ToughNet NAT Router User's Manual

Edition 1.0, September 2015

www.moxa.com/product

© 2015 Moxa Inc. All rights reserved.
Reproduction without permission is prohibited.

ToughNet NAT Router User's Manual

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

Copyright Notice

Copyright ©2015 Moxa Inc.
All rights reserved.
Reproduction without permission is prohibited.

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

Moxa Americas

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

Moxa Europe

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

Moxa China (Shanghai office)

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

Moxa Asia-Pacific

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

Table of Contents

1

Introduction

Welcome to the Moxa TN-5916 ToughNet NAT Router series. The ToughNet NAT Router is designed for connecting Ethernet-enabled devices with network IP security.

The following topics are covered in this chapter:

- ❒ **Overview**
- ❒ **Package Checklist**
- ❒ **Features**
  - ➢ Industrial Networking Capability
  - ➢ Designed for Industrial Applications
  - ➢ Useful Utility and Remote Configuration

Overview

As the world's network and information technology becomes more mature, the trend is to use Ethernet as the major communications interface in many industrial communications and automation applications. In fact, a entirely new industry has sprung up to provide Ethernet products that comply with the requirements of demanding industrial applications.

The ToughNet TN-5916, designed for rolling stock backbone networks, is a high performance M12 router. It supports NAT and routing functionality to facilitate the deployment of applications across networks. The TN-5916 router uses M12 and other circular connectors to ensure tight, robust connections and guarantee reliable resilience against environmental disturbances, such as vibration and shock. In addition, wide temperature models are available that operate reliably in hazardous, -40 to 75°C environments.

Package Checklist

The ToughNet NAT Routers are shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative for assistance.

- 1 Moxa ToughNet NAT Router
- RJ45 to DB9 console port cable
- Protective caps for unused ports
- Hardware installation guide (printed)
- CD-ROM with user's manual and Windows utility
- Warranty card

Features

Industrial Networking Capability

- Network address translation (N-to-1, 1-to-1, and port forwarding)

Designed for Industrial Applications

- Bypass relay ensures non-stop data communication in the event the router stops working due to a power failure
- EN 50155/50121-3-2 compliant. See specs for details about compliance with specific parts of these standards
- -40 to 75°C operating temperature (T models)
- Dual 24 to 110 VDC power inputs
- IP54, rugged high-strength metal case
- DIN rail or panel mounting ability

Useful Utility and Remote Configuration

- Configurable using a Web browser and Telnet/Serial console
- Send ping commands to identify network segment integrity

2

Getting Started

This chapter explains how to access the ToughNet NAT Router for the first time. There are three ways to access the router: (1) serial console, (2) Telnet console, and (3) web browser. The serial console connection method, which requires using a short serial cable to connect the ToughNet NAT Router to a PC’s COM port, can be used if you do not know the ToughNet NAT Router’s IP address. The Telnet console and web browser connection methods can be used to access the ToughNet NAT Router over an Ethernet LAN, or over the Internet. A web browser can be used to perform all monitoring and administration functions, but the serial console and Telnet console only provide basic functions.

The following topics are covered in this chapter:

RS-232 Console Configuration (115200, None, 8, 1, VT100)

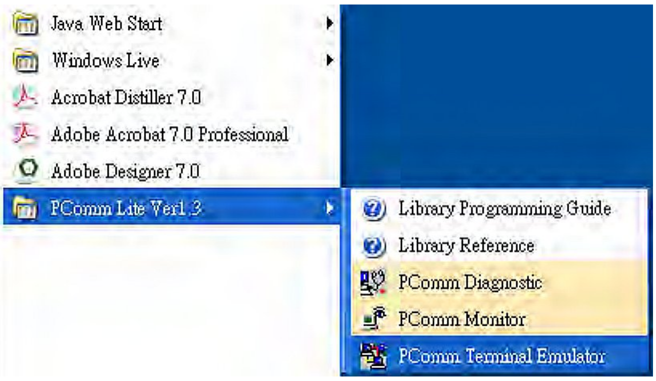
NOTE **Connection Caution!**
We strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your ToughNet NAT Router

NOTE We recommend using Moxa PComm Terminal Emulator, which can be downloaded free of charge from Moxa's website.

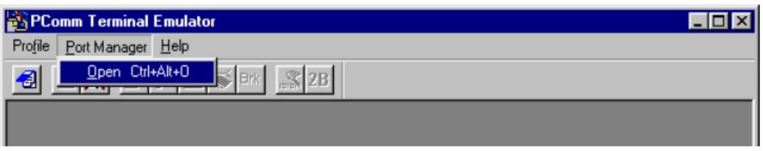
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the ToughNet NAT Router's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

After installing PComm Terminal Emulator, perform the following steps to access the RS-232 console utility.

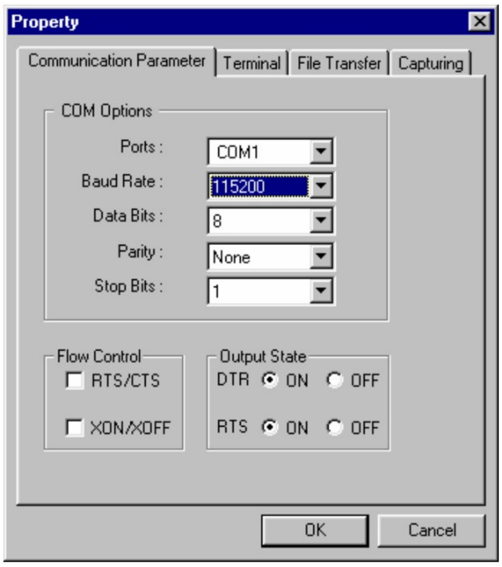
1. From the Windows desktop, click **Start** → **Programs** → **PCommLite1.3** → **Terminal Emulator**.



2. Select **Open** in the Port Manager menu to open a new connection.



3. The **Communication Parameter** page of the **Property** window will appear. Select the appropriate COM port from the **Ports** drop-down list, 115200 for Baud Rate, 8 for Data Bits, None for Parity, and 1 for Stop Bits.

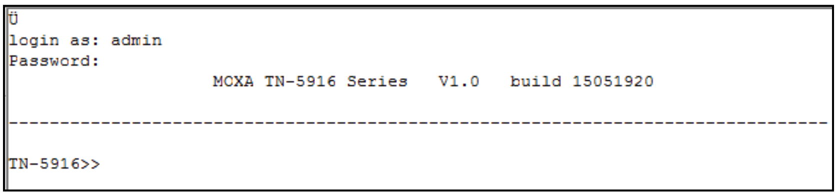


Ports : COM1
Baud Rate : 115200
Data Bits : 8
Parity : None
Stop Bits : 1

□ RTS/CTS
□ XON/XOFF

DTR ● ON ○ OFF
RTS ● ON ○ OFF

4. Click the **Terminal** tab, select VT100 for Terminal Type, and then click **OK** to continue.
5. The **Console** login screen will appear. Use the keyboard to enter the login account (**admin** or **user**), and then press **Enter** to jump to the **Password** field. Enter the console Password (the same as the Web Browser password; leave the Password field blank if a console password has not been set), and then press **Enter**.



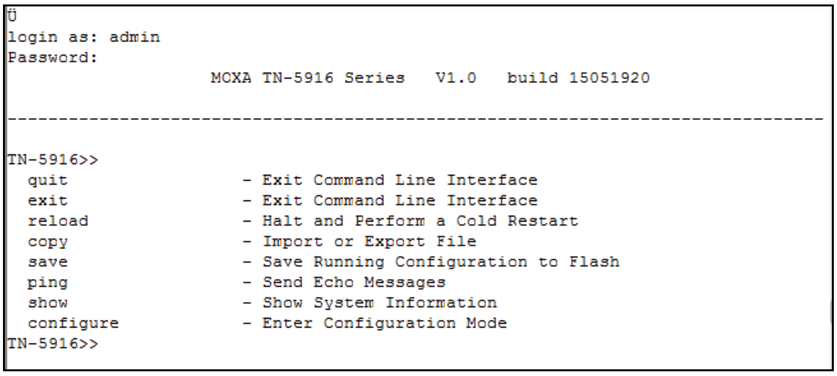
```
Ü
login as: admin
Password:
                        MOXA TN-5916 Series   V1.0   build 15051920

--------------------------------------------------------------------------------

TN-5916>>
```

NOTE The default password is blank. For greater security, please change the default password after the first log in.

6. Enter a question mark (**?**) to display the command list in the console.



```
Ü
login as: admin
Password:
                        MOXA TN-5916 Series   V1.0   build 15051920

--------------------------------------------------------------------------------

TN-5916>>
  quit                     - Exit Command Line Interface
  exit                     - Exit Command Line Interface
  reload                   - Halt and Perform a Cold Restart
  copy                     - Import or Export File
  save                     - Save Running Configuration to Flash
  ping                     - Send Echo Messages
  show                     - Show System Information
  configure                - Enter Configuration Mode
TN-5916>>
```

The following table lists commands that can be used when the ToughNet NAT Router is in console (serial or Telnet) mode:

Login by Admin Account

Command	Description
quit	Exit Command Line Interface
exit	Exit Command Line Interface
reload	Halt and Perform a Cold Restart
terminal	Configure Terminal Page Length
copy	Import or Export File
save	Save Running Configuration to Flash
ping	Send Echo Messages
clear	Clear Information
show	Show System Information
configure	Enter Configuration Mode

Using Telnet to Access the ToughNet NAT Router's Console

You may use Telnet to access the ToughNet NAT Router's console utility over a network. To access the TN's functions over the network (by either Telnet or a web browser) from a PC host that is connected to the same LAN as the ToughNet NAT Router, you need to make sure that the PC host and the ToughNet NAT Router are on the same logical subnet. To do this, check your PC host's IP address and subnet mask. By default, the LAN IP address is 192.168.127.254 and the Industrial subnet mask is 255.255.255.0 (for a Class C subnet). If you do not change these values, and your PC host's subnet mask is 255.255.0.0, then its IP address must have the form 192.168.xxx.xxx. On the other hand, if your PC host's subnet mask is 255.255.255.0, then its IP address must have the form, 192.168.127.xxx.

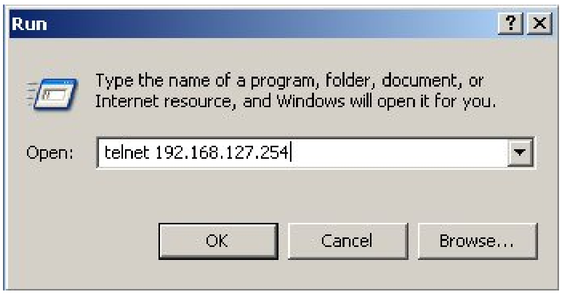
NOTE To use the ToughNet NAT Router's management and monitoring functions from a PC host connected to the same LAN as the ToughNet NAT Router, you must make sure that the PC host and the ToughNet NAT Router are connected to the same logical subnet.

NOTE Before accessing the console utility via Telnet, first connect the ToughNet NAT Router's RJ45 Ethernet LAN ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can use either a straight-through or cross-over Ethernet cable.

NOTE The ToughNet NAT Router's default LAN IP address is 192.168.127.254.

Perform the following steps to access the console utility via Telnet.

1. Click **Star**t → **Run**, and then telnet to the ToughNet NAT Router's IP address from the Windows Run window. (You may also issue the Telnet command from the MS-DOS prompt.)


Run
?
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

Open: telnet 192.168.127.254

2. Refer to instructions 6 and 7 in the **RS-232 Console Configuration (115200, None, 8, 1, VT100)** section on page 2-2.

Using a Web Browser to Configure the ToughNet NAT Router

The ToughNet NAT Router's web browser interface provides a convenient way to modify the router's configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft Internet Explorer 6.0 with JVM (Java Virtual Machine) installed.

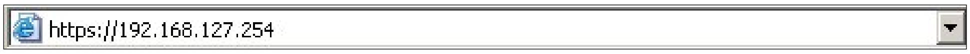
NOTE To use the ToughNet NAT Router's management and monitoring functions from a PC host connected to the same LAN as the ToughNet NAT Router, you must make sure that the PC host and the ToughNet NAT Router are connected to the same logical subnet.

NOTE Before accessing the ToughNet NAT Router's web browser, first connect the ToughNet NAT Router's M12 Ethernet LAN ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can use either a straight-through or cross-over Ethernet cable.

NOTE The ToughNet NAT Router's default LAN IP address is 192.168.127.254.

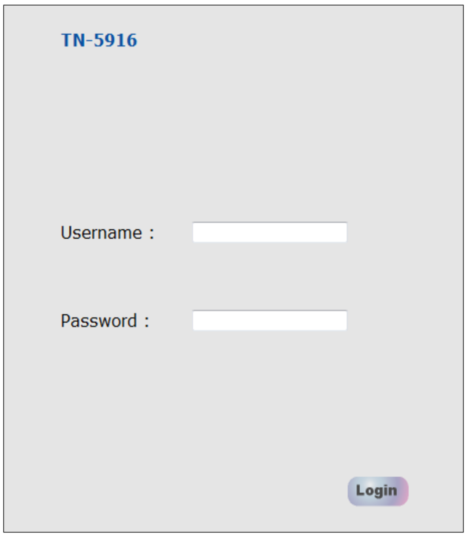
Perform the following steps to access the ToughNet NAT Router's web browser interface.

1. Start Internet Explorer and type the ToughNet NAT Router's LAN IP address in the Address field. Press Enter to establish the connection.



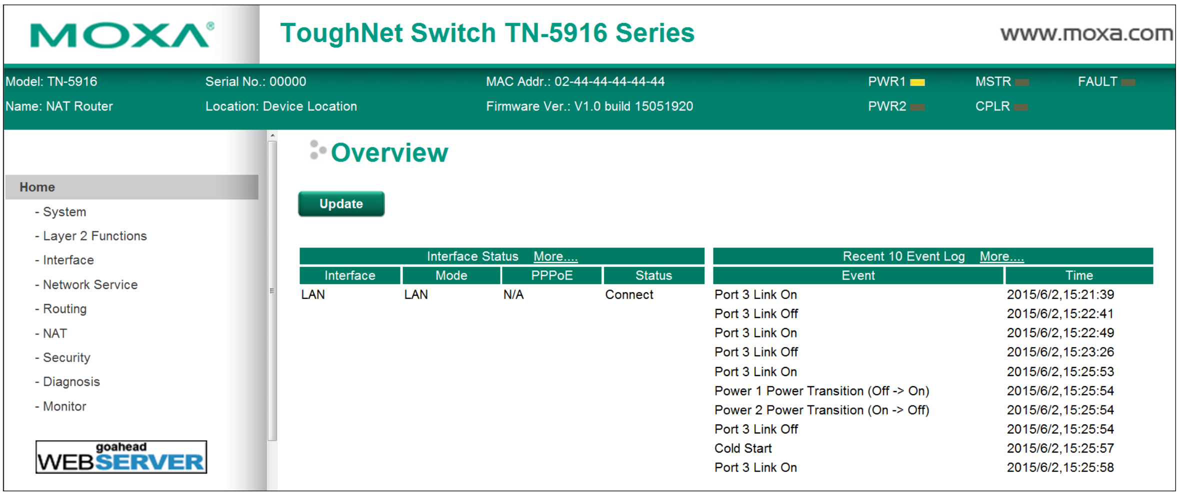
https://192.168.127.254

2. The web login page will open. Select the login account (Admin or User) and enter the **Password** (the same as the Console password), and then click Login to continue. Leave the **Password** field blank if a password has not been set.



NOTE The default password is blank. For greater security, please change the default password after the first log in.

You may need to wait a few moments for the web page to be downloaded to your computer. Use the menu tree on the left side of the window to open the function pages to access each of the router's functions.



Model: TN-5916 Serial No.: 00000 MAC Addr.: 02-44-44-44-44-44
Name: NAT Router Location: Device Location Firmware Ver.: V1.0 build 15051920

Interface Status More....

Interface	Mode	PPPoE	Status
LAN	LAN	N/A	Connect

Recent 10 Event Log More....

Event	Time
Port 3 Link On	2015/6/2,15:21:39
Port 3 Link Off	2015/6/2,15:22:41
Port 3 Link On	2015/6/2,15:22:49
Port 3 Link Off	2015/6/2,15:23:26
Port 3 Link On	2015/6/2,15:25:53
Power 1 Power Transition (Off -> On)	2015/6/2,15:25:54
Power 2 Power Transition (On -> Off)	2015/6/2,15:25:54
Port 3 Link Off	2015/6/2,15:25:54
Cold Start	2015/6/2,15:25:57
Port 3 Link On	2015/6/2,15:25:58

3

TN-5916 Series Features and Functions

In this chapter, we explain how to access the ToughNet NAT Router's configuration options, perform monitoring, and use administration functions. There are three ways to access these functions: (1) RS-232 console, (2) Telnet console, and (3) web browser.

The web browser is the most user-friendly way to configure the ToughNet NAT Router, since you can both monitor the ToughNet NAT Router and use administration functions from the web browser. An RS-232 or Telnet console connection only provides basic functions. In this chapter, we use the web browser to introduce the ToughNet NAT Router's configuration and monitoring functions.

The following topics are covered in this chapter:

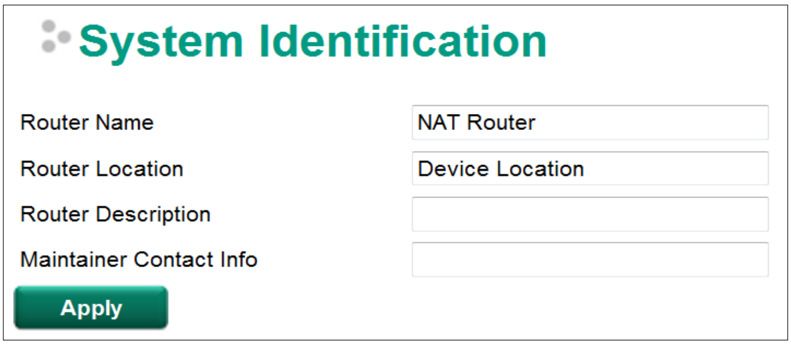
- **System**
  - System Information
  - User Account
  - Date and Time
  - Warning Notification
  - System File Update—by Remote TFTP
  - System File Update—by Local Import/Export
  - Restart
  - Reset to Factory Default
- **Port**
  - Port Settings
  - Link Aggregation
  - The Port Trunking Concept
  - Port Mirror
- **Using Virtual LAN**
  - The VLAN Concept
  - Configuring Virtual LAN
- **Multicast**
  - The Concept of Multicast Filtering
  - IGMP Snooping
  - IGMP Snooping Settings
  - IGMP Table
  - Stream Table
  - Static Multicast MAC
- **QoS**
  - ToS/DSCP Mapping
- **MAC Address Table**
- **Interface**
  - WAN
  - LAN
- **Network Service**
  - DHCP Settings
  - SNMP Settings
- **Security**
  - User Interface Management
  - Trusted Access
- **Monitor**
  - Interface Statistics
  - Port Statistics
- **Event Log**

System

The **System** section includes the most common settings required by administrators to maintain and control a Moxa switch.

System Information

Defining System Information items to make different switches easier to identify that are connected to your network.



