modes > Configure Port(s)		
1 Mode Selection	2 Basic Settings	3 Advanced Settings	4 Confirmation
First, select the application, then cl	hoose the operation mode that suits your n	eeds.	
Application Select One	•		
No Operation			
COM-based Control			
Socket			
Pair Connection			
Connect Console			
Connect Modem			
			CANCEL

There is an Operation Mode Wizard to help you complete the settings. Select the application and operation mode as the first step. The next step involves configuring the basic settings for various scenarios. Set the advanced settings for a few scenarios during the third step. During the final step, go over all the settings mentioned earlier. If they're okay, confirm them and these settings will be activated immediately.

Application: Select an application for the serial port from among the choices. Your application will determine the modes that are available.

Operation Mode: Once you have chosen an application, select the operation mode. The configuration settings will vary depending on the mode that you have selected.

Application	Operation Mode	Description
No Operation	N/A	To decrease the risk of cyberattacks, select "No Operation" to disable the relative service if there are no serial devices connected to a specific port.
	Real COM mode	Installs the Moxa driver to simulate a real COM port over the network.
COM-based Control	RFC2217 mode	Installs a third-party driver to simulate a real COM port over the network.
	Reverse Real COM mode	Installs the Moxa driver to simulate a real COM port over the private/dynamic network of the NPort.
	TCP Server mode	Your application establishes a TCP connection to the NPort, providing access to connected serial devices.
Socket	TCP Client mode	Your application listens to TCP connections from the NPort, providing access to connected serial devices.
	UDP mode	Your application sends and receives UDP packets for establishing communication with connected serial devices.
Pair Connection	Pair Connection Client mode	Connects to another NPort to enable two serial devices to communicate with each other.
	Pair Connection Server mode	Accepts connected NPort to enable two serial devices to communicate with each other.
Connect Concolo	Terminal mode	Connects to remote Telnet/SSH server by connecting the NPort via serial port.
Connect Console	Reverse Terminal mode	Your application establishes a TCP connection to the NPort, providing access to connected serial devices. Your application listens to TCP connections from the NPort, providing access to connected serial devices. Your application sends and receives UDP packets for establishing communication with connected serial devices. Connects to another NPort to enable two serial devices to communicate with each other. Accepts connected NPort to enable two serial devices to communicate with each other. Connects to remote Telnet/SSH server by connecting the NPort via serial port. Connects to a serial console server by connecting the NPort via Telnet/SSH. Enables network data exchange by establishing a PPP connection over PSTN using a modem
Connect Modern	РРР	Enables network data exchange by establishing a PPP connection over PSTN using a modem.
	SLIP	Enables network data exchange by establishing a SLIP connection over PSTN using a modem.

COM-based Control Applications

The COM-based control application requires the installation of a Moxa or third-party driver to open a COM port (on Windows platform) or a TTY port (on Linux/UNIX-like platform) to start the communication with the remote serial devices. To keep the legacy software on the Windows or Linux/UNIX-like platform the same, Moxa provides the drivers on different operating systems. Please download them from Moxa website and refer to <u>Chapter 4 Mapping COM Ports</u>, on how to use them.

Real COM Mode

Home > Serial Port Settings > Operation M	lodes > Configure Port(s)		
(configure rond(s)			
1 Mode Selection	2 Basic Settings	3 Advanced Settings	4 Confirmation
First, select the application, then ch	oose the operation mode that suits your	needs.	×
Application COM-based Control	•		
Info The operation modes require the serial devices. Download the Mo	e installation of a Moxa or third-party dri xa driver from the product page <u>Moxa of</u>	ver to control remote ficial website ^[2] -	
Operation Mode			
Install the Moxa driver to simulate network.	a real COM port over the		
Host PC	NPort	Serial Device	
(Reque	ICP/IP	2/422/485 — 🔊	•
			CANCEL NEXT >

Step 1. Mode Selection

Based on the scenario, selectthe application COM-based Control and Operation Mode Real COM. Then, click **NEXT** button to proceed to the next step.

Home > Serial Port Settings > Operation Modes > Configure Port(s)			
← Configure Port(s)			
3			
✓ Mode Selection	2 Basic Settings	Advanced Settings	Confirmation
No basic settings for Real COM mode. Please click "NEXT" to p	proceed to the next step.		
¢ BACK			CANCEL NEXT >

Step 2. Basic Settings

In most scenarios, when configuring the Operation Mode to the Real COM mode, you have already completed the setup. Real COM mode does not have any basic settings. Click the **NEXT** button to go to Step 3.

Step 3. Advanced Settings—Connection Settings

In some scenarios, you may need to change the advanced settings to fulfill these special cases.

Home > Serial Port Settings > Operat ← Configure Port(s	tion Modes > Configure Port(s)			
J (,			
Mode Selection	Basic Settings	3 Advanced	Settings 4	Confirmation
Advanced settings can general	lly be used with default values. Custo	omize the settings if needed.		
Connection Settings	Data Transmission Settings			
Max. Connection				
1	*			
Enable TCP alive check				
Allow the NPort to reset the receiving of the last TCP pa	e TCP session by checking the cket until the check time timeout.			- 11
Check Time (min)				
/				
Enable port buffering				
To prevent loss of serial dat disconnection, enable this t means that RTS/DTR will als	ta during an Ethernet function. Enabling port buffering ways be set to on.			*
< BACK			CANC	EL NEXT >

To communicate with multiple hosts on the NPort, enable **Max. Connection** and set the number to match the number of hosts. The NPort will now allow multiple hosts to connect at the same time. For example, let's suppose Host 1 is the primary computer, responsible for sending requests and receiving responses, while Host 2 is the backup computer, designated solely for receiving responses. Then, you should set the number to 2.

Connection Settings	Data Transmission Settings	
Max. Connection		
2	.	
Enable NPort to acc the serial port settin	ept commands from hosts to adjust igs.	
Connection Process		
	all hosts 👻	
Send serial data to		
Send serial data to	ling①	

Max. connection (default=1): 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 6000-G2, and the Real COM driver on that host will have full control over the port.

When the value is set to 2 or higher, multiple hosts' Real COM drivers can simultaneously open this port, up to the specified number. When several hosts' Real COM drivers open the port simultaneously, the COM driver only acts as a pure data tunnel and lacks control functionality. The serial port parameters will use firmware settings instead of depending on your application program (AP).

The firmware will only send data back to the driver on the host. When the data is received on the serial port and passed to the Ethernet side of the NPort, all the hosts will receive the same data. When the data is received on the Ethernet port and passed to the serial side of the NPort, the data will be sent first-in firstout.

If the situation described above doesn't match your site, there are several advanced functions at **Multiple Connection Settings** to do some modifications.

Allow driver control: As mentioned above, when **Max. connection** is set to 2 or higher, the serial port parameters will use firmware settings. If you want the serial parameters to still use the settings of your application program, enable the **Allow driver control** function. When you enable it, the serial port settings of your AP will overwrite the firmware settings while opening the COM port. Usually, you should only enable this function on one of the hosts. If you enable it on two or more hosts, then the serial parameters will be overwritten every time these hosts open the COM port.

To handle the unexpected data communication of multiple connections, there are different combinations for different scenarios.

Connection Control	Congestion Handling	Description
	-	This is the default data communication behavior for multiple connections. The serial data will be transmitted to the hosts. What happens if one host cannot receive the data?
Send serial data to all hosts	Wait until transmission succeeds	Wait until the host can receive data again. If the host cannot return, this option will store the serial data in the NPort's serial buffer as a side-effect. Once the serial data reaches 1,024 bytes, the buffer becomes full and can no longer receive data. Any new incoming data will be discarded.
	Keep sending data to other hosts	Ignore the abnormal host, keep sending data to other online hosts. The downside of this option is the communication seems OK when the user only checks the status on the succeed host(s). A mechanism might be necessary to alert the user when a host is unable to receive data.
	-	At times, the other hosts are unable to handle unrequested responses. In this scenario, choose to Send serial data to the requested host , ensuring that each host only receives the response specific to their request. What happens if the serial device fails to respond or responds too slowly in this situation?
	Discard	If the serial response times out, then the NPort will discard all the new incoming serial data before the NPort receives an Ethernet request.
Send serial data to the requested host	Send to the last request	If the serial response times out and new serial data arrives, the NPort will forward the data to the host that made the most recent request.
	Send to all open connections	If the serial response times out and new serial data is received, the NPort will distribute the data to all hosts that are still connected.
	Enable response timeout	To ensure smooth operation in this one-request-one-response application, you should specify the waiting time for the NPort to receive the serial response. The default timeout time is 10,000 ms. This value shall be less than the timeout time on user's AP. Make sure this value is smaller than the AP's timeout time. If not, this unusual situation could occur where AP identifies it as a timeout error, but the NPort is still waiting for a response.

Enable TCP alive check

Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.

Check Time (min) **7**

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort 6000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort 6000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort 6000-G2 will terminate the TCP connection.



Poor cable contact or a damaged switch/router could cause it to be disconnected or broken. When this happens, the serial data cannot transmit over Ethernet because the receiver does not exist. As time passes, the serial data could be discarded and lost. If the serial data is important, u enable the Enable port buffering function. The NPort can store serial data either in its internal memory, which is 64 Kbytes, or in an external SD card (if supported).

Enable port buffering (default=No): To prevent serial data loss when the Ethernet connection is down, check the checkbox to enable port buffering. If you enable port buffering, RTS/DTR will remain in the on position.

Buffering Location: Select the location of buffering. Memory (64K) or SD card.



In a serial bus, the host and the serial device can use RTS/DTR signals to indicate their status to each other. Using the RTS/DTR Behavior function, the NPort can simulate the RTS/DTR behavior on Ethernet connections. When using legacy software, enable the RTS/DTR signal and keep it constantly on to prevent the host from entering sleep mode or shutting down. This will ensure the host is always ready for communication.

RTS/DTR Behavior (default=always on): Configures what happens to the RTS and DTR signals when the TCP session is disconnected. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent via the serial port. If the serial devices detect the RTS or DTR is off, it may jump into sleeping mode or low-power mode. Then, it may take a while to come back from the sleeping/low-power mode, which will cause issues because the host PC will come back quicker. In this case, set the signal to always on.

When the Enable port buffering function is enabled, the RTS and DTS signals will be always be set to ON to keep the serial device sending data. This function may be disabled at the same time.

Step 3. Advanced Settings—Data Transmission Settings

When the serial data is transmitted on the serial bus, it's continuous data. A "Read" command allows the software to receive all of the data. When everything switches to Ethernet, it's a different story. Ethernet data can be divided into packets, which are then assembled by the receiver into a complete frame to interpret the transmission request from the other device. However, a legacy serial software might lack support for the fundamental "assemble" function found in socket programs. Here, the NPort enables the Data Transmission function to deliver the correct frame at the beginning, requiring no changes to the legacy serial software for reading accurate data.

🗸 Mo	ode Selection	Basic Setti	ngs	3 Advanced Settings
Advanc	ed settings can gene	rally be used with default values.	Customize the settings if nee	eded.
Con	nection Settings	Data Transmission Settings		
∠ E S	nable data packing pecify the packing and	sending of serial data to the host.		
	Packing Method Select One	•		
	Packet length			
	Delimiter (hex)			
As	llow the packaging and pecified force transmit t	transmission of serial data until the ime is met.		

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the **Enable data packing** function.

Enable data packing: With the drop-down menu Packing Method, select Packet length or Delimiter (hex).

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When you specify a packet length between 1 and 1024 bytes, the data in the buffer will be sent as soon as it reaches the specified length.

Connec	tion Settings	Data Transmission Settings
🗹 Enab	le data packing	
Speci	fy the packing and s	ending of serial data to the host.
Pac	king Method	
De	imiter (hex)	*
	Delimiter 1	
	0× 0	
	Delimiter 2 - Optio	nal
	0x	
Dat	a Transmit Process	
۲	Default process	
\sim	Send data with delir	miter characters.
0	Delimiter + 1 byte	e mitor characters and following 1
	byte.	initer characters and following i
0	Delimiter + 2 byte	es
	Send data with delir bytes.	miter characters and following 2
0	Strip delimiter	
	Send data without d	delimiter characters.

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data. Then, send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: If Delimiter 1 is configured in hex format, the NPort will treat the designated character as the end character. If there are two ending characters, use Delimiter 2 and ensure they are received in the correct order (Delimiter 1 first, then Delimiter 2). The NPort will package all the data in the serial buffer and follow the Data Transmit Process to handle the delimiter(s) before transmitting the data to the Ethernet port.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

- **Default process:** Data in the buffer and the delimiter(s) will be transmitted.
- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two bytes will be transmitted after two additional bytes are received following the delimiter.
- Strip delimiter: Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time (ms)** field.



Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

Home > Serial Port Settings > Operation Modes > Conf	igure Port(s)		
← Configure Port(s)			
Mode Selection	Basic Settings	Advanced Settings	4 Confirmation
Selected Port: 1			
And looking COM based Control			
Application: COM-based Control			
Operation wode: RealCOM			
Info			
Confirm that Moxa driver has been installed.	You may download it from the product page.		
Moxa official website@			
Connection Settings			
Max. Connection: 2			
Allow driver control: Disabled			
Connection Process: Send serial data to the requester	d host		
Non-requested Data Handling: Discard			
Response Timeout: Disabled			
TCP Alive Check: Enabled			
Check Time: 7 mins			
Port Buffering: Enabled			
Buffering Location: Memory (64K)			
RTS Always On: Enabled			
DTR Always On: Enabled			
Data Transmission Settings			
Data Packing: Disabled			
Force Transmit: Disabled			
. BACK			CANCEL
C DAUN			CANCEL

RFC2217 Mode

If you prefer a virtual COM driver or have different brands of serial device servers, install a third-party driver to communicate with the NPort and with all the other brands of device servers. In this case, please select the RFC2217 mode.

Step 1. Mode Selection

Select the COM-based control and select RFC2217 mode.

Home > Se	nial Port Settings > Op	eration Modes > Configur t(S)	e Port(s)		
1 M	ode Selection	2	Basic Settings –		3 Advanced Settings
Ri In	FC2217 stall the third-party dri etwork.	ver to simulate a real COM	port over the		
	Host PC		NPort		Serial Device
	Third-party driver	RFC2217 (Request connection from Host PC)	NPort	— RS-232/422/485 —	• : :::•

Step 2. Basic Settings

Home > Serial Port Settings > Operation I	Modes > Configure Port(s))	
← Configure Port(s)			
Mode Selection	2 Basic Se	ettings	3 Advanced Settings
RFC2217 Server Settings			
Assign TCP port starting from	4001	to selected port(s).	

Assign TCP port starting from: This is the TCP port number assignment for the serial port on the NPort 6000-G2. It is the port number that the serial port uses to listen. If more than two serial ports are configured as RFC2217 mode, the listen port will start from this assigned number (the first port will listen on TCP port 4001 and the second port will listen on TCP port 4002). For the host (or other network devices) this TCP port number is also the target TCP port for them to establish the TCP connection. To avoid conflicts with well-known TCP ports, set the default to 4001.

baaaced settings can generally be used with default values. Customize the settings if needed. Connection Setting Data Transmission Settings If challen CCP allve check Allow the North works that TCP sector until the check time timesout. Check Time (min) 7	Mode Selection		Basic Settings	Advanced Settings	4 Confirma
Connection Setting Data Transmission Settings Connection Setting Allow the Work Is event the TEP setsion by checking the needed uses time times. Check Time (min) Check Time (min) 7 T	ivanced settings can gene	erally be used with default values.	Customize the settings if needed.		
Fabile TCP allve check Allow the RPort to rest the TCP assion by checking the restwing of the same ICP passion with the check time timesu. Check Time (min) 7	Connection Settings	Data Transmission Settings			
Allow the NPCH to read the TCP assiss by clocking the receiving of the Intel Paralettic III of the Intel Paralettic III of the Intel III of the IIII of the IIIII of the IIIII of the IIIII of the IIII of the IIII of the III	Enable TCP allve chee	:k			
Check Time (min) 7	Allow the NPort to reset receiving of the last TCP	t the TCP session by checking the packet until the check time timeout.			
7	Check Time (min)				
	7				
Step 3. Advanced Settings—Connection Settings



Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the Enable TCP alive check time function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort 6000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort 6000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort 6000-G2 will terminate the TCP connection.

Step 3. Advanced Settings—Data Transmission Settings

When the serial data is transmitted on the serial bus, it's continuous data. A "Read" command allows the software to receive all of the data. When everything switches to Ethernet, it's a different story. Ethernet data can be divided into packets, which are then assembled by the receiver into a complete frame to interpret the transmission request from the other device. However, a legacy serial software might lack support for the fundamental "assemble" function found in socket programs. Here, the NPort enables the Data Transmission function to deliver the correct frame at the beginning, requiring no changes to the legacy serial software for reading accurate data.

Mode Selection	Basic Setti	ngs	3 Advanced Settings
Advanced settings can ger	nerally be used with default values.	Customize the settings if ne	eeded.
Connection Settings	Data Transmission Settings•		
Enable data packing Specify the packing an) Id sending of serial data to the host.		
Packing Method Select One	•		
Packet length		1	
Delimiter (hex)			
Allow the packaging a specified force transm	nd transmission of serial data until the it time is met.		

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the **Enable data packing** function.

Enable data packing: With the drop-down menu Packing Method, select **Packet length** or **Delimiter** (hex).

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When you specify a packet length between 1 and 1024 bytes, the data in the buffer will be sent as soon as it reaches the specified length.

Conne	Contraction Settings Data Transmission Settings
🗹 Ena	able data packing
Spe	cify the packing and sending of serial data to the host.
Pa	cking Method
D	elimiter (hex) 👻
	Delimiter 1
	0× 0
	Delimiter 2 - Optional
	0x
Da	ita Transmit Process
C	Default process
	Send data with delimiter characters.
C) Delimiter + 1 byte
	Send data with delimiter characters and following 1 byte.
C) Delimiter + 2 bytes
	Send data with delimiter characters and following 2 bytes.
C) Strip delimiter
	Send data without delimiter characters.

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data. Then, send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

Default process: Data in the buffer and the delimiter(s) will be transmitted.

- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- Delimiter+2 bytes: Data in the buffer and the delimiter(s) plus two bytes will be transmitted after two
 additional bytes are received following the delimiter.
- Strip delimiter: Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time (ms)** field..



Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

me > Serial Port Settings > Operation Modes > Config	jure Port(s)		
← Configure Port(s)			
Mode Selection	Basic Settings	Advanced Settings	4 Confirm
Selected Port: 1			
Application: COM-based Control Operation Mode: RFC2217			
Info Confirm that the third-party driver has been in	nstalled.		
RFC2217 Server Settings			
TCP Port: 4001			
Connection Settings			
TCP Alive Check: Enabled			
Check Time: 7 mins			
Data Transmission Settings			
Data Packing: Disabled			
Force Transmit: Disabled			
BACK			CANCEL

Reverse Real COM Mode

If the host PC and NPort are on separate networks, with potentially untrusted networks in between, a firewall/router might be present before the NPort to regulate which connections can access the internal/local network. The host PC might encounter difficulty connecting to the NPort in this scenario. By selecting Reverse Real COM mode, you can trigger the connection direction from NPort, which may bypass the firewall/router.

Reverse Real COM Install the Moxa driver to private/dynamic networ	o simulate a real COM po k of the NPort.	rt over the		
Host PC		NPort		Serial Device
	TCP/IP	NPort	— RS-232/422/485 —	• · ···••
Moxa driver	from the NPort)	Private/dynamic IP		

Step 1. Mode Selection

Mode Selection 2 Basic Settings 3 Advanced Settings Remote Host Settings Specify the host address to transmit data, and up to 10 sets of host can be added. Host 1 Destination Address Data Port Command Port 60950 60966 Assign local data port starting from 7010 incrementing by 10 to selected port(s). Assign local command port starting from 8010 incrementing by 10 to selected port(s). + ADD HOST

Select the COM-based Control and select Reverse Real COM mode.

Step 2. Basic Settings

Destination address: Specifying an IP address, domain name, or the name defined in the host table that the NPort 6000-G2 connects to.

Data Port: This is the target TCP port number that is assigned by the NPort Windows Driver Manager on the Remote Host/Server (refers to <u>Chapter 4 Mapping COM Ports</u>). To avoid conflicts with well-known TCP ports, set the default to 60950.

Command Port: This is the target TCP port number that is assigned by the NPort Windows Driver Manager on the Remote Host/Server (refers to <u>Chapter 4 Mapping COM Ports</u>). This port will be used for the communication commands, for example changing the RTS signal. To avoid conflicts with well-known TCP ports, set the default set 60966.

Assign local data port starting from: Use this field to specify the designated local data port on the NPort.

Assign local command port starting from: Use this field to specify the designated local command port on the NPort.

Mode Selection	Basic Settings	3 Advanced Settings	4 Confirmati
ivanced settings can generally be used with default values. C	ustomize the settings if needed.		
Connection Settings Data Transmission Settings			
Enable TCP alive check			
Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.			
Check Time (min) 7			
Enable port buffering To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.			
Buffering Location			
Memory (64K) -			
RTS/DTR Behavior			
If the port buffering is disabled, you may customize the RTS/DTR behaviors when TCP session is disconnected.			
RTS always on			
- 070			

Step 3. Advanced Settings—Connection Settings

Enable TCP alive check Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.	
Check Time (min) 7	

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the Enable TCP alive check time function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort 6000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort 6000-G2 sends keep-zalive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort 6000-G2 will terminate the TCP connection.

Step 3. Advanced Settings—Data Transmission Settings

When the serial data is transmitted on the serial bus, it's continuous data. A "Read" command allows the software to receive all of the data. When everything switches to Ethernet, it's a different story. Ethernet data can be divided into packets, which are then assembled by the receiver into a complete frame to interpret the transmission request from the other device. However, a legacy serial software might lack support for the fundamental "assemble" function found in socket programs. Here, the NPort enables the Data Transmission function to deliver the correct frame at the beginning, requiring no changes to the legacy serial software for reading accurate data.

🗸 Mo	ode Selection	Basic Setti	ngs	3 Advanced Settings
Advanc	ed settings can gene	rally be used with default values.	Customize the settings if nee	eded.
Con	nection Settings	Data Transmission Settings		
☑ E S	nable data packing	sending of serial data to the host.		
	Packing Method Select One	•		
	Packet length			
	Delimiter (hex)			
As	Now the packaging and pecified force transmit	transmission of serial data until the ime is met.		

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the **Enable data packing** function.

Enable data packing: With the drop-down menu Packing Method, select Packet length or Delimiter (hex).

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When you specify a packet length between 1 and 1024 bytes, the data in the buffer will be sent as soon as it reaches the specified length.

Connec	tion Settings	Data Transmission Settings
🗹 Enab	le data packing	
Spec	ify the packing and	sending of serial data to the host.
Pac	king Method	
De	limiter (hex)	*
	Delimiter 1	
	0× 0	
	Delimiter 2 - Opt	ional
	0x	
Dat	a Transmit Process	
۲	Default process	
\sim	Send data with de	limiter characters.
0	Delimiter + 1 by	te limitar characters and following 1
	byte.	initial characters and following i
0	Delimiter + 2 by	tes
	Send data with de bytes.	limiter characters and following 2
0	Strip delimiter	
	Send data without	t delimiter characters.

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data. Then send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: When Delimiter 1 is set up in hex format, the NPort will looking to the specific character and consider it as the ending character. If there are two ending characters, please set the Delimiter 2, these two delimiters will need to be received by the correct order (delimiter 1 first and then delimiter 2), then NPort will package all the data in the serial buffer and follow the Data Transmit Process to handle the delimiter(s) then transmit the data to the Ethernet port.

Data Transmit Process: This field determines how the serial data and the delimiter(s) is handled when the delimiter(s) is received. If Delimiters 1 and 2 are both set up, both characters must be received with the correct order then the process will take place.

- **Default process:** Data in the buffer and the delimiter(s) will be transmitted.
- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two byte will be transmitted after two additional bytes are received following the delimiter.
- Strip delimiter: Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time** (ms) field.

Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.Step 4 Confirmation

Please review and **SAVE** above settings to make them affective.

Home > Serial Port Settings > Operation Modes > Configure Po	lort(s)		
(Configure Fort(3)			
✓ Mode Selection	Basic Settings	Advanced Settings	4 Confirmation
Selected Port: 1			<u>.</u>
Application: COM-based Control			
Operation Mode: ReverseRealCOM			I
Info Confirm that Moxa driver has been installed. You m Moxa official website@	nay download it from the product page.		
- Remote Host Settings			
Host 1			
Destination Address: 10.5.9.123			
Data Port: 60950			
Command Port: 60966			
Local Data Port: Start from 7010			
Local Command Port: Start from 8010			
Connection Settings			I
TCP Alive Check: Enabled			
Check Time: 7 mins			
Port Buffering: Enabled			
Buffering Location: Memory (64K)			
RTS Always On: Enabled			
DTR Always On: Enabled			
Data Transmission Settings			
Data Packing: Disabled			
Force Transmit: Disabled			v
A BACK			
			CHINGLE SHITE

Socket Applications

The Socket application requires the user to have or create a socket program to establish the TCP session or send UDP packets to the destination NPort. Usually when the user wants to manage multiple brands of the network devices, he may have the resources to create or integrate a socket program to fulfill this need.

TCP Server Mode

If the user's program will initiate the TCP session actively, the NPort shall be a TCP Server to listen to a specific TCP port and wait for user's program to establish the TCP session. Please select **TCP Server** mode on NPort.



Step 1. Mode Selection

Select the Socket and select TCP Server mode.



Step 2. Basic Settings

Assign data port: This is the TCP port number assignment for the serial port on the NPort 6000-G2. 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.

Assign command port: The Command port is the TCP port for listening to Moxa commands from the host. To prevent a TCP port conflict with other applications, the user can set the Command port to another port if needed.

Mode Selection	Basic Settings	3 Advanced Settings
dvanced settings can gene	erally be used with default values. Customize the se	ettings if needed.
Connection Settings	Data Transmission Settings	
Max. Connection		
1	•	
Enable TCP alive check Allow the NPort to reset receiving of the last TCP	★ the TCP session by checking the packet until the check time timeout.	
Check Time (min) 7		
 Enable inactivity time 	out	
If there is no data from o specified timeout time, and command connection	or to the serial device within the allow the termination of both data ons.	

Step 3. Advanced Settings–Connection Settings

In some scenarios, the user may need to modify the advanced settings to fulfill his special cases.