System Identification

Router Name	NAT Router
Router Location	Device Location
Router Description	
Maintainer Contact Info	

Router Name

Setting	Description	Factory Default
Max. 30 characters	This option is useful for differentiating between the roles or applications of different units. Example: Factory Switch 1.	Firewall/VPN Router

Router Location

Setting	Description	Factory Default
Max. 80 characters	This option is useful for differentiating between the locations of different units. Example: production line 1.	Device Location

Router Description

Setting	Description	Factory Default
Max. 30 characters	This option is useful for recording a more detailed description of the unit.	None

Maintainer Contact Info

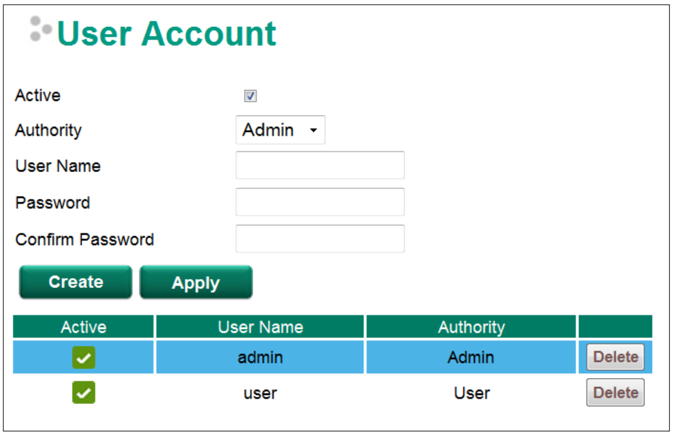
Setting	Description	Factory Default
Max. 30 characters	This option is useful for providing information about who is responsible for maintaining this unit and how to contact this person.	None

User Account

The Moxa ToughNet NAT Router supports the management of accounts, including establishing, activating, modifying, disabling and removing accounts. There are two levels of configuration access, admin and user. The account belongs to **admin** privilege has read/write access of all configuration parameters, while the account belongs to **user** authority has read access to view the configuration only.

NOTE

1. In consideration of higher security level, strongly suggest to change the default password after first log in
2. The user with 'admin' account name can't be deleted and disabled by default



Active ☑
Authority Admin
User Name
Password
Confirm Password

Active	User Name	Authority	
✓	admin	Admin	Delete
✓	user	User	Delete

Active

Setting	Description	Factory Default
Checked	The Moxa switch can be accessed by the activated user name	Enabled
Unchecked	The Moxa switch can't be accessed by the non-activated user	

Authority

Setting	Description	Factory Default
admin	The account has read/write access of all configuration parameters.	admin
user	The account can only read configuration but without any modification.	

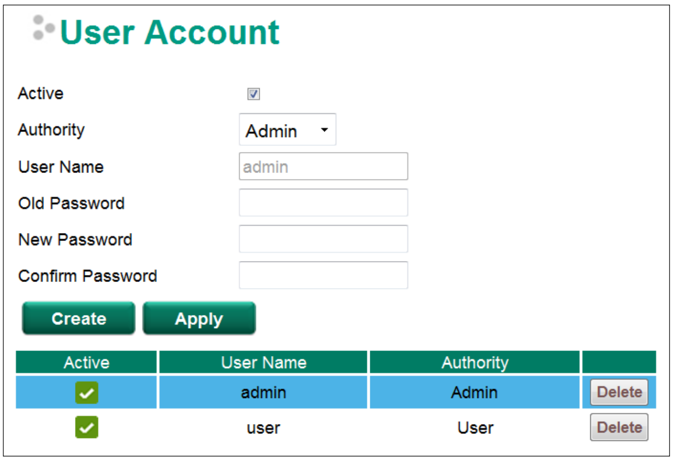
Create New Account

Input the user name, password and assign the authority to the new account. Once apply the new setting, the new account will be shown under the Account List table.

Setting	Description	Factory Default
User Name (Max. of 30 characters)	User Name	None
Password	Password for the user account. Minimum requirement is 4 characters, maximum of 16 characters	None

Modify Existing Account

Select the existing account from the Account List table. Modify the details accordingly then apply the setting to save the configuration.



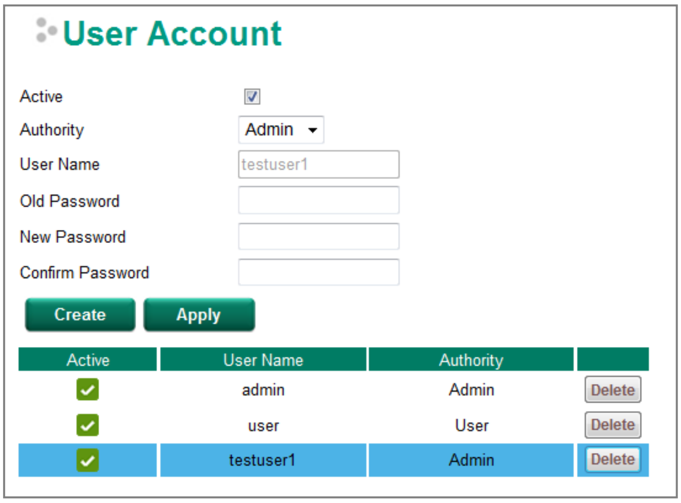
User Account

Active	☑
Authority	Admin
User Name	admin
Old Password	
New Password	
Confirm Password	

Active	User Name	Authority	
✓	admin	Admin	Delete
✓	user	User	Delete

Delete Existing Account

Select the existing account from the Account List table. Press delete button to delete the account.



User Account

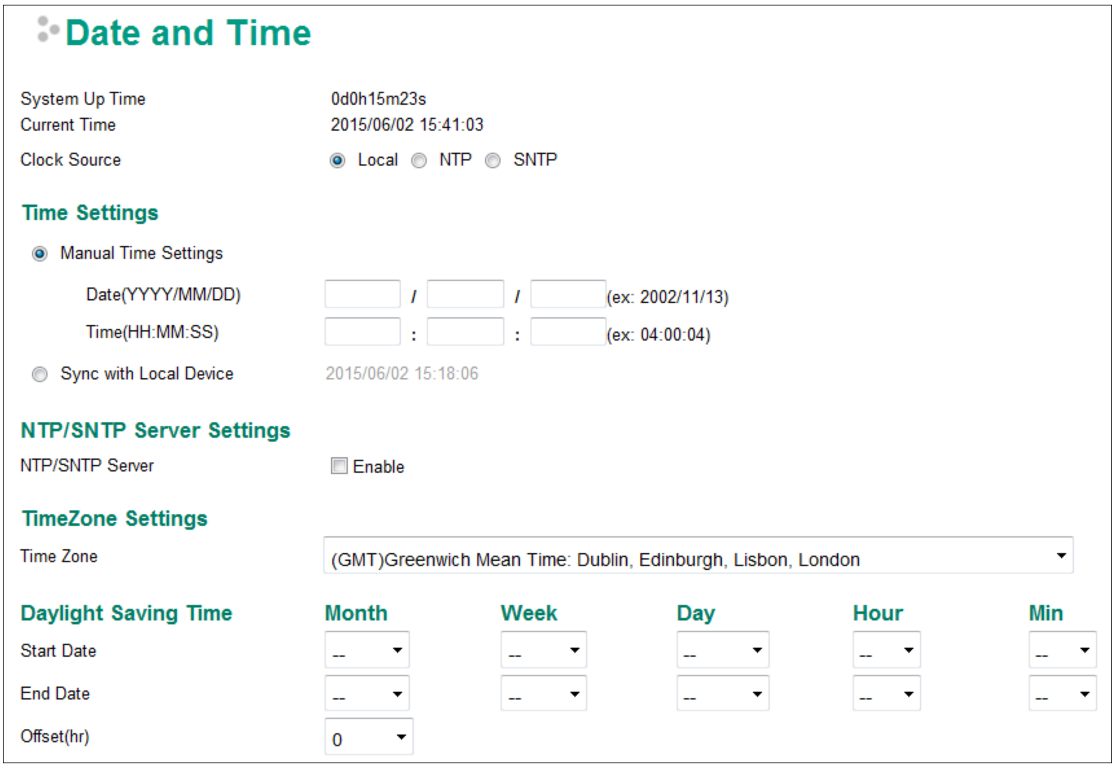
Active	☑
Authority	Admin
User Name	testuser1
Old Password	
New Password	
Confirm Password	

Active	User Name	Authority	
✓	admin	Admin	Delete
✓	user	User	Delete
✓	testuser1	Admin	Delete

Date and Time

The Moxa ToughNet NAT Router has a time calibration function based on information from an NTP server or user specified time and date. Functions such as automatic warning emails can therefore include time and date stamp.

NOTE The Moxa ToughNet NAT Router does not have a real time clock. The user must update the Current Time and Current Date to set the initial time for the Moxa switch after each reboot, especially when there is no NTP server on the LAN or Internet connection.



Date and Time

System Up Time 0d0h15m23s
Current Time 2015/06/02 15:41:03
Clock Source ● Local ○ NTP ○ SNTP

Time Settings

● Manual Time Settings
Date(YYYY/MM/DD) / / (ex: 2002/11/13)
Time(HH:MM:SS) : : (ex: 04:00:04)
○ Sync with Local Device 2015/06/02 15:18:06

NTP/SNTP Server Settings

NTP/SNTP Server □ Enable

TimeZone Settings

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

Daylight Saving Time	Month	Week	Day	Hour	Min
Start Date	--	--	--	--	--
End Date	--	--	--	--	--
Offset(hr)	0				

System Up Time

Indicates how long the Moxa ToughNet NAT Router remained up since the last cold start.

Current Time

Setting	Description	Factory Default
User-specified time	Indicates time in yyyy-mm-dd format.	None

Clock Source

Setting	Description	Factory Default
Local	Configure clock source from local time	Local
NTP	Configure clock source from NTP	
SNTP	Configure clock source from SNTP	

Time Zone

Setting	Description	Factory Default
Time zone	Specifies the time zone, which is used to determine the local time offset from GMT (Greenwich Mean Time).	GMT (Greenwich Mean Time)

Daylight Saving Time

The Daylight Saving Time settings are used to automatically set the Moxa switch’s time forward according to national standards.

Start Date

Setting	Description	Factory Default
User-specified date	Specifies the date that Daylight Saving Time begins.	None

End Date

Setting	Description	Factory Default
User-specified date	Specifies the date that Daylight Saving Time ends.	None

Offset

Setting	Description	Factory Default
User-specified hour	Specifies the number of hours that the time should be set forward during Daylight Saving Time.	None

NOTE Changing the time zone will automatically correct the current time. Be sure to set the time zone before setting the time.

Time Server IP/Name

Setting	Description	Factory Default
IP address or name of time server	The IP or domain address (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	None
IP address or name of secondary time server	The Moxa switch will try to locate the secondary NTP server if the first NTP server fails to connect.	

Enable NTP/SNTP Server

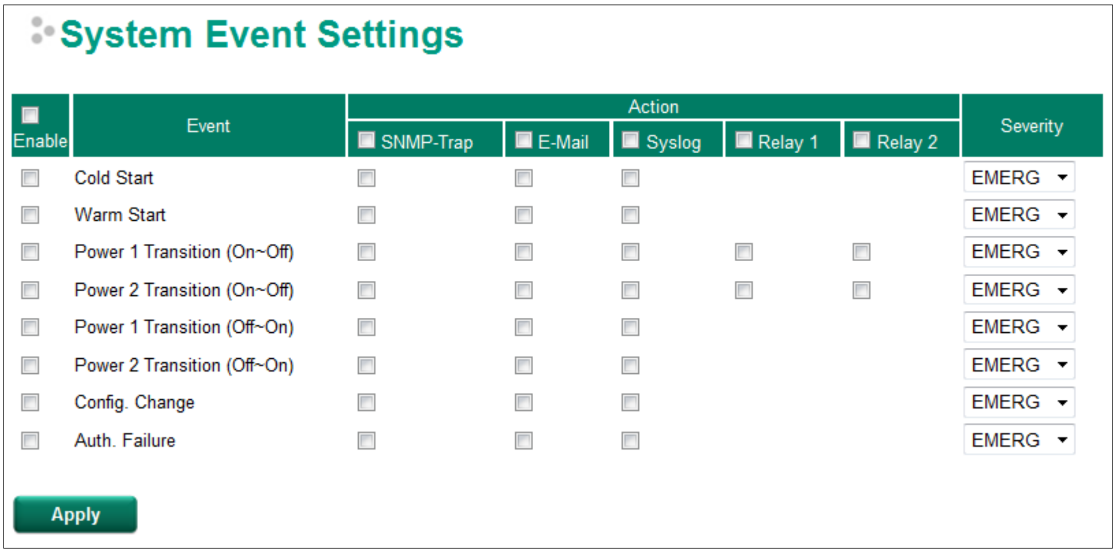
Setting	Description	Factory Default
Enable/Disable	Enables SNTP/NTP server functionality for clients	Disabled

Warning Notification

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an ToughNet NAT Router that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The Moxa ToughNet NAT Router supports different approaches to warn engineers automatically, such as email, trap, syslog and relay output. It also supports one digital input to integrate sensors into your system to automate alarms by email and relay output.

System Event Settings

System Events are related to the overall function of the switch. Each event can be activated independently with different warning approaches. Administrator also can decide the severity of each system event.



System Event Settings

□ Enable	Event	Action					Severity
		□ SNMP-Trap	□ E-Mail	□ Syslog	□ Relay 1	□ Relay 2	
□	Cold Start	□	□	□			EMERG
□	Warm Start	□	□	□			EMERG
□	Power 1 Transition (On~Off)	□	□	□	□	□	EMERG
□	Power 2 Transition (On~Off)	□	□	□	□	□	EMERG
□	Power 1 Transition (Off~On)	□	□	□			EMERG
□	Power 2 Transition (Off~On)	□	□	□			EMERG
□	Config. Change	□	□	□			EMERG
□	Auth. Failure	□	□	□			EMERG

System Events	Description
Cold Start	Power is cut off and then reconnected.
Warm Start	Moxa ToughNet NAT Router is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	Moxa ToughNet NAT Router is powered down.
Power Transition (Off→On)	Moxa ToughNet NAT Router is powered up.
Configuration Change	Any configuration item has been changed
Authentication Failure	An incorrect password was entered.

There are four response actions available on the EDS E series when events are triggered.

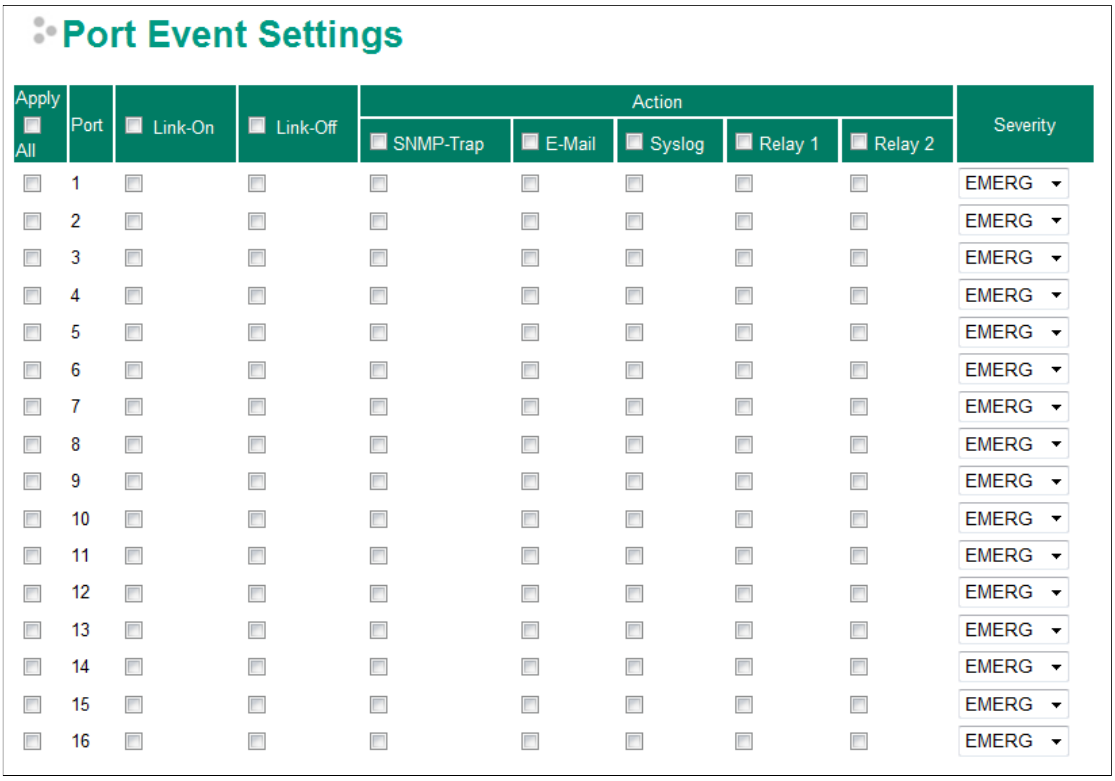
Action	**Description**
Trap	The ToughNet NAT Router will send notification to the trap server when event is triggered
E-Mail	The ToughNet NAT Router will send notification to the email server defined in the Email Setting
Syslog	The ToughNet NAT Router will record a syslog to syslog server defined in Syslog Server Setting
Relay	The ToughNet NAT Router supports digital inputs to integrate sensors. When event is triggered, the device will automate alarms by relay output

Severity

Severity	**Description**
Emergency	System is unusable
Alert	Action must be taken immediately
Critical	Critical conditions
Error	Error conditions
Warning	Warning conditions
Notice	Normal but significant condition
Information	Informational messages
Debug	Debug-level messages

Port Event Settings

Port Events are related to the activity of a specific port.

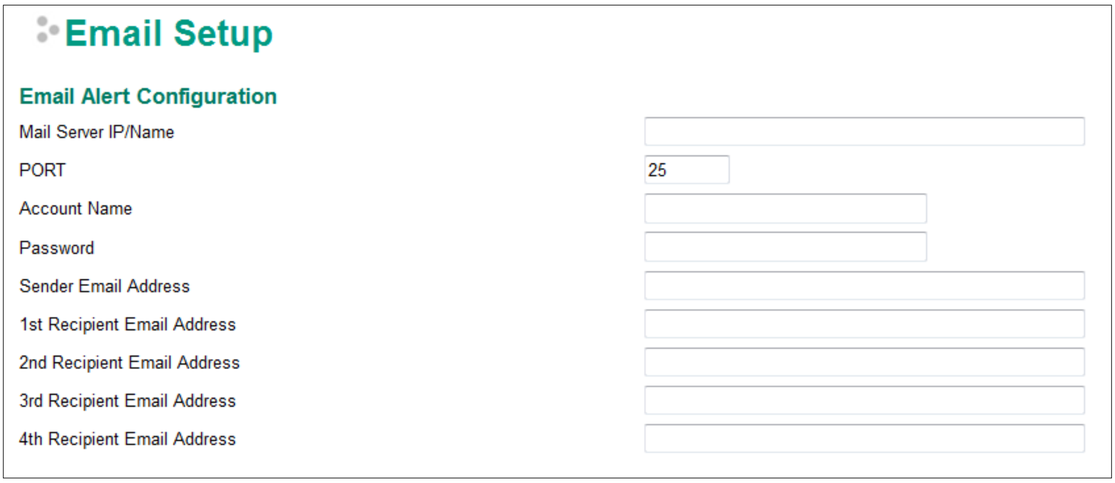


Port Event Settings

Apply □ All	Port	□ Link-On	□ Link-Off	Action					Severity
				□ SNMP-Trap	□ E-Mail	□ Syslog	□ Relay 1	□ Relay 2	
□	1	□	□	□	□	□	□	□	EMERG
□	2	□	□	□	□	□	□	□	EMERG
□	3	□	□	□	□	□	□	□	EMERG
□	4	□	□	□	□	□	□	□	EMERG
□	5	□	□	□	□	□	□	□	EMERG
□	6	□	□	□	□	□	□	□	EMERG
□	7	□	□	□	□	□	□	□	EMERG
□	8	□	□	□	□	□	□	□	EMERG
□	9	□	□	□	□	□	□	□	EMERG
□	10	□	□	□	□	□	□	□	EMERG
□	11	□	□	□	□	□	□	□	EMERG
□	12	□	□	□	□	□	□	□	EMERG
□	13	□	□	□	□	□	□	□	EMERG
□	14	□	□	□	□	□	□	□	EMERG
□	15	□	□	□	□	□	□	□	EMERG
□	16	□	□	□	□	□	□	□	EMERG

Port Events	**Warning e-mail is sent when…**
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).

Email Settings



Email Setup

Email Alert Configuration

Mail Server IP/Name	
PORT	25
Account Name	
Password	
Sender Email Address	
1st Recipient Email Address	
2nd Recipient Email Address	
3rd Recipient Email Address	
4th Recipient Email Address	

Mail Server IP/Name

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

Account Name

Setting	Description	Factory Default
Max. 45 of charters	Your email account.	None

Password Setting

Setting	Description	Factory Default
Password	The email account password.	None

Email Address

Setting	Description	Factory Default
Max. of 30 characters	You can set up to 4 email addresses to receive alarm emails from the Moxa switch.	None

Send Test Email

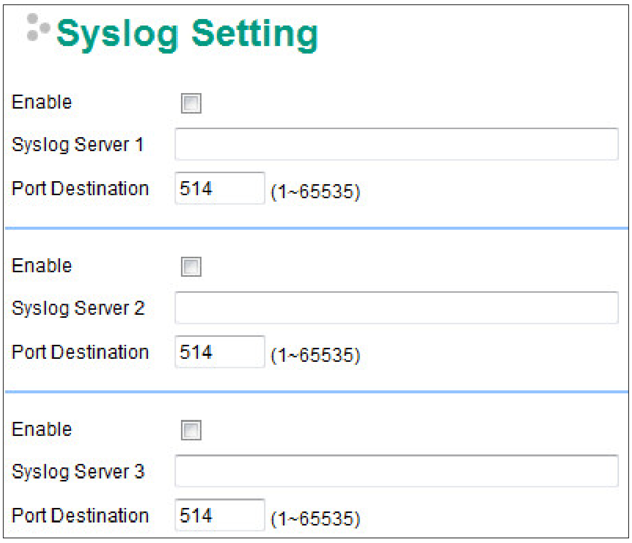
After you complete the email settings, you should first click **Apply** to activate those settings, and then press the **Test** button to verify that the settings are correct.

NOTE Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism.

We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.

Syslog Server Settings

The Syslog function provides the event logs for the syslog server. The function supports 3 configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a syslog UDP packet to the specified syslog servers. Each Syslog server can be activated separately by selecting the check box and enable it.



Syslog Setting

Enable □
Syslog Server 1
Port Destination 514 (1~65535)

Enable □
Syslog Server 2
Port Destination 514 (1~65535)

Enable □
Syslog Server 3
Port Destination 514 (1~65535)

Syslog Server 1/2/3

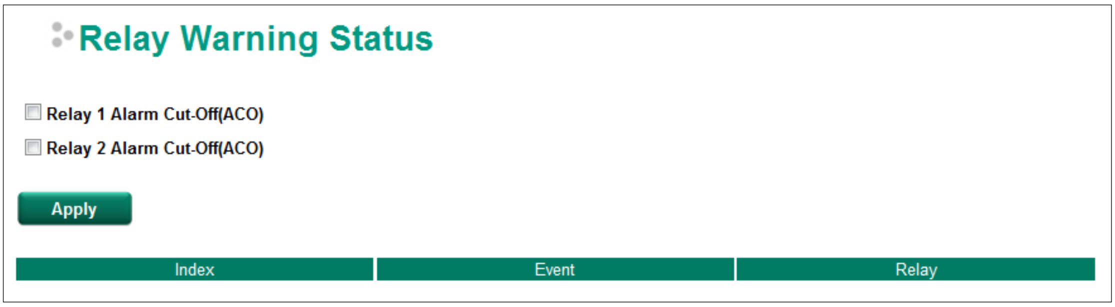
Setting	Description	Factory Default
IP Address	Enter the IP address of Syslog server 1/2/3, used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of Syslog server 1/2/3.	514

NOTE The following events will be recorded into the Moxa ToughNet NAT Router’s Event Log table, and will then be sent to the specified Syslog Server:

- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off (On), Power 1/2 transition (On (Off))
- Authentication fail
- Port link off/on

Relay Warning Status

When relay warning triggered by either system or port events, administrator can decide to shut down the hardware warning buzzer by clicking **Apply** button. The event still be recorded in the event list.



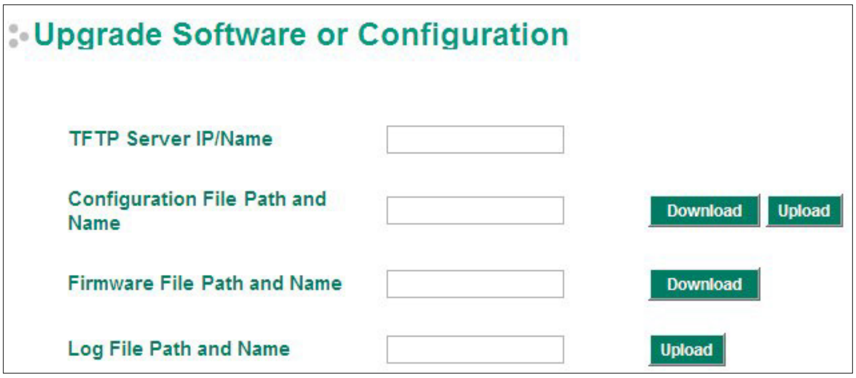
Relay Warning Status

□ Relay 1 Alarm Cut-Off(ACO)
□ Relay 2 Alarm Cut-Off(ACO)

Index	Event	Relay

System File Update—by Remote TFTP

The ToughNet NAT Router supports saving your configuration file to a remote TFTP server or local host to allow other ToughNet NAT Routers to use the same configuration at a later time, or saving the Log file for future reference. Loading pre-saved firmware or a configuration file from the TFTP server or local host is also supported to make it easier to upgrade or configure the ToughNet NAT Router.


Upgrade Software or Configuration

TFTP Server IP/Name

Configuration File Path and Name

Firmware File Path and Name

Log File Path and Name

TFTP Server IP/Name

Setting	Description	Factory Default
IP Address of TFTP Server	The IP or name of the remote TFTP server. Must be configured before downloading or uploading files.	None

Configuration File Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and filename of the ToughNet NAT Router’s configuration file in the TFTP server.	None

Firmware File Path and Name

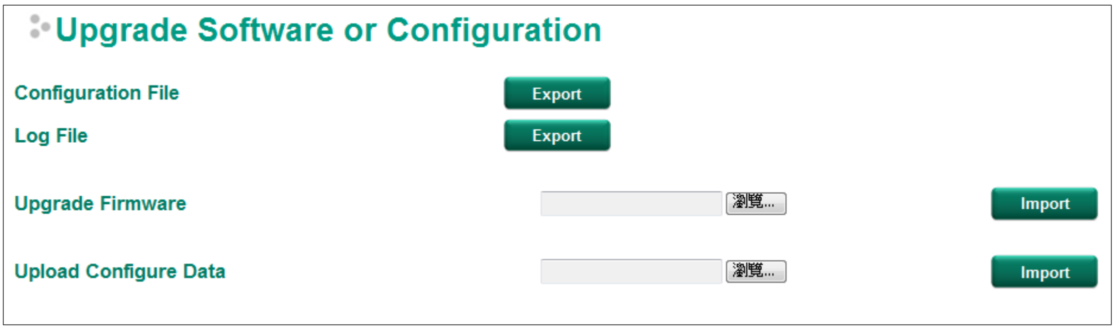
Setting	Description	Factory Default
Max. 40 Characters	The path and filename of the ToughNet NAT Router’s firmware file	None

Log File Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and filename of the ToughNet NAT Router’s log file	None

After setting up the desired path and filename, click **Activate** to save the setting. Next, click **Download** to download the file from the remote TFTP server, or click **Upload** to upload a file to the remote TFTP server.

System File Update—by Local Import/Export


Upgrade Software or Configuration

Configuration File

Log File

Upgrade Firmware

Upload Configure Data

Log File

Click **Export** to export the Log file of the ToughNet NAT Router to the local host.

NOTE Some operating systems will open the configuration file and log file directly in the web page. In such cases, right click the **Export** button and then save as a file.

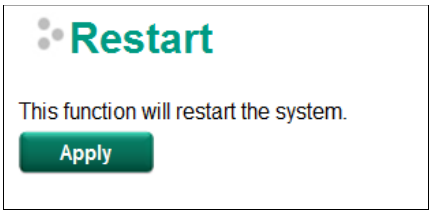
Upgrade Firmware

To import a firmware file that is exported from firmware V1.1 or previous versions into the ToughNet NAT Router, click **Browse** to select a firmware file already saved on your computer. The upgrade procedure will proceed automatically after clicking Import. This upgrade procedure will take a couple of minutes to complete, including the boot-up time.

Upload Configuration Data

To import a configuration file to the ToughNet NAT Router, click **Browse** to select a configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking Import.

Restart

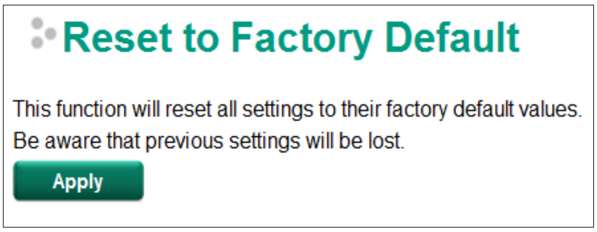


Restart

This function will restart the system.

This function is used to restart the ToughNet NAT Router.

Reset to Factory Default



Reset to Factory Default

This function will reset all settings to their factory default values. Be aware that previous settings will be lost.

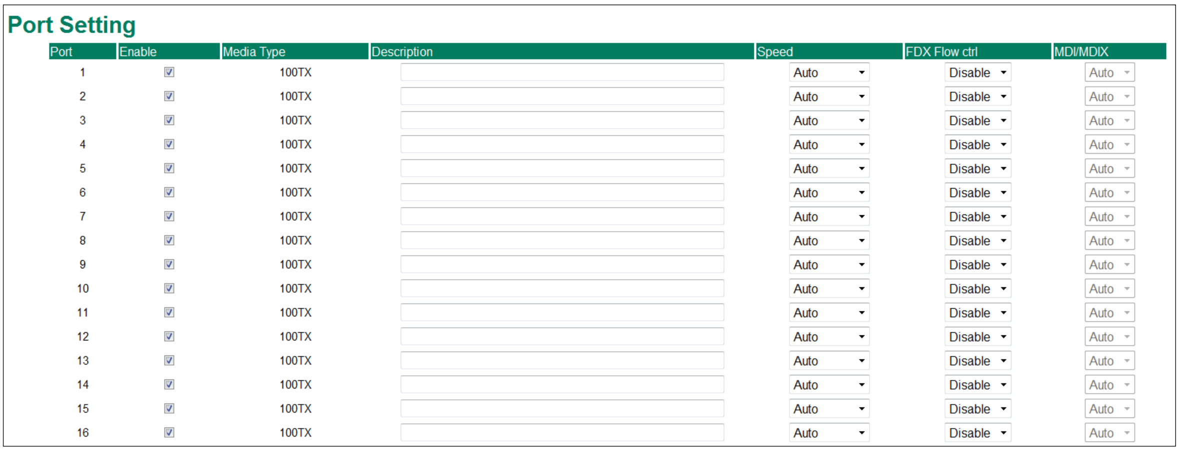
The **Reset to Factory Default** option gives users a quick way of restoring the ToughNet NAT Router’s configuration settings to the factory default values. This function is available in the console utility (serial or Telnet), and web browser interface.

NOTE After activating the Factory Default function, you will need to use the default network settings to re-establish a web-browser or Telnet connection with your ToughNet NAT Router.

Port

Port Settings

Port settings are included to give the user control over port access, port transmission speed, flow control, and port type (MDI or MDIX).



Port Setting

Port	Enable	Media Type	Description	Speed	FDX Flow ctrl	MDI/MDIX
1	☑	100TX		Auto	Disable	Auto
2	☑	100TX		Auto	Disable	Auto
3	☑	100TX		Auto	Disable	Auto
4	☑	100TX		Auto	Disable	Auto
5	☑	100TX		Auto	Disable	Auto
6	☑	100TX		Auto	Disable	Auto
7	☑	100TX		Auto	Disable	Auto
8	☑	100TX		Auto	Disable	Auto
9	☑	100TX		Auto	Disable	Auto
10	☑	100TX		Auto	Disable	Auto
11	☑	100TX		Auto	Disable	Auto
12	☑	100TX		Auto	Disable	Auto
13	☑	100TX		Auto	Disable	Auto
14	☑	100TX		Auto	Disable	Auto
15	☑	100TX		Auto	Disable	Auto
16	☑	100TX		Auto	Disable	Auto

Enable

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

Media Type

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

Description

Setting	Description	Factory Default
Max. 63 characters	Specifies an alias for the port to help administrators differentiate between different ports. Example: PLC 1	None

Speed

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

FDX Flow Ctrl

This setting enables or disables flow control for the port when the port's Speed is set to Auto. The final result will be determined by the Auto process between the Moxa switch and connected devices.

Setting	Description	Factory Default
Enable	Enables flow control for this port when the port's Speed is set to Auto.	Disabled
Disable	Disables flow control for this port when the port's Speed is set to Auto.	

MDI/MDIX

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

Link Aggregation

Link aggregation involves grouping links into a link aggregation group. A MAC client can treat link aggregation groups as if they were a single link.

The Moxa ToughNet NAT Router’s port trunking feature allows devices to communicate by aggregating up to 2 trunk groups, with a maximum of 8 ports for each group. If one of the 8 ports fails, the other seven ports will automatically provide backup and share the traffic.

Port trunking can be used to combine up to 8 ports between two Moxa switches or ToughNet NAT Routers. If all ports on both switches are configured as 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 1600 Mbps.

The Port Trunking Concept

Moxa has developed a port trunking protocol that provides the following benefits:

- Greater flexibility in setting up your network connections, since the bandwidth of a link can be doubled, tripled, or quadrupled.
- Redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.
- Load sharing—MAC client traffic can be distributed across multiple links.

To avoid broadcast storms or loops in your network while configuring a trunk, first disable or disconnect all ports that you want to add to the trunk or remove from the trunk. After you finish configuring the trunk, enable or re-connect the ports.

If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex mode, the potential bandwidth of the connection will be up to 1.6 Gbps. This means that users can double, triple, or quadruple the bandwidth of the connection by port trunking between two Moxa switches.

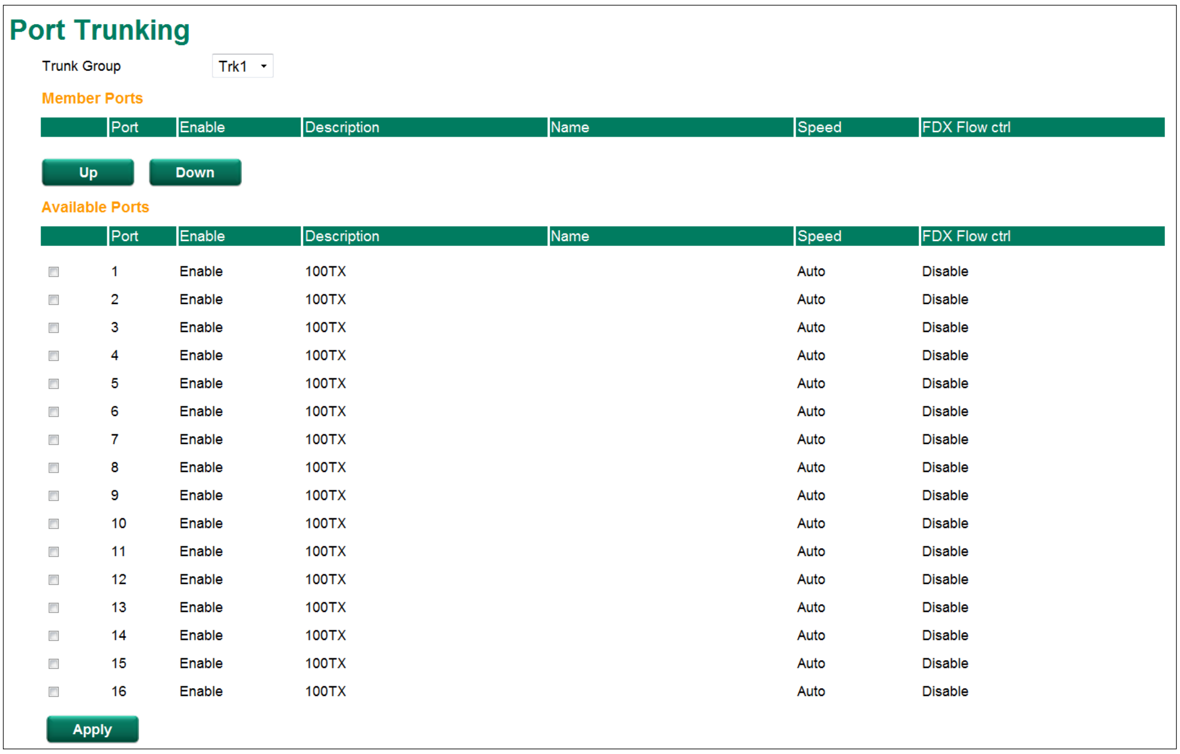
Each Moxa ToughNet NAT Router can set a maximum of 2 port trunking groups. When you activate port trunking, certain settings on each port will be reset to factory default values or disabled:

- Communication redundancy will be reset
- 802.1Q VLAN will be reset
- Multicast Filtering will be reset
- Port Lock will be reset and disabled.
- Set Device IP will be reset
- Mirror will be reset

After port trunking has been activated, you can configure these items again for each trunking port.

Port Trunking

The **Port Trunking Settings** page is where ports are assigned to a trunk group.



Port Trunking

Trunk Group: Trk1

Member Ports

	Port	Enable	Description	Name	Speed	FDX Flow ctrl

Available Ports

	Port	Enable	Description	Name	Speed	FDX Flow ctrl
□	1	Enable	100TX		Auto	Disable
□	2	Enable	100TX		Auto	Disable
□	3	Enable	100TX		Auto	Disable
□	4	Enable	100TX		Auto	Disable
□	5	Enable	100TX		Auto	Disable
□	6	Enable	100TX		Auto	Disable
□	7	Enable	100TX		Auto	Disable
□	8	Enable	100TX		Auto	Disable
□	9	Enable	100TX		Auto	Disable
□	10	Enable	100TX		Auto	Disable
□	11	Enable	100TX		Auto	Disable
□	12	Enable	100TX		Auto	Disable
□	13	Enable	100TX		Auto	Disable
□	14	Enable	100TX		Auto	Disable
□	15	Enable	100TX		Auto	Disable
□	16	Enable	100TX		Auto	Disable

Step 1: Select the desired **Trunk Group**

Step 2: Select the desired **Member Ports** or **Available Ports**

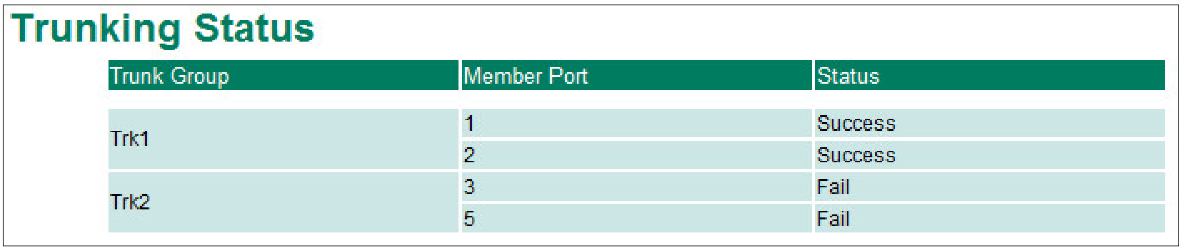
Step 3: Use **Up** and **Down** to modify the Group Members

Trunk Group (maximum of 2 trunk groups)

Setting	Description	Factory Default
Trk1, Trk2 (depends on switching chip capability)	Specifies the current trunk group.	Trk1

Trunking Status

The **Trunking Status table** shows the Trunk Group configuration status.