	Basic Settings	3 Advanced Settings	4 Confirmation
vanced settings can generally	be used with default values. Customize the	settings if needed.	
Connection Settings Da	ata Transmission Settings		
Max. Connection			
1	¥		
Enable TCP alive check			
 Enable TCP alive check Allow the NPort to reset the T receiving of the last TCP packs 	'CP session by checking the et until the check time timeout.		
 Enable TCP alive check Allow the NPort to reset the Treceiving of the last TCP pack Check Time (min) 	CP session by checking the et until the check time timeout.		
Tenable TCP alive check Allow the NPort to reset the T receiving of the last TCP pack Check Time (min) 7	CP session by checking the et until the check time timeout.		
Enable TCP alive check Allow the NPort to reset the T receiving of the last TCP pack Check Time (min) 7 Enable port buffering	ICP session by checking the et until the check time timeout.		

For those users who have more than one Hosts to communicate with the NPort, he will need to enable the Max. Connection by changing the number to the number of the Hosts. With this, the NPort will accept all these Hosts to connect simultaneously. For example, if Host 1 is the primary computer who will send requests and receive the responses and Host 2 is the backup computer to receive all the responses. The user shall set the number to 2.

Connection Settings	Data Transmission Settings
Max. Connection	
2	•
Allow driver contr	ol -
Enable NPort to accu	ent commands from hosts to adjust
Enable NPort to acce the serial port settin	ept commands from hosts to adjust gs.
Enable NPort to acce the serial port settin Connection Process	pt commands from hosts to adjust gs.
Enable NPort to acc the serial port settin Connection Process Send serial data to	ept commands from hosts to adjust gs. all hosts -
Enable NPort to acc the serial port settin Connection Process Send serial data to Congestion Handl	all hosts

Max. connection (default=1): 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 6000-G2, 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).

The firmware will only send data back to the driver on the host. When the data is received on the serial port and passing to the Ethernet side of the NPort, all the Hosts will receive the same data. When the data is received on the Ethernet port and passing to the serial side of the NPort, the data will be sent first-in firstout.

If above scenario is not the case on your site, there are several advanced functions at **Multiple Connection Settings** to do some modifications.

Allow driver control: as mentioned above, when set **Max. connection** to 2 or greater, the serial port parameters will use firmware settings. If you want the serial parameters still use the settings of your application program, please enable the **Allow driver control** function. When you enable it, the serial port settings of your AP will overwrite the firmware settings while opening the COM port. Usually, you should only enable this function on one of the hosts. If you enable it on 2 or more hosts, then the serial parameters will be overwritten every time these hosts open the COM port.

To handle the unexpected data communication of multiple connections, there are different combinations for different scenarios.

Connection Control	Congestion Handling	Description
	-	This is the default data communication behavior for multiple connections, the serial data will be transmitted to all the hosts. What if there is one host cannot receive the data successfully?
Send serial data to all hosts	Wait until transmission succeeds	Just wait, until the host can receive data again. There is a side-effect on this option, if the host just cannot be back, the serial data will be stored on the serial buffer of the NPort. When the serial data is accumulated to 1,024 bytes, the serial buffer will full and cannot receive any data anymore. If there are new coming data, all of them will be dropped.
	Keep sending data to other hosts	Just ignored the abnormal host, keep sending data to other online hosts. The side-effect of this option is the communication seems OK when the user only checks the status on the succeed host(s). There may need a mechanism to notify the user there is an abnormal host cannot receive any data.

Connection Control	Congestion Handling	Description
	-	Sometimes, the other hosts cannot handle the responses they don't request. For this case, please select Send serial data to the requested host then all the hosts will only receive the response based on their own request. For this scenario, what if the serial device doesn't respond the request or respond too late?
Send serial data to the requested host	Discard	If the serial response is timeout, then the NPort will discard all the new coming serial data before NPort receives an Ethernet request.
	Send to the last request	If the serial response is timeout and the NPort receives new coming serial data, it will send the data to the host who send the most recent request to NPort.
	Send to all open connections	If the serial response is timeout and the NPort receives new coming serial data, it will send the data to all the hosts who still connected to NPort.
	Enable response timeout	For this kind of one-request-one-response application, user may need to define how long time the NPort shall wait for the serial response? The default timeout time is 10,000 ms. This value shall be less than the timeout time on user's AP. Otherwise this abnormal scenario might happen, the AP consider it's a timeout error but NPort still waiting for a response.

Enable TCP alive check
 Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.
 Check Time (min)
 7

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort 6000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort 6000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort 6000-G2 will terminate the TCP connection.

~	Enable inactivity timeout
	If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.
	Timeout Time (ms)

This setting is used for applications that may incur high costs for the connection between the remote host and the NPort, such as when it is connected with a cellular/satellite line. .

When the TCP session is established, the NPort will terminate the session actively if there is no new data for a while on the serial port. For the timing to terminate the TCP session, the user will need to set the Timeout time (ms) for this option.



Compared to the serial bus, the Ethernet network is not stable. Poor cable contact or a damaged switch/router could cause it to be disconnected or broken. When this happens, the serial data cannot transmit over Ethernet because the receiver does not exist. As time passes, the serial data could be discarded and lost. If the serial data is important, u enable the **Enable port buffering** function. The NPort can store serial data either in its internal memory, which is 64 Kbytes, or in an external SD card (if supported).

Enable port buffering (default=No): To prevent serial data loss when the Ethernet connection is down, check the checkbox to enable port buffering. If you enable port buffering, RTS/DTR will remain in the on position.

Buffering Location: Select the location of buffering. Memory (64K) or SD card.



In a serial bus, the host and the serial device can use RTS/DTR signals to indicate their status to each other. Using the RTS/DTR Behavior function, the NPort can simulate the RTS/DTR behavior on Ethernet connections. When using legacy software, enable the RTS/DTR signal and keep it constantly on to prevent the host from entering sleep mode or shutting down. This will ensure the host is always ready for communication.

RTS/DTR Behavior (default=always on): Configures what happens to the RTS and DTR signals when the TCP session is disconnected. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent via the serial port. This function may be disabled by enabling the Enable port buffering function.

Step 3. Advanced Settings—Data Transmission Settings

When the serial data is transmitted on the serial bus, it's continuous data. The software can receive the whole data by a simple "Read" command. When everything move to Ethernet based, it's another story. The Ethernet data might be separated to packets, and the receiver will assemble these packets to one complete frame to understand what the other device wants to transmit. But if it's a legacy serial software, it may not support the "assemble" function which is a basic function of a socket program. In this case, NPort provides Data Transmission function to deliver the correct frame at the beginning, then the legacy serial software doesn't need anything changed to read the correct data.

Mode Selection	Basic Setti	ngs	3 Advanced Settings
Advanced settings can gen	erally be used with default values.	Customize the settings if nee	eded.
Connection Settings	Data Transmission Settings		
Enable data packing Specify the packing and Packing Method	d sending of serial data to the host.		
Select One Packet length	Ŧ		
Delimiter (hex) Allow the packaging ar specified force transmi	nd transmission of serial data until the t time is met.		

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the **Enable data packing** function.

Enable data packing: With the dropdown menu Packing Method, select Packet length or Delimiter (hex).

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon as it reaches the specified length.

Connec	tion Settings Data Transmission Settings	
🖌 Enab	le data packing	
Speci	fy the packing and sending of serial data to the host.	
Pack	king Method	
De	limiter (hex)	Ŧ
		-
	Delimiter 1	
	0× 0	
	Delimiter 2 - Optional	
	0x	
Data	a Transmit Process	
۲	Default process	
	Send data with delimiter characters.	
0	Delimiter + 1 byte	
	Send data with delimiter characters and following 1 byte.	
0	Delimiter + 2 bytes	
0	Send data with delimiter characters and following 2 bytes.	
0	Strip delimiter	
	Send data without delimiter characters.	

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data then send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: If Delimiter 1 is configured in hex format, the NPort will treat the designated character as the end character. If there are two ending characters, use Delimiter 2 and ensure they are received in the correct order (Delimiter 1 first, then Delimiter 2). The NPort will package all the data in the serial buffer and follow the Data Transmit Process to handle the delimiter(s) before transmitting the data to the Ethernet port.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

- **Default process:** Data in the buffer and the delimiter(s) will be transmitted.
- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two bytes will be transmitted after two additional bytes are received following the delimiter.
- Strip delimiter: Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time (ms)** field.



Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

н	ome > Serial Port Settings > Operation Modes > Configure Port(s)			
	← Configure Port(s)			
	V Mode Selection	✓ Basic Settings	V Advanced Settings	- 4 Confirmation
	Selected Port: 1			
	Application: Socket Operation Mode: TCPServer			
	TCP Server Settings Data Port: Start from 4001 Command Part: Start from 866			
	Connection Settings Max Connection: 1 CPC Allow Check: Enabled Check: Time: 7 mins Inscrivity Timeou: Diabled Port Buffring: Diabled Buffering Lostein: Memory (640) RTS Manys On: Enabled Data Transmission Settings Data Transmission Settings Data Transmission Settings			
	< BACK			CANCEL SAVE

TCP Client Mode

When your program listens to a specific TCP port and wait for NPort to establish the TCP session. Please select **TCP Client** mode on the NPort.

1 Mode Selection —	2	Basic Settings –		3 Advanced Settings
TCP Client The user's application providing access to co	listens to TCP connections onnected serial devices.	from the NPort,		
Host PC		NPort		Serial Device
User-design app	← TCP/IP (Request connection from the NPort)	NPor.	— RS-232/422/485 —	00000

Step 1. Mode Selection

Select the **Socket** and then **TCP Client** mode.

Home → Serial Port Settings → Operation Modes → Configure Port(s) ← Configure Port(s)			
Mode Selection	2 Basic Settings	Advanced Settings	(4) Confirmation
Remote Server Settings			
Select the connect method and specify the server address to transm	nit data. Up to 10 sets of server can be ac	ided.	
Connect Method			
 Connect to all servers 			
Connect to the first available server			
Server 1			
Destination Address			
Assign the address port starting from 4001 Assign local port starting from 5010 incr + ADD SERVER	to selected port(s). ementing by 10 to selected port(s).		
< BACK			CANCEL NEXT >

Step 2. Basic Settings

There are two types of the TCP Client application. If the serial device needs to connect to all the hosts (the TCP Servers) simultaneously, select **Connect to all servers**. Or, if the serial device will try to connect to all hosts but only needs to establish a connection with the first one, select **Connect to first available server**. With this setting, the NPort will connect the servers in the order they were entered.

Connect Method: Choose whether you want to **Connect to all servers** or **Connect to the first available server**.

Several parameters need to be set for each server:

Destination Address: Specifying an IP address allows the NPort 6000-G2 to connect actively to the remote host. Provide the destination address for each server.

Assign the address port starting from: This is the TCP port number assignment on the remote host to listen to NPort's request. Please confirm that the port on the remote host matches the AP setting. The default port is set to 4001 to avoid conflicts with well-known TCP ports.

Assign local port starting from: Use these fields to specify the designated local port on the NPort.

ADD Server: Click ADD Server to add more remote servers for NPort to connect.

Home > Serial Port Settings > Operation Modes > Configure Port(s)			
← Configure Port(s)			
🗸 Mode Selection	🕢 Basic Settings	3 Advanced Settings	Confirmation
Advanced settings can generally be used with default values -	Tustomize the settings if needed		
randiced settings can generally be used that default tardes	and the second should be a second s		
Connection Settings Data Transmission Settings			
When to Connect			
Device starts up -			
When to Disconnect			
Never 👻			
Chalden in a finite react. Also the finite react. Also the finite react react in the the set into stream in the reacting of the int CD period with the sheet into stream. Check time (min) 7 Chalden port buffering To prevent loss of serial data during an Ethernet disconnection, walde this (change final data) finite finite finite means that Eth (CFR with a during be int to co. Buffering Leastion			
Memory (64K) 👻			
< BACK			CANCEL NEXT >

Step 3. Advanced Settings—Connection Settings

For TCP Client mode, the NPort will start the TCP session. It's important to determine when the NPort shall start or end the session. Based on different scenarios, set the behavior on **When to Connect/ When to Disconnect** function.

When to Connect/Disconnect: This setting determines the parameters under which a TCP connection is established or disconnected. The following table provides the different options. In general, we provide both the Connect conditions and Disconnect conditions.

When to Connect	When to Disconnect	Description
		This setting is used for those serial devices that may
	Never	proactively update data and remain powered on at all times,
		so the NPort needs to start updating data as quickly as
		possible.
Device starts up		The NPort will try to establish the TCP session when the
		firmware is ready. The NPort will not actively terminate the
		session once the TCP session is established. If the TCP session
		is disconnected by the remote host or by an accident, the
		NPort will try to reestablish it automatically.
		This setting is used for serial devices that may proactively
		update data, but they may not be powered at all the time or
	Never	they may update data very frequently. Therefore, the NPort
		can wait until it receives new serial data, and then it starts to
		establish the TCP session.
		The NPort will try to establish the TCP session when it
		receives data on the serial port. The NPort will not actively
		terminate the session once it has established the TCP session.
Receive any		If the TCP session is disconnected by the remote host or by
characters from		accident, the NPort will try to reestablish it automatically.
serial		This setting is for applications that may incur high costs for
		the connection between the remote host and the NPort, such
		as when it is connected with a cellular/satellite line.
		The NPort will try to establish the TCP session when it
	Т	receives data on the serial port. When the TCP session is
		established, the NPort will end the session actively if there is
		no new data for a while on the serial port.
		Set the Timeout time to determine when to end the TCP
		session.

When to Connect	When to Disconnect	Description
DSR on	Never	This setting is used for serial devices that can notify the host of their readiness to update data by turning on the DTR signal. Once the NPort detects the DSR signal is on, it will establish the connection and be ready for serial data update. The NPort will try to establish the TCP session when it detects the DCD signal is on. When the TCP session is established, the NPort will not terminate the session actively. If the TCP session is disconnected by the remote host or by accident, the NPort will try to reestablish it automatically.
	DSR off	This setting is used for those serial devices that can notify the host by changing the DTR signal to on when they are ready to update data. When the serial device finishes data update, it will also notify the host by changing the DTR signal to off. The NPort will try to establish the TCP session when it detects the DSR signal is on. When the TCP session is established, the NPort will only terminate the session actively when detecting the DSR signal is off.
DCD on	Never	This setting is used for serial devices that can notify the host of their readiness to update data by turning on the DCD signal. So, when the NPort detects the DCD signal is on, it shall establish the connection and be ready for serial date update. The NPort will try to establish the TCP session when it detects the DCD signal is on. When the TCP session is established, the NPort will not terminate the session actively. If the TCP session is disconnected by the remote host or by accident, the NPort will try to reestablish it automatically.
	DCD off	This setting is used for those serial devices that can notify the host by changing the DCD signal to on when they are ready to update data. When the serial device finishes the data update, it will also notify the host by changing the DCD signal to off. The NPort will try to establish the TCP session when it detects the DCD signal is on. When the TCP session is established, the NPort will only terminate the session actively when detecting the DCD signal is off.

Enable TCP alive check

Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.
Check Time (min)
7

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort 6000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort 6000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort 6000-G2 will terminate the TCP connection.



Compared to the serial bus, the Ethernet network is not stable. It could be disconnected/broken by a cable poor contact or switch/router damaged. When this happened, the serial data cannot be transmitted on the Ethernet because the receiver does not exist. As time goes by, the serial data may be dropped and gone. If the serial data is important, user can enable the **Enable port buffering** function. The NPort will save the serial data to the internal memory, 64 Kbytes, or the external SD card (for the supported models).

Enable port buffering (default=No): You may enable port buffering by checking the checkbox to prevent the loss of serial data when the Ethernet connection is down. Enabling port buffering means that RTS/DTR will always be set to on.

Buffering Location: Select the location of buffering. Memory (64K) or SD card.



On a serial bus, the Host and the serial device may based on turning on/off the RTS/DTR signals to notify the serial device that the Host is alive or not, and vice versa. The NPort supports RTS/DTR Behavior function to simulate above behavior on the Ethernet connections. Some legacy software on the Host may switch to sleep mode or shutdown itself based on the RTS/DTR signal, when enable this function and keep these two signal always on, it can prevent this to happen and keep the Host is ready for communication.

RTS/DTR Behavior (default=always on): You can configure what happens to the RTS and DTR signals when TCP session is disconnected. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent via the serial port. This function may be disabled by enabling the Enable port buffering function.

Step 3. Advanced Settings—Data Transmission Settings

When the serial data is transmitted on the serial bus, it's continuous data. A "Read" command allows the software to receive all of the data. When everything switches to Ethernet, it's a different story. Ethernet data can be divided into packets, which are then assembled by the receiver into a complete frame to interpret the transmission request from the other device. However, a legacy serial software might lack support for the fundamental "assemble" function found in socket programs. Here, the NPort enables the Data Transmission function to deliver the correct frame at the beginning, requiring no changes to the legacy serial software for reading accurate data.

Mode Selection —	Basic Setti	ngs	Advanced Settings
Advanced settings can ge	nerally be used with default values.	Customize the settings if n	eeded.
Connection Settings	Data Transmission Settings•		
Enable data packin Specify the packing a Packing Method Salast Open	g nd sending of serial data to the host.		
Packet length			
Allow the packaging a specified force transn	and transmission of serial data until the nit time is met.		

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the Enable data packing function..

Enable data packing: With the drop-down menu Packing Method, select **Packet length** or **Delimiter** (hex).

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When you specify a packet length between 1 and 1024 bytes, the data in the buffer will be sent as soon as it reaches the specified length.

Connec	tion Settings Data Transmission Settings
🗹 Enab	ple data packing
Speci	ify the packing and sending of serial data to the host.
Pac	king Method
De	limiter (hex) 👻
	Delimiter 1
	0× 0
	Delimiter 2 - Optional
	0x
Dat	a Transmit Process
۲	Default process
~	Send data with delimiter characters.
0	Delimiter + 1 byte
	byte.
0	Delimiter + 2 bytes
	Send data with delimiter characters and following 2 bytes.
\cap	Strin delimiter
0	outp deminiter

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data. Then, send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: If Delimiter 1 is configured in hex format, the NPort will treat the designated character as the end character. If there are two ending characters, use Delimiter 2 and ensure they are received in the correct order (Delimiter 1 first, then Delimiter 2). The NPort will package all the data in the serial buffer and follow the Data Transmit Process to handle the delimiter(s) before transmitting the data to the Ethernet port.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

Default process: Data in the buffer and the delimiter(s) will be transmitted.

- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two bytes will be transmitted after two additional bytes are received following the delimiter.
- Strip delimiter: Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time** (ms) field.



Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

Home > Serial Port Settings > Operation Modes > Configur	e Port(s)		
← Configure Port(s)			
-			
✓ Mode Selection	✓ Basic Settings	Advanced Settings	4 Confirmation
Selected Port: 1			
Application: Socket Operation Mode: TCPClient			
Remote Server Settings Connect Mathod: Connect to all servers Server 1 Destination Address: 10.9.9.10 Address Port: Start from 4001			
Connection Settings When to Connect: Device starts up When to Disconnect: Never TCP Allice Nete: Enabled Check Time: 7 mins Port Buffering: Enabled Buffering Catolicon. Nemery (SHQ)			
Data Transmission Settings Data Packing: Disabled Force Transmit: Disabled			
< BACK			CANCEL SAVE

UDP Mode

If your application requires faster data arrival at the device without the need for guaranteed data reception, then he may choose to use UDP packets for the application. For example, at the train station, the message displayed on the LCM could be missed because there are so many displays. If the passenger misses the message on one display, they can find it on the others. The train arrival message may be useless if it arrives on the display one minute after the train has already arrived. This is the typical application of the UDP mode.

he user's application s stablishing communic	ends and receives UDP p ation with connected ser	ackets for ial devices.		
Host PC		NPort		Serial Device
ليان	UDP	- R	S-232/422/485 —	<u>ەنىيە</u>
User-design app				

Step 1. Mode Selection

Select the **Socket** and then **UDP** mode.

Home > Serial Port Settings > Operation № ← Configure Port(s)	odes > Configure Port(s)				
Mode Selection	2 Ba	sic Settings	3 Advanced Settings	🕘 Cor	nfirmation
Destination Address Settings [●]	Listen Port Settings				
Destination Mode Static destination	•				
Specify the destination address to	o transmit data, and up to 4 sets of dest	nation can be added.			
Destination 1					
Single address		-			
Destination Address					
Assign the address por	t starting from 4001	to selected port(s).			
+ ADD DESTINATION					
< BACK				CANCEL	NEXT >

Step 2. Basic Settings

There are two types of UDP applications. The data may be sent to static destinations, or it may depend on different serial data going to different destinations.

Destination Mode	Address Type	Description
		This setting allows serial devices to proactively update data to
Static destination	Single address	specific remote hosts. You can input the target IP address and
		listen UDP port with this option.
Static destination	Addross range (up to	This setting allows users to proactively update data from serial
		devices to specific remote hosts. You can input a range of the
	10 autresses)	IP addresses and listen UDP port with this option.
		This setting is used for the one- request, one-response
	Learning by packet	scenario. The NPort will record the source IP address and UDP
		port as the destination IP address and UDP port when the
		NPort receives serial data.
Dynamic learning		Every time the NPort receives an Ethernet request, it will
		update the destination IP address and UDP port.
	Learning when	Until the timeout time is reached, the NPort will remove the
	reaching the timeout	old destination IP address and UDP port and update the
	reaching the timeout	information of the next UDP request to the table.

Destination Address Settings	Listen Port Settings	
Destination Mode		
	· · · · · · · · · · · · · · · · · · ·	
Specify the destination address to	transmit data, and up to 4 sets	of destination can be added.
Address Type		
Single address		•
Destination Address		
Assign the address port	starting from 4001	to selected port(s).
+ ADD DESTINATION		

Destination Mode: Specify the way the determines the destination address to transmit data. There are two options, the **Static destination** or **Dynamic learning**. This snapshot shows the parameters for the Static destination.

The parameters for Destination 1 are:

Address Type: Specify Single address or Address range (up to 16 addresses) as the destination for communication.

Destination Address: Input unicast, multicast IP addresses or domain names as the destination address. At least one destination range must be provided.

Assign the address port starting from: This is the UDP port number assignment for the serial port on the NPort.

ADD DESTINATION: Click the button to add more destinations.

 Serial Port Settings > Operation Modes > Configure Port(s) Configure Port(s) 	Home > Serial Port Settings > Operation Modes > Configure Port(s) ← Configure Port(s)
V Mode Selection 2	Basic Settings 20 Mode Selection 20 Basic Setting
Destination Address Settings	Destination Address Settings Listen Port Settings
Destination Mode Dynamic learning	Destination Mode Dynamic learning
Learning Method Learning by packet	Learning Method Learning when reaching the timeout
	Timeout Time (ms)

Destination Mode: Specify the way the determines the destination address to transmit data. There are two options, the **Static destination** or **Dynamic learning**. This snapshot shows the parameters for the Dynamic learning.

Learning Method: Under **Dynamic learning** mode, the NPort will record the source IP address and UDP port from the UDP packet. Depends on different user scenarios:

- The different UDP hosts may send the requests frequently, and the NPort (also the serial device) needs to reply to every request. Select **Learning by packet**. With this setting, the NPort will update the Destination IP address and UDP port for each UDP packet, so all the UDP hosts can receive the expected results.
- The different UDP hosts may take turns to send requests and get responses. Only when one host has finished its turn for updating, the token will pass to the second host to start another turn for requesting/responding. Here, set **Learning when reaching the timeout** and a specific timeout time (ms) for the hosts to exchanging the token. The NPort can learn the new host's IP address and UDP port.

No matter which Destination Mode was selected, assign the local listen port at Listen Port Settings tab:



Assign the local listen port from (default=4001): This is the UDP port that the NPort 6000-G2 listens to and that other devices must use. To avoid conflicts with well-known UDP ports, the default is set to 4001.

Step 3. Advanced Settings

✓ Mode Selection	Basic Settings	3 Advanced Settings
Advanced settings can generally be u	sed with default values. Customize the se	ettings if needed.
Data Transmission Settings		
Enable data packing Specify the packing and sending of se	rial data to the host.	
Packing Method Packet length	•	
Packet Length (Byte)		
Enable force transmit		
Allow the packaging and transmissior specified force transmit time is met.	n of serial data until the	

When the serial data is transmitted on the serial bus, it's continuous data. A "Read" command allows the software to receive all of the data. When everything switches to Ethernet, it's a different story. Ethernet data can be divided into packets, which are then assembled by the receiver into a complete frame to interpret the transmission request from the other device. However, a legacy serial software might lack support for the fundamental "assemble" function found in socket programs. Here, the NPort enables the Data Transmission function to deliver the correct frame at the beginning, requiring no changes to the legacy serial software for reading accurate data.

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the **Enable data packing** function.

Enable data packing: With the drop-down menu Packing Method, select Packet length or Delimiter (hex).

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon as it reaches the specified length.

Connec	tion Settings Data Transmission Settings
Enab	ble data packing
spec	ny the packing and scholing of senal data to the nost.
Pac	king Method
De	limiter (nex)
	Delimiter 1
	0x 0
	Delimiter 2 - Optional
	0x
Dat	a Transmit Process
۲	Default process
0	Send data with delimiter characters.
0	Send data with delimiter characters and following 1 byte.
0	Delimiter + 2 bytes
	Send data with delimiter characters and following 2 bytes.
0	Strip delimiter
	Send data without delimiter characters.

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data then send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: If Delimiter 1 is configured in hex format, the NPort will treat the designated character as the end character. If there are two ending characters, use Delimiter 2 and ensure they are received in the correct order (Delimiter 1 first, then Delimiter 2). The NPort will package all the data in the serial buffer and follow the Data Transmit Process to handle the delimiter(s) before transmitting the data to the Ethernet port.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

Default process: Data in the buffer and the delimiter(s) will be transmitted.

- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two byte will be transmitted after two additional bytes are received following the delimiter.
- Strip delimiter: Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time** (ms) field.

Enable force transmit Allow the packaging and transmission of serial data until the specified force transmit time is met.
Force Transmit Time (ms)

Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** above settings to make them affective.

Home > Serial Port Settings > Operation Modes > Configure Port(s)			
← Configure Port(s)			
Mode Selection	V Basic Settings	Advanced Settings	Confirmation
Selected Port: 1			
Application: Socket Operation Mode: UDP			
Destination Address Settings Databation Mode: Static destination Destination Address Type: Single address Destination: Address 10:0.5 Address Port: Stati from 40:01 Listen Port Settings Listen Port Adol Data Transmission Settings Data Packing: Disabled Force Transmit: Disabled			
< BACK			CANCEL SAVE

Pair Connection Applications

The Pair Connection application is designed for serial applications that keep the serial host and serial device. Here, the serial host cannot install any driver or socket program since it might not have Ethernet ports. But let's say the factory refurbishes, and the distance between the serial host and serial device increases significantly or maybe the network transitions to an Ethernet-based network. In this scenario, buying two NPorts with the Pair Connection application is a good fit.

Pair Connection Client Mode

With Pair Connection Application, set one NPort to Pair Connection Client mode to establish the connection and set the other NPort to Pair Connection Server mode to receive the request.

1 Mode Selection	2 Basic Settings	3	Advanced Se	ettings	4	Confirmation
Operation Mode Pair Connection Client Connect to another NPort, e communicate with each other	nabling two serial devices to er.					
Serial Device	NPort		NPort		Serial Device	
•	RS-232/422/485	TCP/IP (Request connection from Client NPort)	Client	— RS-232/422/485 —	••	

Step 1. Mode Selection

Select Pair Connection and Pair Connection Client mode.

NPort Server Settings Assign the server address and port of the connected NPort to the serial port(s). Server Address	Mode Selection	2 Basic Setting	js	Advanced Setting
Server Address	NPort Server Settings Assign the server address and port of th	e connected NPort to t	he serial port(s).	
	Server Address			
Assign conver port(c) starting from (1001 to selected port(c))	Assign sorver port(c) starting from	4001	to solocitod port(s)	

Step 2. Basic Settings

Server Address: The Pair Connection Client will try to establish the TCP session with this IP address. Input an IP address or a domain name.

Assign server port(s) starting from: This is the TCP port number assignment for the serial port on the NPort. It is the TCP port number on the remote NPort to listen to the request from the Pair Connection Client. To avoid conflicts with well-known TCP ports, set the default to 4001.

Step 3. Advanced Settings

V	Mode Selection 🛛 🕜 Basic	Settings 3	Advanced Settings
Ad	vanced settings can generally be used with default va	ues. Customize the settings if needed	
Сс	nnection Settings		
	Enable TCP alive check		
	Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeou	t	
	Check Time (min)		
	7		
~	Enable port buffering		
	To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.		
	Buffering Location		
	Memory (64K)	•	

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort 6000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort 6000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort 6000-G2 will terminate the TCP connection.

\checkmark	Enable port buffering	
	To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.)
	Buffering Location	

Compared to the serial bus, the Ethernet network is not stable. Poor cable contact or a damaged switch/router could cause it to be disconnected or broken. When this happens, the serial data cannot transmit over Ethernet because the receiver does not exist. As time passes, the serial data could be discarded and lost. If the serial data is important, u enable the **Enable port buffering** function. The NPort can store serial data either in its internal memory, which is 64 Kbytes, or in an external SD card (if supported).

Enable port buffering (default=No): To prevent serial data loss when the Ethernet connection is down, check the checkbox to enable port buffering. If you enable port buffering, RTS/DTR will remain in the on position.

Buffering Location: Select the location of buffering. Memory (64K) or SD card.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

Home > Serial Port Settings > Operation Modes > Configu ← Configure Port(s)	ure Port(s)		
Mode Selection	Basic Settings	Advanced Settings	4 Confirmation
Selected Port: 1			
Application: Pair Connection Operation Mode: PairConnectionClient			
NPort Server Settings Server Address: 10.0.0.1 Server Port: Start from 4001			
Connection Settings TCF Allow Check: Enabled Check Time: Minis Part Buffering: Enabled Buffering Location: Memory (540)			
< BACK			CANCEL SAVE

Pair Connection Server Mode

With Pair Connection Application, set one NPort to Pair Connection Client mode to establish the connection and set the other NPort to Pair Connection Server mode to receive the request.

 Pair Connection Serv Accept connected NPo communicate with each 	/er rt to enable two serial dev n other.	rices to				
Serial Device		NPort	_	NPort		Serial Device
••	— RS-232/422/485 —	NPar	← TCP/IP	MPore	— RS-232/422/485 —	••
		Server	from Client NPort)	Client		

Step 1. Mode Selection

Select the Pair Connection and Pair Connection Server mode.



Step 2. Basic Settings

Assign TCP listen port starting from (default=4001): This is the TCP port that the NPort listens to, which shall match with the Pair Connection Client's setting. To avoid conflicts with well-known UDP ports, set the default to 4001.

	Mode Selection	Basic Settings	3 Advanced Settings
Ad	vanced settings can generally be used wi	th default values. Customize the sett	ings if needed.
Co	nnection Settings		
	Enable TCP alive check		
	Allow the NPort to reset the TCP session by c receiving of the last TCP packet until the chec	hecking the :k time timeout.	
	Check Time (min)		
	7		
	Enable port buffering		
	lo prevent loss of serial data during an Ether disconnection, enable this function. Enabling means that RTS/DTR will always be set to on.	net port buffering	
	Buffering Location		
	Memory (64K)	•	

Step 3. Advanced Settings

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check** time function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort 6000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort 6000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort 6000-G2 will terminate the TCP connection.

~	Enable port buffering
	To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.
	Buffering Location
	Memory (64K)

Compared to the serial bus, the Ethernet network is not stable. Poor cable contact or a damaged switch/router could cause it to be disconnected or broken. When this happens, the serial data cannot transmit over Ethernet because the receiver does not exist. As time passes, the serial data could be discarded and lost. If the serial data is important, u enable the Enable port buffering function. The NPort can store serial data either in its internal memory, which is 64 Kbytes, or in an external SD card (if supported).

Enable port buffering (default=No): To prevent serial data loss when the Ethernet connection is down, check the checkbox to enable port buffering. If you enable port buffering, RTS/DTR will remain in the on position.

Buffering Location: Select the location of buffering. Memory (64K) or SD card.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

Home > Serial Port Settings > Operation Modes > Configure Port(s) ← Configure Port(s)			
Mode Selection	🕢 Basic Settings	Advanced Settings	4 Confirmation
Selected Port: 1			
Application: Pair Connection Operation Mode: PairConnectionServer			
Listen Port Settings TCP Port: Start from 4001			
Connection Settings TCP Alive Check: Enabled Check: Time: 7 mms Port Buffering: Exabled Buffering Location: Memory (640)			
< BACK			CANCEL SAVE

Connect Console Applications

Use the Connect Console application to connect to the console port of a server or a router/switch. There are two types of Connect Console Application:

- If the console port is Ethernetbased, the serial terminal connects to the NPort's serial port, and the NPort will establish a connection with the remote server using Telnet or SSH. Select the Terminal mode.
- If the console port is a serial based, the Ethernet-based terminal connects to the NPort with Telnet or the SSH protocol, and the NPort connects to the serial console of the server. Select the Reverse Terminal mode.

Terminal Mode

The remote server is listening on TCP port 22 for SSH or TCP port 23 for Telnet for a terminal to connect and provide the service. If you only have a serial-based terminal, it cannot establish a Telnet/SSH session to have the service. In this scenario, adding an NPort with Terminal mode can help. There's no need to eliminate the serial-based terminal equipment.

1 Mode Selection	2 Basic Settings	3 Advanced Settings
First, select the application, then choose the o	operation mode that suits your needs.	
Application		
Connect Console 🗸	_	
Operation Mode		
Terminal		
Connect to remote Telnet/SSH server by conr serial port.	necting the NPort via	
Server	NPort	Terminal
■ Telnet/SSH —	RS-232/422/485	
(Request connection from the NPort)	on Gar	

Step 1. Mode Selection

Select the **Connect Console** and **Terminal** mode.

Home > Serial Port Settings > Operation Modes > Configure Port(s)			
← Configure Port(s)			
✓ Mode Selection	2 Basic Settings	Advanced Settings	🕢 Confirmation
Terminal Type Settings			
Select the type of terminal to access the remote server by a serial	port.		
Туре			
Terminal ASCII			
O Terminal Binary			
O SSH			
< BACK			CANCEL NEXT >

Step 2. Basic Settings

The Terminal Type selection depends on the supported protocols of the remote server or your preferred protocol for the NPort connection.

Terminal Type	Description
Terminal ASCII	If the remote server supports Telnet protocol and there is no need to receive a file from the serial terminal, you may select Terminal ASCII mode on the NPort. Terminal ASCII mode can handle up to 8 sessions per port with the ability to switch between sessions on the same terminal. This mode is used for text-based terminals with no file-transfer capability or encryption
Terminal Binary	If the remote server supports Telnet protocol and the is no need to receive files from the serial terminal, you may select Terminal Binary mode on the NPort. Terminal Binary mode allows one session per port and is used for terminal applications that include file-transfer features.
SSH	If the remote server supports SSH protocol, you may select SSH mode on the NPort. SSH mode allows one session per port and is used for secure terminal applications that abide by the SSH protocol.

Home > Serial Port Settings > Operation Modes > Configure Port(s) ← Configure Port(s)			
Mode Selection	🕑 Basic Settings	3 Advanced Settings	Confirmation
Advanced settings can generally be used with default values.	Customize the settings if needed.		
Terminal Connection Settings Preference Settings			
Suble 1CP alve check Missue the NETs to uses the TCP assiss by checking the cleack time timescue. Cleack Time (min) 7 fable bile timeout Missue to a state of the state of advancement for the state of advancement for the time of the state of advancement for the time of the state of advancement for the time of the state of the state of the state for the time of the state of the state of the state for the time of the state of the state of the state for the time of the state of the state of the state for the state of the state			
< BACK			CANCEL NEXT >

Step 3. Advanced Settings—Terminal Connection Settings



Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort 6000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort 6000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort 6000-G2 will terminate the TCP connection.

\checkmark	Enable idle timeout	
	If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.	
	Timeout Time (min)	
	and command connections.	

Since the resource of the remote server is limited, the NPort as the session initiator can end the session actively. The duration of no data transmission or reception on the serial port determines it.

Enable idle timeout: User can specify how many minutes without any data been sent or received from the serial port, then NPort will terminate the Telnet session actively to release the remote server's resource to other terminals.



The administrator can use the **Enable the terminal authentication** function to verify if the user has the privilege to connect to the serial port of NPort and access the server. The NPort authenticates users for serial port access based on either the local username/password database or the remote RADIUS/TACACS+ server. Only users in the read/write privilege user group can access it in operation mode.

Enable remote server auto-connect	
Auto-connect Settings	
Protocol Telnet Rlogin 	
Create up to 2 terminal hosts to automatic con	nect by NPort.
Primary Host Address	Port 23
+ ADD HOST	

In general, the NPort will attempt to connect with the remote server when the serial port requires it. To avoid waiting, you can configure the NPort to automatically connect to the remote server when it's ready. Check the Enable remote server auto-connect function. The NPort will establish the connection when the firmware is ready.

For each remote server, specify the protocol the NPort shall use to establish the connection. There are two options: Telnet or Rlogin.

Primary Host Address: The NPort will try to establish the TCP session with this IP address. Input an IP address or a domain name.

Port: This is the TCP port number assignment on the remote server to listen to the request from the NPort. The default value is 23, which is the default TCP port of Telnet protocol. If you select Rlogin protocol, the default TCP port is 513.

Auto-login Pro	mpt	
ogin:		
Password Pror	npt	
assword:		
Login Usernan	1e	

The serial terminal user needs to input the username/password to get authorized on the remote server to use the service. For a convenient purpose, the user can pre-configure the value he will need to input to skip the process. If the values are correct, the NPort will input them.

Auto-login Prompt: The NPort will read the messages delivered by the remote server at the login process. When it reads this string, it will help to input the string in the field of Login Username.

Password Prompt: The NPort will read the messages delivered by the remote server at the login process. When it reads this string, it will help to input the string in the field of Login Password.

Login Username: Input the user account that has the privilege of using the necessary services on the remote server.

Login Password: User shall input the correct password to get the authority on the remote server.

Home > Serial Port Settings > Operation Modes > Configure Port(s) ← Configure Port(s)			
Mode Selection	Basic Settings	3 Advanced Settings	- d Confirmation
Advanced settings can generally be used with default values.	Customize the settings if needed.		
Terminal Connection Settings Preference Settings			
Terminal Type ansi	_		Î
Max. Session 4			
Hotkey Settings			
Click and press the hotkey to input the result.			
Change Session			
Quit Session			
Send Break Signal			
+			
Interrupt			
* +			
Welcome Message on Terminal - Optional			
< BACK			CANCEL NEXT >

Step 3. Advanced Settings—Preference Settings

The Preference Settings may be different on different Terminal Types, Terminal ASCII, Terminal Binary and SSH. The snapshot above shows the Preference Settings of the Terminal ASCII mode. **Terminal type** (default=ansi): Some older terminal applications may require that the terminal type be transmitted before the connection can be established. You may need to refer to the server's documentation to determine the appropriate terminal type. For most applications, this setting will be unnecessary and will have no effect. The most popular terminal types may be ansi or vt100.

Max. Sessions (default=4): The Terminal ASCII mode can support up to eight sessions on each serial port. This setting allows you to configure/limit the maximum number of sessions allowed for the specific serial port.

Generation Specify th Click and p	Setting e hotke press th	s y to e ho	the corresponding commands. tkey to input the result.
Change Se	ession		
Ctrl	•	+	Т
Quit Sessio	on		
Ctrl	•	+	E
Send Brea	k Signal		
	•	+	
Interrupt			
	•	+	

The Hotkey Settings section defines the hotkeys that a serial terminal user can use while logging in to the remote server. These hotkeys are supported by the NPort, and they will be executed by the NPort and not be transmitted to the remote server. For example, when you input Ctrl+T, it will switch to another session, and the string Ctrl+T will not be sent to the remote server.

Change Session (default=Ctrl+T): This field defines the quick key to change a session. As mentioned above, there are up to eight sessions of a serial port connection. You can switch to another session by entering this quick key.

Quit Session (default=Ctrl+E): This field defines the quick key to quit a session.

Send Break Signal: This field defines the quick key to send a break signal to the remote server.

Interrupt: This field defines the quick key for sending an interrupt signal to the remote server.



Welcome Message on Terminal – Optional: When the serial terminal user logs in to the NPort, the messages defined in this field will show to the user.

ome > Serial Port Settings > Operation Modes > Configure P ← Configure Port(s)	(s)		
✓ Mode Selection	Basic Settings	3 Advanced Settings	Confirmation
Advanced settings can generally be used with default	values. Customize the settings if needed.		
Terminal Connection Settings Preference Set	tings		
Terminal Type ansi			
Hotkey Settings Specify the hotkey to the corresponding comman Click and press the hotkey to input the result. Quit Session	nds.		
Ctrl + E			
Welcome Message on Terminal - Optional			
4	0/1280		
BACK			CANCEL NEXT >

The Preference Settings may be different on different Terminal Types, Terminal ASCII, Terminal Binary and SSH. The snapshot above shows the Preference Settings of the Terminal Binary mode.

Terminal type (default=ansi): Some older terminal applications may require that the terminal type be transmitted before the connection can be established. You may need to refer to the server's documentation to determine the appropriate terminal type. For most applications, this setting will be unnecessary and will have no effect. The most popular terminal types may be ansi or vt100.

Hotkey Settings	
Specify the hotkey to the corresponding commands. Click and press the hotkey to input the result.	
Quit Session	
Ctrl 🕶 + E	
Velcome Message on Terminal - Optional	
Velcome Message on Terminal - Optional	
Velcome Message on Terminal - Optional	
Velcome Message on Terminal - Optional	
Velcome Message on Terminal - Optional	
Velcome Message on Terminal - Optional	

The Hotkey Settings section defines the hotkeys that a serial terminal user can use while logging in to the remote server. These hotkeys are supported by the NPort, and they will be executed by the NPort and not be transmitted to the remote server. For example, when you input Ctrl+T, it will switch to another session, and the string Ctrl+T will not be sent to the remote server.

Quit Session (default=Ctrl+E): This field defines the quick key to quit a session.

Welcome Message on Terminal – Optional: When the serial terminal user logs in to the NPort, the messages defined in this field will be displayed to the user.

Mode Selection		3 Advanced Settings	Confirma
vanced settings can generally be used with default values. C	istomize the settings if needed.		
Terminal Connection Settings Preference Settings			
Hotkey Settings			
Specify the hotkey to the corresponding commands. Click and press the hotkey to input the result.			
Quit Session			
Ctrl 👻 + E			
Sand Break Signal			
Send break Signal			
• +			
Welcome Message on Terminal - Optional			
4			

The Preference Settings may be different on different Terminal Types, Terminal ASCII, Terminal Binary and SSH. The snapshot above shows the Preference Settings of the SSH mode. The Hotkey Settings section defines the hotkeys that a serial terminal user can use while logging in to the remote server. These hotkeys are supported by the NPort, and they will be executed by the NPort and will not be transmitted to the remote server. For example, when the user input Ctrl+E, the session will be terminated, and the string Ctrl+E will not be sent to the remote server.

Quit Session (default=Ctrl+E): This field defines the quick key to quit a session.

Send Break Signal: This field defines the quick key to send a break signal to the remote server.



Welcome Message on Terminal – Optional: When the serial terminal user logs in to the NPort, the messages defined in this field will be displayed to the user.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.



Reverse Terminal Mode

When a PC needs to establish a connection with the serial console of a server, router, or network device, but lacks a serial port (or doesn't have enough). The user might want to connect the serial console to an NPort's serial port. The NPort can then listen on TCP port 22 or 23 for SSH or Telnet connections respectively, allowing a terminal software on the PC to connect and provide the service. The PC can still use the Ethernet based software (supports Telnet or SSH) to connect the serial console of a network device. It's not necessary to increase the number of serial ports on the PC.

Connect to serial cons Telnet/SSH.	ole server by connecting the N	Port via	
Host PC		NPort	Server/Router
Ē,	──── Telnet/SSH ───★ (Request connection from Host PC)	NPor RS	-232/422/485 — •••••

Step 1. Mode Selection

Select the Connect Console and Reverse Terminal mode.

-

Step 2. Basic Settings

It depends on which protocol the terminal software on the PC supports (or which protocol you prefer to use to connect to the NPort) for choosing the Service

Service	Description
	If the PC supports Telnet protocol, then select Reverse Terminal mode on the NPort.
	The Telnet protocol or the Reverse Telnet mode of NPort is widely used for device
Doverse Telpet	management in control rooms. The system waits for a host on the network to start a
Reverse Temet	connection. Since TCP Server mode does not assist with conversion of CR/LF commands,
	if the management of the serial console of the device requires these CR/LF commands,
	the user shall use Reverse Telnet mode.
	Since the Telnet is a plaintext protocol, you may have cybersecurity concerns. In this
Reverse SSH	case, select the Reverse SSH mode to encode the communication between the PC and
	the NPort.

Assign TCP port starting from (default=4001): This is the TCP port that the NPort listens to, which shall match with the TCP port of the terminal software such as PuTTY on the PC. To avoid conflicts with well-known UDP ports, set the default to 4001.


Step 3. Advanced Settings—Connection Settings



Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort 6000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort 6000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort 6000-G2 will terminate the TCP connection.



Since the resources of the remote server is limited, the NPort as the session initiator can terminate the session. The duration of no data transmission or reception on the serial port determines it.

Enable idle timeout: You can specify the number of minutes with no data being sent or received from the serial port, and then the NPort will actively terminate the Telnet session to release the remote server's resources to other terminals.

Enable terminal authentication Enable to authenticate the connection based on system account privileges. The operation mode permission setting is in Account Management > Groups .

The administrator can use the **Enable the terminal authentication** function to verify if the user has the privilege to connect to the serial port of NPort and access the server. The NPort authenticates users for serial port access based on either the local username/password database or the remote RADIUS/TACACS+ server. Only users in the read/write privilege user group can access it in operation mode.

Home > Serial Port Settings > Op ← Configure Por	peration Modes → Configure Port(s) * t(s)	
✓ Mode Selection —	✓ Basic Settings	3 Advanced Settings
Advanced settings can gen	nerally be used with default values. Customize the settings if needed.	
Connection Settings	Preference Settings	
End-of-line Character CR-LF	*	
CR-LF CR LF		

Step 3. Advanced Settings—Preference Settings

End-of-line Character (default=CR-LF): This specifies how the ENTER key is mapped at the serial console of the network device. If the terminal software on the PC has the limitation of sending the ENTER key, for example, it will always send <CR> to represent the ENTER key. But the serial console of the network device can only accept <LF> as the ENTER key. This mismatch may cause problems while using the terminal software to manage the network device. To solve this issue, set the end-of-line character as LF, then every time NPort receives the <CR> from the terminal software that will automatically change it to <LF> and then pass it to the network device. Everything will then work smoothly.

End-of-line Character	Description
	Officially <cr-lf> represents carriage return + line feed (i.e., the cursor will jump</cr-lf>
<cr-lf></cr-lf>	to the next line and return to the first character of the line). This is the formal
	definition of the ENTER key.
	Officially <cr> represents carriage return (i.e., the cursor will return to the first</cr>
<cr></cr>	character of the line). For some operation systems, this also represents the ENTER
	key.
	Officially <lf> represents line feed (i.e., the cursor will jump to the next line, but</lf>
<lf></lf>	not move horizontally). For some operation systems, this also represents the
	ENTER key.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

Home > Serial Port Settings > Operation Modes > Configu	re Port(s)		
✓ Mode Selection	Basic Settings	Advanced Settings	4 Confirmation
Selected Port: 1			
Application: Connect Console Operation Mode: ReverseTerminal			
Reverse Terminal Settings Service: Reverse SSH TCP Port: Satt from 4001 Connection Settings TCP Alive Check: Enabled Check: Line: 7 mins Line: Timeiro: Doabled Terminal Authentication: Disabled Preference Settings End-of-line Character: CR-LF			
< BACK			CANCEL SAVE

Connect Modem Application

A modem is a computer hardware device that converts data from a digital format into a format suitable for an analog transmission medium, such as telephone or radio. Usually, the computer may need a serial port to connect to a modem. Nowadays, most computers do not have serial ports. To fulfill this need, the NPort can help to connect to a modem on its serial port and bring it as an accessory to the computer. Due to the specific modem signals and behavior required for communication, the Connect Modem Application is designed for this application.



The Connect Modem Application has two operation modes, depending on the communication protocol used by the host PC. If the PPP protocol is used on the host PC, switch the NPort to **Connect Modem Application > PPP mode**. The support for multiple PPP/SLIP sessions on multiple serial ports is unnecessary if the Connect Modem Application can establish a network session via PSTN to access the NPort and the local network behind the NPort. There's a possibility that this will escalate the cybersecurity risk. Hence, only a single serial port can be set up as the Connect Modem Application on an NPort.

PPP Mode

Depending on the protocol used on the host PC, set the operation mode on the NPort. This setting will enable network data exchange by establishing a PPP connection over PSTN using a modem.



Step 1. Mode Selection

Select the Connect Modem and PPP mode.

Home > Serial Port Settin	igs > Operation Modes > Configure Port(s) Port(s)					
Mode Selection	n —	2 Basic Settings	3 Adva	anced Settings	(4) Co	nfirmation
Network and Mo	dem Settings					
Destination Address						
Source Address						
Subnet Mask						
Enable modem						
Initial String						
Enable dial To make dial information	-out function -out function operational, configure routing in Network Settings > Routing Table .					
Dial-up Stri	ing					
Phone Nun	nber					Ţ
< BACK					CANCEL	NEXT >

Step 2. Basic Settings

To establish a PSTN connection to a remote network, the NPort will need to know the serial port, the remote site's IP addresses and the subnet mask. Then, it can help to route the packets to local and remote networks.

Destination Address: This is the IP address of the remote Host PC's serial port.

Source Address: The Source IP address is the IP address assigned to the NPort's serial port.

Subnet Mask: The subnet mask defines the netmask for the PPP connection, which includes the NPort and remote PC's serial ports.

🗹 Ena	able modem
In	itial String
	Enable dial out function
_ <u>∽</u>	Enable dial-out function
	To make dial-out function operational, configure routing information in Network Settings > Routing Table .
	Dial-up String
	Phone Number

The local PC connected to the NPort might have a PPP program that can establish a PSTN connection using built-in commands. To ensure compatibility with the PPP program and NPort, configure the following settings.

Initial string: Input the command used by the PPP program to trigger the modem to establish the connection with the remote site. In general, the initial string may be AT.

Dial-up String: Input the command used by the PPP program to start the dialing to the remote site. In general, the dial-up string may be ATD.

Phone Number: Use this field to configure the phone number to be dialed out.

Mode Selection	Basic Settings	3 Advanced Settings	4 Confirmation
dvanced settings can generally be used with default values. Cus	tomize the settings if needed.		
connection Settings			
When to Disconnect			
Never -			
Enable inactivity timeout			
If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.			
Enable connection authentication			
Enable to authenticate the connection based on system account privileges. The operation mode permission setting is in Account Management > Groups .			
Enable remote login			
TCP/IP Compression			
Enable the link quality report			

Step 3. Advanced Settings

Since the PSTN or Radio connection may be expensive, you may want to manage the time it stays connected.

When to Disconnection (default=Never): To manage when the NPort will end the connection actively, there are three mechanisms: Never, DCD-Off or DSR Off.

- Never means the NPort will not end the connection actively.
- DCD-Off means the NPort will end the connection when it detects the DCD signal is turned off.
- DSR-Off means the NPort will end the connection when it detects the DSR signal is turned off.

/	Enable inactivity timeout
	If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.
	Timeout Time (ms)

This setting is used for applications that may incur high costs for the connection between the remote host and the NPort, such as when it is connected with a cellular/satellite line.

When the TCP session is established, the NPort will actively end the session if there is no new data for a while on the serial port. For the time interval to end the TCP session, the user will need to set the Timeout time (ms) for this option.

\checkmark	Enable connection authentication
	Enable to authenticate the connection based on system account privileges. The operation mode permission setting is in Account Management > Groups .

The administrator can use the **Enable the terminal authentication** function to verify if the user has the privilege to connect to the serial port of NPort and access the server. The NPort authenticates users for serial port access based on either the local username/password database or the remote RADIUS/TACACS+ server. Only users in the read/write privilege user group can access it in operation mode.

~	Enable remote login	
	Username	
	Password	ND I
		<i><i><i></i></i></i>

When the remote side enables user authentication, the NPort user must enter their authorized username and password for each connection attempt. By enabling the remote login function and entering the username/password, NPort can automatically input the information.

Username: This is the dial-out user ID account.

Password: This is the dial-out user password.