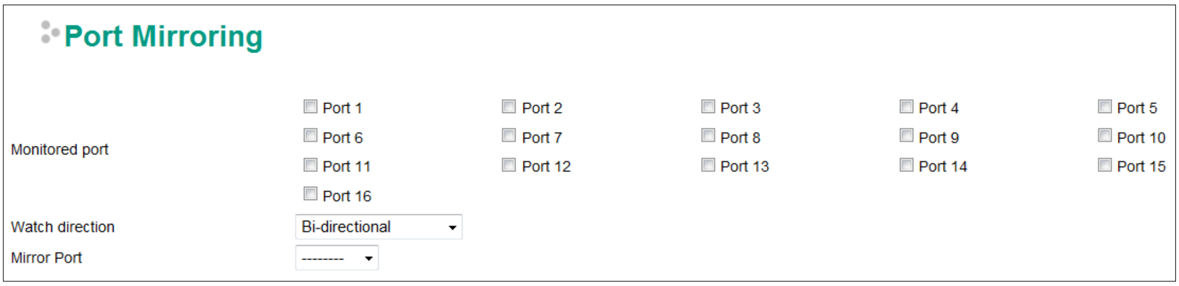


Trunking Status

Trunk Group	Member Port	Status
Trk1	1	Success
	2	Success
Trk2	3	Fail
	5	Fail

Port Mirror

The **Port Mirror** function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. Using a mirror port allows the network administrator to **sniff** the observed port to keep tabs on network activity.



Port Mirroring

Monitored port
□ Port 1 □ Port 2 □ Port 3 □ Port 4 □ Port 5
□ Port 6 □ Port 7 □ Port 8 □ Port 9 □ Port 10
□ Port 11 □ Port 12 □ Port 13 □ Port 14 □ Port 15
□ Port 16

Watch direction: Bi-directional

Mirror Port: --------

Port Mirroring Settings

Setting	Description
Monitored Port	Select the number of the ports whose network activity will be monitored. Multiple port selection is acceptable.
Watch Direction	Select one of the following two watch direction options: • Input data stream: Select this option to monitor only those data packets coming into the Moxa ToughNet NAT Router’s port. • Output data stream: Select this option to monitor only those data packets being sent out through the Moxa ToughNet NAT Router’s port. • Bi-directional: Select this option to monitor data packets both coming into, and being sent out through, the Moxa ToughNet NAT Router’s port.
Mirror Port	Select the number of the port that will be used to monitor the activity of the monitored port.

Using Virtual LAN

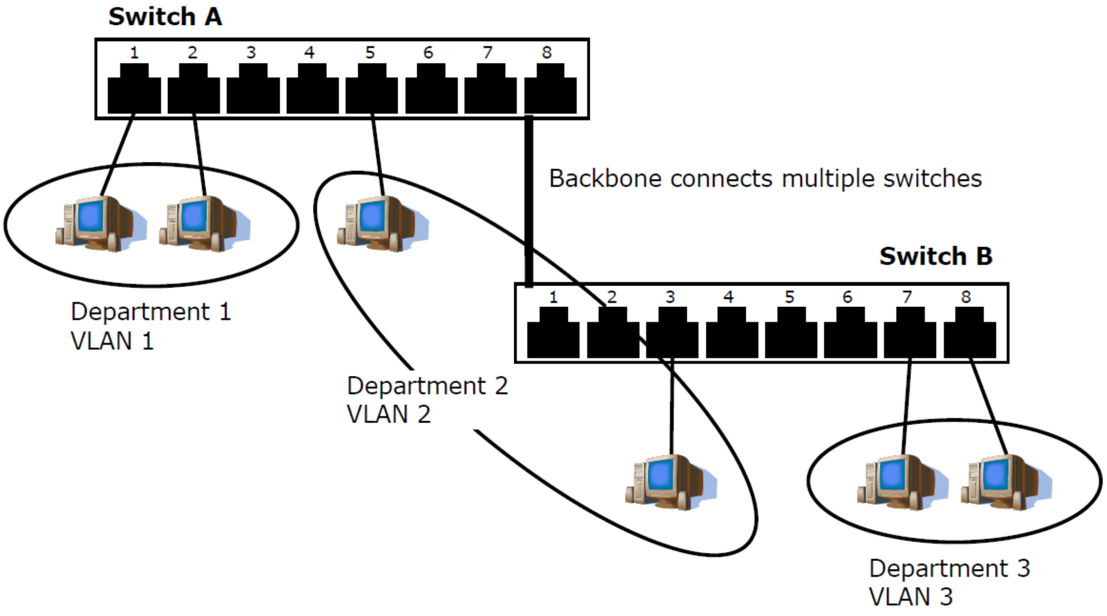
Setting up Virtual LANs (VLANs) on your Moxa ToughNet NAT Router increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

The VLAN Concept

What is a VLAN?

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

- **Departmental groups**—you could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups**—you could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—you could have one VLAN for email users and another for multimedia users.



Benefits of VLANs

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

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

Managing a VLAN

A new or initialized Moxa ToughNet NAT Router contains a single VLAN—the Default VLAN. This VLAN has the following definition:

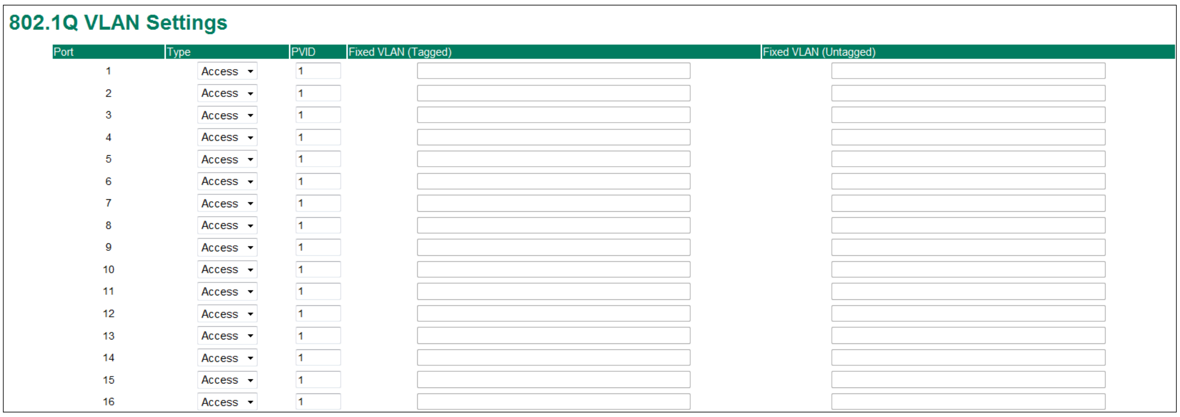
- **VLAN Name**—Management VLAN
- **802.1Q VLAN ID**—1 (if tagging is required)

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

Configuring Virtual LAN

To configure **802.1Q VLAN** on the Moxa switch, use the **802.1Q VLAN Settings** page to configure the ports.

802.1Q VLAN Settings



802.1Q VLAN Settings

Port	Type	PVID	Fixed VLAN (Tagged)	Fixed VLAN (Untagged)
1	Access	1		
2	Access	1		
3	Access	1		
4	Access	1		
5	Access	1		
6	Access	1		
7	Access	1		
8	Access	1		
9	Access	1		
10	Access	1		
11	Access	1		
12	Access	1		
13	Access	1		
14	Access	1		
15	Access	1		
16	Access	1		

Management VLAN ID

Setting	Description	Factory Default
VLAN ID from 1-4094	Assigns the VLAN ID of this Moxa switch.	1

Port Type

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

PVID

Setting	Description	Factory Default
VLAN ID from 1-4094	Sets the default VLAN ID for untagged devices that connect to the port.	1

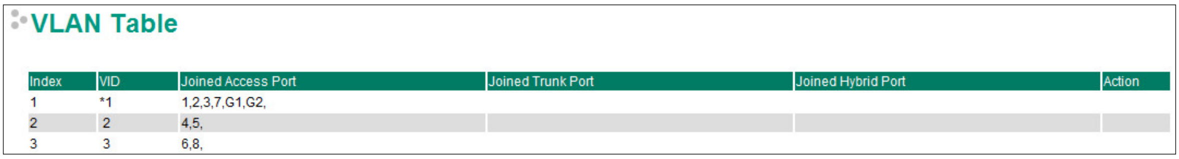
Tagged VLAN

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

Untagged VLAN

Setting	Description	Factory Default
VLAN ID from 1-4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	None

VLAN Table



VLAN Table

Index	VID	Joined Access Port	Joined Trunk Port	Joined Hybrid Port	Action
1	*1	1,2,3,7,G1,G2,			
2	2	4,5,			
3	3	6,8,			

Use the **802.1Q VLAN Table** to review the VLAN groups that were created, Joined Access Ports, Trunk Ports, and Hybrid Ports, and also Action for deleting VLANs which have no member ports in the list.

Multicast

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your Moxa ToughNet NAT Router.

The Concept of Multicast Filtering

What is an IP Multicast?

A *multicast* is a packet sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations on a LAN or VLAN that belong to the multicast group. Multicast group members can be distributed across multiple subnets, so that multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only *one* copy of the desired information across the network until the delivery path that reaches group members diverges. To make more efficient use of network bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

The benefits of using IP multicast are:

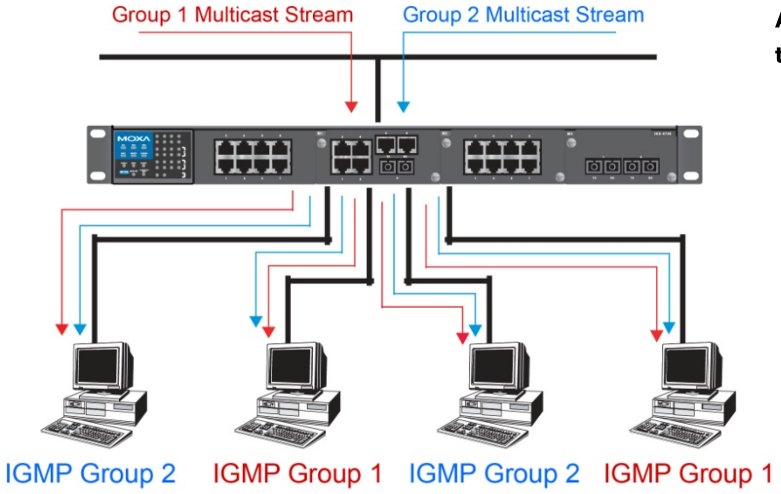
- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- Works with other IP protocols and services, such as Quality of Service (QoS).

Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all end-stations would cause a substantial reduction in network performance. Furthermore, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use multicast. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

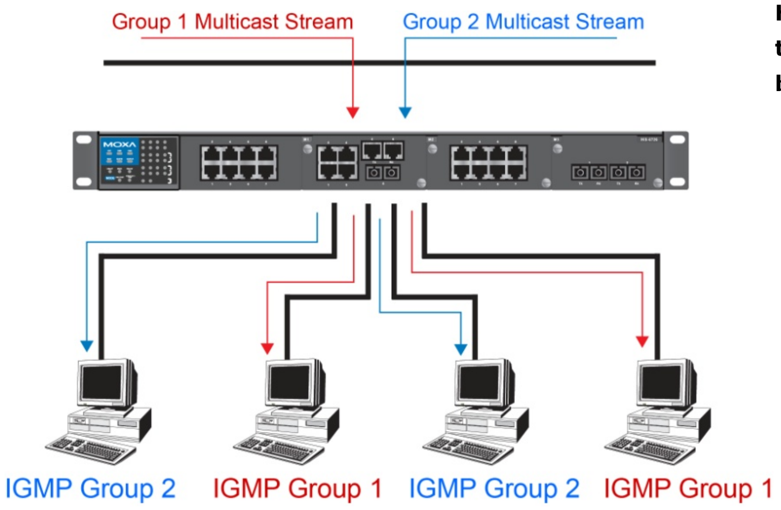
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves without multicast filtering, and with multicast filtering.

Network without multicast filtering



All hosts receive the multicast traffic, even if they don't need it.

Network with multicast filtering



Hosts only receive dedicated traffic from other hosts belonging to the same group.

Multicast Filtering and Moxa's ToughNet NAT Routers

The Moxa ToughNet NAT Router has two ways to achieve multicast filtering: IGMP (Internet Group Management Protocol) Snooping and adding a static multicast MAC manually to filter multicast traffic automatically.

Snooping Mode

Snooping Mode allows your ToughNet NAT Router to forward multicast packets only to the appropriate ports. The router **snoops** on exchanges between hosts and an IGMP device to find those ports that want to join a multicast group, and then configures its filters accordingly.

Query Mode

Query mode allows the Moxa router to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs.

IGMP querying is enabled by default on the Moxa router to ensure proceeding query election. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers). Query mode allows users to enable IGMP snooping by VLAN ID. Moxa ToughNet NAT Router support IGMP snooping version 1 and version 2. Version 2 is compatible with version 1.The default setting is IGMP V1/V2. "

IGMP Multicast Filtering

IGMP is used by IP-supporting network devices to register hosts with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router, and on other network devices that support multicast filtering. Moxa switches support IGMP version 1 and 2. IGMP version 1 and 2 work as follows::

- The IP router (or querier) periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with IP address lower than the IP address of any other IGMP queriers connected to the LAN or VLAN can become the IGMP querier.
- When an IP host receives a query packet, it sends a report packet back that identifies the multicast group that the end-station would like to join.
- When the report packet arrives at a port on a switch with IGMP Snooping enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.
- When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
- When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

IGMP version comparison

IGMP Version	Main Features	Reference
V1	a. Periodic query	RFC-1112
V2	Compatible with V1 and adds: a. Group-specific query b. Leave group messages c. Resends specific queries to verify leave message was the last one in the group d. Querier election	RFC-2236

Static Multicast MAC

Some devices may only support multicast packets, but not support either IGMP Snooping. The Moxa ToughNet NAT Router supports adding multicast groups manually to enable multicast filtering.

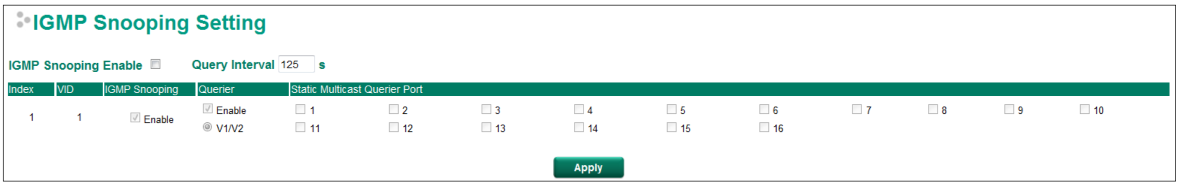
Enabling Multicast Filtering

Use the USB console or web interface to enable or disable IGMP Snooping and IGMP querying. If IGMP Snooping is not enabled, then IP multicast traffic is always forwarded, flooding the network.

IGMP Snooping

IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.

IGMP Snooping Settings



IGMP Snooping Setting

IGMP Snooping Enable □ Query Interval 125 s

Index	VID	IGMP Snooping	Querier	Static Multicast Querier Port
1	1	☑ Enable	☑ Enable ● V1/V2	□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16

Enable IGMP Snooping (Global)

Setting	Description	Factory Default
Enable/Disable	Checkmark the Enable IGMP Snooping checkbox near the top of the window to enable the IGMP Snooping function globally.	Disabled

Query Interval (sec)

Setting	Description	Factory Default
Numerical value, input by the user	Sets the query interval of the Querier function globally. Valid settings are from 20 to 600 seconds.	125 seconds

Enable IGMP Snooping

Setting	Description	Factory Default
Enable/Disable	Enables or disables the IGMP Snooping function on that particular VLAN.	Enabled if IGMP Snooping is enabled globally

Querier

Setting	Description	Factory Default
Enable/Disable	Enables or disables the Moxa ToughNet NAT Router's querier function.	Disabled
V1/V2 Checkbox	V1/V2: Enables the Moxa ToughNet NAT Router to send IGMP snooping version 1 and 2 queries	V1/V2

Static Multicast Querier Port

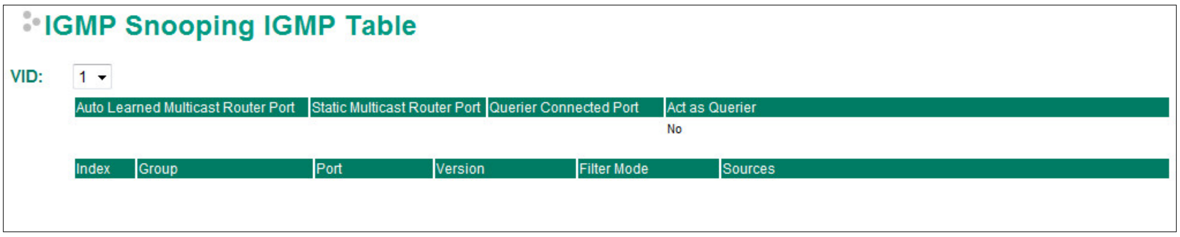
Setting	Description	Factory Default
Select/Deselect	Select the ports that will connect to the multicast routers. These ports will receive all multicast packets from the source. This option is only active when IGMP Snooping is enabled.	Disabled

NOTE If a router or layer 3 switch is connected to the network, it will act as the Querier, and consequently this Querier option will be disabled on all Moxa layer 2 switches.

If all switches on the network are Moxa layer 2 switches, then only one layer 2 switch will act as Querier.

IGMP Table

The Moxa ToughNet NAT Router displays the current active IGMP groups that were detected. View IGMP group setting per VLAN ID on this page.



IGMP Snooping IGMP Table

VID: 1

Auto Learned Multicast Router Port	Static Multicast Router Port	Querier Connected Port	Act as Querier
			No

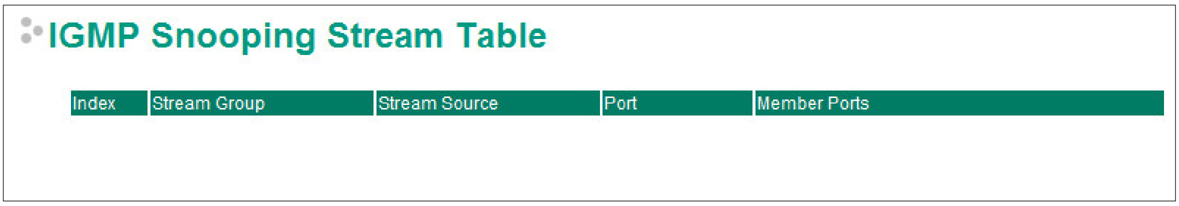
Index	Group	Port	Version	Filter Mode	Sources

The information shown in the table includes:

- Auto Learned Multicast Router Port: This indicates that a multicast router connects to/sends packets from these port(s).
- Static Multicast Router Port: Displays the static multicast querier port(s)
- Querier Connected Port: Displays the port which is connected to the querier
- Act as a Querier: Displays whether or not ths VLAN is a querier (winner of a election)
- Group: Displays the multicast group addresses
- Port: Displays the port which receive the multicast stream/the port the multicast stream is forwarded to
- Version: Displays the IGMP Snooping version

Stream Table

This page displays the multicast stream forwarding status. It allows you to view the status per VLAN ID.