TCP/IP compression (default=Disable): The setting of this field depends on whether the remote user's application requests compression.

Enable the link quality report (default=Disable): Setting this field to enable allows the NPort to disconnect a connection if the link noise exceeds a certain threshold.

Step 4. Confirmation

Please review and **SAVE** above settings to make them affective.

Home > Serial Port Settings > Operation Modes > Con	ifigure Port(s)		
← Configure Port(s)			
]			
Mode Selection	Rasic Settings	Advanced Settings	Confirmation
Wode Selection	basic settings	Auvaliced Settings	Commation
Selected Port: 1			
Application: Connect Modem			
Operation Mode: PPP			
Network and Modem Settings			
Destination Address: 198.0.0.1			
Source Address: 198.0.0.2			
Subnet Mask: 255.255.255.0			
Enable modem: Disabled			
Connection Settings			
When to Disconnect: Never			
Inactivity Timeout: Disabled			
Enable Connection Authentication: Enabled			
Enable Remote Login: Disabled			
TCP/IP Compression: Enabled			
Enable The Link Quality Report: Enabled			
< BACK			CANCEL SAVE

SLIP Mode

The operation mode on the NPort can be set based on the protocol used on the host PC, as determined by you. This setting will enable network data exchange by establishing a SLIP connection over PSTN using a modem.

SLIP Enable network data exchange by establishing a SLIP connection over PSTN using a modem.								
LAN	Ē	NPort	_	Modem	— Dial-in (SLIP) -	Modem		Host PC
品	– Ethernet –	MPore	— RS-232 —	mə	— PSTN —	[111.9	— RS-232 —	: _
					– Dial-out (SLIP)			

Step 1. Mode Selection

Select the **Connect Modem** and select **SLIP** mode.

Home → Serial Port Settings → Operation Modes → Configure Port(s) ← Configure Port(s)			
✓ Mode Selection	2 Basic Settings	Advanced Settings	4 Confirmation
Network and Modem Settings			
Source Address			
Subnet Mask			
Enable modem			
Initial String			
Enable dial-out function			
To make dial-out function operational, configure routing information in Network Settings > Routing Table .			
Dial-up String			
Phone Number			
< BACK			CANCEL NEXT >

Step 2. Basic Settings

To establish a PSTN connection to a remote network, the NPort will need to know the serial port's IP addresses and the subnet mask. Then, it can help to route the packets to local and remote networks.

Source Address: The Source IP address is the IP address assigned to the NPort's serial port.

Subnet Mask: The subnet mask defines the netmask for the SLIP connection.

🔽 Ena	ble modem
Init	tial String
	Enable dial-out function
	To make dial-out function operational, configure routing information in Network Settings > Routing Table .
	Dial-up String
	Phone Number

The local PC connected to the NPort might have a PPP program that can establish a PSTN connection using built-in commands. To ensure compatibility with the PPP program and NPort, configure the following settings.

Initial string: Input the command used by the PPP program to trigger the modem to establish the connection with the remote site. In general, the initial string may be AT.

Dial-up String: Input the command used by the PPP program to start the dialing to the remote site. In general, the dial-up string may be ATD.

Phone Number: Use this field to configure the phone number to be dialed.

Home > Serial Port Settings > Operation Modes > Configure Port(s) ← Configure Port(s)					
Mode Selection	Basic Settings	3 Advanced Se	ettings	4 Co	onfirmation
Advanced settings can generally be used with default value	s. Customize the settings if needed.				
Connection Settings					
When to Disconnect Never					
Enable inactivity timeout If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.					
TCP/IP Compression					
< BACK				CANCEL	NEXT >

Step 3. Advanced Settings

Since the PSTN or Radio connection may be expensive, you may want to manage the time it stays connected.

When to Disconnection (default=Never): There are three mechanisms to actively manage when the NPort will terminate the connection: Never, DCD-Off, or DSR Off..

- Never means the NPort will not end the connection actively.
- DCD-Off means the NPort will end the connection when it detects the DCD signal is turned off.
- DSR-Off means the NPort will end the connection when it detects the DSR signal is turned off.

Enable inactivity timeout If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.
Timeout Time (ms)

This setting is used for applications that may incur high costs for the connection between the remote host and the NPort, such as when it is connected with a cellular/satellite line.

When the TCP session is established, the NPort will terminate the session actively if there is no new data for a while on the serial port. For the timing to terminate the TCP session, the user will need to set the Timeout time (ms) for this option.



TCP/IP compression (default=Disable): The setting of this field depends on whether the remote user's application requests compression.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

- Configure Port(s)			
Mode Selection	V Basic Settings	V Advanced Settings	4 Confirmation
Selected Port: 1			
Application: Connect Modem			
Operation Mode: SLIP			
Network and Modem Settings			
Source Address: 198.0.0.1			
Subnet Mask: 255.255.255.0			
Enable modem: Disabled			
Connection Settings			
When to Disconnect: Never			
Inactivity Timeout: Disabled			
TCP/IP Compression: Disabled			
			_
BACK			CANCEL SA

No Operation

To address cybersecurity concerns, users can set a serial port to No Operation if it is not connected to any serial devices. Disabling unused services can decrease cybersecurity risks.

Serial Parameters

Matching serial parameters between the serial device and the NPort device server is an essential factor for communication. Refer to the device manual to obtain its serial parameters. Then, navigate to **Serial Port Settings > Serial Parameters** to modify the serial parameters.

Only if the NPort is configured as a **COM-based Control** application, can you skip this step/section. The COM port software or TTY software will overwrite the serial parameters while it opens a COM port/TTY port.

:	Dashboard	Home > Serial Port Settings > Serial Parameters									
> =	≓ System Settings	Select	port(s)) and click "C	ONFIGURE" to conf	igure the serial settin	gs.				
> 4	Network Settings										
~ (🕈 Serial Port Settings										
	Operation Modes			Port	Interface	Baudrate	Parity	Data Bits	Stop Bit(s)	Flow Control	
	Serial Parameters	>		1	RS-232	115200	None	8	1	None	:
> (Secure Connection	>		2	RS-232	115200	None	8	1	None	:
> [Account Management										
> 4	* Maintenance										
> {	Diagnostics										

Select Serial Port Settings > Serial Parameters in the navigation panel to configure the parameters for each serial port. You may click on the button and select **EDIT** to change the serial parameters on a specific serial port. The Edit Port window will open to change the existing parameters.

	Port	Interface	Baudrate	Parity	Data Bits	Stop Bit(s)	Flow Control	
>	1	RS-232	115200	None	8	1	None	:
>	2	RS-232	115200	None	8	1	None	Edit
								Assign port alias
								Copy port settings

Edit Port 1		
Interface RS-232		•
Basic Settings		
Baudrate (bps) 115200		•
Parity None		•
Data Bits 8		•
Stop Bit(s) 1		•
Flow Control None		•
Advanced Settings		
 Enable FIFO Enabling FIFO results in increased throughput for 	serial communi	cation.
	CANCEL	SAVE

If you want to change multiple serial ports simultaneously, select the checkboxes of the target ports and click the **CONFIGURE** button. The Configure Port window allows you to set new values for all selected ports by displaying empty parameter fields.

								CONFIGURE
	Port	Interface	Baudrate	Parity	Data Bits	Stop Bit(s)	Flow Control	
>	Z 1	RS-232	115200	None	8	1	None	:
>	2	RS-232	115200	None	8	1	None	:

Configure Port(S)
Selected Port: 1, 2
Interface Select One 🔻
Basic Settings
Baudrate (bps) Select One
Parity Select One
Data Bits Select One ▼
Stop Bit(s) Select One
Flow Control Select One
CANCEL SAVE

Basic Settings

Interface (default=RS-232): You may configure the serial interface to RS-232, RS-422, RS-485 2-wire, or RS-485 4-wire

Baudrate (bps) (default=115200): This field configures the port's baudrate. Select one of the standard baudrates from the drop-down box or select Other and input the specific baudrate of the serial device in the Value box.

Parity (default=None): This field configures the parity parameter.

Data Bits (default=8): This field configures the data bits parameter; 5, 6, 7, or 8 are supported.

Stop Bits (default=1): This field configures the stop bits parameter;1 or 2 are supported.

Flow control (default=None): This field configures the flow control type, including RTS/CTS, DTR/DSR, Xon/Xoff, RTS Toggle and None. When set interface as RS-232, it supports all above flow control mechanisms. When set interface as RS-422, RS-485 2-wire or RS-485 4-wire, it only supports None and Xon/Xoff.

Advanced Settings

Advanced Settings Enable FIFO Enabling FIFO results in increased throughput for serial communication. Disabling FIFO reduces latency.

Enable FIFO:

The Enable FIFO function is enabled by default for improved data throughput. There are two situations where the user may choose to disable the Enable FIFO function by unchecking the checkbox.

- If the serial device does not have FIFO/buffer or does not support the flow control function. In this case, the serial device may not receive the serial data from the NPort on time, which means that some data might be dropped.
- If the data latency is more important than data throughput. To achieve higher data throughput, data can be temporarily stored in the buffer, allowing for larger amounts of data to be sent at once. The downside is that the latency of a single data may be slower. If the latency is important for the serial device to read data correctly, then you should consider disabling the Enable FIFO function.

This field enables or disables the 512-byte FIFO buffer. The NPort 6000-G2 provides FIFO buffers for each serial port, for both the Tx and Rx signals.

🗌 Enable terminator (120 Ω)	
For RS-422/485, especially for long distance communication, we recommend you enable the terminator to prevent the reflection of serial signals on the first and the last RS-422/485 devices.	
Resistor ①	
150 ΚΩ	-

When configuring the interface as RS-422, RS-485 2-wire, or RS-485 4-wire, you can choose to enable the terminator (120 Ω) and set the resistor. Because these interfaces can handle communication distances of over 1 km and accommodate more than 10 serial devices on the same bus, there are more factors that need to be taken into account.

Enable terminator (120 Ω): For RS-422/485, especially for long-distance communication, we recommend you enable the terminator to prevent the reflection of serial signals on the first and the last RS-422/485 devices.

Resistor: If the remote devices are unable to receive data correctly for RS-422/485, try adjusting the pull high/low resistors which can strengthen the serial signal, and it might help on this. Two values are selectable, 1 K Ω or 150 K Ω .

Secure Connection

To face the increasing cybersecurity threats, user may want to consider how you can protect important data on the serial device. The communication distance on the serial bus is short and hard to steal (usually in a factory with a security guard). When using a device server to pass the serial data to an Ethernet network, it is another story. An Ethernet network is more vulnerable than a serial bus. The NPort device server provides the ability to communications on the Ethernet network.

Select **Serial Port Settings > Secure Connection** in the navigation panel to configure the **TCP Connection Type** for each serial port. You can also select multiple serial ports and click the **CONFIGURE** button to change them simultaneously.

Dashharand	Home > Serial Port Setting	as > Secure Connection				
Dashboard	Cocura Conno	Secure Connection				
> 荘 System Settings > 홃 Network Settings ✓ ♂ Serial Port Settings	Secure connection supports Real COM, Reverse Real COM, TCP Server, TCP Client, and Pair Connection modes in TCP connection. Configure the TCP connection type as needed. Refer to the cipher suites for an encrypted connection.					
Operation Modes						
Serial Parameters	Select port(s) and clic	k "CONFIGURE" to configure the TCP connect	tion type.			
Secure Connection				CONFIGURE		
> 😯 Security						
> 😫 Account Management	Port	Application	Operation Mode	TCP Connection Type		
> 🚔 Maintenance	□ 1	COM-based Control	Real COM	Unencrypted connection		
> 🙊 Diagnostics	2	COM-based Control	Real COM	Unencrypted connection		
	4			•		

TCP Connection Type



Option	Description
Unencrypted connection	Data sent through the Ethernet will not be encrypted. This is the default value.
Encrypted connection	Data sent through the Ethernet will be encrypted with TLS v1.2.
Encrypted and	Data sent through the Ethernet will be encrypted with TLS v1.2, and the connection will be authenticated by certificate before the connection is
authenticated connection	established. Please upload the certificate at Remote Device Certificate tab for authentication if you choose this type.

Remote Device Certificate

Dashboard	Hom	me > Serial Port Settings > Secure	Connection				
 > : System Setting > . Network Setti > . Serial Port Set 	s Sec gs <u>Ref</u>	Secure connection supports Real COM, Reverse Real COM, TCP Server, TCP Client, and Pair Connection modes in TCP connection. Configure the TCP connection type as needed. Refer to the cipher suites for an encrypted connection.					
Operation N	odes	TCP Connection Type Rer	note Device Certific	ate			
Serial Param	ters T	The port(s) with encrypted and authenticated connections will verify the uploaded certificates.					
Secure Conn	ction						UPLOAD
> 🕐 Security		71. N.				21. L	
> 🖹 Account Mana	jement	Flie Name	Issued to		issued by	Status	
> 💐 Maintenance		No certificate to display. Click	UPLOAD butt	on to upload the certificat	e.		
> 🛞 Diagnostics							

Encrypting the TCP session safeguards the confidentiality of the serial data, but how can we ensure the authenticity of the network device being communicated with? It's possible that the server is fake and attempting to extract valuable data from the serial device. To avoid this, it is recommended to enable certificate-based authentication. The NPort will verify the user-uploaded certificate and request verification of the remote server's certificate before establishing a secure connection. Once both devices are confirmed as correct, they will establish an encrypted TCP session to safeguard the crucial serial data. To enable it, remember to select **TCP Connection Type** to **Encrypted and authenticated connection** and upload the certificate at **Remote Device Certificate** tab.

When switching to the **Remote Device Certificate** tab, click the **UPLOAD** button to upload your certificate for authentication.

Upload Certificate		
Choose one or multiple certificates to uploa that can be uploaded is limited to 10.	ad. The number of	certificates
Choose Files No file chosen		
	CANCEL	UPLOAD

Security

With cyberattacks growing in number and sophistication, device server vendors are adding functions geared towards protecting sensitive business and personal information. All the relative functions are listed under the **Security** category.

Services

Based on different user scenarios, you may need different services to meet these requirements. Click **Security > Services** to enable/disable the services he needs or no need.

Hons > Security > Services	
Services	
Set the software and hardware services by toggling the buttons or editing the options below.	
Software Services	
Web Console TCP: Port 443	•
Serial Console Command-Line Interface	•
SNMP Agent () UDP: Port 161	
MOXA Service () RESTful API(TCP: Port 443), mDNS(UDP: Port 5353), LLDP.	•
WINS UDP. Port 137	
Gratuitous ARP Periodic to send gratuitous ARP 🖌	
Hardware Services	
Beeper	-
Reset Button on Device Only enable within 60s after boo	ting EDIT

Software Services	Value	Default Value	Description
Web Console Enable/ Disable Enable		Enable	This setting is to enable/disable the web console. To ensure security, the NPort 6000-G2 device server only supports HTTPS console using TLS v1.2 or newer. The web console provides all the settings that the NPort 6000-G2 supports. We don't recommend a user to disable it.
Serial Console	Enable/ Disable	Enable	This setting is to enable/disable the serial console on the serial port 1 of the NPort 6150-G2/6250-G2. Log in the serial console while the device server is booting up to configure the network settings like the IP address. After setting the network settings, it is advisable to disable the serial console. This prevents accidental triggering of the console by the serial device during simultaneous boot-up.
SNMP Agent	Enable/ Disable	Disable	This setting is to enable/disable the SNMP Agent service. If you want to use the SNMP protocol to monitor the status or change some configuration settings of the NPort 6000-G2, enable the service. If your site doesn't match this scenario, please disable it.
Moxa Service	Enable/ Disable	Enable	This setting is to enable/disable Moxa proprietary service. NPort Windows Driver Manager, DSU-G2, and MXStudio are based on this service to work. This software cannot be used when Moxa Service is disabled.
WINS	Enable/ Disable	Disable	This setting is to enable/disable the WINS service. Windows Internet Name Service (WINS) is the Microsoft implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names. If the service is not enabled in your network, keep it as disabled.
Gratuitous ARP	Enable Disable	Disable	This setting is to enable/disable the Gratuitous ARP service. In some applications, you may need the NPort 6000-G2 to send broadcast packets to update the ARP table on the server. If you enable this function and set the send period, the NPort 6000-G2 will periodically send broadcast ARP packets at the specified time interval.

Sratuitous ARP	
Veriodic to send gratuitous ARP 🖌	

When click the edit button of Gratuitous ARP service, set the time for the ARP packets. The default value is 300 seconds.

Edit Periodi	c Time		
Periodic Time (se 300	ec)		
	CANCEL	SAVE	

Reset Button on Device

Hardware Services	Value	Default Value	Description
Beeper	Enable/Disable	Enable	This setting is to enable/disable the beeper of the device. You will hear the beeper when the device is ready after a power cycle. If you don't want to hear the sound, you may disable the service.
Reset Button on Device	Only enable within 60s after booting up/Always enable	Only enable within 60s after booting up	By default, the device disables the reset button after booting up for 60 seconds to prevent someone from accidentally pushing the button and resetting the device to its default settings.

Only enable within 60s after booting EDIT

The EDIT button in the Reset Button On Device service allows you to specify when the reset button should be enabled. Either the button is enabled for just one minute after the device boots up, or it stays enabled indefinitely.

Reset Button On Device		
Considering the possibility of an accidental operation, there are two modes for the reset button on device. You may set it according to your needs.		
Mode Only enable within 60s after booting Always enable		
CANCEL SAVE		

Allowlist

An allowlist is a list of IP addresses or domains that are provided privileged access. Enabling this function limits the number of the IP addresses that can access the device server, which can prevent unauthorized access from an untrusted network.

Но	ome > Security > Allowlist			
A	llowlist			
	Info All communications are only allowed for the enabled IPs on the list after enabling t	tis allowlist.		
	Allowlist			
	lpv4 (0) lpv6 (0)			
				ADD RULE
	No. IPv4 Address	Subnet Mask	Status	
	No data to display. Click ADD RULE button to create the first data.			

Before you enable Allowlist, add at least one rule on the table. And remember to make sure the host PC's IP address is on the list, or you may not access the web console of the device server.

Add IPv4 Rule		
IPv4 Address		
Subnet Mask		
Enable this rule		
	CANCEL	SAVE

Click the ADD RULE button to add a new rule. You may fill an IP Address or a domain name in the IP Address column, and then input the subnet mask to allocate a range of IP addresses. We recommend you enable this function, so the new rules will be enabled while adding a new rule. If you don't want to enable it, remember to uncheck the checkbox **Enable this rule**.

Certificate

The NPort 6000-G2 will automatically generate a self-certification for all the TLS sessions, including web console (HTTPS), secure operation modes, and syslog-ng service.

If you have company generated or a third-party verified certification, click the MANAGE button to import the certification to mitigate the cybersecurity risks to the network.

ŀ	Home > Security > Certificate	
(Certificate	
1	The device automatically generates a certificate based on its IP address for system identification. The user certificate can be imported to replace the system's default certificate.	
	System Certificate © Valid	MANAGE 👻
	Issued to: 10.90.60.63 Issued by: 10.90.60.63 Start Time: 2023/8//6 Expiration Time: 2023/9/6	

When access the **Security > Certificate** page, it shows the status of the system certificate:

- Is the system certificate still valid? Or has it expired?
- Who requested the system certificate?
- Who issued the system certificate? If it is a self-certification, the IP address will be NPort's IP address.
- When was the system certificate issued?
- When will the system certificate expire?

MANAGE 🗸
Download system certificate
Regenerate system certificate
Import user certificate

When you click the MANAGE button, there are three actions:

- Download system certificate: The browser or the software on a PC may request the target device to
 provide a valid certificate before establishing a secure connection. In this case, download the system
 certificate from the NPort. and then upload it to the browser or the software. Then the secure
 connection will be established.
- Regenerate system certificate: If the system certificate has expired or no longer sucure, regenerate the system certificate for new secure connections.
- Import user certificate: If you have company generated or a third-party verified certification, import that certificate to the NPort to establish new secure connections.

Import User Certificate		
Info The web server will automatically certificate. The imported certifica	restart after ir te will take eff	nporting the ect after the restart.
Please import the certificate file with	n a private key.	
Choose File No file chosen		
	CANCEL	IMPORT & RESTART

When clicking the **MANAGE > Import user certificate**, click **Choose File** button to find the certification on the PC. Click the **IMPORT & RESTART** button to ensure the NPort will restart itself to use the imported certificate.

Login Settings

The NPort device server administrator may need to send messages to a user upon successful or failed login attempts. The administrator can edit related messages or functions here.

Home > Security > Login Settings	Hame > Security > Lagin Settings
Login Settings	Login Settings
Login Message Login Lockout Session Control	Login Message Login Lockout Session Control
The following text description will be displayed on the system's login page.	The following text description will be displayed on the system's login page.
Login Message	Login Message
Message Text - Optional	Message Text - Optional
0/256	
Login Authentication Failure Message	Login Authentication Failure Message
Mode	Mode
Default message 👻	Customized message 👻
Message Text The account or password you entered is incorrect. (Your account will be temporarily locked if tried excessively.)	Message Text The account or password you entered is incorrect. (Your account will be temporarily locked if excessive tried.)
	111/256
SAVE	SAVE

When you successfully log in to an NPort 6000-G2 device server, the Login Message column will be shown. The message input by the administrator can be up to 256 characters long.

To communicate with users who couldn't login, the administrator can opt for Customized message mode and enter the message in the Message Text column. When the mode is set to Default message, the NPort 6000-G2 also offers a recommended message for the administrator to refer to.

Home	s Security > Log gin Setting	in Settings JS	
Lo	ogin Message	Login Lockout	Session Control
To fail	prevent hackers lure lockout and Enable login fai	from repeatedly atten adjust the necessary s lure lockout	npting to log in and crack passwords, you can enable login settings.
	Max. Failure Ret	ry (times)	
	Enable rese The login fai recalculate b Lockout Time (n	t login failure counter lure counter will reset an ased on the period you b nin)	r id ve set.
	SAVE		

To prevent hackers from repeatedly attempting to log in and crack passwords, we recommend you enable the Login Lockout function. It will be enabled on default.

Name	Value	Default Value	Description
Enable login failure lockout	Cheked / uncheck	Checked	When checked, the Login Lockout function will be enabled.
Max. Failure Retry (times)	1 - 10	5	If the Login Lockout function is enabled, it sets the number of attempts a user has before being locked out. Let's say the value is 5, then five password attempts are allowed. Regardless of whether the password is right or wrong on the sixth attempt, access to the device will be denied.
Enable reset login failure counter	Checked / uncheck	Unchecked	If this function is enabled, the user can wait a bit and then retry logging in. If this feature is turned off, the only option is to contact the administrator and request an account unlock.
Lockout Time (min)	1 - 60	5	If the option to reset the login failure counter is turned on, it sets the waiting time for the user before another login attempt.

н L	ome > Security > Logi ogin Setting	n Settings	
	Login Message	Login Lockout	Session Control
	Max. Login User for H 5	HTTPS (count)	
	Session Timeout (min	1)	
	SAVE		

For security and resource arrangement reasons, the NPort will limit the usage of the HTTPS sessions.

Name	Value	Default Value	Description
Max. Login User for	1 - 10	5	The number of users with different user accounts that
HTTPS (count)			can establish a HTTPS connection to the NPort.
Session Timeout (min)	1 - 1440	60	The time the NPort allows for inactivity when a user logs in before ending the HTTPS session

Account Management

For security concerns, different users need different accounts and privileges on one device. With the Account Management function of the NPort 6000-G2 Series, administrators can easily add, delete, or change user account names. They can also assign access to specific function categories based on different user groups. Furthermore, administrators can effectively manage passwords and login policies to ensure that only authorized users can use the device.

Accounts

In the NPort 6000-G2 Series, the categories that you can access have a strong correlation with the user groups defined by the administrator(s) (for managing the groups, please refer to the next section, Groups). Administrators are allowed to add user accounts to the NPort 6000-G2 device by clicking the Create button on the **Accounts** page.

Dashboard	Home > Account Management >	Accounts			
> 큐는 System Settings > 톫 Network Settings					CREATE
	Account Name 👙	Group 🌩	Status 🌻	Date of Creation 👙	
Security	admin	Administrator	Ø Active	2024-08-06	:
Accounts					

The **Create New Account** window will pop up for you to input account information and assign a password to the user. Also, the Administrator(s) shall assign a proper **Group** to users to limit their privileges of using the NPort 6000-G2. To add/delete/edit the **Group**, please go to the **Groups** section in the menu. The **Password** rules can be set up in **Password Policy** section.

Account Name Moxa	
Group	
Administrator	*
Password	Ø
× Contains at leas	t 8 characters
Confirm New Password	ø

You may also click more menu button on an exited user to edit the account's above information/settings.)

ədmin	Administrator	Ø Active	2024-08-06	i
Users	Viewer	Ø Active	2024-08-26	1
				Change password Change group
				Deactivate
				Delete

Change password

As an administrator, you can change every user's password. The Change Password window will appear. Input the new password twice and **SAVE** the new password. The password will be changed.

As a general user, you can only change your password. Click the More menu button in your account name and select **Change password** so that the Change password window opens. Input the new password twice and **SAVE** the new password. The password will be changed.

Change group

Change Group	~
Account Name: Users Date of Creation: 2024-08-26	
Group Viewer	•
CANCE	SAVE

Only the administrator can change the group of a user account. Click the More menu button in the target account name and select **Change group** to open the Change Group window. On te drop-down menu, select the group you want to move click the **SAVE** button. The user account will move to the new group.

Deactivate

Deactivate Account
Deactivating the account will result in the account being blocked from accessing the system.
Are you sure you want to deactivate the account "Users" ?
CANCEL DEACTIVATE

Only the administrator deactivate a user account. When deactivating an user, the user account still exists on the NPort, but the user cannot log in to the device. Only when the administrator activates the user account can the user lock in. Click the More menu button on the target account name and select **Deactivate** to open the Deactivate Account window. Click the **DEACTIVATE** button and the user account will be deactivated.

Delete

Delete Account
Deleting the account will remove the account permanently from the system and revoke all access.
Are you sure you want to delete the account "Users" ?
CANCEL DELETE

Only the administrator can delete a user account. When deleting a user account, it will be removed from the NPort. Click the More menu button on the target account name and select **Delete** to open the Delete Account window. Click the **DELETE** button to delete the user account.

Groups

Users can access different function categories with the NPort 6000-G2 based on their group affiliation. Customizing access permissions for different groups is restricted to the group administrator by default, or any group which is granted with Read/Write permission on Account Management category.

A maximum of four user groups can be created, with up to four user accounts per group. By default, the NPort 6000-G2 has the Administrator, Operator, and Viewer user groups built in.

- The Administrator group cannot be removed, and the name cannot be changed.
- The Operator group can be removed, and the name can be changed.
- The Viewer group cannot be removed , but the name can be changed.

Clicking the Create button on the Groups page to create a new group.

EE Dashboard	Nome > Account Management > Droupe			
> 표 System Settings > 흛 Network Settings				CREATE
🕂 Serial Port Settings	Group	Number of Accounts	TACACS+ Privilege Level	
Account Management	Administrator This group is designed for the supervisor of the device. The accounts of this group will have full privileges. This is a built-in group and cannot be modified or delated.	1 account(s)	15	3
Accounts Groups	Operator This group is designed for the maintainer of the device. The accounts of this group can modify and monitor must of the settings and troubleshooting functions.	0 account(s)	1	1
Password Policy	Viewer	1 account(s)		1
Authentication Server	Sample	0 account(s)	** :	1

Basic Information	
Group Name	
Group Description - Optional	
	0/300
TACACS+ Privilege Level - Optional⊕	
Dearation Mode Permission	
he permission of operation mode is requ	uired for operating the
erminal, reverse terminal , or dial-in/out -	PPP modes.
erminal, reverse terminal , or dial-in/out -	PPP modes.
erminal, reverse terminal , or dial-in/out - Enable operation mode permission Console Permissions	PPP modes.
erminal, reverse terminal, or dial-in/out - Enable operation mode permission Console Permissions System Settings	PPP modes.
erminal, reverse terminal, or dial-in/out - Enable operation mode permission Console Permissions System Settings Select One	PPP modes.
erminal, reverse terminal, or dial-in/out - Enable operation mode permission Console Permissions System Settings Select One Network Settings	PPP modes.
erminal, reverse terminal, or dial-in/out - Enable operation mode permission Console Permissions System Settings Select One Network Settings Select One	PPP modes.
erminal, reverse terminal, or dial-in/out - Enable operation mode permission Console Permissions System Settings Select One Network Settings Select One Serial Port Settings	PPP modes.
erminal, reverse terminal, or dial-in/out - Enable operation mode permission Console Permissions System Settings Select One Network Settings Select One Serial Port Settings Select One	PPP modes.
erminal, reverse terminal, or dial-in/out - Enable operation mode permission Console Permissions System Settings Select One Serial Port Settings Select One Security	PPP modes.
erminal, reverse terminal , or dial-in/out - Enable operation mode permission Console Permissions System Settings Select One Serial Port Settings Select One Security Select One	PPP modes.
erminal, reverse terminal , or dial-in/out - Enable operation mode permission Console Permissions System Settings Select One Serial Port Settings Select One Security Select One Account Management	PPP modes.

Group Name: The name of the group user is going to create. You need to give the group name. When the NPort enables a central account management mechanism with RADIUS, the group name shall match the Filter-ID parameter on the RADIUS server.

Group Description – Optional: Decribe the group to understand the purpose for creating this group. For example, creating a group named "Operator" with the description: "This group is designed for the maintainenance of the device. The accounts of this group can change and monitor most of the settings and troubleshooting functions." This is an optional column.

TACACS+ Privilege Level – Optional: When the NPort enables the central account management mechanism with TACACS+, this column will need to be filled with a number between 0 and 15. This value must match the Privilege Level parameter on the TACACS+ server. This value is crucial for coworking with a TACACS+ server.

Operation Mode Permission: When the serial port(s) is configured with these operation modes—Terminal, Reverse Terminal or Dial-in/out PPP mode—can check if the remote user has the necessary privilege to access the serial port. For these users, add them to a group that enabled this function.

Console Permissions: Assign the privileges for different categories using the drop-down menu. There are three types of the permissions:

- **No Display:** The user in this user group will not see this function group when accessing the NPort 6000-G2.
- **Read Only:** The user in this user group can only view the function/setting in this function group but cannot make modifications.
- **Read Write:** The user in this user group can view the function/setting in this function group and make modifications.

There are totally seven categories:

- System Settings: Includes all the settings for the NPort itself, like the server's name and notification.
- Network Settings: Includes all the settings related to the Ethernet port, like the IP address and subnet mask.
- Serial Port Settings: Includes all the settings related to the serial port, like the operation mode and serial parameters.
- Security: Includes all the settings related to cybersecurity, like the allowlist and login settings.
- Account Management: Includes all the settings related to account and group, like create/modify/delete an account or group.
- Maintenance: Includes all the settings related to routine maintenance jobs, like firmware upgrade and configuration import/export.
- Diagnostics: Includes all the functions which help the user troubleshoot, like device status and traffic monitoring.

Click the More menu button on an existing group to edit its access privilege or delete the group.

roups			
1777 F 7			
			CREAT
Group	Number of Accounts	TACACS+ Privileg	e Level
Administrator This group is designed for the supervisor of the device. The accounts of this group will have full privileges. This is a built-in group and cannot be modified or deleted.	1 account(s)	15	
Operator This group is designed for the maintainer of the device. The accounts of this group can modify and monitor most of the settings and troubleshooting functions.	0 account(s)	1	
Viewer	1 account(s)		
Sample Sample group	0 account(s)	¥¥)	
			Edit
			Delete

Password Policy

With the PC platform becoming increasingly powerful, users worry about the risk of password brute-force attacks. The administrator can mitigate cybersecurity risk by enabling the Password Policy function to boost password complexity.

Home > Account Management	t > Password Policy
Password Policy	y .
You have the option to enha policy.	ince password security by selecting a minimum length and strength
Min. Password Length	
8	
Password Strength Policy	
At least one digit (0-9	1
Mixed upper and lowe	r case letters (A-Z, a-z)
At least one special cf	aaracter (~! @#\$%^&•+=` '(){[]:;*'<>,.?/)
You can enhance account s lifetime threshold and a use	ecurity by setting a password lifetime. When an account reaches the r logs in, the system will mandate password changes.
Enable password lifetim	ie .
Password Lifetime (day	
90	

Parameter	Setting	Default	Description
Password minimum longth	8 to 256		Define the minimum length of the login
	characters	0	password for NPort 6000-G2
At least one digit (0-9)	Enable/Disable	Dicablo	The password must contain at least one
	LIIdDie/Disable	DISADIC	number (0 to 9) when enabling this parameter
Mixed upper- and lowercase	Enable/Dicable	Dicablo	The password must contain an upper- and a
letters (A~Z, a~z)	LIIdDie/Disable	DISADIC	lowercase letter when enabling this parameter
At least one special character	Enable/Dicable	Dicablo	The password must contain at least one special
(~!@#\$%^&* ;:,.<>[]{}())	LIIdDie/Disable	DISADIC	character when enabling this parameter
Enable password lifetime	Enable/Dicable	Enablo	Enhancing account security by setting a
	LIIdDie/Disable	LIIADIE	password lifetime.
			Users can set a specific lifetime for their
Password Lifetime (day)	1 to 180 days	90 days	passwords, and receive system notifications to
			change them if the option is enabled.

On completion of the settings, click the **SAVE** button to save the changes and make them effective.

For setting related to failure logins, for example, to lock out an IP address after five failure password inputs, find the **Security > Login Settings > Login Lockout** section.

Authentication Server

For a medium or big network topology (maybe more than 50 network devices), setting up the username/password database on each network device is tedious work, especially when you need to update the passwords quarterly. Setting up a centralized account management system is a solution. Select the **Account Management > Authentication Server** of the Navigation Panel to configure the relative settings.

E Dashboard	Home > Account M Authentica	anagement > Authentication	n Server						
➤ ﷺ System Settings	When available, t	he active authentication se	erver will be the main meth	od for authenticating web					
> 🚠 Network Settings	logins. The local a Refer to the acces	account database will be u as permission for the remo	sed as a secondary option te user.	if necessary.					
➤ III Serial Port Settings									
> 🕲 Security									CREATE
🛩 😫 Account Management	Priority	Server Type	Status	Server Address	Port	Authentication Type	Timeout (sec)	Accounting	
Accounts	1	RADIUS	@ Enabled	10.90.60.51	1812	PAP	5	Disabled	:
Password Policy									
Authentication Server									
> 🚉 Maintenance									
> @ Diagnostics									

Click the CREATE button to create an authentication server in the network.

erver Type ACACS +	
Server Settings	
Server Address	
Port 49	
+3	
Authentication Type CHAP	•
Share Secret	Ø
Timeout (sec) @	
5	

Enable the server: Click the CREATE button to open the Create Server window and enable the **Enable** the server function. If you want to add a server without enabling server authentication, make sure to disable it.

Server Type: The NPort 6000-G2 Series supports TACACS+ or RADIUS server of a central account management system.

Server Address: Input the IP address or the domain name of the TACACS+ or RADIUS server.

Port: Enter the TCP port for the TACACS+ or RADIUS server to listen for authentication.

Authentication Type: The NPort 6000-G2 Series supports two authentication types, PAP or CHAP. PAP uses a two-way handshake and sends the secret in clear-text form, whereas CHAP uses a three-way handshake and never sends the secret between the parties. Therefore, CHAP is a stronger authentication method than PAP, because the secret is not transmitted over the network, and it provides protection against repeated attacks during the life of the link.

Share Secret: The shared secret key is a text string used to encrypt/decrypt data in TACACS+/RADIUS packets transmitted between the two parties during authentication sessions. It must match the setting on the RADIUS/TACACS+ server.

Timeout: The time NPort will wait for the server response before trying another server or local account database.

Enable Accounting: The TACACS+/RADIUS may support an accounting function to calculate the time each user uses a specific service. To enable support for this, the administrator needs to activate it for the NPort.

On completion of the settings, click the SAVE button to save the changes and make them effective.

Maintenance

Operators may have to perform routine tasks every month or quarter to maintain the system when it is online. NPort categorizes these actions as Maintenance to simplify their completion for the user.

Config. Import/Export

You may want to back up the configuration settings of the NPort to access the **Maintenance > Config. Import/Export** to accomplish it.

Home > Maintenance > Config. Import/Export	
Config. Import/Export	
The configuration file will be encrypted and authenticated by the default password while exporting and importing the file. The default password could be changed to a custom one for security enhancement if your configuration file is from the legacy NPort 6000 Series, please go to Legacy Configuration import.	
File Authentication Default password	MANAGE 🗸
Import Export	
Choose File No file chosen	
IMPORT	

File Authentication

Because of security concerns, the NPort 6000-G2 can no longer export a configuration file without a password. Click the MANAGE button to set a password for the exported configuration file.

	MANAGE 👻
Set custo	om password
Reset to	default password

When clicking the **Set custom password**, give a customized password for the exported configuration file. The NPort 6000-G2 will use this password to decode the imported configuration file. The password policy for the configuration file allows for 8 to 64 characters and does not have any complex requirements.

When clicking the **Reset to default password**, the NPort 6000-G2 will use the default password to encode or decode a configuration file.

Import/Export the Configuration File



At the **Import** tab, click the **Choose File** button to select the configuration file you want to import.



At the **Export** tab, click the **EXPORT** button to select where you want to save the configuration file to.

Firmware Upgrade

It's highly advised to always upgrade to the latest firmware version due to the increasing number of cybersecurity threats. Consistently using the latest firmware helps reduce cybersecurity risks.

When you want to upgrade the firmware, click **Maintenance > Firmware Upgrade**, and click the **Choose File** button to find the firmware file. Click the UPLOAD button to proceed.



Ensure the device remains powered on and click the UPLOAD & RESTART button. The device will upgrade to the new firmware version and restart itself.



When the login page appears, it means that the firmware upgrade process has been completed.

	ΜΟΧΛ
System restarting	Log in to NPort-6250-G2_3456
Warning Do not leave the page during the process. The system will redirect to the login page later.	Account Name
	Password 🗞
	Forgot password?
	LOG IN

Reset to Default

This function will reset all the NPort 6000-G2's settings to the factory default values. All previous settings, including the console password, will be lost. If you wish to keep the NPort 6000-G2 IP address, netmask, and other network settings, make sure **Keep current device network settings** is checked before loading the factory defaults.

_		
Г	Hame > Maintenance > Reset to Default	
	Reset To Default	
	The initial default setting is the factory default, and it can also be set as a custom profile using the current device configuration. Click "RESET" to restore the device to its default setting.	
	Default Setting Factory default	MANAGE 👻
	Keep current device network settings Preserved items include mode, IP address, netmask (IPv4), prefix (IPv6), gateway, and DNS.	
	RESET	

Machine builders or system integrators may have their preferred default values on the NPort. The NPort 6000-G2 provides **Set as custom profile** function to allow users to set the settings as the default setting. In this case, when the customer triggers the Reset to Default function, the device will restore the custom default settings. The hardware reset button is the only way to reset it to the Moxa factory default. Clicking the **MANAGE** button and selecting the **Set as custom profile** will enable this function. The configuration file will be saved as default when the customer initiates a reset using the web console, DSU-G2, or MCC Tool.

	IVIANAGE 👻
Seta	as custom profile
Seta	as factory default

Restart

If you want to restart the device, access **Maintenance > Restart** and click the **RESTART** button. The device will restart itself.



Diagnostics

System integrators and technical engineers may encounter issues when configuring a new application or receiving error reports during system operation. When that happens, you might find it helpful to have some diagnostic tools for troubleshooting.

In the Navigation Panel, the Diagnostics section brings together all the necessary functions for quick troubleshooting..

Support

If users need direct support from Moxa, they can find it on the Diagnostics à Support page. There, we provide a list of recommended information to collect before contacting Moxa, as well as contact information for seeking assistance.



Product Information

Find here the basic information of the NPort device server, including the Model Name, Serial Number, Firmware Version of the NPort 6000-G2 device.



Diagnostic Information

Previously, users would typically reach out to Moxa customer service initially, and the engineer would then request additional information for problem analysis. For the NPort 6000-G2 Series, we advise users to gather Diagnostic Information and send it along with their inquiry to Moxa customer service. This can make it simpler for the customer service engineer to pinpoint the root cause of the problem.



The Download Diagnostic Information window will open and list what information on the NPort device server will be collected/downloaded. Click **DOWNLOAD** to save the data after providing your consent for collection. The diagnostic information is encrypted to ensure it is secure when delivered on the Internet and can only be unzipped by Moxa engineers for troubleshooting purposes. Access will not be granted with the password.

To verify this information, please use the NPort device server's web console.

Contact Support

Contact Support

For any assistance, please contact your distributor or Moxa technical support:

- Distributor finder 12
- Moxa technical support 🛛

After downloading the Diagnostic Information, you can find the contact window by clicking the **Distributor finder** or **Moxa technical support**, which will guide you to the corresponding resources on the official website.

System Log

It is very important to record the activities of a device. At the System Settings > Notification page, configure which events will be recorded. Under the **Diagnostics > System Log > Log View** tab, find the recorded events on the NPort device server. Under the **Log Settings** tab, set the advanced settings for the local system log.

	Dashboard	Home Svs	> Dia tem	gnostics 1 Loa	> System Log							
> 7	System Settings	,		0								
> #	Network Settings	b	og Vie	ew	Log Settings							
> ល	Serial Port Settings									. EXPORT	DEEDECH	
> 🕲	Security							Y FILLER	CLEAR	▲ EXPORT	REFRESH	
> 🖻	Account Management		١	No	Severity 🌲	c	Category 🌲	Event Name 🍦	Timesta	imp 🌲		Î
>	Maintenance		> 1	1	Informational	S	Security	Login success	2024-0	9-16 15:02:51		
~	Diagnostics		> 2	2	Informational	5	Security	Login success	2024-0	9-16 11:23:59		1
	Support		> 3	3	Informational	S	Security	Login success	2024-0	9-12 10:12:59		-
•	System Log								2024			1
	Operation Mode Statistics		, '	4	Informational	5	security	Login success	2024-0	9-12 10:01:57		
	Network Monitor		> 5	5	Error	S	Security	Authentication fail	2024-0	9-12 10:01:57		
	Ping		> 6	5	Notice	S	Serial	Port disconnect	2024-0	9-11 17:35:05		
	Traffic Monitor		> 7	7	Notice	S	Serial	Port restart	2024-0	9-11 17:35:05		•
								Items per page: 10	▼ 1 - 10 of 39	1 K K _ 1	/ 40 > >	4

An event will be recorded under these columns: Severity, Category, Event Name, and Timestamp. You may find more information at **System Settings > Notification** section. also, there is the event list in the appendix.

Home >	Diagnostic	s > System Log g				
Log	View	Log Settings				
					🝸 FILTER 👗 CLEAR 🛓 EXPOR	T REFRESH
	No	Severity 🌲	Category 🌲	Event Name 🌲	Timestamp 🍦	î
~	1	Informational	Security	Login success	2024-09-20 14:56:12	
	Source: Messag	nport-pm 10.123.124.200 e: A web user 'nport-pm' from 10.123.124.200	login the device successfully.			

Click the arrow icon by to read more details about the event.

The NPort device server provides some management functions for you to easily read the events.

Home >	Diagnostics	s > System Log				
Log	View	Log Settings				
				Y FILTER	📥 CLEAR 🔮 EXPORT	REFRESH
	No	Severity 🌲	Category 🌲	Event Name 🔺	Timestamp 🍦	*
>	1	Informational	Security	Login success	2024-09-16 15:02:51	
>	2	Informational	Security	Login success	2024-09-16 11:23:59	
>	3	Informational	Security	Login success	2024-09-12 10:12:59	

FILTER: Filter the event by Severity, Category, Event Name, or Timestamp.

Ŧ	Severity	•
	Severity	
+	Category	
	Event Name	
	Timestamp (Date)	

CLEAR: Delete all system logs on the device.

Clear System Log	
This action is irreversible and will result in the deletion of all sys the device. Are you sure that you want to proceed?	tem logs on
CANCEL	CLEAR

EXPORT: Export the system log for troubleshooting.

REFRESH: Refresh the logs on the panel.

Under the Log Settings tab, you will see the Current Log Capacity displayed as a percentage for reference. Since the events are stored on the local flash memory, there is a limitation on the number of events that can be saved. Click the **EDIT** button to manage the settings.

System Log	
Log View Log Settings	
Log Settings Ø 50 enabled event(s)	EDIT -
Current Log Capacity: 3% Log Capacity Policy: Overwrite the oldest log	Events Settings Log Capacity Settings

Events Settings

Select the events you will like to save in the local system log.

Home > Diagno	stics > System Log > Events Settings		
← Even	ts Settings		
Select the even Refer to the de	nts you would like to save in the system log. The events can be sorted by severity. <u>stails of the severity</u>		
Severity:	Frror Warning V Notice Informational		Q SEARCH
System	(16) Network (7) Security (23) Maintenance (8) Serial (8)		
	Event Name	Severity 🌲	A
	Firmware ready	Notice	
	Detect SD card	Informational	
	SD card removed	Warning	
	No SD card inserted	Error	
\checkmark	User trigger reboot	Notice	•
			SAVE

Find more information in the **System Settings > Notification** section. Also, there is the event list in the appendix.

Log Capacity Settings

Home > Diagnostics > System Log > Log Capacity Settings
← Log Capacity Settings
Capacity Management
Current Log Capacity: 3%
The maximum number of system logs that can be stored on the device is 10,000. You may manage the log capacity by clearing all system logs.
CLEAR
Policy Settings
Please select the overwrite policy when the log capacity reaches its limit.
Overwrite Policy
Overwrite the oldest log
O Stop recording the log
The system will notify or log the "log threshold reached" event according to the value set below.
Capacity Threshold (%)
80
SAVE

Capacity Management: The NPort 6000-G2 provides 10,000 audit records. Click the CLEAR button to clear the local system log when it's getting full.
Policy Settings: When the log capacity reaches its limit, decide what action the NPort should take due to limited recording system log capacity.

- Overwrite the oldest event log
- Stop recording events

Capacity Threshold (%): The system will notify you or record an event "log threshold reached" when the log capacity reaches the value set here. The default value is 80.

Operation Mode Statistics

The key feature of an NPort device server is to transmit serial data to the Ethernet network and vice versa. Everything that happens on the serial interface will be recorded here, **Diagnostics > Operation Mode Statistics**, to help the user understand the serial data transmitted/received or the modem status changes.

:	Dashboard	Home Ope	Home > Diagnostics > Operation Mode Statistics Operation Mode Statistics							
> = > =	 System Settings Network Settings 	The information below provides an overview of the operation mode status. For detailed information on each port, please access the "Port" link within the list.								
> (🖞 Serial Port Settings	Real-time data displaying						➔ RESET COUNTERS		
> (Security Account Management		Port	Operation Mode	Connection Status	Ethernet Tx / Serial Rx (Byte)	Serial Tx / Ethernet Rx (Byte)	Serial Errors (Count) 💿		
> 3	Maintenance	>	Port 1	Real COM	© Disconnected	0 / 0	0 / 0	0		
~ {	Diagnostics	>	Port 2	Real COM	⊗ Disconnected	0/0	0/0	0		
	Support									
	System Log Operation Mode Statistics Network Monitor Ping									
	Traffic Monitor									

- The Operation Mode Statistics contains the operation mode, connection status, the transmitted/received packets on Ethernet and serial connections, and the serial errors. The status or numbers for each port and column are shown here.
- Port: The serial port number of this NPort. When clicking the Port, there are more details.
- Operation Mode: The operation mode which is set a the specific serial port.
- Connection Status: Whether or not the Ethernet session is connected
- Ethernet Tx / Serial Rx (Byte): The Ethernet port and the serial port recorded a total of transmitted bytes and received bytes, respectively. Normally, these two numbers ought to match. If the Ethernet session disconnects, the number will reset.
- Serial Tx / Ethernet Rx (Byte): The serial port and the Ethernet port recorded a total of transmitted bytes and received bytes, respectively. Normally, these two numbers ought to match. If the Ethernet session disconnects, the number will reset.
- Serial Errors (Count): If the NPort detects an error in the received serial data (1 byte), for example, a frame error or parity error, it increments this column by 1.

Home > Diagnostics > Operation Mode Statistics > Port 1								
← Port 1								
Operation Mode: Real COM (Secure)								
Serial Parameters	Serial Connections	Ethernet Connections						
Real-time data displa	Real-time data displaying							
Interface	RS-232							
Baudrate	115200							
Parity	None							
Data Bits	8							
Stop Bit(s)	1							
Flow Control	None							
FIFO	Enabled							

When clicking a specific port number, the Port window will open with the information below.

Serial Parameters tab:

This tab displays the current settings of the serial parameters like the interface, baudrate, and so on.

Home > Diagnostics > Ope	ome > Diagnostics > Operation Mode Statistics > Port 1							
← Port 1								
Operation Mode: Real CC	DM (Secure)							
Serial Parameters	Serial Connections	Ethernet Connections						
Real-time data display	ing							
Serial Total Tx 🛈 746	219520 byte(s)							
Serial Total Rx 🛈 746	213992 byte(s)							
Serial Statistics								
Serial Tx (Byte) 🛈	Serial Rx (Byte) 🛈	Frame Error (Count)	Parity Error (Count)	Overrun Error (Count)	Break Error (Count)			
0	0	0	0	0	0			
Serial Signal								
DSR	DTR	RTS		CTS	DCD			
• Off	• On	• On		• Off	• Off			

Serial Connections tab:

This tab displays the current statistics of the serial port:

- Serial Total Tx: The total amount of data transmitted on the serial port since the device was powered up. The number resets when performing a power cycle.
- Serial Total Rx: The total amount of data received on the serial port since the device was powered up.. The number resets when performing a power cycle.
- Serial Tx (Byte): The total amount of data transmitted on the serial port since the TCP session is connectied. The number resets when the TCP session disconnects.
- Serial Rx (Byte): The total amount of data received on the serial port since the TCP session is connectied.. The number resets when the TCP session disconnects.
- Frame Error (Count): When NPort receives a byte of serial data, it will check if the frame format matches the serial parameters. If not, it will count one frame error.

- **Parity Error (Count):** When NPort receives a byte of serial data, it will check if the parity value is correct. If not, it will count one parity error.
- **Overrun Error (Count):** If the serial device sends data too quickly for the NPort to read, resulting in dropped data bytes, it will be considered an overrun error.
- Break (Count): When the NPort receives a break signal, it will count it as one break.
- Serial Signal: Displays the current status of all modem signals, including DSR, DTR, RTS, CTS and DCD.

Home > Diagnostics > Op	peration Mode Statistics > Po	rt 1		
← Port 1				
Operation Mode: Real C	OM (Secure)			
Serial Parameters	Serial Connections	Ethernet Connections		
Real-time data displa	ying			
Overview				
Connections	Ethernet Tx (Byte) 🗇	Ethernet Rx (Byte) 💿	Buffering (Byte) 💿	Strip Delimiter (Byte) 💿
0	0	0	0	0
Connections				
IP Address	Connection Tx (Byte)	Connection Rx (Byt	e) TCP State	Cipher Suite
No data to display.				

Ethernet Connections tab:

This tab displays the current statistics of the Ethernet port, related to serial communications:

- **Connections:** The number of TCP sessions established on this serial port.
- **Ethernet Tx (Byte):** The amount of data transmitted on the Ethernet port since the TCP session was established. The number will reset when TCP session disconnects. The number needs to match the Serial Rx (Byte). It is easy to check this on the **Diagnostics > Operation Mode Statistics** page.
- Ethernet Rx (Byte): The amount of data received on the Ethernet port since the TCP session was established. The number will reset when TCP session disconnects. The number needs to match the Serial Tx (Byte).. It is easy to check this on the Diagnostics > Operation Mode Statistics page.
- **Buffering (Byte):** Byte numbers are still stored in the NPort buffer. If the numbers above don' t match (Ethernet Tx & amp; Serial Rx or Ethernet Rx & amp; Serial Tx), it could be because there are still some data bytes in the buffer.
- **Strip Delimiter (Byte):** If you enable the Delimiter function with the Strip delimiter process, the total dropped delimiters will be recorded here.

The Connections sheet displays more detailed information about the TCP sessions:

- IP Address: This column displays the IP address connected to the NPort.
- **Connection Tx (Byte):** The amount of data transmitted on the Ethernet port since the TCP session was established. The number resets when the TCP session disconnects. The number needs to match the Serial Rx (Byte). It is easy to check this on the **Diagnostics > Operation Mode Statistics** page.
- **Connection Rx (Byte):** The amount of data received on the Ethernet port since the TCP session was established. The number resets when the TCP session disconnects. The number needs to match the Serial Tx (Byte). It is easy to check this on the **Diagnostics > Operation Mode Statistics** page.
- **TCP State:** Displays the status of this TCP session, which may be CLOSED, LISTEN, ESTABLISHED, CLOSING and TIME-WAIT.
- **Cipher Suite:** If the TCP session has the Encrypted connection feature enabled (Serial Port Settings à Secure Connection), this column will show the cipher suite used for the TCP session.