IGMP Snooping Stream Table

Index	Stream Group	Stream Source	Port	Member Ports

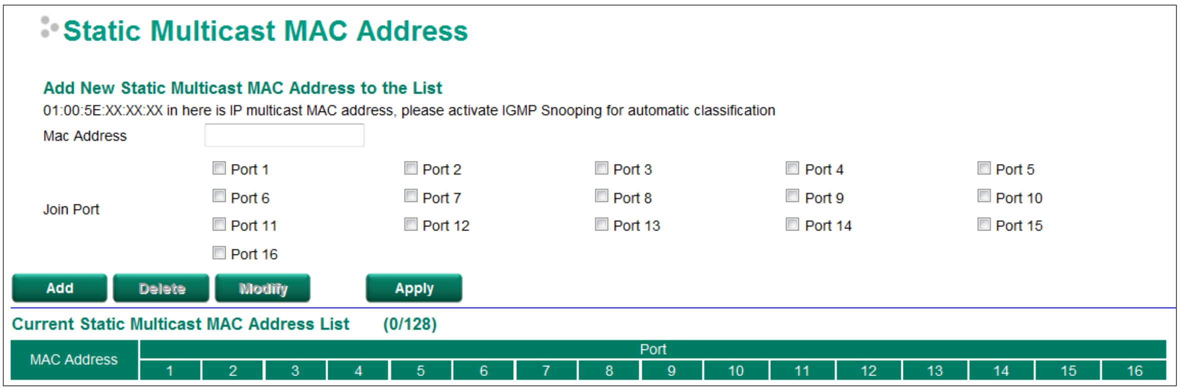
Stream Group: Multicast group IP address

Stream Source: Multicast source IP address

Port: Which port receives the multicast stream

Member ports: Ports the multicast stream is forwarded to

Static Multicast MAC



Static Multicast MAC Address

Add New Static Multicast MAC Address to the List

01:00:5E:XX:XX:XX in here is IP multicast MAC address, please activate IGMP Snooping for automatic classification

Mac Address

Join Port

□ Port 1 □ Port 2 □ Port 3 □ Port 4 □ Port 5
□ Port 6 □ Port 7 □ Port 8 □ Port 9 □ Port 10
□ Port 11 □ Port 12 □ Port 13 □ Port 14 □ Port 15
□ Port 16

Current Static Multicast MAC Address List (0/128)

MAC Address	Port															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

NOTE 01:00:5E:XX:XX:XX on this page is the IP multicast MAC address. Please activate IGMP Snooping for automatic classification.

MAC Address

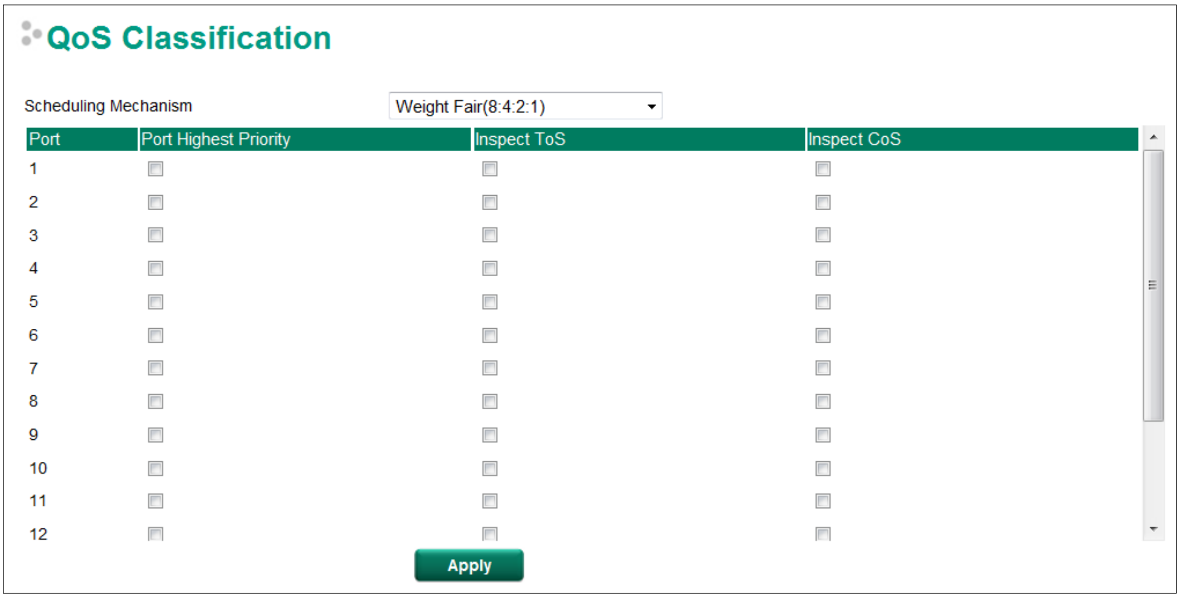
Setting	Description	Factory Default
Integer	Input the number of the VLAN that the host with this MAC address belongs to.	None

Join Port

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to select the join ports for this multicast group.	None

QoS

QoS Classification



QoS Classification

Scheduling Mechanism: Weight Fair(8:4:2:1)

Port	Port Highest Priority	Inspect ToS	Inspect CoS
1	□	□	□
2	□	□	□
3	□	□	□
4	□	□	□
5	□	□	□
6	□	□	□
7	□	□	□
8	□	□	□
9	□	□	□
10	□	□	□
11	□	□	□
12	□	□	□

The Moxa switch supports inspection of layer 3 ToS and/or layer 2 CoS tag information to determine how to classify traffic packets.

Scheduling Mechanism

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

Inspect ToS

Setting	Description	Factory Default
Enable/Disable	Enables or disables the Moxa ToughNet NAT Router for inspecting Type of Service (ToS) bits in the IPV4 frame to determine the priority of each frame.	Enabled

Inspect COS

Setting	Description	Factory Default
Enable/Disable	Enables or disables the Moxa ToughNet NAT Router for inspecting 802.1p CoS tags in the MAC frame to determine the priority of each frame.	Enabled

Port Priority

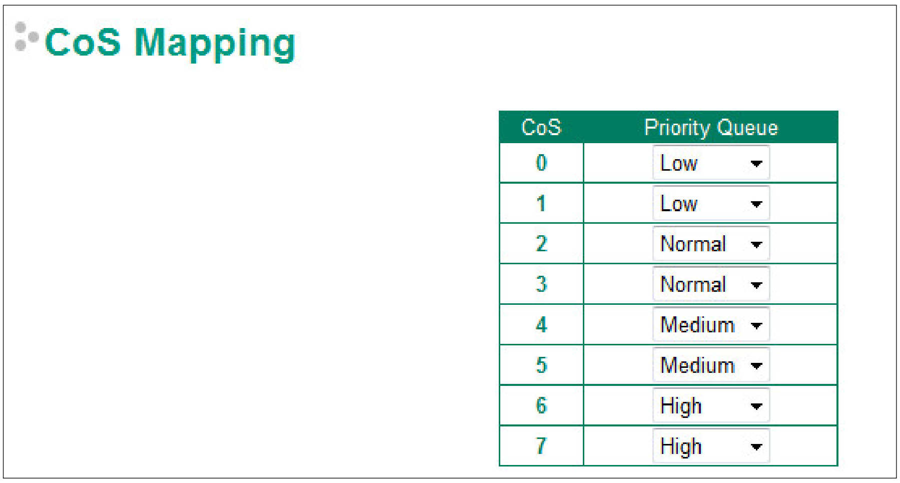
Setting	Description	Factory Default
Port priority	The port priority has 4 priority queues. Low, normal, medium, high priority queue option is applied to each port.	3(Normal)

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

1. Inspect CoS
2. Inspect ToS
3. Port Priority

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

CoS Mapping



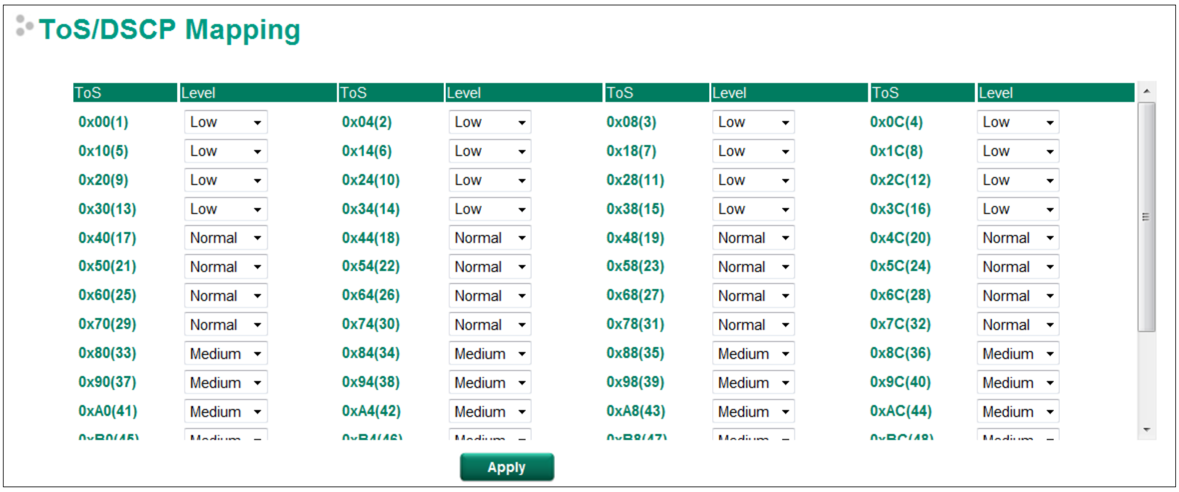
CoS Mapping

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

CoS Value and Priority Queues

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different CoS values to 4 different egress queues.	Low Normal Medium High

ToS/DSCP Mapping



ToS/DSCP Mapping

ToS	Level	ToS	Level	ToS	Level	ToS	Level
0x00(1)	Low	0x04(2)	Low	0x08(3)	Low	0x0C(4)	Low
0x10(5)	Low	0x14(6)	Low	0x18(7)	Low	0x1C(8)	Low
0x20(9)	Low	0x24(10)	Low	0x28(11)	Low	0x2C(12)	Low
0x30(13)	Low	0x34(14)	Low	0x38(15)	Low	0x3C(16)	Low
0x40(17)	Normal	0x44(18)	Normal	0x48(19)	Normal	0x4C(20)	Normal
0x50(21)	Normal	0x54(22)	Normal	0x58(23)	Normal	0x5C(24)	Normal
0x60(25)	Normal	0x64(26)	Normal	0x68(27)	Normal	0x6C(28)	Normal
0x70(29)	Normal	0x74(30)	Normal	0x78(31)	Normal	0x7C(32)	Normal
0x80(33)	Medium	0x84(34)	Medium	0x88(35)	Medium	0x8C(36)	Medium
0x90(37)	Medium	0x94(38)	Medium	0x98(39)	Medium	0x9C(40)	Medium
0xA0(41)	Medium	0xA4(42)	Medium	0xA8(43)	Medium	0xAC(44)	Medium
0xB0(45)	Medium	0xB4(46)	Medium	0xB8(47)	Medium	0xBC(48)	Medium

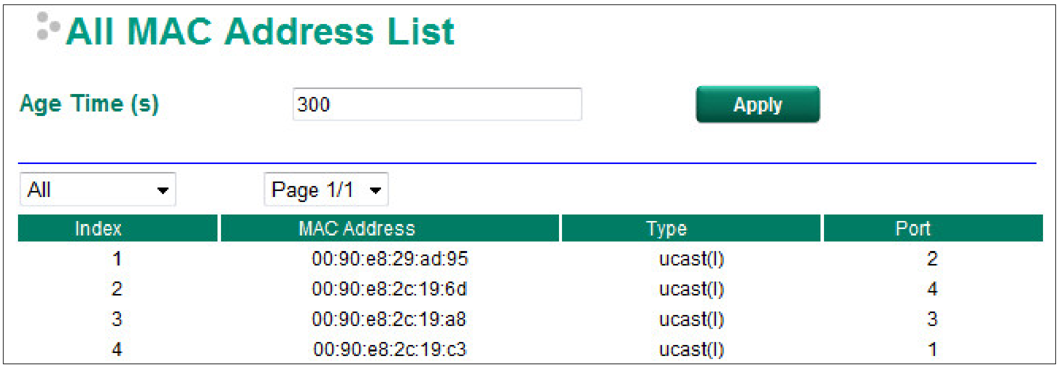
ToS (DSCP) Value and Priority Queues

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different TOS values to 4 different egress queues.	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

MAC Address Table

The MAC address table shows the MAC address list pass through Moxa ToughNet NAT Router. The length of time(Ageing time: 15 to 3825 seconds) is the parameter defines the length of time that a MAC address entry can remain in the Moxa router. When an entry reaches its aging time, it "ages out" and is purged from the router, effectively cancelling frame forwarding to that specific port.

The MAC Address table can be configured to display the following Moxa ToughNet NAT Router MAC address groups, which are selected from the drop-down list.



All MAC Address List

Age Time (s): 300

Index	MAC Address	Type	Port
1	00:90:e8:29:ad:95	ucast(l)	2
2	00:90:e8:2c:19:6d	ucast(l)	4
3	00:90:e8:2c:19:a8	ucast(l)	3
4	00:90:e8:2c:19:c3	ucast(l)	1

Drop Down List

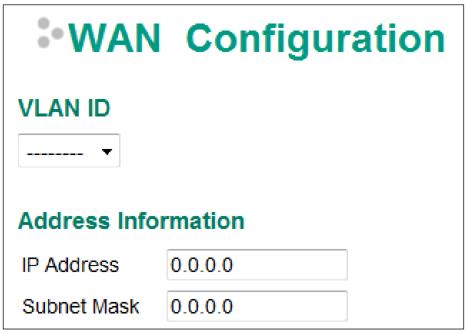
ALL	Select this item to show all of the Moxa ToughNet NAT Router's MAC addresses.
ALL Learned	Select this item to show all of the Moxa ToughNet NAT Router's Learned MAC addresses.
ALL Static	Select this item to show all of the Moxa ToughNet NAT Router's Static, Static Lock, and Static Multicast MAC addresses.
ALL Multicast	Select this item to show all of the Moxa ToughNet NAT Router's Static Multicast MAC addresses.
Port x	Select this item to show all of the MAC addresses dedicated ports.

The table displays the following information:

MAC Address	This field shows the MAC address.
Type	This field shows the type of this MAC address.
Port	This field shows the port that this MAC address belongs to.

Interface

WAN



WAN Configuration

VLAN ID

--------- ▾

Address Information

IP Address	0.0.0.0
Subnet Mask	0.0.0.0

VLAN ID

Moxa ToughNet NAT Router’s WAN interface is configured by VLAN group. The ports with the same VLAN can be configured as one WAN interface.

Address Information

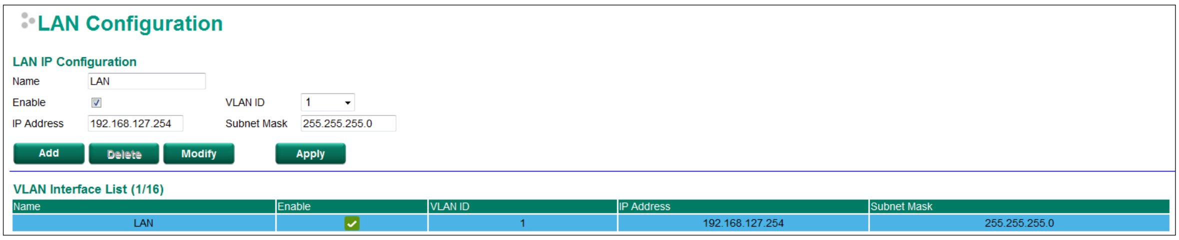
IP Address

Setting	Description	Factory Default
IP Address	The interface IP address	None

Subnet Mask

Setting	Description	Factory Default
IP Address	The subnet mask	None

LAN



LAN Configuration

LAN IP Configuration

Name: LAN

Enable: ☑ VLAN ID: 1 ▾

IP Address: 192.168.127.254 Subnet Mask: 255.255.255.0

VLAN Interface List (1/16)

Name	Enable	VLAN ID	IP Address	Subnet Mask
LAN	✓	1	192.168.127.254	255.255.255.0

Create a VLAN Interface

Input a name of the LAN interface, select a VLAN ID that is already configured in VLAN Setting under the Layer 2 Function, and assign an IP address / Subnet Mask for the interface. Checkmark the **Enable** checkbox to enable this interface.

Delete a LAN Interface

Select the item in the LAN Interface List, and then click **Delete** to delete the item.

Modify a LAN Interface

Select the item in the LAN Interface List. Modify the attributes and then click **Modify** to change the configuration.

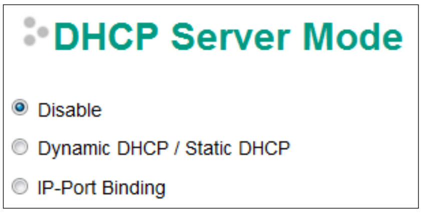
Activate the LAN Interface List

After adding/deleting/modifying any LAN interface, be sure to click **Activate**.

Network Service

DHCP Settings

Global Settings



DHCP Server Mode

● Disable

○ Dynamic DHCP / Static DHCP

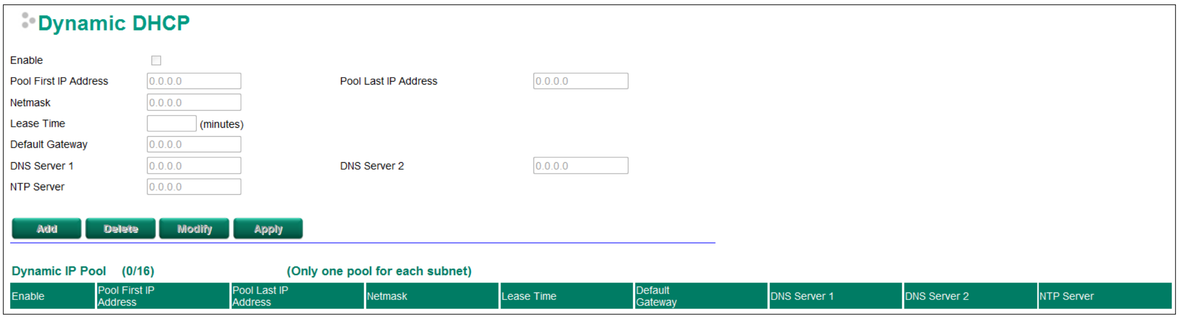
○ IP-Port Binding

DHCP Server Mode

Setting	Description	Factory Default
Disable/ Dynamic/Static IP Assignment/ IP-Port Binding	Select the DHCP Server Mode	Disabled

DHCP Server

The ToughNet NAT Router provides a DHCP (Dynamic Host Configuration Protocol) server function for LAN interfaces. When configured, the ToughNet NAT Router will automatically assign an IP address to a Ethernet device from a defined IP range.



Dynamic DHCP

Enable □

Pool First IP Address 0.0.0.0 Pool Last IP Address 0.0.0.0

Netmask 0.0.0.0

Lease Time (minutes)

Default Gateway 0.0.0.0

DNS Server 1 0.0.0.0 DNS Server 2 0.0.0.0

NTP Server 0.0.0.0

Dynamic IP Pool (0/16) (Only one pool for each subnet)

Enable	Pool First IP Address	Pool Last IP Address	Netmask	Lease Time	Default Gateway	DNS Server 1	DNS Server 2	NTP Server

Dynamic IP Assignment

DHCP Server Enable/Disable

Setting	Description	Factory Default
Enable/Disable	Enable or disable DHCP server function	Disable

Pool First IP Address

Setting	Description	Factory Default
IP Address	The first IP address of the offered IP address range for DHCP clients	0.0.0.0

Pool Last IP Address

Setting	Description	Factory Default
IP Address	The last IP address of the offered IP address range for DHCP clients	0.0.0.0

Netmask

Setting	Description	Factory Default
Netmask	The netmask for DHCP clients	0.0.0.0

Lease Time

Setting	Description	Factory Default
≥ 5min.	The lease time of the DHCP server	None

Default Gateway

Setting	Description	Factory Default
IP Address	The default gateway for DHCP clients	0.0.0.0

DNS Server

Setting	Description	Factory Default
IP Address	The DNS server for DHCP clients	0.0.0.0

NTP Server

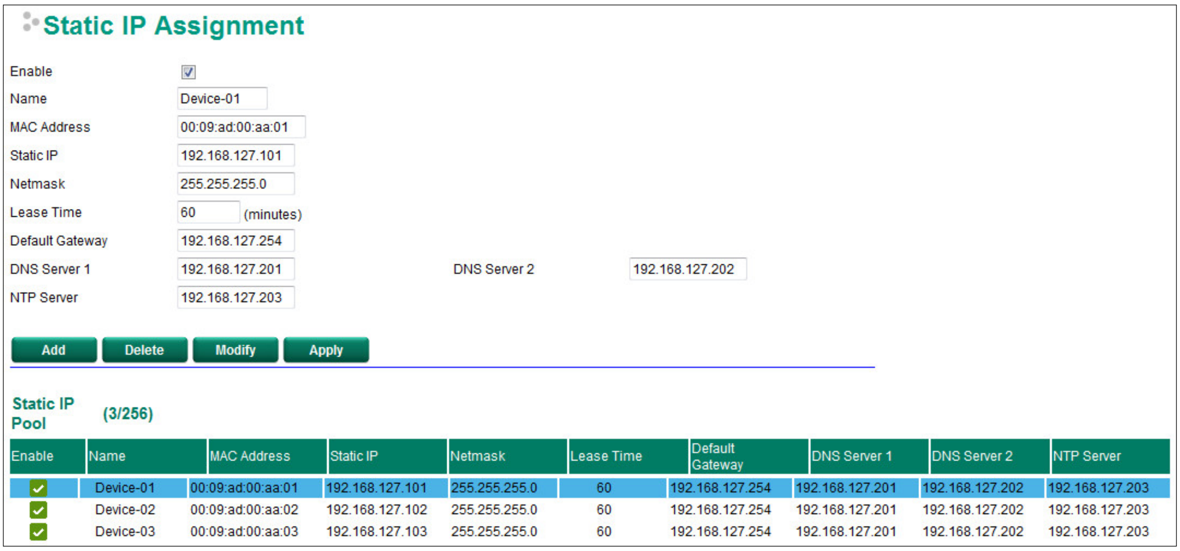
Setting	Description	Factory Default
IP Address	The NTP server for DHCP clients	0.0.0.0

NOTE

1. The DHCP Server is only available for LAN interfaces.
2. The Pool First/Last IP Address must be in the same Subnet on the LAN.

Static DHCP

Use the Static DHCP list to ensure that devices connected to the ToughNet NAT Router always use the same IP address. The static DHCP list matches IP addresses to MAC addresses.



Static IP Assignment

Enable	☑
Name	Device-01
MAC Address	00:09:ad:00:aa:01
Static IP	192.168.127.101
Netmask	255.255.255.0
Lease Time	60 (minutes)
Default Gateway	192.168.127.254
DNS Server 1	192.168.127.201
DNS Server 2	192.168.127.202
NTP Server	192.168.127.203

Static IP Pool (3/256)

Enable	Name	MAC Address	Static IP	Netmask	Lease Time	Default Gateway	DNS Server 1	DNS Server 2	NTP Server
✓	Device-01	00:09:ad:00:aa:01	192.168.127.101	255.255.255.0	60	192.168.127.254	192.168.127.201	192.168.127.202	192.168.127.203
✓	Device-02	00:09:ad:00:aa:02	192.168.127.102	255.255.255.0	60	192.168.127.254	192.168.127.201	192.168.127.202	192.168.127.203
✓	Device-03	00:09:ad:00:aa:03	192.168.127.103	255.255.255.0	60	192.168.127.254	192.168.127.201	192.168.127.202	192.168.127.203

In the above example, a device named "Device-01" was added to the Static DHCP list, with a static IP address set to 192.168.127.101 and MAC address set to 00:09:ad:00:aa:01. When a device with a MAC address of 00:09:ad:00:aa:01 is connected to the ToughNet NAT Router, the ToughNet NAT Router will offer the IP address 192.168.127.101 to this device.

Static DHCP Enable/Disable

Setting	Description	Factory Default
Enable/Disable	Enable or disable Static DHCP server function	Disable

Name

Setting	Description	Factory Default
Max. 30 characters	The name of the selected device in the Static DHCP list	None

MAC Address

Setting	Description	Factory Default
MAC Address	The MAC address of the selected device	None

Static IP

Setting	Description	Factory Default
IP Address	The IP address of the selected device	None

Netmask

Setting	Description	Factory Default
Netmask	The netmask for the selected device	0.0.0.0

Lease Time

Setting	Description	Factory Default
≥ 5min.	The lease time of the selected device	None

Default Gateway

Setting	Description	Factory Default
IP Address	The default gateway for the selected device	0.0.0.0

DNS Server

Setting	Description	Factory Default
IP Address	The DNS server for the selected device	0.0.0.0

NTP Server

Setting	Description	Factory Default
IP Address	The NTP server for the selected device	0.0.0.0

Clickable Buttons

Add

Use the **Add** button to input a new DHCP list. The Name, Static IP, and MAC address must be different from any existing list.

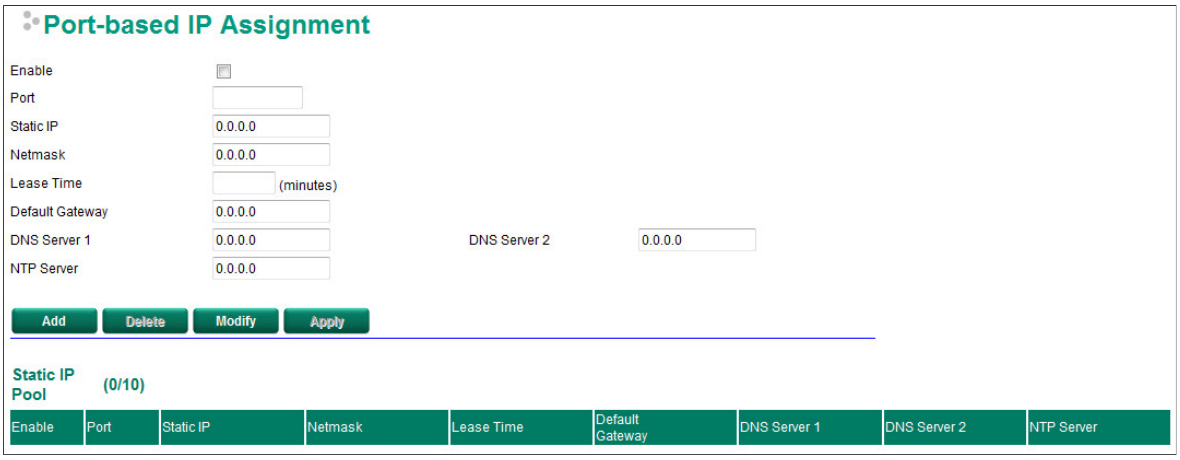
Delete

Use the **Delete** button to delete a Static DHCP list. Click on a list to select it (the background color of the device will change to blue) and then click the **Delete** button.

Modify

To modify the information for a particular list, click on a list to select it (the background color of the device will change to blue), modify the information as needed using the check boxes and text input boxes near the top of the browser window, and then click **Modify**.

IP-Port Binding



Port-based IP Assignment

Enable	☐		
Port			
Static IP	0.0.0.0		
Netmask	0.0.0.0		
Lease Time	(minutes)		
Default Gateway	0.0.0.0		
DNS Server 1	0.0.0.0	DNS Server 2	0.0.0.0
NTP Server	0.0.0.0		

Static IP Pool (0/10)

Enable	Port	Static IP	Netmask	Lease Time	Default Gateway	DNS Server 1	DNS Server 2	NTP Server

IP-Port Binding Enable/Disable

Setting	**Description**	**Factory Default**
Enable/Disable	Enable or disable IP-Port Binding function	Disable

Port

Setting	**Description**	**Factory Default**
IP Address	Set the desired IP of the connected devices	None

Static IP

Setting	**Description**	**Factory Default**
IP Address	The IP address of the connected device	None

Netmask

Setting	**Description**	**Factory Default**
Netmask	The netmask for the connected device	0.0.0.0

Lease Time

Setting	**Description**	**Factory Default**
≥ 5min.	The lease time of the connected device	None

Default Gateway

Setting	**Description**	**Factory Default**
IP Address	The default gateway for the connected device	0.0.0.0

DNS Server

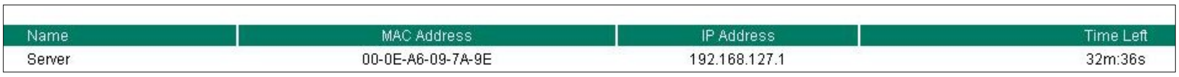
Setting	**Description**	**Factory Default**
IP Address	The DNS server for the connected device	0.0.0.0

NTP Server

Setting	**Description**	**Factory Default**
IP Address	The NTP server for the connected device	0.0.0.0

Client List

Use the Client List to view the current DHCP clients.



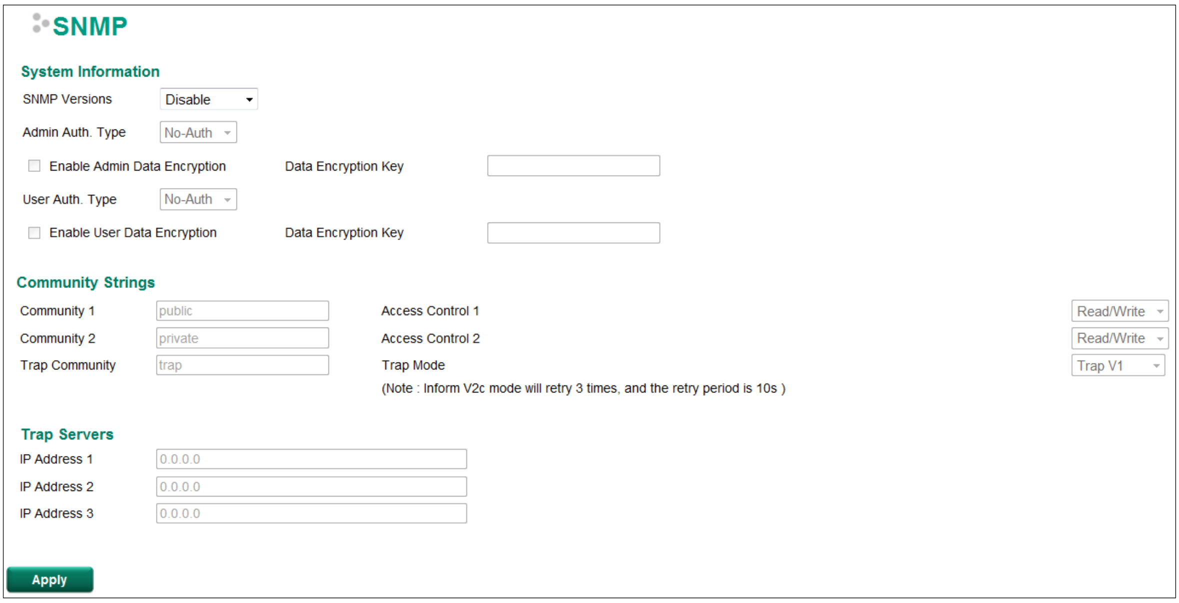
Name	MAC Address	IP Address	Time Left
Server	00-0E-A6-09-7A-9E	192.168.127.1	32m:36s

SNMP Settings

The ToughNet NAT Router supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only permissions using the community string public (default value). SNMP V3, which requires that the user selects an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security. SNMP security modes and security levels supported by the ToughNet NAT Router are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	UI Setting	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication
SNMP V3	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based onHMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

These parameters are configured on the SNMP page. A more detailed explanation of each parameter is given below.



SNMP

System Information

SNMP Versions: Disable

Admin Auth. Type: No-Auth

□ Enable Admin Data Encryption   Data Encryption Key

User Auth. Type: No-Auth

□ Enable User Data Encryption   Data Encryption Key

Community Strings

Community 1	public	Access Control 1	Read/Write
Community 2	private	Access Control 2	Read/Write
Trap Community	trap	Trap Mode	Trap V1

(Note : Inform V2c mode will retry 3 times, and the retry period is 10s)

Trap Servers

IP Address 1	0.0.0.0
IP Address 2	0.0.0.0
IP Address 3	0.0.0.0

SNMP Versions

Setting	Description	Factory Default
Disable V1, V2c, V3, or V1, V2c, or V3 only	Select the SNMP protocol version used to manage the secure router.	Disable

Auth. Type

Setting	Description	Factory Default
MD5	Provides authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	MD5
SHA	Provides authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	
No-Auth	Provides no authentication	

Data Encryption Enable/Disable

Setting	Description	Factory Default
Enable/Disable	Enable of disable the data encryption	Disable

Data Encryption Key

Setting	Description	Factory Default
Max. 30 Characters	8-character data encryption key is the minimum requirement for data encryption	None

Community Name

Setting	Description	Factory Default
Max. 30 Characters	Use a community string match for authentication	Public

Access Control

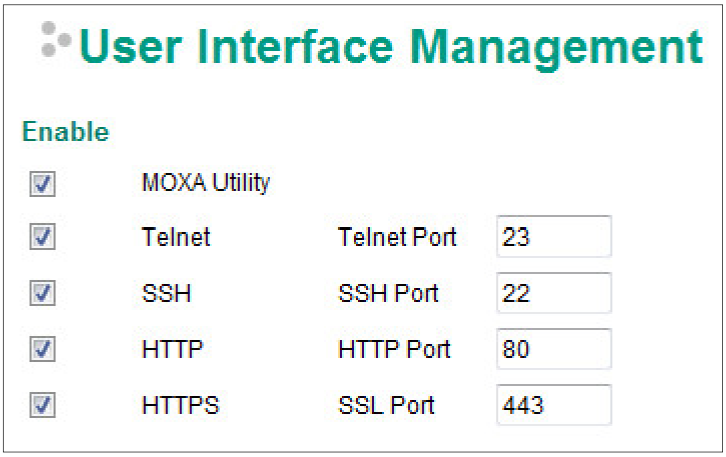
Setting	Description	Factory Default
Read/Write	Access control type after matching the community string	Read/Write
Read only (Public MIB only)		
No Access		

Target IP Address

Setting	Description	Factory Default
IP Address	Enter the IP address of the Trap Server used by your network.	0.0.0.0.

Security

User Interface Management



User Interface Management

Enable

☑ MOXA Utility

☑ Telnet Telnet Port 23

☑ SSH SSH Port 22

☑ HTTP HTTP Port 80

☑ HTTPS SSL Port 443

Enable MOXA Utility

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable MOXA Utility	Selected

Enable Telnet

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable Telnet	Selected Port: 23

Enable SSH

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable SSH	Selected Port: 22

Enable HTTP

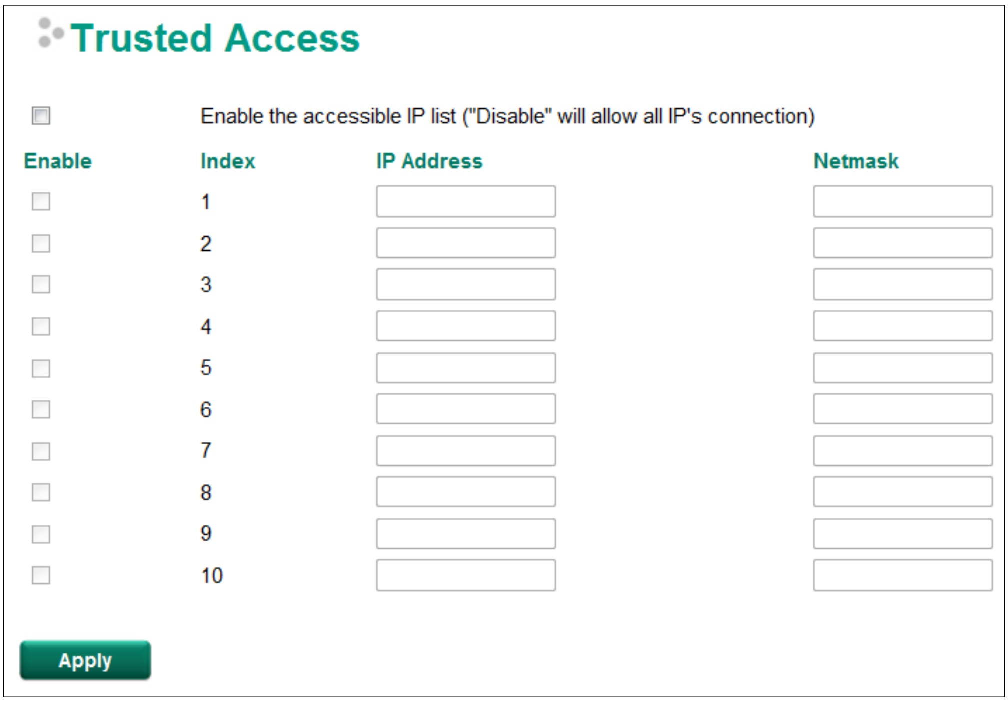
Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable HTTP	Selected Port: 80

Enable HTTPS

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable HTTPS	Selected Port: 443

Trusted Access

The Moxa ToughNet NAT Router uses an IP address-based filtering method to control access.



Trusted Access

□ Enable the accessible IP list ("Disable" will allow all IP's connection)

Enable	Index	IP Address	Netmask
□	1		
□	2		
□	3		
□	4		
□	5		
□	6		
□	7		
□	8		
□	9		
□	10		

You may add or remove IP addresses to limit access to the Moxa ToughNet NAT Router. When the accessible IP list is enabled, only addresses on the list will be allowed access to the Moxa ToughNet NAT Router. Each IP address and netmask entry can be tailored for different situations:

- **Grant access to one host with a specific IP address**
  For example, enter IP address 192.168.1.1 with netmask 255.255.255.255 to allow access to 192.168.1.1 only.
- **Grant access to any host on a specific subnetwork**
  For example, enter IP address 192.168.1.0 with netmask 255.255.255.0 to allow access to all IPs on the subnet defined by this IP address/subnet mask combination.
- **Grant access to all hosts**
  Make sure the accessible IP list is not enabled. Remove the checkmark from **Enable the accessible IP list**.