Network Monitor

The key feature of an NPort device server is to transmit serial data to the Ethernet network and vice versa. Everything that happens on the Ethernet interface will be recorded here, **Diagnostics > Network Monitor**, to help you understand the Ethernet data transmitted/received.

Home > Diagnos	ome > Diagnostics > Network Monitor								
Jetwork Monitor									
Network Statistics Network Connections									
Real-time da	Real-time data displaying								
Ethernet Pa	cket Coun	t							
Direction		Unicast		Broadcast		Multicast	Error		
Sent		2437737 (+	37737 (+2/s) 5		5 (+0/s)		9 (+0/s)	0 (+0/s)	
Received		8603682 (+12/s)		5431646 (+10/s)		1159879 (+0/s)	635742 (+0/s)		
Protocol Pa	cket Coun [.]	t							
✓ TCP	UDP	ICMP	IPv4	IPv6	PPP				
Sent			Received			Drop	Retransmitte	ed Receive RST	
1583934 (·	+2/s)		4252706 (+	4/s)		11941 (+0/s)	8 (+0/s)	9986 (+0/s)	

Network Statistics tab:

The Ethernet Packet Count sheet separates the Ethernet data in two directions, Send and Received, to count the number of unicasts, broadcasts, and multicasts. If there are any error bytes, the Error column will count them.

The Protocol Packet Count sheet separates the Ethernet data by different protocols to count the numbers of TCP, UDP, ICMP, IPv4, IPv6 and PPP.

Network Connections tab:

This tab displays the status of all the TCP sessions.

н М	Home > Diagnostics > Network Monitor Network Monitor								
Network Statistics Network Connections			onnections						
	Real-time data d	isplaying ·							
	Protocol	Recv-Q	Send-Q	Local Address	Foreign Address	State	•		
	TCP	0	0	0.0.0.0:950	0.0.0:0	LISTEN			
		0	0	AF_PACKET					
	TCP	0	0	[::]:63512	[::]:0	LISTEN			
	TCP	0	0	[::]:36418	[::]:0	LISTEN			
	ТСР	0	0	[::]:56438	[::]:0	LISTEN			
	TCP	0	0	0.0.0.0:443	0.0.0.0:0	LISTEN			
	TCP	0	0	[::]:443	[::]:0	LISTEN	•		

Ping

The Ping function is a good tool for troubleshooting. Engineers can use the NPort device server in this tool to verify the status of network nodes.

Directly input the IP address and click the PING button. The NPort will check if the target node can respond to the ping request and display the result.

Dashboard	Home > Diagnostics > Ping Ping
> ﷺ System Settings	Enter the IP address or domain name for testing. Click the "PING" button and wait for the results.
> 👗 Network Settings	Remote Host Destination Address [©]
> 🐧 Serial Port Settings	10.160.122.41 PING
> 😯 Security	Results
> 🖄 Account Management	<pre>Reply from 10.160.122.41: bytes=32 icmp_seq=0 ttl=124 time=7 ms</pre>
> 🚔 Maintenance	Reply from 10.160.122.41: bytes=32 icmp_seq=1 ttl=124 time=9 ms
🗸 🥘 Diagnostics	Reply from 10.160.122.41: bytes=32 icmp_seq=2 ttl=124
Support	Reply from 10.160.122.41: bytes=32 icmp_seq=3 ttl=124
System Log	
Operation Mode Statistics	
Network Monitor	
• Ping	
Traffic Monitor	

Traffic Monitor

The key feature of an NPort device server is to transmit serial data to the Ethernet network and vice versa. To troubleshoot, it's crucial to check if the serial data is transferred correctly to the Ethernet side. Previously, the customer service engineer had the option to use a third-party tool to indirectly check the data and provide an answer. Engineers can now use the Traffic Monitor function to compare recorded serial and Ethernet data.

Dashboard	Home > Diagnostics > Traffic Monitor						
	Traffic Monitor						
> ∃≟ System Settings	Select the port(s) to be monitored for real-time traffic data, enabling the detection of connection						
> 🛔 Network Settings	: Settings problems. The existing traffic data will be cleared automatically when leaving or restarting the page.						
> \iint Serial Port Settings	Port(s) Select Port(s) 👻 START						
> 😲 Security							
> 🖻 Account Management	✓ Hex ASCII						
> 💐 Maintenance							
🗸 🕘 Diagnostics							
Support	Time Port Direction Remote Device Length (Byte) Data						
System Log							
Operation Mode Statistics	No data to display. Select port(s) and click "START" to monitor the traffic.						
Network Monitor							
Ping							
Traffic Monitor							

As a troubleshooting tool, it may not be proper to monitor normal communication for a very long time because of the limited local memory size. Moxa recommends that the engineer use this tool to capture both abnormal and normal communication for a few minutes, allowing them to compare and analyze them.

To initiate capturing, choose the target port and click the START button; the transactions captured will be shown below. You can decide whether to view the data as HEX or ASCII.

After finishing the capturing, you have the option to click the FILTER button to narrow down the data for analysis or click the EXPORT button to save the transactions for further analysis by Moxa customer service.

Once a user completes the settings on a device server, they may need to deploy those settings to multiple devices or sites. Moxa provides the GUI tool Device Search Utility v3.0 or the CLI tool Moxa CLI Command Tool, MCC Tool, to meet this requirement.

After the devices were set up at the locations, the maintainer might need to perform routine tasks on a regular basis to run the system. This includes tasks such as firmware upgrades or password updates. The Device Search Utility v3.0 and MCC Tool can assist the maintainer in carrying out these tasks effortlessly.

Mass Configuration With GUI Tool: Device Search Utility v3.0 or Newer

The Device Search Utility v3.0 is a web-based utility. Make sure the operation system and browser version are compliant with the below version before using the tool:

Chrome:

- > For Windows 7, 8/8.1, Server 2012 and Server 2012 R2: Chrome 109 and newer
- > For Windows 10 and newer, Server 2016 and newer: All Chrome versions
- Firefox:

> For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions

- Edge:
 - > For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions

Device Search Utility							
Search Device 🗸				€ ▷~ ♡~	₽ ~		
Please click search device button					幸	:	
🗆 Seq. 🔒	Model	Lan1 IPv4	Lan1 MAC	Firmware Version			

Execute the Device Search Utility and click the Search Device button to find the target NPort(s). Remember to unlock them before any further actions.

Import/Export Configuration

Select the NPort device server(s) to import/export configuration, and then move the mouse to the More

functions to choose the 🗹 Import Configuration function.

м	OXA [®] Device Sea	① \$					
	Search Device 🗸	I					
5	Please click search devic	ce button					
(Seq.	Ô	Model	Lan1 IPv4	Lan1 MAC	Firmware Version	

Import Configuration is to import one configuration file to one or more devices with the same model. Click the BROWSER... button to find there the configuration file is saved.

Import Configuration						
Choose the configuration file to upload and import.						
Configuration File						
BROWSE						
Keep current device network settings Preserved items include mode, IP address, netmask (IPv4), prefix (IPv6), gateway, and DNS.						
CANCEL	IMPORT & RESTART					

Keep the Current Device Network Settings

If the target NPort device server(s) already has the proper IP address(es) configured, you may choose to retain the existing network settings for the device(s). Select the option.

After importing the configuration, Device Search Utility will display the success or failure in the Status & Message columns for each device.

Info: It may take a while to to end before performing	o execute this process, please other actions.	e wait for it			
Execution is completed !					
Device Name	Model Name	Status	Message	Last Updated Time	
NP5210A_8205	NPort 5210A	Failed	File format incorrect.	Feb 06, 2024 10:08:59	
NP5210A_8295	NPort 5210A	Success	Success.	Feb 06, 2024 10:08:59	
				Items per page: 10 ▼ 1 − 2 of 2 < <	> >

Your device may restart again to make the configuration effective, and it will stop your work in progress.

NOTE

For the cause of failure, please refer to the **DSU** User Manual Appendix: Error Messages.



Export Configuration is to export the configuration file from one or more devices with the same model. When exporting one device only, the file format may be *.ini, *.dat, *.txt, *.cfg, *.dec. The file name will be [ModelName] - [IP] _ [Date] .xxx, e.g., NPort6150-10.123.10.1_220724.ini.

When exporting multiple devices, the system will zip the configuration files.

Import Certificate

To build a more secure or a zero-trust network environment, you may want to set a public key infrastructure (PKI). The certificate needs to be imported into all network devices for this scenario. To simplify the loading process, the Device Search Utility supports importing certificates to multiple NPort device servers.

You can find the ${f G}$ Import Certificate function under the More functions button.

Import Certificate is to exchange certificate files to one or more devices to establish secured command/data transferring.

- Step 1: Select NPort G2 models
- Step 2: Import certificate file
- **Step 3:** Import and restart

Import Certificate	
Choose the certificate to upload and import. If on the device, it will be replaced with the new o	there is already a certificate ne.
Certificate File BROWSE	
CANCEL	IMPORT AND RESTART

Firmware Upgrade

The increasing convergence of IT and OT poses a cybersecurity risk as more OT network devices connect to office networks. Upgrading the firmware version to the latest one is crucial for all network devices. In order to meet this requirement, the Device Search Utility supports firmware updates on multiple NPort device servers.

You can find the **Firmware Upgrade** function under the More functions button. **Firmware Upgrade** is to send one firmware file to one or more devices with the same model. The firmware file extension normally comes with .ROM.

- Step 1: Select NPort G2 models
- **Step 2:** Import firmware file
- **Step 3:** Imported and the device will restart.

Mass Configuration with CLI tool: MCC Tool

The MCC Tool is a command line utility based on Windows and Linux platforms. Make sure you have downloaded the correct file for your operating system.

Unzip the file and install the MCC Tool. Execute the MCC Tool under the command line to manage the NPort device servers in the network.

Import/Export Configuration

Import/Export the device configuration for a specific device or a range of devices through the device list file. The password must be specified by the parameter or by the device list file. Device configurations are stored in individual files, using device type, IP address, and file create date as the filename. The result log is directly printed on the screen, or you can specify a result_log file for it.

```
MCC_Tool -cfg -ex -i [ip_address] -u [user] -p [password] -dk [key] -l [result_log]
MCC_Tool -cfg -ex -d [Device_list] -l [result_log]
MCC_Tool -cfg -ex -d [Device_list] -l [result_log] -t [timeout_value]
MCC_Tool -cfg -im -i [ip_address] -u [user] -p [password] -dk [key] -f [cfg_file] -l
[result_log] -n -nr
MCC_Tool -cfg -im -d [Device_list] -l [result_log] -n -nr
MCC_Tool -cfg -im -d [Device_list] -l [result_log] -t [timeout_value]
```

Parameters Description:

Command	Function	Remark
-cfg	Execute actions for configuration related	
-ex	Export the configuration file	
-im	Import the configuration file	
-i	Device IP address (ex. 192.168.1.1)	
-d	Device list	
-u	Device's user account for login	
-р	Device's password for login	
	When Exporting configuration:	
-dk	 The command decrypts the exported file with the pre-shared key. If this parameter is not used, the exported file will be encrypted by the pre-shared key set on the firmware of the device. If this parameter is used, the exported file will be decrypted to a clear-txt file for editing. When Importing configuration: If the configuration file that needs to be imported is encrypted, the command is needed with pre-shared key. If the import configuration file is without -n, The MCC tool will ignore -dk (won't return -11). If the import configuration file is with - n, the MCC tool will use pre-shared key to decrypt the encrypted file. Therefore, if the key is wrong for decrypting the file, the MCC tool will return -10. However, if the file is in plain text, and you input the pre-shared key, it will ignore the key (won't return -10).* 	
-f	The configuration file to be imported	Only for the import
-n	Keep original network parameters (includes IP, subnet mask, gateway, and DNS)	Only for the import configuration function
-nr	Do not reboot the device after importing the configuration file	Only for the import configuration function.
-1	Export result log file	
	Timeout (1 to 120 seconds)	
-t	Export function Default value: 30 seconds Import function Default	
	value: 60 seconds	

Example: Export the configuration using a device list and export the results to a result log

MCC_Tool -cfg -ex -d [DeviceList] -l [result_log]

The result_log will include the following items:

Model	ServerName	IP	MAC	FwVer	ExportCfgFile	Key	ErrCode
NPort6650;	NPort6650_123;	192.168.1.1;	00:90:e8:01:02:03;	1.3;	NP6650_192_168_1_1_20170622.ini;	moxa;	0;
NPort6150;	NPort6150_456;	192.168.1.2;	00:90:e8:04:05:06;	1.3;	NP6650_192_168_1_2_20170622.ini;	moxa;	0;

Example: Import the configuration to a device list (with restarting the units) and export the results to a result log.

MCC_Tool -cfg -im -d [DeviceList] -l [result_log]

The result_log will include the items below:

Model	ServerName	IP	MAC	FwVer	CfgFile	Key	ErrCode
NPort6650;	NPort6650_123;	192.168.1.1;	00:90:e8:01:02:03;	1.3;	NP6650_192_168_1_1_20170622.ini	moxa;	0;
NPort6150;	NPort6150_456;	192.168.1.2;	00:90:e8:04:05:06;	1.3;	NP6650_192_168_1_2_20170622.ini	moxa;	0;

Example: Import the configuration to a device list without restarting the units and export the results to a result log.

MCC_Tool -cfg -im -d [DeviceList] -nr -l [result_log]

Firmware Upgrade

With the IT/ OT convergence trend, office networks may see an increase in OT network devices, posing cybersecurity risks. Upgrading the firmware version is crucial for all network devices. The MCC Tool allows users familiar with the command line interface to update the firmware on multiple NPort device servers to fulfill this need.

The NPort 6000-G2 Series supports password protection by default and cannot be disabled. The password(s) must be specified by a command parameter or by the DeviceList file before upgrading the firmware and restarting a specific device (or multiple devices simultaneously).

```
MCC_Tool -fw -up -i [ip_address] -u [user] -p [password] -f [firmware_file] -l [result_log]
```

MCC_Tool -fw -up -d [Device_list] -l [result_log]

MCC_Tool -fw -up -d [Device_list] -l [result_log] -t [timeout_value]

Parameters Description:

Command	Function	Remark
-fw	Execute actions for firmware related	
-up	Upgrade firmware version	
-i	Device's IP address (192.168.1.1)	
-u	Device's user account for login	
-р	Device's password for login	
-d	Device list	
-f	Firmware file to be upgraded	
-1	Export result log file	
+	Timeout (1~1200 seconds)	
-1	Default value: 800 seconds	
-print	Print upgrade process status message	

Example: Upgrade firmware using a device list and capture the results in an import log.

MCC_Tool -fw -u -d [DeviceList] -l [result_log]

The result_log will include the items below:

Model	ServerName	IP	MAC	FwFile	ErrCode
NPort6650;	NPort6650_123;	192.168.1.1;	00:90:e8:01:02:03;	NP6000_V1.3.rom;	0;
NPort6150;	NPort6150_456;	192.168.1.2;	00:90:e8:04:05:06;	NP6000_V1.3.rom;	0;

Change Password

Due to the IT/OT convergence trend, an increasing number of companies require their employees to regularly update their login password, as do the network devices. The owner/maintainer of the network devices may need to update the password regularly. The MCC Tool helps you to ease this routine job by generating a small script to update the password.

Set the password of the target device specified by an IP address. The current password must be specified by a parameter or by the Device List file.

MCC_Tool -pw -ch -i [ip_address] -u [user] -p [old_password] -npw [new_password]

MCC_Tool -pw -ch -d [Device_list] -nd [device_list_new_password] -l [result_log]

MCC_Tool -pw -ch -d [Device_list] -nd [device_list_new_password] -l [result_log] -t [timeout_value]

Parameters Description:

Command	Function	Remark
-pw	Execute actions for password	
-ch	Change password	
-npw	The new password for the specific user	
-i	Device's IP address (192.168.1.1)	
-u	Device's user account for login	

Command	Function	Remark
-р	Device's password for login (old password)	
-d	Device list	
-nd	The Device list with new password settings	Youwill need to assign a new password in the Device List when using -nd command.
-1	Export result log file	
-nr	Don't reboot the device after changing the password	
-t	Timeout (1to120 seconds) Default value: 60 seconds	

Example: Set the new password as "5678" and restart the device to make it effective. Print the result on the screen.

MCC_Tool -pw 5678 -i 192.168.1.1 -u admin -p moxa

Example: Set the new password from a device list and then restart the device to make it effective. Export the results to a result log

MCC_Tool -pw DeviceList_New -d [DeviceList] -l [result_log]

The result_log will include the items below:

Model	ServerName	IP	MAC	FwVer	User	PWD	ErrCode
NPort6650;	NPort6650_123;	192.168.1.1;	00:90:e8:01:02:03;	1.3;	admin;	5678;	0;
NPort6150;	NPort6150_456;	192.168.1.2;	00:90:e8:04:05:06;	1.3;	admin;	moxa;	0;

9. Advanced Settings of NPort Windows Driver Manager

The NPort Windows Driver Manager has additional capabilities apart from being a driver for the virtual COM application. There are many advanced settings to help you face different user scenarios. In this chapter, we will explain which functions/settings are useful in different scenarios.

Configure the mapped COM ports

After mapping the COM ports, refer to Chapter 4 for instructions. In many instances, the legacy COM port software can establish communication with the serial devices by opening either the COM port or the TTY port. In specific cases, the user may need to modify the advanced settings of the NPort Windows Driver Manager for certain applications.

To reconfigure settings for a specific serial port on the NPort device server, select the corresponding row and click the **Setting** icon in Real COM Mode/Reverse Real COM Mode.

🐝 NPort Windo	vs Driver Manager	_	\times
<u> </u>	ng C <u>o</u> nfiguration <u>V</u> iew <u>H</u> elp		
Exit Ad	r Remove Apply Undo Setting		
No COM Po	it 🛆 Address 1	Address 2	
1 COM1	192.168.127.254 950:966 (Port1)		
2 COM5	192.168.127.254 951:967 (Port2)		
3 COM6	192.168.127.254 952:968 (Port3)		
4 COM8	192.168.127.254 953:969 (Port4)		

Change the number of a mapped COM port

Some legacy COM port software is restricted to using specific COM ports like COM1 or COM2. Nevertheless, the NPort Windows Driver Manager has the capability to automatically assign COM ports starting from COM3. To modify the COM port number, click on the **Setting** button and locate the **COM Number** drop-down menu in the Basic Settings. Simply select the COM port requested by the legacy COM port software.

	7 Port(s) are Selected.		
Basic Settings Adv	anced Settings Serial Para	ameters Sec	urity IPv6 Setting
TT Auto Emmand	ine COM Number for Colory	- d Davia	
J♥ Auto Enumera	ang COM Number for Select	ed Forts.	
COM Number	COM10 (current) (in use)		
	COM45 (in use)	<u>^</u>	
	COM46 (in use)		
Enable CO	COM47 (in use)		
	COM48 (in use)	·L	
Index	COM50 (in use)		
Index	COM50 (in use) COM51 (in use)		Add COM
Index	COM50 (in use) COM51 (in use) COM52 (in use)	~	Add COM
Index	COM50 (in use) COM51 (in use) COM52 (in use)	~ _	Add COM

To assign the serial ports of the NPort device server to COM port numbers in sequence, choose **Auto Enumerating COM Number** option for selected ports.

COM Splitting

When you activate COM Splitting, you can use multiple COM port software to communicate with the same serial device. Only one software can open/occupy a COM port, causing others to wait until it is closed. The COM Splitting function allows multiple COM port numbers to be assigned to the same serial port on the NPort device server. The first software accesses COM1, while the second software uses COM2, but both communicate with the same serial device.

Since both softwares will be using the same serial port and device, they must coordinate when the first software sends a command and when the second one does. Or there may be a data collision. Using this feature could be a better option for enabling one-way communication from the serial device to multiple host PCs on the Ethernet network. Let's say there's a serial temperature sensor that constantly updates temperature data to the control servers. If the temperature gets too high or too low, one of the servers will send a request to activate the fan or heater. The purpose of the second server might be to serve as the database for recording temperature readings.

The COM Splitting function will group all the selected COM ports into one COM port. Even if you use varying software to communicate via different COM port numbers, all the software will receive identical data from the serial device.

In order to handle various host PCs connecting to the same serial port, it is necessary to modify the **Max**. **Connection** setting according to the number of ports grouped in your NPort. For example, if you split to two COM ports, **Max**. **Connection** needs to be adjusted to 2. The grouped serial ports must be directed to the same NPort device server; they cannot be combined from different NPorts.

Enabled COM Splitting

on Number.	1 Port(s) are Selected.	
asic Settings Adv	anced Settings Serial Parameters	Security IPv6 Settings
🗖 Auto Enumera	ting COM Number for Selected Ports.	
COM Number	COM5 (current) (in use)	
	,,	
🔽 Enable CO	IM Splitting	
Index	COM Number	
		Add COM
		Berrove COM

- 1. Select the target COM port number and click the **Setting** button.
- 2. Select to enable the Enable COM Splitting function.
- 3. Add COM to select target COM ports for splitting; the COM port must be available.

Add Split COM		×
COM Number	COM30	

Settings Advanced Settings Serial Parameters Security IPv6 Auto Enumerating COM Number for Selected Ports. COM Number COM14 (current) (in use) • Index COM Number • Add COM 1 COM14 Add COM 2 COM27 Add COM 3 COM28 Remove COM	in realized.	I Port(s) are Selected.	
Auto Enumerating COM Number for Selected Ports. COM Number COM14 (current) (in use)	ic Settings Adv	vanced Settings Serial Parame	eters Security IPv6 Se
COM Number COM14 (current) (in use)	Auto Enumera	ting COM Number for Selected	Ports.
Enable COM Splitting Index COM Number COM 14 COM14 COM27 COM28 Remove CO	COM Number	COM14 (current) (in use)	v
Index COM Number 1 COM14 2 COM27 3 COM28 Remove CO			
Index COM Number 1 COM14 2 COM27 3 COM28	Enable CC	0M Splitting	
1 COM14 2 COM27 3 COM28 Remove CO	Index	COM Number	
3 COM28 Remove CO	2	COM14 COM27	Add COM
Remove CC	3	COM28	
			Remove COM
	1		
? Help	? Help		

4. After pressing **OK**, check if the COM ports you just selected are grouped together. Click **Apply** to save the change.

<u>F</u> ile	COM Mapping Configuration View I	lelp	
Ēxi	t Add Remove Apply Unc	o Setting	
No	COM Port	Address 1	Address 2
1	COM1	192.168.127.254 950:966 (Port1)	
2	COM5	192.168.127.254 951:967 (Port2)	
3	COM6	192.168.127.254 952:968 (Port3)	
4	COM8	192.168.127.254 953:969 (Port4)	
5	COM9	192.168.127.101 950:966 (Port1)	
6	COM12	192.168.127.101 951:967 (Port2)	
7	COM13	192.168.127.101 952:968 (Port3)	
8	[S] COM14, COM27, COM28	192.168.127.101 953:969 (Port4)	
9	COM15	192.168.127.101 954:970 (Port5)	
10	COM16	192.168.127.101 955:971 (Port6)	
11	COM17	192.168.127.101 956:972 (Port7)	
12	COM18	192.168.127.101 957:973 (Port8)	
13	COM19	192.168.127.102 950:966 (Port1)	
14	COM20	192.168.127.102 951:967 (Port2)	
15	COM21	192.168.127.102 952:968 (Port3)	
16	COM22	192.168.127.102 953:969 (Port4)	
17	COM23	192.168.127.102 954:970 (Port5)	
18	COM24	192.168.127.102 955:971 (Port6)	
19	COM25	192.168.127.102 956:972 (Port7)	
20	COM26	192.168.127.102 957:973 (Port8)	

5. Once the COM port number changes to black text, the software can open multiple COM Splitting ports to receive serial data.

Advanced Setting

Transferring serial data to an Ethernet network can result in timing differences and variations in behavior compared to TCP socket behavior. The NPort Windows Driver Manager offers various advanced settings to accommodate these differences, ensuring that your original software remains unchanged and communication functions properly.

COM Port Setting X
Port Number: 1 Port(s) are Selected.
Basic Settings Advanced Settings Serial Parameters Security IPv6 Settings
Apply All Selected Ports
The FIFO settings will overwrite the firmware setting. Tx Mode
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
Enable Auto IP Report
MAC Address 00:90:E8:9A:DF:7F
? Help
✓ OK X Cancel

Tx Mode

Because Ethernet and serial technology have significantly different speeds, the serial line's maximum baudrate is only 921,600bps, while Ethernet's minimum speed is 10Mbps. The Tx Mode offers two options for the driver to mimic either Ethernet or serial bus behavior more closely.

The default setting for the Tx Mode is **Hi-Performance** mode, which sends as much data as possible to the serial side. This behavior will be closer to Ethernet. The driver buffer will temporarily store the data before sending it all at once over Ethernet, resulting in higher data delivery throughput.

This might pose issues for older serial applications or devices that lack sufficient buffer or performance to handle large amounts of data quickly. To handle these situations, switch the Tx Mode to **Classical** mode. In Classical mode, the NPort sends the serial data one byte at a time, eliminating the need for a large buffer size in the serial device. This is designed to work with serial devices like these. Additionally, the **Classical** mode allows for quicker data delivery by minimizing latency. The serial data can bypass the driver buffer's waiting time.

FIFO

This FIFO setting is the same setting on the NPort device server. If they're not the same, the value in the NPort Windows Driver Manager will overwrite the setting on the firmware and apply either Real COM mode or Reverse Real COM mode.

The Enable FIFO function is enabled by default for improved data throughput. There are two scenarios you may consider disabling the Enable FIFO function (uncheck the checkbox).

- The serial device does not have FIFO/buffer or does not support flow control function. In this case, the serial device may not be able to receive the serial data from NPort on time, which means that some data might be dropped.
- The data latency is more important than data throughput. Higher data throughput involves temporarily storing data in the buffer to enable sending larger amounts of data at once. This behavior may result in slower latency for individual data. If maintaining low latency is a priority for reading data correctly on the serial device, it is recommended to disable the Enable FIFO function.

This field enables or disables the 512-byte FIFO buffer. The NPort 6000-G2 provides FIFO buffers for each serial port, for both the Tx and Rx signals.

Network Timeout

This function shares similarities with the **TCP alive check time** function on the NPort device server. The only difference is the source of each function. The source of the **TCP alive check time** is the NPort device server; it will check if the remote host PC is alive or not. The source of the **Network Timeout** function is the host PC (which installed the NPort Windows Driver Manager); it will check if the remote NPort is alive or not. Use this option to prevent blocking when the target NPort is unavailable.

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. Following the execution of the PurgeComm() function, the NPort driver persists in querying the firmware of the NPort multiple times to ensure the absence of queued data in the firmware buffer, instead of solely flushing the local buffer on the host PC. The purpose of this design is to meet specific requirements. The additional time required for Ethernet communication means it may take longer (about several hundred milliseconds) than a native COM1. PurgeComm() is noticeably faster on native COM ports than on mapped COM ports on the NPort 6000-G2. In order to support applications with faster response requirements, the new NPort driver incorporates a Fast Flush option. This function is enabled by default.

If you disable Fast Flush and notice a significant decrease in performance for COM ports mapped to the NPort 6000-G2, check if your application uses "PurgeComm()" functions. If so, try enabling the Fast Flush function and see if there is a significant improvement in performance.

Auto Network Reconnection

While serial communication is always connected, Ethernet communication is not. The NPort Windows Driver Manager offers Auto Network Reconnection for automatic re-establishment of connections, ensuring the serial device is always considered connected and capable of sending data.

If this option is turned on, the driver will keep trying to reconnect the TCP connection if the NPort 6000-G2 doesn't respond to "check-alive" packets, which are sent in the background. The Network Timeout function, which cannot be disabled, determines the timing of these packets..

Always Accept Open Requests

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



Return Error If Network Is Unavailable

We discovered that some legacy COM port software always opens a fixed range of COM ports, from COM1 to COM10, when executed by the user. For the real application, only COM3, COM5 and COM7 are available, so the software will always return failure since it cannot open the COM1 to COM10 successfully. To temporarily resolve this issue with the outdated software, you can deactivate the **Return error if network is unavailable** option..

Disabling this option will prevent the driver from reporting errors for failed connections to the NPort 6000-G2. Enabling this option will result in the Win32 Comm function returning the error code "STATUS_NETWORK_UNREACHABLE" if a connection to the NPort 6000-G2 cannot be established. Typically, this indicates that your host's network connection is offline, possibly due to a disconnected cable. But if you're able to access other network devices, it's likely that the NPort 6000-G2 is either disconnected or not powered on. To use this feature, make sure **Auto Network Re-Connection** is turned on.

Ignore TX Purge

When programming for legacy COM port software, it is common practice to clear the buffer before and after writing data, to prevent any unwanted data from being present. In the past, there were no troubles, making it an effective method to avoid sending incorrect data to the serial device.

Due to advancements in technology, PCs now have significantly improved performance compared to the past. There's a possibility that the clear buffer command might be sent to the NPort device server prematurely, following the write command The NPort may still have correct data in its buffer, but it will be lost when the clear buffer command, which is the Win32 API PurgeComm command, is received. You might notice that the received serial data is missing the last few bytes. Enabling the **Ignore TX Purge** function might be the solution when this occurs.

Security

When addressing the growing cybersecurity threats, it is crucial to devise ways to protect vital data on serial devices. The serial bus has a short communication distance and is difficult to steal, especially in secure manufacturing facilities with guards. However, it's a different situation when it comes to using a device server to transmit serial data over an Ethernet network. The Ethernet network is much more vulnerable than the serial bus. The NPort device server enables encryption of Ethernet network communications. With the NPort Windows Driver Manager, you can encrypt communications on the host PC.

Select target serial port, click the **Setting** button, and switch to **Security** tab:

Basic	Setting	s Advanced Settings	Serial Parameters	Security	IPv6 Setting
Π	No	File Name	Issue by	Expired	date
	1	cert_RSA.pem	HTTPS Certifica	2022-9-	18
	<				>
1 1					
			Import	De	elete
v	Apply A	Il Selected Ports Ible Encryption Data only (For model na Data and command (Fo Certificate authenticatic	Import	De G2')	lete

Enable Encryption

Enable the SSL encryption for data and command transmission of the selected COM port.

Data Only

The NPort 6000 Series supports data encryption only. Select this option if you are using the NPort 6000 Series.

Data and Command

The NPort 6000-G2 Series supports both data and command encryption. Select this option if you are using NPort G2 models.

Certification Authentication

This security enhancement allows you to verify the server and client using an imported certificate from a trusted Certificate Authority (CA). Click the **Import** button above to import the certification of your own.

Keep Connection

For quicker operations, it is recommended to enable this option if the COM port software frequently opens and closes the COM port with data encryption and the NPort is dedicated to one host. The opening time of a COM port with encryption enabled will be brief (300 to 500ms) due to the SSL protocol. By enabling these options, you can ensure a continuous SSL connection for the COM port. The opening and closing of the COM port will be faster here. The Keep Connection feature is not supported in Reverse Real COM mode.

Importing/Exporting COM mapping

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

File	COM Mapping	Configura	tion Vi	ew Help	1			
Ēx	🚮 Add	Ctrl+N Ctrl+D	Apply	Undo	Setting			
o	Setting	Ctrl+C			Address 1	Address 2		
	Apply Undo	Ctrl+S Ctrl+Z			192.168.1.222 950:966 (Port1) 192.168.1.222 951:967 (Port2) 192.168.1.222 952:968 (Port3) 192.168.1.222 953:969 (Port4)			
	LUM52				192.168.1.201 950:966 (Port1) 192.168.1.201 951:967 (Port2) 192.168.127.254 950:966 (Port1) 192.168.127.254 950:966 (Port2) 192.168.127.254 951:967 (Port2)			
	COM53				00:90:e8:12:fa:42 (Port1)			

Port Sniffer Wizard

At times, engineers may require an analyzer to track the commands and responses exchanged between the Windows platform and the NPort Windows Driver Manager to diagnose communication issues. The Port Sniffer Wizard is a tool that tracks and records activity on all serial ports of a system. Its advanced filtering and search capabilities make it a powerful tool for exploring Windows functionality, monitoring port usage, and troubleshooting system or application configurations.

How to Use the Port Sniffer

Click **Port Sniffer Wizard** in the drop-down menu under Help.

<u>File</u>	OM Mapping	Configura	ition ⊻iew	<u>H</u> elp					
î.	d.	65		🤣 Online Help					
Exit	Add	Remove	Apply U	Port Sniffer Wizard					
No	COM Port	Δ.		About			Address 2		
1	COM11			192.168.127.254	950:966	(Port1)			
2	COM12			192 168 127 254	951.967	(Port2)			

Task Page

Select the task you need, and click Next:

- Capture serial data logs
- Monitor runtime serial data (for developers)
- Display existing settings
- Delete existing settings

Moxa Port Sniffer	×
Select your task	
Capture serial data logs	
O Monitor runtime serial data (for developers)	
O Display existing settings	
O Delete existing settings	
Click Next, select COM ports to capture serial logs.	
< Back Next > Ca	incel

Capture Serial Data Logs

If errors occur, you can capture serial data logs from specific ports and send the logs back to Moxa. We can help you check the problems. Select this function to export log files.

NOTE

Enabling the capture serial data logs function may cause slight latency.

Step 1: COM port setting

- Select one or more COM ports to capture.
- Turn on the function you need.
 - Display IRP direction

IRP will inform users whether an error occurs when issuing a command or returning a response.

Hide sensitive data The system will hide the data, so that you don't need to worry about data leakage. Used specifically for sensitive data.

Port Sniffer	×					
Select COM ports to capture	 Display IRP direction Log to file Hide sensitive data Refresh 					
Click Next, set the parameters of logging files. Click Back, return to the task page.						
	< Back Next > Cancel					

Step 2: Set the parameters of logging files

• Enable log service.

NOTE

Disabling the log service will not capture the serial data.

- Choose the location of log files.
- Set the max. number of log files and max. file size (MB).

Poi	rt Sn	iffer		\times			
	Set	the attribute of logging file					
		Log Service :	ENABLED ~				
		Location of log files :	C: \mxportsf				
		Max. number of log files :	10				
		Max. file size (MB) :	30				
Click Finish, Sniffer will start/stop to log serial data in the background. Click Back, return to check the COM port settings.							
			< <u>B</u> ack Finish Cancel				

• Click finish and check log files at the locations you set.

Monitor Runtime Serial Data (for developers)

The difference between the "Capture serial data logs" and "Monitor runtime serial data" functions is that the latter presents the status in real time.

Step 1: COM port setting

- Select one or more COM ports to monitor the serial log in the runtime.
 - Turn on the function you need.
 - Display IRP direction

IRP will inform users whether the error occurs when issuing a command or returning a response.

Log to file

Export log files simultaneously. (Exporting log files simultaneously will cause latency)

NOTE

Monitor runtime is usually used by developers or serial driver programmers to troubleshoot. Download debug tools like "DebugView" from a third party to view the real-time status.

Hide sensitive data

The system will hide the data. Used specifically used for sensitive data.

Port Sniffer		\times				
Select COM ports to capture	 Display IRP direction Log to file Hide sensitive data Refresh 					
Click Next, set the parameters of logging files. Click Back, return to the task page.						
	< Back Next > Cance	1				

Step 2: Set the parameters of logging files. Skip this step if you disabled Log to file function

- Enable log service.
- Choose the location of log files.
- Set the max. number of log files and max. file size (MB).

Port S	niffer		×
Se	t the attribute of logging file		
	Log Service :	ENABLED ~	
	Location of log files :	C: \mxportsf	
	Max. number of log files :	10	
	Max. file size (MB) :	30	
C	lick Finish, Sniffer will start/stop lick Back, return to check the CC	to log serial data in the background. M port settings.	
		< Back Finish Cancel	

Step 3: Set the environment settings.

- Enable the Debug Print Filter to dump messages from the kernel. The setting will take effect after the system restarts.
- NOTE

- 1. Disabling the Debug Print Filter will not output the serial data to the monitor.
- 2. You can see the runtime serial data from the debug output monitor.

Port Sniffer X	
Environment settings Sniffer Service : Debug Print Filter : DisABLED Note: In Windows Vista or later versions, you must enable the Debug Print Filter to dump messages from kernel. This setting will take effect after system restart. Then, you can see the run-time serial data from the debug output monitor, like DebugView. (DebugView is an application distributed by Sysinternals ®)	
Click Finish, Sniffer will enable the service and apply the filter. Then, the sniffer will output serial data to the debug monitor. Click Back, return to check the COM port settings.	
< <u>B</u> ack Finish Cancel	

• Click **finish** and open "DebugView" to Monitor runtime serial data.

👯 De	ebugView on \\JASONCHEN-	- NB (local)	×
File	Edit Capture Options Co	omputer Help	
i 😅 i	3 🛛 🍳 😣 🎢 🦛		
#	Time	Debug Print	^
1	0.0000000		- 11
2	0.00000310	Moxa Fort Shifter Driver is loaded successfully	
3	0.00000490	Build Into: Ver1.7 Build 22101315	- 11
5	17.17764664	manaster 1 MOVA UPart COM Part 1 (COMA) IDD MU CREATE STATUS SUCCESS	
6	17 17768288	mynority, 1, WOAR OF OF OF OWNER OF THE COMPANY, INC. MELANDARID, OF THE STATUS SUCCESS. Rand Rate: 1200	
ž	17.17769814	mxportsf, 3, MOXA UPort COM Port 1 (COM44), IOCTL SERIAL GET LINE CONTROL STATUS SUCCESS, 7-NONE-1	
8	17.17771149	mxportsf, 4, MOXA UPort COM Port 1 (COM44), IOCTL SERIAL GET CHARS, STATUS SUCCESS, EOF:0 BR:0 EV:0 XON:17 XOFF:19	
9	17.17772865	mxportsf, 5, MOXA UPort COM Port 1 (COM44), IOCTL_SERIAL_GET_HANDFLOW, STATUS_SUCCESS, Handshake:0x000000001 FlowReplace:0x00000000 XonLimit:64 XoffLimit:16	
10	17.17774582	mxportsf, 6, MOXA UPort COM Port 1 (COM44), IOCTL_SERIAL_SET_TIMEOUTS, STATUS_SUCCESS, RI:-1 RM:0 RC:0 WM:0 WC:0	
11	17.17775917	mxportsf, 7, MOXA UPort COM Port 1 (COM44), IOCTL_SERIAL_GET_BAUD_RATE, STATUS_SUCCESS, Baud Rate: 1200	
12	17.1777/252	mxportst, 8, MOXA UPort COM Port I (COM44), IOCTL SERIAL GET LINE CONTROL, STATUS SUCCESS, 7-NONE-1	
13	17.17778387	mxports, 9, MOXA UPort COM Port I (COM44), IOCIL SERIAL GET CHARS, STATUS SUCCESS, SOF DERU EVU XONIT XOPFIL9	
14	17.1779922	mxports, 10, MOXA 0Fort COM Fort 1 (COM44), IOCIT_SERIAL_051_HAUDELOW, 51A 105_SUCCESS, Handsazet8000000000 FlowRepiace5000000000 AonLimit50 AonLimit50	
16	17 17905672	myports, 1, MOVA OFOIL COM FOIL (COM44) IOCIT_SERIAL_SET_PROD_KATELS, STATUS SUCCESS, Balt Rate, 50400	
17	17,17813683	mynorth 13 MOXA UPort COM Port 1 (COM44) IOCTL SERIAL SET DTR STATUS SUCCESS	
18	17.17829514	mxportsf, 14, MOXA UPort COM Port 1 (COM44), IOCTL SERIAL SET LINE CONTROL, STATUS SUCCESS, 8-NONE-1	
19	17.17845154	mxportsf, 15, MOXA UPort COM Port 1 (COM44), IOCTL_SERIAL_SET_CHARS, STATUS_SUCCESS, EOF:0 BR:0 EV:0 XON:17 XOFF:19	
20	17.17846489	mxportsf, 16, MOXA UPort COM Port 1 (COM44), IOCTL_SERIAL_SET_HANDFLOW, STATUS_SUCCESS, Handshake:0x00000001 FlowReplace:0x80000040 XonLimit:64 XoffLimit:16	
21	17.17847633	mxportsf, 17, MOXA UPort COM Port 1 (COM44), 0x001b2000, STATUS_SUCCESS	
22	17.17848778	mxportsf, 18, MOXA UPort COM Port 1 (COM44), IOCTL_SERIAL_GET_TIMEOUTS, STATUS_SUCCESS, RI:-1 RM:0 RC:0 WM:0 WC:0	
23	17.17849922	mxportsf, 19, MOXA UPort COM Port 1 (COM44), IOCTL_SERIAL_SET_TIMEOUTS, STATUS_SUCCESS, RI-1 RM:0 RC:0 WM:0 WC:100	
24	17.17851830	mxportst, 20, MOXA UPort COM Fort I (COM44), IOCTL SERIAL_GEL_BAD_KATE, STATUS SUCCESS, Baud Rate: 38400	~
<			> .::

Display existing settings

Step 1:	Click Display	existing	settings to	view the	current setting.
---------	---------------	----------	-------------	----------	------------------

Moxa Port Sniffer	×
Select your task	
Capture serial data logs	
O Monitor runtime serial data (for developers)	
Display existing settings	
O Delete existing settings	
Click Next, view the current settings	
< Back Next > Cance	ł

Step 2: Check the COM port settings.

Port Sniffer		×
Select COM ports to capture	1	
COM Number	✓ Display IRP direction	
	Log to file	
	✓ Hide sensitive data	
	Refresh	
Click Next, check the parameters o Click Back, return to the task page	of logging files.	
	< Back Next > Car	ncel

Step 3: Check the parameters for logging files.

Port Sniffer	×
Set the attribute of logging file	
Log Service : ENABLED	
Location of log files : C: \mxportsf	
Max. number of log files : 10	
Max. file size (MB) : 30	
Click Next, check the environment settings.	
Click Back, return to check the COM port settings.	
a Pade Next S Ca	acal
	itei

Step 4: Check the environment settings.

Po	rt Sniffer	×
	Environment settings Sniffer Service : ENABLED Debug Print Filter : ENABLED Note: In Windows Vista or later versions, you must enable the Debug Print Filter to dump messages from kernel. This setting will take effect after system restart. Then, you can see the run-time serial data from the debug output monitor, like DebugView. (DebugView is an application distributed by Sysinternals ®)	
	Click Finish, finish Port Sniffer settings. Click Back, return to check the COM port settings.	
	< Back Finish Cancel	

Step 5: Click **Finish** to finish Port Sniffer settings.

Delete existing settings

Step 1:	Select	Delete	existing	settings.
---------	--------	--------	----------	-----------

Moxa Port Sniffer	\times
Select your task	
Capture serial data logs	
O Monitor runtime serial data (for developers)	
O Display existing settings	
• Delete existing settings	
Click Finish, delete all COM ports to capture or monitor.	
< Back Finish Ca	ncel

Step 2: Click **Finish** to delete existing settings.

We have designed this section to list the Frequently Asked Questions so that users can solve their own questions.

Q1. If I disable the Web console, how can I change the settings?

The web console is the major management console of the NPort 6000-G2. It configures all the functions of the NPort 6000-G2 and monitors the status of the device server. We don't recommend you to disable the web console service.

When operating in an extremely high-risk cybersecurity environment, you may opt to disable the web console service after completing the configuration and confirming that no further adjustments are needed. The web console service can be enabled through SNMP private MIB in this scenario.

If the SNMP Agent service is also turned off, the only way to reset the device to factory settings and reenable the web console service is to use the hardware reset button.

Q2. Can different users use the same account to log in to the device server?

Different connections are not allowed for one user account on the device server because of cybersecurity measures.

For example, the administrator is already logged into the NPort as account "admin". And, now a second user uses "admin" to log in to the same device server:

- If the password is wrong, the device server will record a login failed event on the syslog. The administrator can check the syslog to notice this failure.
- If the password is correct, the user will log in to the device and the former connection will be terminated. The administrator will be notified by this unexpected behavior. By logging in again, the administrator can find the IP address from the syslog to prevent the user to try again.

Q3. Why Device Search Utility v3.0 and later cannot be executed on my Windows 7 or Windows 2008 R2?

Since the Device Search Utility v3.0 is a web-based application, it has the minimum requirements for the browser version and operating system:

- Chrome:
 - ▶ For Windows 7, 8/8.1, Server 2012 and Server 2012 R2: Chrome 109 and newer
 - > For Windows 10 and newer, Server 2016 and newer: All Chrome versions
- Firefox:
 - > For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions
- Edge:
 - > For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions

Q4. How can I check the CRC value of the runtime settings?

The NPort 6000-G2 provides private MIB for the CRC value of the runtime settings, the OID is xxx. Use a MIB browser or send a SNMP command to get the CRC value.

Q5. Is there an easier way to copy the settings of a NPort 6000 device server to a NPort 6000-G2?

If you have NPort 6000 device servers on site, you may wonder how to transfer the same settings to the NPort 6000-G2 device servers. Is it possible to configure each setting individually, one page at a time, even if it takes a lot of time?

The NPort 6000-G2 device servers have the capability to import the configuration file directly from a NPort 6000. Export the NPort 6000 settings and import them into the NPort 6000-G2. The NPort 6000-G2 can then replace the device server on site.

Q6. If there is a power outage during a firmware upgrade, how can I recover the device?

The NPort 6000-G2 supports a fail-safe mechanism during firmware upgrade. If there is a power outage, just power up the device. The device will be ready with the previous version of firmware. Try again or arrange another proper time to upgrade the firmware.

Q7. Before calling Moxa customer service, is there anything I can prepare to save both of us time?

Please find the **Support > Diagnostic Information** and click the **DOWNLOAD** button to collect all the settings and logs for troubleshoot. This will help Moxa customer service to understand the case background and try to replicate the issue you are experiencing.



As mentioned in Chapter 2, the pin assignment of NPort 6000-G2 Series is as below:

The serial port RS-232/422/485 pin assignment (male DB9):

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



The Ethernet port pin assignment (RJ45):

Pin	RJ45
1	Tx+
2	Tx-
3	Rx+
4	-
5	-
6	Rx-
7	-
8	-



Cable Wiring Diagrams

To connect dserialhe serial devices/Ethernet devices, customize the connecting cable to connect the NPort and the serial/Ethernet devices. Here are some of most popular cable wiring for your reference.

Ethernet Cables

There are two major types of the RJ45 Ethernet cable, straight-through and crossover cables.



Serial Cables

Depending on different connectors on the serial devices, we provide several serial cables to connect easily to the NPort and the device.

CBL-RJ45F9-150

The CBL-RJ45F9-150 is a 150-cm long cable to connect the NPort's DB9 male connector to a serial device with RJ45 serial connector. The pin assignment of this cable is as below:

Pin on DB9 male	RS-232 signal	Pin on RJ45	RS-232 signal	
1	DCD	6	DCD	
2	RxD	4	RxD	
3	TxD	5	TxD	
4	DTR	1	DTR	
5	GND	3	GND	
6	DSR	8	DSR	
7	RTS	7	RTS	
8	CTS	2	CTS	
9	_	-	-]

CBL-RJ45SF9-150

Industrial applications such as the factory floor are typically electrically noisy environments. The CBL-RJ45SF9-150 is a 150-cm long cable, shielded to protect the signals from the noise and connect the NPort's DB9 male connector to a serial device with a RJ45 serial connector. The pin assignment of this cable is as below:

Pin on DB9 male	RS-232 signal
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	-

Pin on RJ45	RS-232 signal
6	DCD
4	RxD
5	TxD
1	DTR
3	GND
8	DSR
7	RTS
2	CTS
_	_



CN-20070

The CN-20070 is a 150-cm long cable to connect the NPort's DB9 male connector to a serial device with a 10-pin RJ45 serial connector. The pin assignment of this cable is as below:

Pin on DB9 male	RS-232 signal
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	-
10	-

Pin on 10-pin RJ45	RS-232 signal
1	DCD
5	RxD
6	TxD
2	DTR
7	GND
9	DSR
8	RTS
3	CTS
-	-
_	_



ınal

Moxa provides different accessories for different user scenarios. The scenarios will be introduced with the appropriate accessory in this appendix.

Convert the DB9 Connector to Other Connectors

The DB9, RJ45 and terminal block are the most popular interfaces on serial communications. The NPort device server has built-in DB9 connector as the default. Moxa provides a connector to convert the DB9 interface to other connectors.

ADP-RJ458P-DB9F

The ADP-RJ458P-DB9F is a connector that transforms the NPort's DB9 male connector to an 8-pin RJ45 serial connector. The pin assignment of this connector is as below:

Pin on DB9 male	RS-232 signal	Pin on RJ45	RS-232 sig
1	DCD	6	DCD
2	RxD	4	RxD
3	TxD	5	TxD
4	DTR	1	DTR
5	GND	3	GND
6	DSR	8	DSR
7	RTS	7	RTS
8	CTS	2	CTS
9	-	-	-



Mini DB9F-to-TB

The Mini DB9F-to-TB is a connector that transforms the NPort's DB9 male connector to a 5-pin terminal block serial connector. This connector usually is used on a RS-422/RS-485 application. The pin assignment of this connector is as below:

Pin on DB9 male	RS-422 signal	F
1	TxD-(A)	
2	TxD+(B)	
3	RxD+(B)	
4	RxD-(A)	
5	GND	
6	-	
7	-	
8	_	
9	_	

Pin on RJ45	RS-422 signal
2	TxD-(A)
1	TxD+(B)
3	RxD+(B)
4	RxD-(A)
5	GND
-	-
-	-
-	-
-	-



Pin on DB9 male	4w RS-485 signal
1	TxD-(A)
2	TxD+(B)
3	RxD+(B)
4	RxD-(A)
5	GND
6	-
7	-
8	-
9	-

Pin on RJ45	4w RS-485 signal
2	TxD-(A)
1	TxD+(B)
3	RxD+(B)
4	RxD-(A)
5	GND
-	-
-	-
-	-
_	-

Pin on DB9 male	2w RS-485 signal
1	_
2	_
3	Data+(B)
4	Data-(A)
5	GND
6	_
7	-
8	-
9	_

Pin on RJ45	2w RS-485 signal
_	_
_	-
3	Data+(B)
4	Data-(A)
5	GND
-	-
-	-
-	-
-	_

LB-DB9F-G-01

The LB-DB9F-G-01 is a loop-back connector for the NPort's DB9 male connector. It shortens Pin2 and Pin3;;Pin4, Pin6, and Pin7; and Pin8 and Pin1, so the serial port can have a self-test to verify if the serial communication works properly. The pin assignment of this connector is as below:

Pin on DB9 male	RS-232 signal	Notes
1	DCD	Shorted with Pin7, Pin8
2	RxD	Shorted
3	TxD	
4	DTR	Shorted with Pin6
5	GND	-
6	DSR	Shorted with Pin4
7	RTS	Shorted
8	CTS	
9	-	-



Selecting Suitable Power Adapter Depends on the Environment

The standard temperature models (NPort 6150-G2 and NPort 6250-G2) default will be shipped with a power adapter suitable for user's region.

- PWR-12050-AU-S1: with the Australia power plug
- PWR-12050-CN-S1: with the China power plug
- PWR-12050-EU-S1: with the European power plug
- PWR-12050-IN-S1: with the India power plug and certificate
- PWR-12050-KR-S1: with the Korea power plug and certificate
- PWR-12050-UK-S1: with the United Kingdom power plug and certificate
- PWR-12050-USJP-S1: with the United States and Japan power plug

With these power adapters, the operating temperature is from 0 to 40 degrees Celsius. Generally, the NPort device server may be set up in an indoor environment, like a control room. If the NPort device server may be set in an outdoor area or a cabinet without air conditioning, the temperature change may be big. Consider to buying the wide temperature models (NPort 6150-G2-T and NPort 6250-G2-T), and the power adapters may need to be ordered separately (it is not included in the box of NPort 6150-G2-T/6250-G2-T).

- PWR-12150-AU-SA-T: with the Australia power plug
- PWR-12150-CN-SA-T: with the China power plug
- PWR-12150-EU-SA-T: with the European power plug
- PWR-12150-UK-SA-T: with the United Kingdom power plug and certificate
- PWR-12150-USJP-SA-T: with the United States and Japan power plug

With these wide temperature models and power adapters, the operating temperature is from -40 to 75 degrees Celsius. Generally, the NPort device server may be set up in an outdoor environment, like a cabinet at the remote site, where it may be really extremely hot in summer and extremely cold in winter.