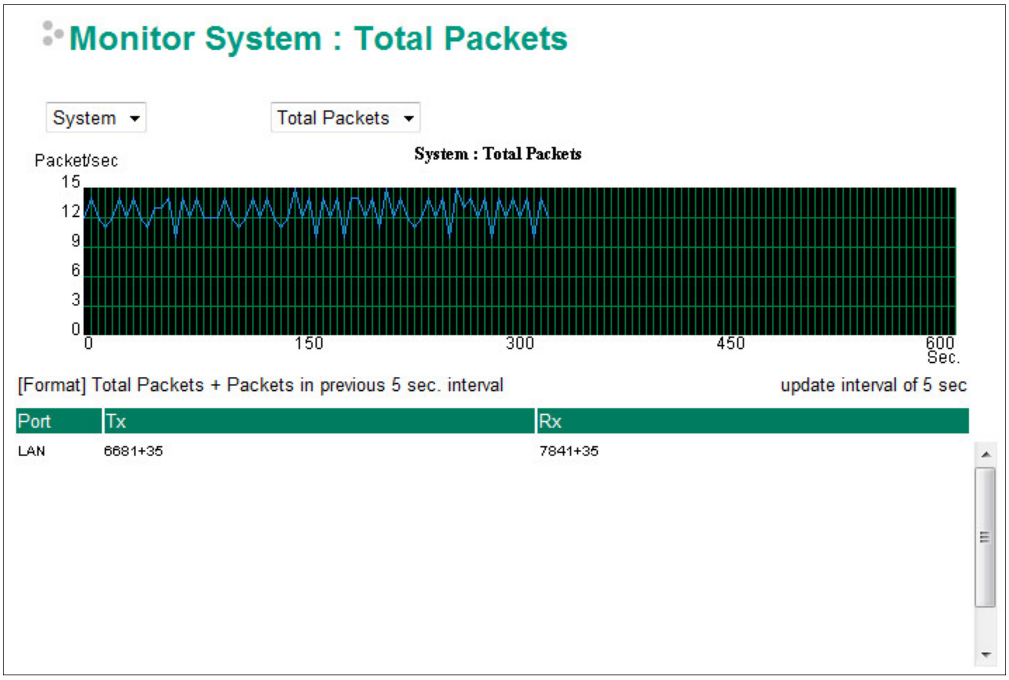
The following table shows additional configuration examples:

Hosts That Need Access	Input Format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

Monitor

Interface Statistics

Access the Monitor by selecting **Monitor** from the left selection bar. **Monitor by System** allows the user to view a graph that shows the combined data transmission activity of all of the Moxa ToughNet NAT Router’s ports. Click one of the three options—**Total Packets, TX Packets,** or **RX Packets**—to view transmission activity of specific types of packets. Recall that TX Packets are packets sent out from the Moxa ToughNet NAT Router, and RX Packets are packets received from connected devices. The Total Packets option displays a graph that combines TX and RX Packets activity. The graph displays data transmission activity by showing Packets/s (i.e., packets per second, or pps) versus sec. (seconds). The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



Monitor System : Total Packets

System ▾ Total Packets ▾

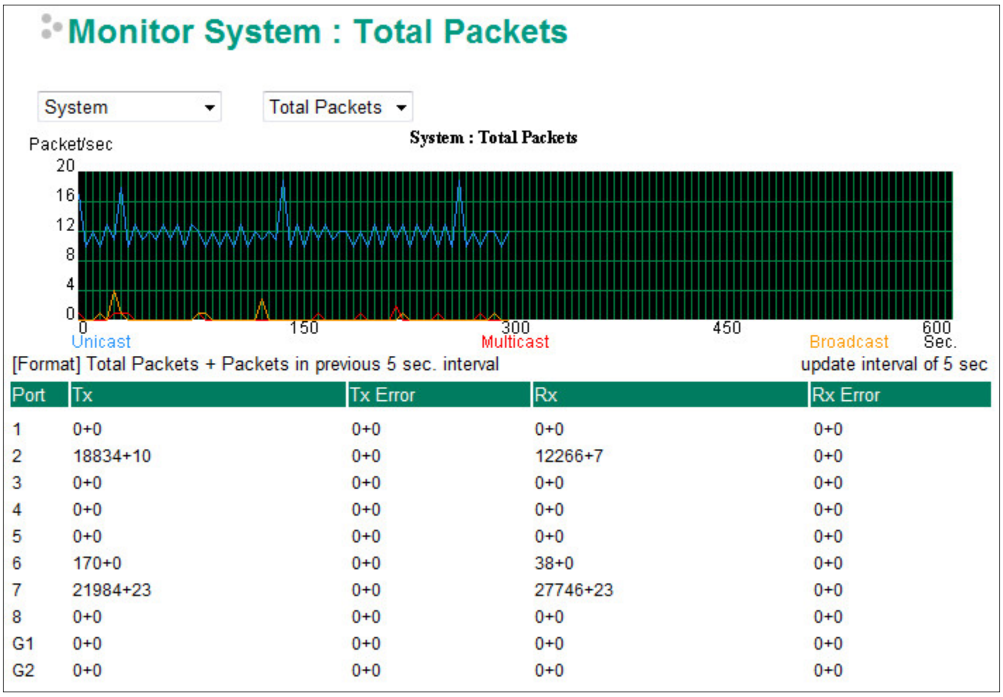
[Format] Total Packets + Packets in previous 5 sec. interval

update interval of 5 sec

Port	Tx	Rx
LAN	6681+35	7841+35

Port Statistics

Access the Monitor by selecting **Monitor** from the left selection bar. Monitor by System allows the user to view a graph that shows the combined data transmission activity of all of the Moxa ToughNet NAT Router's ports. Click one of the four options—**Total Packets**, **TX Packets**, **RX Packets**, or **Error Packets**—to view transmission activity of specific types of packets. Recall that TX Packets are packets sent out from the Moxa ToughNet NAT Router, RX Packets are packets received from connected devices, and Error Packets are packets that did not pass TCP/IP's error checking algorithm. The Total Packets option displays a graph that combines TX, RX, and TX Error, RX Error Packets activity. The graph displays data transmission activity by showing Packets/s (i.e., packets per second, or pps) versus sec. (seconds). In fact, three curves are displayed on the same graph: Uni-cast packets (in blue), Multi-cast packets (in red), and Broad-cast packets (in amber). The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.

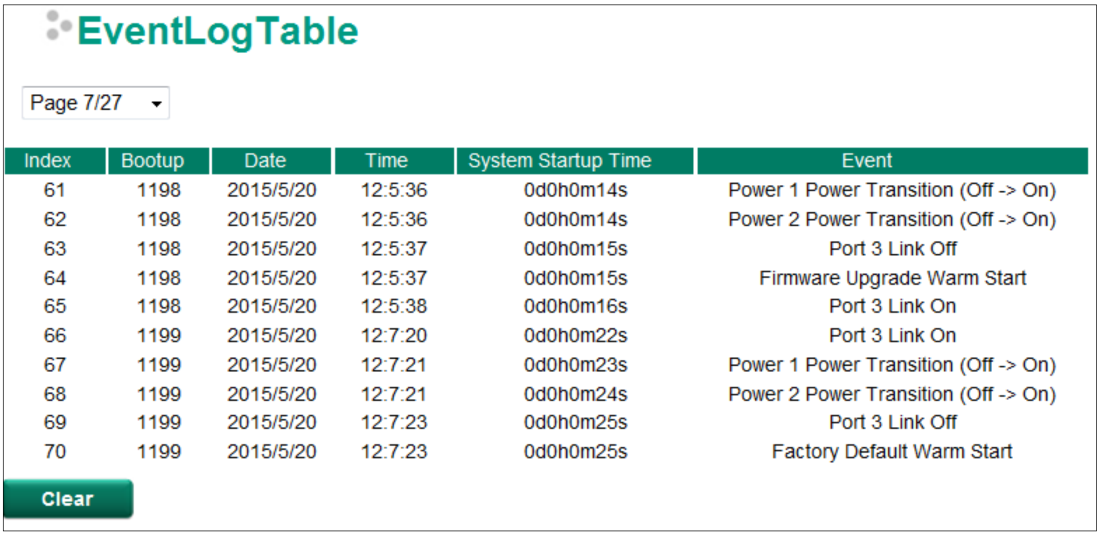


[Format] Total Packets + Packets in previous 5 sec. interval

update interval of 5 sec

Port	Tx	Tx Error	Rx	Rx Error
1	0+0	0+0	0+0	0+0
2	18834+10	0+0	12266+7	0+0
3	0+0	0+0	0+0	0+0
4	0+0	0+0	0+0	0+0
5	0+0	0+0	0+0	0+0
6	170+0	0+0	38+0	0+0
7	21984+23	0+0	27746+23	0+0
8	0+0	0+0	0+0	0+0
G1	0+0	0+0	0+0	0+0
G2	0+0	0+0	0+0	0+0

Event Log



Index	Bootup	Date	Time	System Startup Time	Event
61	1198	2015/5/20	12:5:36	0d0h0m14s	Power 1 Power Transition (Off -> On)
62	1198	2015/5/20	12:5:36	0d0h0m14s	Power 2 Power Transition (Off -> On)
63	1198	2015/5/20	12:5:37	0d0h0m15s	Port 3 Link Off
64	1198	2015/5/20	12:5:37	0d0h0m15s	Firmware Upgrade Warm Start
65	1198	2015/5/20	12:5:38	0d0h0m16s	Port 3 Link On
66	1199	2015/5/20	12:7:20	0d0h0m22s	Port 3 Link On
67	1199	2015/5/20	12:7:21	0d0h0m23s	Power 1 Power Transition (Off -> On)
68	1199	2015/5/20	12:7:21	0d0h0m24s	Power 2 Power Transition (Off -> On)
69	1199	2015/5/20	12:7:23	0d0h0m25s	Port 3 Link Off
70	1199	2015/5/20	12:7:23	0d0h0m25s	Factory Default Warm Start

By default, all event logs will be displayed in the table. You can filter three types of event logs, **System** combined with **severity level**.

4

Routing

The following topics are covered in this chapter:

❒ **Unicast Routing**

- Static Routing
- RIP (Routing Information Protocol)
- Routing Table

Unicast Routing

The ToughNet NAT Router supports two routing methods: static routing and dynamic routing. Dynamic routing makes use of RIP V1/V2. You can either choose one routing method, or combine the two methods to establish your routing table. A routing entry includes the following items: the destination address, the next hop address (which is the next router along the path to the destination address), and a metric that represents the cost we have to pay to access a different network.

Static Route

You can define the routes yourself by specifying what is the next hop (or router) that the ToughNet NAT Router forwards data for a specific subnet. The settings of the Static Route will be added to the routing table and stored in the ToughNet NAT Router.

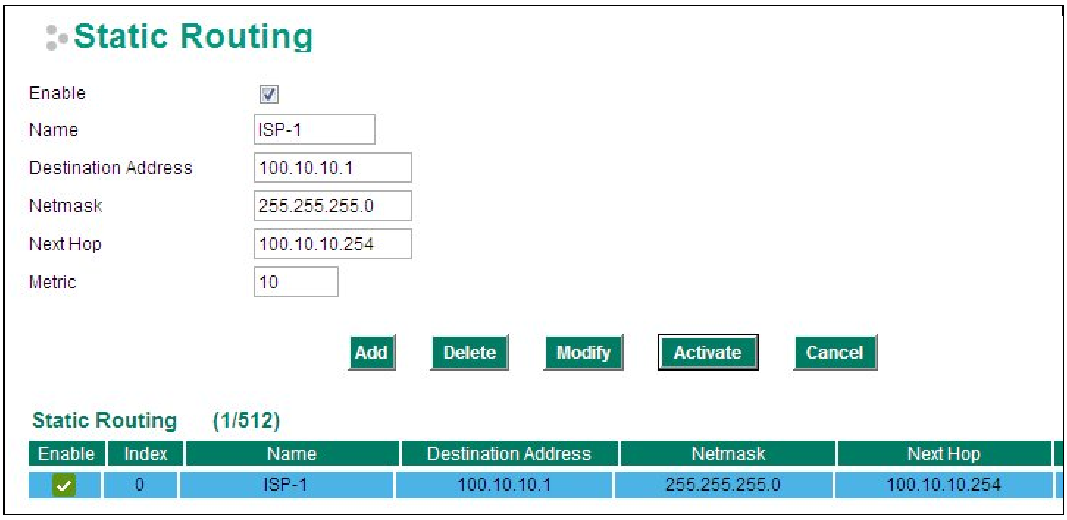
RIP (Routing Information Protocol)

RIP is a distance vector-based routing protocol that can be used to automatically build up a routing table in the ToughNet NAT Router.

The ToughNet NAT Router can efficiently update and maintain the routing table, and optimize the routing by identifying the smallest metric and most matched mask prefix.

Static Routing

The Static Routing page is used to configure the ToughNet NAT Router's static routing table.



Static Routing

Enable	☑
Name	ISP-1
Destination Address	100.10.10.1
Netmask	255.255.255.0
Next Hop	100.10.10.254
Metric	10

Static Routing (1/512)

Enable	Index	Name	Destination Address	Netmask	Next Hop
✓	0	ISP-1	100.10.10.1	255.255.255.0	100.10.10.254

Enable

Click the checkbox to enable Static Routing.

Name

The name of this Static Router list

Destination Address

You can specify the destination IP address.

Netmask

This option is used to specify the subnet mask for this IP address.

Next Hop

This option is used to specify the next router along the path to the destination.

Metric

Use this option to specify a "cost" for accessing the neighboring network.

Clickable Buttons

Add

For adding an entry to the Static Routing Table.

Delete

For removing selected entries from the Static Routing Table.

Modify

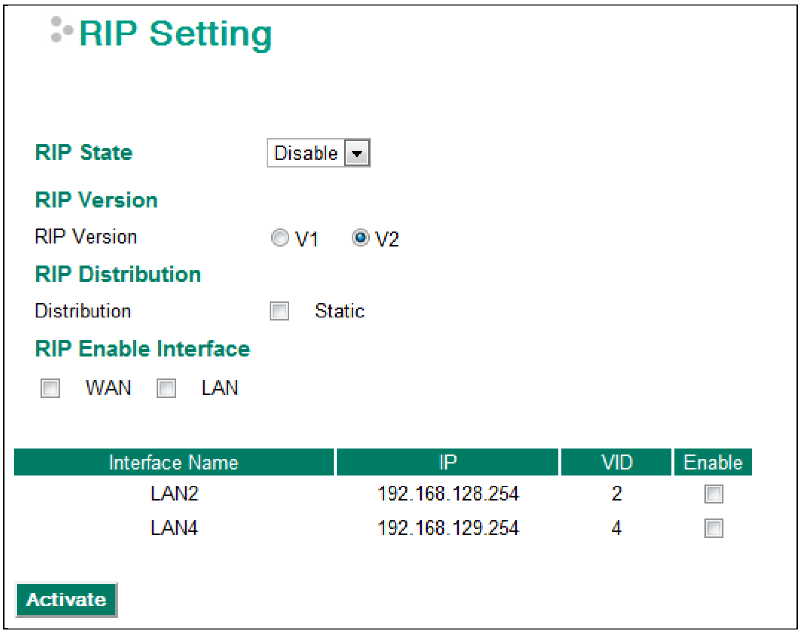
For modifying the content of a selected entry in the Static Routing Table.

NOTE The entries in the Static Routing Table will not be added to the ToughNet NAT Router's routing table until you click the Activate button.

RIP (Routing Information Protocol)

RIP is a distance-vector routing protocol that employs the hop count as a routing metric. RIP prevents routing from looping by implementing a limit on the number of hops allowed in a path from the source to a destination.

The RIP **Setting** page is used to set up the RIP parameters.



RIP Setting

RIP State: Disable

RIP Version

RIP Version ○ V1 ● V2

RIP Distribution

Distribution □ Static

RIP Enable Interface

□ WAN □ LAN

Interface Name	IP	VID	Enable
LAN2	192.168.128.254	2	□
LAN4	192.168.129.254	4	□

RIP State

Setting	Description	Factory Default
Enable/Disable	Enable or Disable RIP protocol	Disable

RIP Version

Setting	Description	Factory Default
V1/V2	Select RIP protocol version.	V2

RIP Distribution

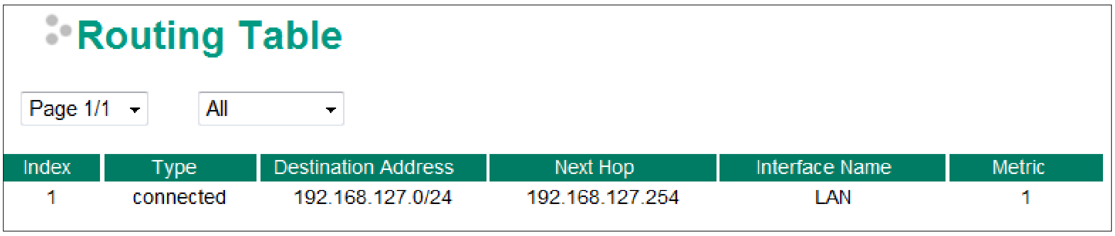
Setting	Description	Factory Default
Static	Check the checkbox to enable the Redistributed Static Route function. The entries that are set in a static route will be re-distributed if this option is enabled.	Unchecked

RIP Enable Interface

Setting	Description	Factory Default
WAN	Check the checkbox to enable RIP in the WAN interface.	Unchecked
LAN	Check the checkbox to enable RIP in the LAN interface.	

Routing Table

The **Routing Table** page shows all routing entries.



Routing Table

Page 1/1 ▾ All ▾

Index	Type	Destination Address	Next Hop	Interface Name	Metric
1	connected	192.168.127.0/24	192.168.127.254	LAN	1

All Routing Entry List

Setting	Description	Factory Default
All	Show all routing entries	N/A
Connected	Show connected routing entries	N/A
Static	Show Static routing entries	N/A
RIP	Show RIP routing entries	N/A
Others	Show others routing entries	N/A

5

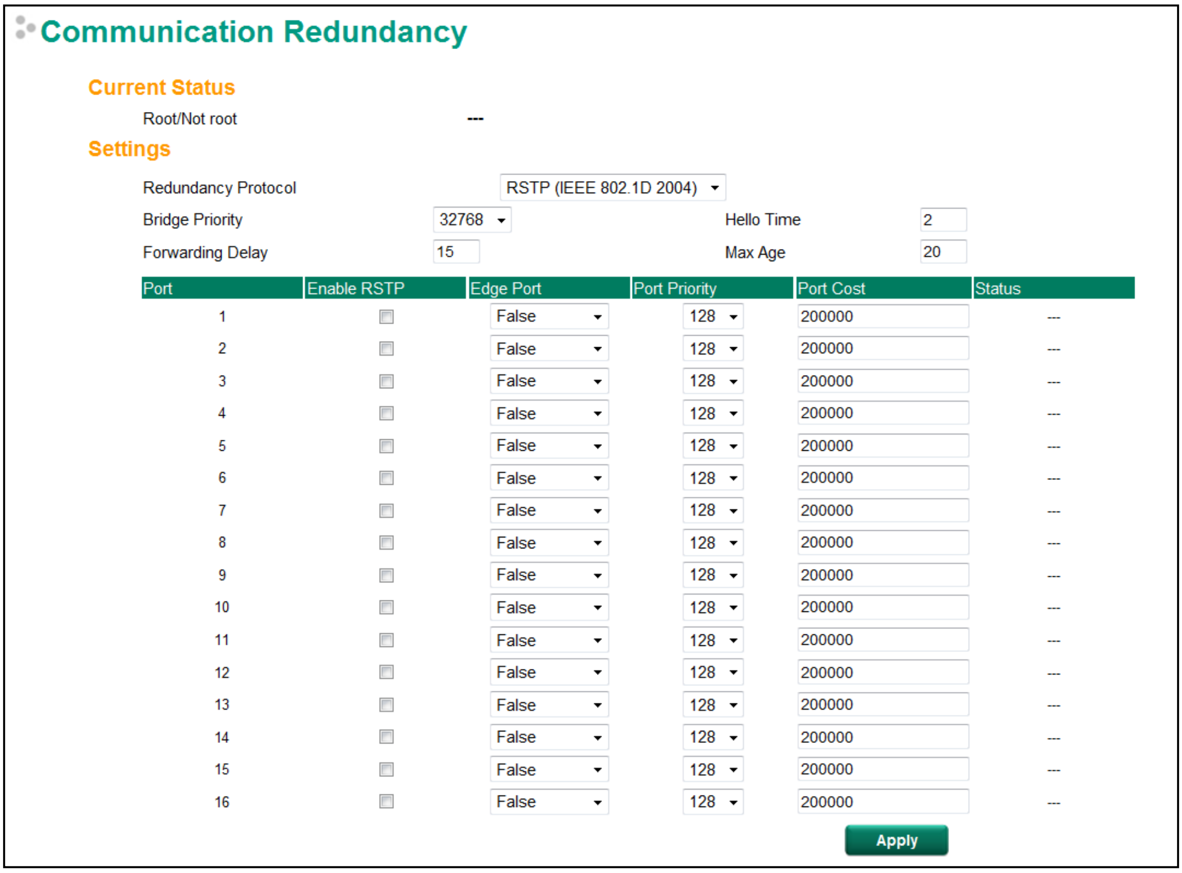
Network Redundancy

The following topics are covered in this chapter:

Layer 2 Redundant Protocols

Configuring RSTP

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



Communication Redundancy

Current Status

Root/Not root ---

Settings

Redundancy Protocol: RSTP (IEEE 802.1D 2004)

Bridge Priority: 32768

Hello Time: 2

Forwarding Delay: 15

Max Age: 20

Port	Enable RSTP	Edge Port	Port Priority	Port Cost	Status
1	□	False	128	200000	---
2	□	False	128	200000	---
3	□	False	128	200000	---
4	□	False	128	200000	---
5	□	False	128	200000	---
6	□	False	128	200000	---
7	□	False	128	200000	---
8	□	False	128	200000	---
9	□	False	128	200000	---
10	□	False	128	200000	---
11	□	False	128	200000	---
12	□	False	128	200000	---
13	□	False	128	200000	---
14	□	False	128	200000	---
15	□	False	128	200000	---
16	□	False	128	200000	---

At the top of this page, the user can check the **Current Status** of this function. For RSTP, you will see:

Now Active:

It shows which communication protocol is being used—Turbo Ring, RSTP, or neither.