For those regions which do not have wide temperature power adapters, there are two options:

- 1. Try to locate a power adapter that a local UL Listed power supply (LPS) supplies externally, with a power output that meets SELV and LPS requirements and is rated between 12 to 48 VDC, with a minimum current of 0.16 A and a minimum Tma of 75°C.
- 2. Find a DIN-rail power supply that functions under a wide range of the temperatures and supply higher watts to multiple devices simultaneously. For example, Moxa provides:
 - MDR-40-24: DIN-rail 24 VDC power supply with 40W, -20 to 70°C operating temperature
 - > MDR-60-24: DIN-rail 24 VDC power supply with 60W, -20 to 70°C operating temperature
 - > HDR-60-24: 60 W/2.5 A DIN-rail 24 VDC power supply, -30 to 70°C operating temperature

For easy connections with these DIN-rail power supplies, Moxa provides a power cable: CBL-PJ21NOPEN-BK-30 w/Nut, which is a power plug at one side and with two cables V+ and V- at the other side to connect to the power supply.



C. Well-known Port Numbers

In this appendix, we provide a list of well-known port numbers that may cause network problems if you set the NPort 6000-G2 to one of these ports. Refer to RFC 1700 for well-known port numbers or 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 range from 0 through 1023. The Registered Ports range from 1024 through 49151.

The Dynamic and/or Private Ports range from 49152 through 65535.

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

TCP Socket	Application Service	
0	Reserved	
1	TCP Port Service Multiplexer	
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 to 223	Reserved for future use	
UDP Socket	Application Service	
------------	---	
0	Reserved	
2	Management Utility	
7	Echo	
9	Discard	
11	Active Users (systat)	
13	Daytime	
35	Any private printer server	
39	Resource Location Protocol	
42	Host name server (names server)	
43	Whois (nickname)	
49	Login Host Protocol (login)	
53	Domain Name Server (domain)	
69	Trivial Transfer Protocol (TETP)	
70	Gopher Protocol	
79	Finger Protocol	
80	World Wide Web (HTTP)	
107	Remote Telnet Service	
111	Sun Remote Procedure Call (Sunrpc)	
119	Network News Transfer Protocol (NNTP)	
123	Network Time Protocol (NTP)	
161	SNMP (Simple Network Management Protocol)	
162	SNMP Traps	
213	IPX (used for IP Tunneling)	

The NPort 6000-G2 has built-in SNMP (Simple Network Management Protocol) agent software that supports SNMP Trap, RFC1317 and RS-232-like groups, and RFC 1213 MIB-II. The following table lists the standard MIB-II groups and the variable implementation for the NPort 6000-G2.

RFC1213 MIB-II Supported SNMP Variables

System MIB	Interfaces MIB	IP MIB	ІСМР МІВ
sysDescr	ifNumber	ipForwarding	icmpInMsgs
sysObjectID	ifIndex	ipDefaultTTL	icmpInErrors
sysUpTime	ifDescr	ipInReceives	icmpInDestUnreachs
sysContact	ifType	ipInHdrErrors	icmpInTimeExcds
sysName	ifMtu	ipInAddrErrors	icmpInParmProbs
sysLocation	ifSpeed	ipForwDatagrams	icmpInSrcQuenchs
sysServices	ifPhysAddress	ipInUnknownProtos	icmpInRedirects
	ifAdminStatus	ipInDiscards	icmpInEchos
	ifOperStatus	ipInDelivers	icmpInEchoReps
	ifLastChange	ipOutRequests	icmpInTimestamps
	ifInOctets	ipOutDiscards	icmpTimestampReps
	ifInUcastPkts	ipOutNoRoutes	icmpInAddrMasks
	ifInNUcastPkts	ipReasmTimeout	icmpInAddrMaskReps
	ifInDiscards	ipReasmReqds	icmpOutMsgs
	ifInErrors	ipReasmOKs	icmpOutErrors
	ifInUnknownProtos	ipReasmFails	icmpOutDestUnreachs
	ifOutOctets	ipFragOKs	icmpOutTimeExcds
	ifOutUcastPkts	ipFragFails	icmpOutParmProbs
	ifOutNUcastPkts	ipFragCreates	icmpOutSrcQuenchs
	ifOutDiscards	ipAdEntAddr	icmpOutRedirects
	ifOutErrors	ipAdEntIfIndex	icmpOutEchos
	ifOutQLen	ipAdEntNetMask	icmpOutEchoReps
	ifSpecific	ipAdEntBcastAddr	icmpOutTimestamps
		ipAdEntReasmMaxSize	icmpOutTimestampReps
		ipRouteDest	icmpOutAddrMasks
		ipRouteIfIndex	icmpOutAddrMaskReps
		ipRouteMetric1	
		ipRouteMetric2	
		ipRouteMetric3	
		ipRouteMetric4	
		ipRouteNextHop	
		ipRouteType	
		ipRouteProto	
		ipRouteAge	
		ipRouteMask	
		ipRouteMetric5	
		ipRouteInfo	
		ipNetToMediaIfIndex	
		ipNetToMediaPhysAddress	
		ipNetToMediaNetAddress	
		ipNetToMediaType	
		ipRoutingDiscards	

Address Translation MIB	тср мів	UDP MIB	SNMP MIB
atIfIndex	tcpRtoAlgorithm	udpInDatagrams	snmpInPkts
atPhysAddress	tcpRtoMin	udpNoPorts	snmpOutPkts
atNetAddress	tcpRtoMax	udpInErrors	snmpInBadVersions
	tcpMaxConn	udpOutDatagrams	snmpInBadCommunityNames
	tcpActiveOpens	udpLocalAddress	snmpInBadCommunityUses
	tcpPassiveOpens	udpLocalPort	snmpInASNParseErrs
	tcpAttemptFails		snmpInTooBigs
	tcpEstabResets		snmpInNoSuchNames
	tcpCurrEstab		snmpInBadValues
	tcpInSegs		snmpInReadOnlys
	tcpOutSegs		snmpInGenErrs
	tcpRetransSegs		snmpInTotalReqVars
	tcpConnState		snmpInTotalSetVars
	tcpConnLocalAddress		snmpInGetRequests
	tcpConnLocalPort		snmpInGetNexts
	tcpConnRemAddress		snmpInSetRequests
	tcpConnRemPort		snmpInGetResponses
	tcpInErrs		snmpInTraps
	tcpOutRsts		snmpOutTooBigs
			snmpOutNoSuchNames
			snmpOutBadValues
			snmpOutGenErrs
			snmpOutGetRequests
			snmpOutGetNexts
			snmpOutSetRequests
			snmpOutGetResponses
			snmpOutTraps
			snmpEnableAuthenTraps
			snmpSilentDrops
			snmpProxyDrops

RFC1317 RS-232 Like Groups

RS-232 MIB	Async Port MIB	
rs232Number	rs232AsyncPortIndex	
rs232PortIndex	rs232AsyncPortBits	
rs232PortType	rs232AsyncPortStopBits	
rs232PortInSigNumber	rs232AsyncPortParity	
rs232PortOutSigNumber		
rs232PortInSpeed		
rs232PortOutSpeed		

Input Signal MIB	Output Signal MIB	
rs232InSigPortIndex	rs232OutSigPortIndex	
rs232InSigName	rs232OutSigName	
rs232InSigState	rs232OutSigState	

Moxa-NP6000-G2-MIB

overview	basicSetting	networkSetting	opModeSetting
modelName	serverName	ipConfiguration	portIndex
serialNumber	serverLocation	sysIpAddress	portApplication
firmwareVersion	timeZone	netMask	portMode
macAddress	localTime	defaultGateway	
viewLanSpeed	timeserver	dnsServer1IpAddr	
viewLanModuleSpeed		dnsServer2IpAddr	
upTime		pppoeUserAccount	
moduleType		pppoePassword	
configCRC32		winsFunction	
		winsServer	
		lan1Speed	
		routingProtocol	
		gratuitousArp	
		gratuitousArpSendPerios	

deviceControl Mode	socket Mode
deviceControlTcpAliveCheck	socketTcpAliveCheck
deviceControlMaxConnection	socketInactivityTime
deviceControlIgnoreJammedIp	socketMaxConnection
deviceControlAllowDriverControl	socketIgnoreJammedIp
deviceControlSecure	socketAllowDriverControl
deviceControlLocalTcpPort	socketSecure
deviceControlConnectionDownRTS	socketLocalTcpPort
deviceControlConnectionDownDTR	socketCmdPort
	socketTcpServerConnectionDownRTS
	socketTcpServerConnectionDownDTR
	socketTcpClientDestinationAddress1
	socketTcpClientDestinationPort1
	socketTcpClientDestinationAddress2
	socketTcpClientDestinationPort2
	socketTcpClientDestinationAddress3
	socketTcpClientDestinationPort3
	socketTcpClientDestinationAddress4
	socketTcpClientDestinationPort4
	socketTcpClientDesignatedLocalPort1
	socketTcpClientDesignatedLocalPort2
	socketTcpClientDesignatedLocalPort3
	socketTcpClientDesignatedLocalPort4
	socketTcpClientConnectionControl
	socketUdpDestinationAddress1Begin
	socketUdpDestinationAddress1End
	socketUdpDestinationPort1
	socketUdpDestinationAddress2Begin
	socketUdpDestinationAddress2End
	socketUdpDestinationPort2
	socketUdpDestinationAddress3Begin
	socketUdpDestinationAddress3End
	socketUdpDestinationPort3
	socketUdpDestinationAddress4Begin
	socketUdpDestinationAddress4End
	socketUdpDestinationPort4
	socketUdpLocalListenPort

pairConnection Mode	ethernetModem Mode
pairConnectionTcpAliveCheck	ethernetModemTcpAliveCheck
pairConnectionSecure	ethernetModemTcpPort
pairConnectionDestinationAddress	
pairConnectionDestinationPort	
pairConnectionTcpPort	

terminal Mode	reverseTerminal Mode
terminalTcpAliveCheck	reverseTerminalTcpAliveCheck
terminalInactivityTime	reverseTerminalInactivityTime
terminalAutoLinkProtocol	reverseTerminalTcpPort
terminalPrimaryHostAddress	reverseTerminalAuthenticationType
terminalSecondHostAddress	reverseTerminalMapKeys
terminalTelnetTcpPort	
terminalSshTcpPort	
terminalType	
terminalMaxSessions	
terminalChangeSession	
terminalQuit	
terminalBreak	
terminalInterrupt	
terminalAuthenticationType	
terminalAutoLoginPrompt	
terminalPasswordPrompt	
terminalLoginUserName	
terminalLoginPassword	

printer Mode	dial Mode	dataPacking
printerTcpAliveCheck	dialTERMBINMode	portPacketLength
printerTcpPort	dialPPPDMode	portDelimiter1Enable
printerGroup	dialSLIPDMode	portDelimiter1
printerQueueNameRaw	dialAuthType	portDelimiter2Enable
printerQueueNameASCII	dialDisconnectBy	portDelimiter2
printerAppendFromFeed	dialDestinationIpAddress	portDelimiterProcess
	dialSourceIpAddress	portForceTransmit
	dialIpNetmask	
	dialTcpIpCompression	
	dialInactivityTime	
	dialLinkQualityReport	
	dialOutgoingPAPID	
	dialPAPPassword	
	dialIncomingPAPCheck	

comParamSetting	dataBuffering	modemSetting
portAlias	portBufferingEnable	portEnableModem
portInterface	portBufferingLocation	portInitialString
portBaudRate	portBufferingSDFileSize	portDialUp
portBaudRateManual	portSerialDataLoggingEnable	portPhoneNumber
portDataBits		
portStopBits		
portParity		
portFlowControl		
portFIFO		
portOnDelay		
portOffDelay		

welcomeMessage	sysManagement
portEnableWelcomeMessage	enableAccessibleIpList
portMessage	accessibleIpListIndex
	activeAccessibleIpList
	accessibleIpListAddress
	accessibleIpListNetmask
	snmnEnable
	snmpContactName
	snmpl ocation
	dDNSEnable
	dDNSServerAddress
	dDNSHostName
	dDNSUserName
	dDNSPassword
	hostTableIndex
	hostName
	hostinAddress
	routoTabloIndox
	destination
	matricBautaTable
	InterfaceDeuteTable
	udpBortAuthonticationSorver
	radiusAccounting
	systocallog
	networkl ocall og
	mailWarningColdStart
	mailWarningWarmStart
	mailWarningAuthFailure
	mailWarningInChanged
	mailWarningPasswordChanged
	trapServerColdStart
	trapServerWarmStart
	trapServerAuthFailure
	alarmServerEthernet1LinkDown
	alarmServerEthernet2LinkDown
	alarmServerEthernet3LinkDown
	mailDCDchange
	trapDCDchange
	alarmDCDchange
	mailDSRchange
	trapDSRchange
	alarmDSRchange
	emailWarningMailServer
	emailRequiresAuthentication
	emailWarningUserName
	emailWarningPassword
	emailWarningFromEmail
	emailWarningFirstEmailAddr
	emailWarningSecondEmailAddr

welcomeMessage	sysManagement
	emailWarningThirdEmailAddr
	emailWarningFourthEmailAddr
	snmpTrapReceiverIp
	trapVersion
	httpConsole
	httpsConsole
	telnetConsole
	sshConsole
	IcmReadOnlyProtect
	resetButtonFunction
	loadFactoryDefaultSetting
	maxHttpLoginUsers
	autoLogoutSetting
	loginNotificationMessage
	loginFailureMessage
	userAccountIndex
	activeUserAccount
	accountName
	accountGroupName
	groupName
	networkConfig
	serialConfig
	systemConfig
	adminConfig
	monitorLogWarning
	commonSetting
	pwdMinLength
	pwdComplexityCheckEnable
	pwdComplexityCheckDigitEnable
	pwdComplexityCheckAlphabetEnable
	pwdComplexityCheckSpecialCharEnable
	pwdLifetime
	loginFailureLockoutEnable
	loginFailureLockoutRetrys
	loginFailureLockoutTime

sysStatus	saveConfiguration	restart
remoteIpIndex	saveConfig	restartPorts
monitorRemoteIp		restartSystem
monitorTxCount		
monitorRxCount		
monitorTxTotalCount		
monitorRxTotalCount		
monitorDSR		
monitorDTR		
monitorRTS		
monitorCTS		
monitorDCD		
monitorErrorCountFrame		
monitorErrorCountParity		
monitorErrorCountOverrun		
monitorErrorCountBreak		
monitorBaudRate		
monitorDataBits		
monitorParity		
monitorRTSCTSFlowControl		
monitorXONXOFFFlowControl		
monitorFIFO		

sysStatus	saveConfiguration	restart
monitorInterface		
monitorRTSToggleFlowControl		
relayOutputEthernet1LinkDown		
ethernet1LinkDownAcknowledge		
relayOutputEthernet2LinkDown		
ethernet2LinkDownAcknowledge		
relayOutputEthernet3LinkDown		
ethernet3LinkDownAcknowledge		
portDCDChangedStatus		
portDCDChangedAcknowledge		
portDSRChangedStatus		
portDSRChangedAcknowledge		

The NPort 6000-G2 provides event logs to help users to troubleshoot. All the events that may be recorded are listed below.

Item	Category	Severity	Default Setting	Event Name	Description
1		Notice	Disable	Firmware ready	The system is ready for operation.
2		Informational	Disable	Detect SD card	Mount SD card successfully.
3		Warning	Disable	SD card removed	Detect SD card is removed.
4		Error	Disable	No SD card inserted	No SD card in the system when Port Buffering is enabled and targeting to save in the SD card.
5		Notice	Disable	User trigger reboot	The device was rebooted by the user.
6		Informational	Disable	Configuration changed	A user changed the configuration setting, and the new settings are activated.
7		Notice	Disable	Configuration changed failed	A user changed the configuration setting, but the new settings activated failed.
8		Warning	Disable	Power input failure	The device detects Power Input doesn't provide the electricity (only happens on multiple power inputs models).
9		Informational	Disable	NTP success	The device synchronizes the time with NTP server successfully.
10	System	Warning	Disable	NTP fail	The device failed to synchronize the time.
11	System	Informational	Disable	Manual setting time success	Manual setting time success.
12		Notice	Disable	Email fail	The device failed to deliver the email message.
13		Notice	Disable	SNMP inform fail	The device failed to deliver the SNMP Inform message.
14		Notice	Disable	Syslog fail	The device failed to deliver the Syslog message.
15		Notice	Disable	Email service is back	Email service resumed; the event recorded for successfully sending after a failure.
16		Notice	Disable	SNMP inform service is back	SNMP information service resumed; the event recorded for successfully sending after a failure.
17		Notice	Disable	Syslog service is back	Syslog service resumed; the event recorded for successfully sending after a failure.
18		Informational	Disable	LCM display ready	The system detects the LCM display, and it's ready for use.
19		Notice	Disable	LCM display not work	The system detects the LCM display, but it doesn't work.
20		Informational	Disable	Ethernet link up	The Ethernet port is linked up.
21		Notice	Disable	Ethernet link down	The Ethernet port is linked down.
22		Notice	Disable	IP changed	A user changed the network configuration setting, and the new settings are activated.
23		Error	Disable	IP conflict	The device detects an IP conflict, this may make the device malfunctioned.
24	-Network	Warning	Disable	Not get IP from DHCP server	The device shall get an IP address from the DHCP server, but it failed.
25		Warning	Disable	Connect DHCP server fail	The device cannot find a DHCP server in the network.
26		Notice	Disable	Using 169.254.x.x IP	The device is using 169.254.x.x IP address, which is abnormal.
27		Informational	Disable	IP renew	IP of the device is renewed (with DHCP enabled).
28		Notice	Disable	Topology change	When Redundant protocol (RSTP or TurboRing) enabled, the Slave port is blocked to prevent data loop. When the master path is broken and the

Item	Category	Severity	Default Setting	Event Name	Description
					network communication is working with the Slave path (only for the models which supports Redundant protocols).
29		Informational	Disable	Network module ready	The network module is detected and ready for communication (only for the models which can plug-in a network module).
30		Informational	Disable	No network module	There is no network module detected (only for the models which can plug-in a network module).
31		Notice	Disable	Network module not work	The system detects the network module, but it doesn't work (only for the models which can plug- in a network module).
32		Warning	Enable	Clear log	Clear all the system logs on the device.
33		Informational	Disable	System log export	The system log is exported.
34		Notice	Enable	Log threshold reached	The number of the log events reached the number of the threshold setting.
35		Informational	Disable	Login success	A user from the IP address login the device successfully.
36		Notice	Enable	Login fail	A user from the IP address try to login the device but failed.
37		Informational	Disable	Account/group changed	A user changed the configuration setting of username, password or group privilege.
38		Warning	Enable	Account lockout	An account is locked out because he failed to login too many times.
39		Informational	Disable	Service enabled	The device enables the service successfully.
40		Notice	Enable	Service disabled	The device disables the service successfully.
41		Warning	Enable	Service enabled/disabled failed	The device tries to enable/disable service failed.
42		Informational	Disable	Syslog certificate export	The Syslog certificate was exported.
43		Notice	Enable	Syslog certificate import	The Syslog certificate was imported.
44	Security	Notice	Enable	Syslog certificate deleted	The Syslog certificate was deleted.
45		Notice	Enable	Syslog certificate expired	The Syslog certificate was expired.
46		Informational	Disable	Syslog certificate will expire	The Syslog certificate will expire in one month.
47		Warning	Enable	Connect authentication server fail	The device failed to connect to the RADIUS/TACACS+ server.
48		Error	Enable	Authentication fail	A user failed to pass the authentication process.
49		Informational	Disable	SSL certificate export	The SSL certificate was exported.
50		Notice	Enable	SSL certificate import	The SSL certificate was imported.
51		Notice	Enable	SSL certificate deleted	The SSL certificate was deleted.
52		Notice	Enable	SSL certificate expired	The SSL certificate was expired.
53		Notice	Enable	SSL certificate regenerated	The SSL certificate was regenerated.
54		Warning	Enable	DoS Defense is triggered	The DoS Defense functions were triggered.
55		Informational	Disable	Password reached lifetime	Account's password reached the lifetime.
56	Maintenance	Informational	Disable	Firmware upgrade	The firmware is upgraded.

Item	Category	Severity	Default Setting	Event Name	Description
57		Warning	Disable	Firmware upgrade fail	A user tried to upgrade the firmware, but the device rejects to upgrade it because of the wrong file format/checksum error.
58		Notice	Disable	Configuration import	The config file was imported.
59		Warning	Disable	Configuration import fail	The device failed to import a config file because of the wrong file format or invalid authentication.
60		Informational	Disable	Configuration export	The config file was exported.
61		Notice	Disable	Load factory default	Load factory default.
62		Notice	Disable	Load customized default	Load customized default.
63		Notice	Disable	Log collection	When use click One-click data collection function to collect the event logs and relative information for diagnostics purpose, the device will record this event.
64		Informational	Disable	Serial port CTS changed	The CTS signal of the serial port is turned ON from OFF or is turned OFF from ON.
65		Informational	Disable	Serial port DSR changed	The DSR signal of the serial port is turned ON from OFF or is turned OFF from ON.
66		Informational	Disable	Serial port DCD changed	The DCD signal of the serial port is turned ON from OFF or is turned OFF from ON.
67	Serial	Notice	Disable	Port OP mode disabled	The Operation mode of the port is disabled; the port cannot be connected by any network devices.
68	1	Informational	Disable	Port connect	The session is connected on the port.
69	-	Notice	Disable	Port disconnect	The session is disconnected on the port.
70		Error	Disable	Port authentication fail	A user failed to login on the port in terminal, Reverse Terminal. or dial-in/out operation modes.
71		Notice	Disable	Port restart	The serial port is restarted.
72		Notice	Disable	Serial data error	There is an error happened on the received serial data of the Port, for example, a framed error, parity error, or overrun error.

F. Command List of the Serial Console

The NPort 6000-G2 provides a serial console as a command-line interface for the user who prefers to log in with the serial port. The serial console only supports limited configuration settings. View the basic information and configure the network settings.

When you first enter the serial console, input ? to view a list of basic commands and the description of each command.

<i>‡⊧</i> <i>‡⊧</i>	? show configure reload	- Show running system information - Enter configuration mode - Halt and perform a cold restart
‡ ⊧	-	- EXIT COMMAND LINE INTERIACE

For the users with READ privilege of the serial console, execute the **show** command to view relative settings. For the users with WRITE privilege, execute the **configure** command to set or modify relative settings.

Input # configure to access the subcategory to show or change the network related settings.

Syntax Description	ip	Configure IP parameters		
	address	Configure IPv4 address parameters		
	static	Configure static IPv4 address		
	ipv4-address	The IPv4 address		
	ipv4-netmask	The IPv4 subnet mask		
	dhcp	Assign the IPv4 address by DHCP		
Defaults	IPv4 Address: 192.168.127.254			
	IPv4 Netmask: 255.255.255.0			
	IPv4 Gateway: 0.0.0.0			
Command Modes	Global Configuration			
Usage Guidelines	N/A			
Examples	# configure			
	(config)# ip address static 192.168.127.254 255.255.255.0			
Related Commands	no ip address			

Set statis ip address of the network interface:

Set the default gateway:

Syntax Description	ip	Configure IP parameters	
	default-gateway	Configure IPv4 default gateway address	
	ipv4-address	The IPv4 address	
Defaults	N/A		
Command Modes	Global Configuration		
Usage Guidelines	N/A		
Examples	# configure		
	(config)# ip default-gateway 192.168.127.1		
Related Commands	no ip address		

Show the network status:

Syntax Description	show Display configuration/status information		
	ip	Display IP information	
	management	Display IP information	
Defaults	N/A		
Command Modes	Privileged EXEC		
Usage Guidelines	N/A		
Examples	# show ip management IPv4 IP configuration : DHCP IP address : 192.168.127.254		
	Subnet mask : 255.255.25 Default gateway : 0.0.0.0 DNS server : 0.0.0.0		
Related Commands	N/A		

User can input # reload to access the sub-category to show or modify the network related settings.

Restart the device:

Syntax Description	reload	Halt and perform a cold restart.		
Defaults	N/A			
Command Modes	Privileged EXEC	Privileged EXEC		
Usage Guidelines	N/A	N/A		
Examples	# reload			
	Proceed with reload? [y/n] y			
	Resetting system			
Related Commands	N/A			

Reset the device to factory default settings:

Syntax Description	reload	Halt and perform a cold restart.		
	factory-default	Halt and perform a cold restart with factory default.		
Defaults	N/A			
Command Modes	Privileged EXEC	Privileged EXEC		
Usage Guidelines	N/A			
Examples	# reload factory-default			
	Proceed with reload	Proceed with reload to factory default? [y/n] y		
	Reset to factory default			
Related Commands	N/A			

Logout the serial console:

Syntax Description	quit	Logout from the command line interface.
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	# quit	
Related Commands	N/A	

By becoming a registered user on Moxa.com, you gain access to all updates for your purchased or interested products, including software and documentation.To become a registered user and receiving all updates, you need to do following:

Register a Moxa Account

1. Go to Moxa.com and click 'Sign in' at the top-right corner.



2. In the Sign-n page, click "Create your Moxa member account" as below.'

Email*	
Please input your email address Password*	
Forgot your password?	
Password is required	
SIGN IN	

3. Fill the necessary fields.

Work Email*		
First Name*	Last Name*	
Company*		
Phone*		
Region*		
Select		•
Please input a password*		

Request for Product Updates

1. Go to the specific product page to receive updates. Click $"+FOLLOW \ UPDATE"$

Home > Products > Industrial Edge Connectivity > Serial Device Servers > Terminal Servers > NPort 6100/6200 Series				
NPort 6100/6200 S	eries			
1/2-port RS-232/422/485 secure terminal	servers			
	⊕ (Features and Benefits		
	8	Secure operation modes for Real COM, TCP Server, TCP Client, Pair Connection Terminal, and Reverse Terminal		
(Boot Int		Supports nonstandard baudrates with high precision		
		⊘ NPort 6250: Choice of network medium: 10/100BaseT(X) or 100BaseFX		
		S Enhanced remote configuration with HTTPS and SSH		
MOXA		Ort buffers for storing serial data when the Ethernet is offline		
	1	Supports IPv6		
8000		Generic serial commands supported in Command-by-Command mode		
		Security features based on IEC 62443		
		Certifications		
		GET A QUOTE + FOLLOW UPDATES		

2. Once completes, see the FOLLOW UPDATES button changes.