Root/Not Root

This field only appears when RSTP mode is selected. The field indicates whether or not this switch is the Root of the Spanning Tree (the root is determined automatically).

At the bottom of this page, the user can configure the **Settings** of this function. For RSTP, you can configure:

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	None

Bridge priority

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

Forwarding Delay (sec.)

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

Hello time (sec.)

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

Max. Age (sec.)

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

Enable RSTP per Port

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

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

Setting	Description	Factory Default
Auto	1. If the port does not receive a BPDU within 3 seconds, the port will be in the forwarding state. 2. Once the port receives a BPDU, it will start the RSTP negotiation process.	Auto
Force Edge	The port is fixed as an edge port and will always be in the forwarding state	
False	The port is set as the normal RSTP port	

Port Priority

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

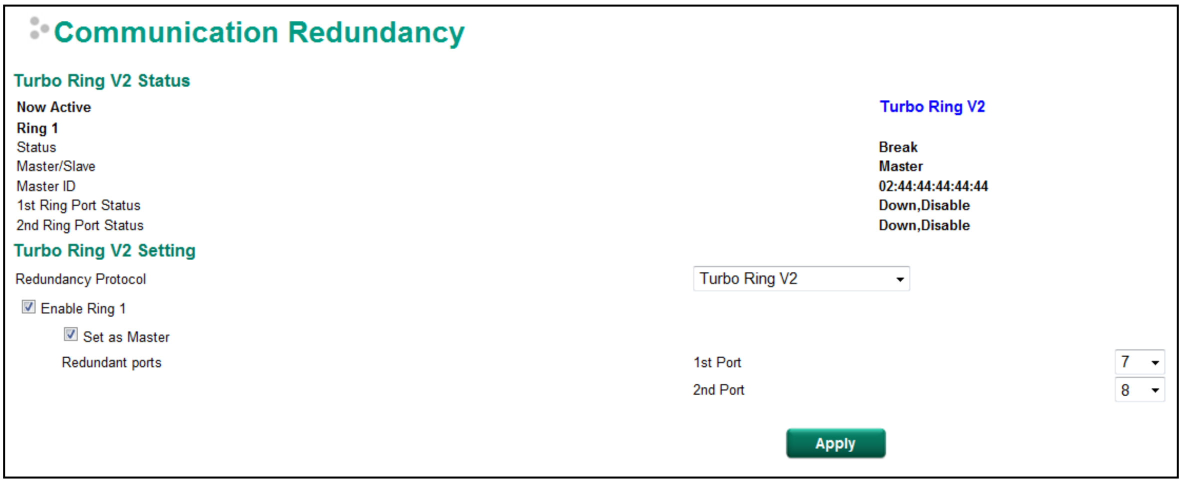
Port Cost

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

Port Status

Indicates the current Spanning Tree status of this port. **Forwarding** for normal transmission, or **Blocking** to block transmission.

Configuring Turbo Ring V2



Communication Redundancy

Turbo Ring V2 Status

Now Active	Turbo Ring V2
Ring 1	
Status	Break
Master/Slave	Master
Master ID	02:44:44:44:44:44
1st Ring Port Status	Down,Disable
2nd Ring Port Status	Down,Disable

Turbo Ring V2 Setting

Redundancy Protocol: Turbo Ring V2

☑ Enable Ring 1

☑ Set as Master

Redundant ports: 1st Port 7, 2nd Port 8

Explanation of "Current Status" Items

Now Active

It shows which communication protocol is in use: **Turbo Ring V2**, **RSTP**, or **none**.

Ring 1—Status

It shows **Healthy** if the ring is operating normally, and shows **Break** if the ring's backup link is active.

Ring 1—Master/Slave

It indicates whether or not this EDS is the Master of the Turbo Ring. (This field appears only when Turbo Ring or Turbo Ring V2 modes are selected.)

NOTE The user does not need to set the master to use Turbo Ring. If master is not set, the Turbo Ring protocol will assign master status to one of the TN units in the ring. The master is only used to determine which segment serves as the backup path.

Ring Port Status

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

Explanation of "Settings" Items

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	None
RSTP (IEEE 802.1W/ 802.1D-2004)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Enable Ring

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

Set as Master

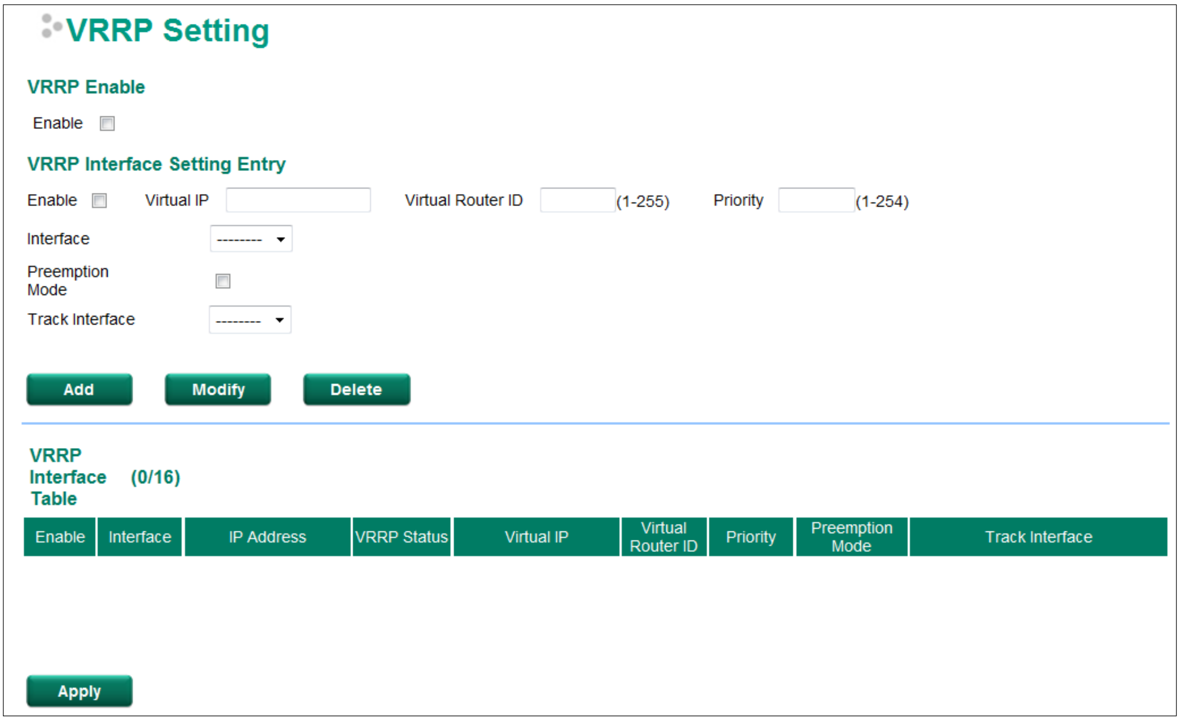
Setting	Description	Factory Default
Enabled	Select this device as Master	Not checked
Disabled	Do not select this device as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the device to be one of the redundant ports.	See the following table
2nd Port	Select any port of the device to be one of the redundant ports.	See the following table

Layer 3 Redundant Protocols

VRRP Settings



VRRP Setting

VRRP Enable

Enable □

VRRP Interface Setting Entry

Enable □ Virtual IP ____ Virtual Router ID ____ (1-255) Priority ____ (1-254)

Interface --------

Preemption Mode □

Track Interface --------

VRRP Interface Table (0/16)

Enable	Interface	IP Address	VRRP Status	Virtual IP	Virtual Router ID	Priority	Preemption Mode	Track Interface

Virtual Router Redundancy Protocol (VRRP) can solve the problem with static configuration. VRRP enables a group of routers to form a single virtual router with a virtual IP address. The LAN clients can then be configured with the virtual router’s virtual IP address as their default gateway. The virtual router is the combination of a group of routers, and is also known as a VRRP group.

Enable

Setting	Description	Factory Default
Enable	Enables VRRP	Disable

VRRP Interface Setting Entry

Setting	Description	Factory Default
Enable	Enables VRRP entry	Disabled
Virtual IP	L3 switches / routers in the same VRRP group must be set to the same virtual IP address as the VRRP ID. This virtual IP address must belong to the same address range as the real IP address of the interface.	0.0.0.0
Virtual Router ID	Virtual Router ID is used to assign a VRRP group. The L3 switches / routers, which operate as master / backup, should have the same ID. Moxa L3 switches / routers support one virtual router ID for each interface. IDs can range from 1 to 255.	0
Priority	Determines priority in a VRRP group. The priority value range is 1 to 255 and the 255 is the highest priority. If several L3 switches / routers have the same priority, the router with higher IP address has the higher priority. The usable range is "1 to 255".	100
Preemption Mode	Determines whether a backup L3 switch / router will take the authority of master or not.	Enabled
Track Interface	The Track Interface is used to track specific interface within the router that can change the status of the virtual router for a VRRP Group. For example, the WAN interface can be tracked and if the link is down, the other backup router will become the new master of the VRRP group.	Disable

6

Network Address Translation

The following topics are covered in this chapter:

- ❒ **Network Address Translation (NAT)**
  - ➢ NAT Concept
  - ➢ 1-to-1 NAT
  - ➢ Bidirectional 1-to-1 NAT
  - ➢ N-to-1 NAT
  - ➢ Port Forward

Network Address Translation (NAT)

NAT Concept

NAT (Network Address Translation) is a common security function for changing the IP address during Ethernet packet transmission. When the user wants to hide the internal IP address (LAN) from the external network (WAN), the NAT function will translate the internal IP address to a specific IP address, or an internal IP address range to one external IP address. The benefits of using NAT include:

- Uses the N-1 or Port forwarding Nat function to hide the Internal IP address of a critical network or device to increase the level of security of industrial network applications.
- Uses the same private IP address for different, but identical, groups of Ethernet devices. For example, 1-to-1 NAT makes it easy to duplicate or extend identical production lines.

NOTE The NAT function will check if incoming or outgoing packets match the policy. It starts by checking the packet with the first policy (Index=1); if the packet matches this policy, the ToughNet NAT Router will translate the address immediately and then start checking the next packet. If the packet does not match this policy, it will check with the next policy.

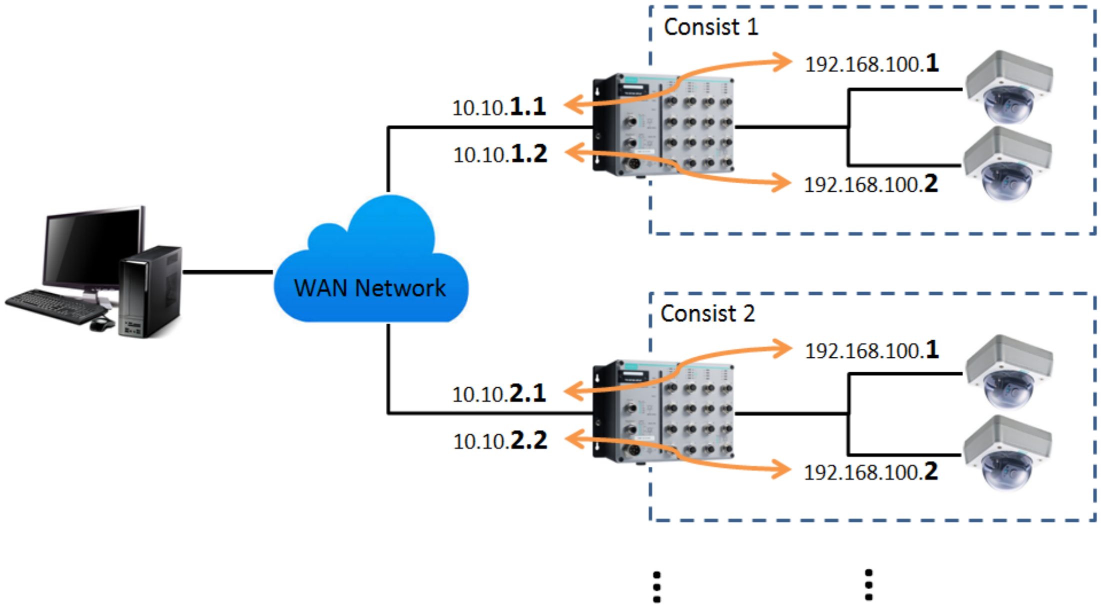
NOTE The maximum number of NAT policies for the ToughNet NAT Router is 128.

1-to-1 NAT

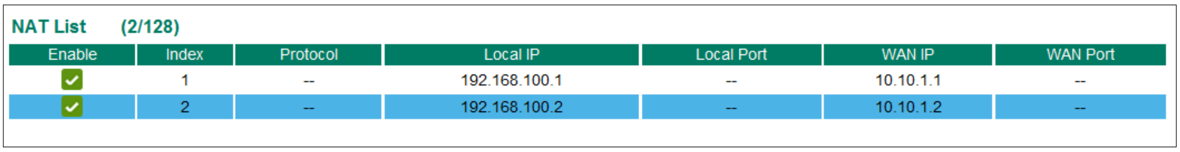
If the internal device and external device need to communicate with each other, choose 1-to-1 NAT, which offers bi-directional communication (N-to-1 and Port forwarding are both single-directional communication NAT functions).

1-to-1 NAT is usually used when you have a group of internal servers with private IP addresses that must connect to the external network. You can use 1-to-1 NAT to map the internal servers to public IP addresses. The IP address of the internal device will not change.

The figure below illustrates how a user could extend production lines, and use the same private IP addresses of internal devices in each production line. The internal private IP addresses of these devices will map to different public IP addresses. Configuring a group of devices for 1-to-1 NAT is easy and straightforward.



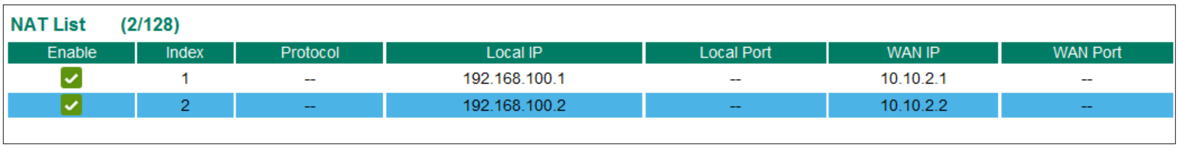
1-to-1 NAT Setting in TN-5916 for Consist 1



NAT List (2/128)

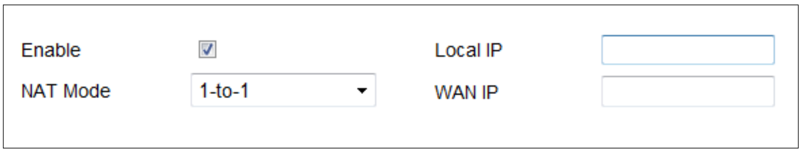
Enable	Index	Protocol	Local IP	Local Port	WAN IP	WAN Port
✓	1	--	192.168.100.1	--	10.10.1.1	--
✓	2	--	192.168.100.2	--	10.10.1.2	--

1-to-1 NAT Setting in TN-5916 for Consist 2



NAT List (2/128)

Enable	Index	Protocol	Local IP	Local Port	WAN IP	WAN Port
✓	1	--	192.168.100.1	--	10.10.2.1	--
✓	2	--	192.168.100.2	--	10.10.2.2	--



Enable	☑	Local IP	
NAT Mode	1-to-1	WAN IP	

Enable/Disable NAT policy

Setting	Description	Factory Default
Enable or Disable	Enable or disable the selected NAT policy	None

NAT Mode

Setting	Description	Factory Default
N-1 1-1 Port Forward	Select the NAT types	None

LAN IP (1-1 NAT type)

Setting	Description	Factory Default
IP Address	Select the Internal IP address in LAN network area	None

WAN IP (1-1 NAT type)

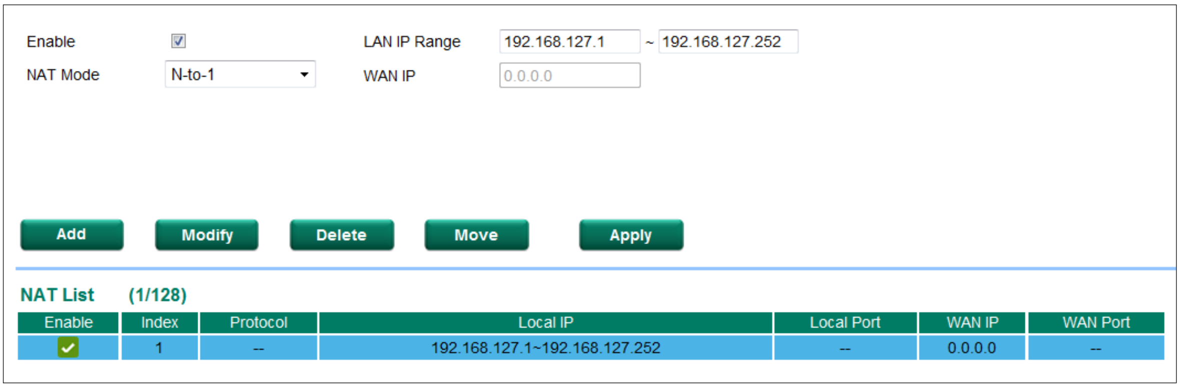
Setting	Description	Factory Default
IP Address	Select the external IP address in WAN network area	None

NOTE The ToughNet NAT Router can obtain an IP address via DHCP or PPPoE. However, if this dynamic IP address is the same as the WAN IP for 1-to-1 NAT, then the 1-to-1 NAT function will not work. For this reason, we recommend disabling the DHCP/PPPoE function when using the 1-to-1 NAT function.

N-to-1 NAT

If the user wants to hide the Internal IP address from users outside the LAN, the easiest way is to use the N-to-1 (or N-1) NAT function. The N-1 NAT function replaces the source IP Address with an external IP address, and adds a logical port number to identify the connection of this internal/external IP address. This function is also called "Network Address Port Translation" (NAPT) or "IP Masquerading."

The N-1 NAT function is a one-way connection from an internal secure area to an external non-secure area. The user can initialize the connection from the internal to the external network, but may not be able to initialize the connection from the external to the internal network.



Enable ☑ LAN IP Range 192.168.127.1 ~ 192.168.127.252

NAT Mode N-to-1 WAN IP 0.0.0.0

NAT List (1/128)

Enable	Index	Protocol	Local IP	Local Port	WAN IP	WAN Port
✓	1	--	192.168.127.1~192.168.127.252	--	0.0.0.0	--

Enable/Disable NAT Policy

Setting	Description	Factory Default
Enable or Disable	Enable or disable the selected NAT policy	Enabled

NAT Mode

Setting	Description	Factory Default
N-1 1-1 Port Forwarding	Select the NAT types	N-1

IP Range

Setting	Description	Factory Default
IP address	Select the Internal IP range for IP translation to WAN IP address	None

WAN IP (N-1 mode)

Setting	Description	Factory Default
IP address	The IP address of the user selected interface in this N-to-1 policy.	None

Add a NAT Rule

Checked the "Enable" checkbox and input the correspondent NAT parameters in the page, and then click "New/Insert" to add it into the NAT List Table. Finally, click "Activate" to activate the configuration.

Delete a NAT Rule

Select the item in the NAT List Table, then, click "Delete" to delete the item.

Modify a NAT Rule

Select the item in the NAT List Table. Modify the attributes and click "Modify" to change the configuration.

Activate NAT List Table

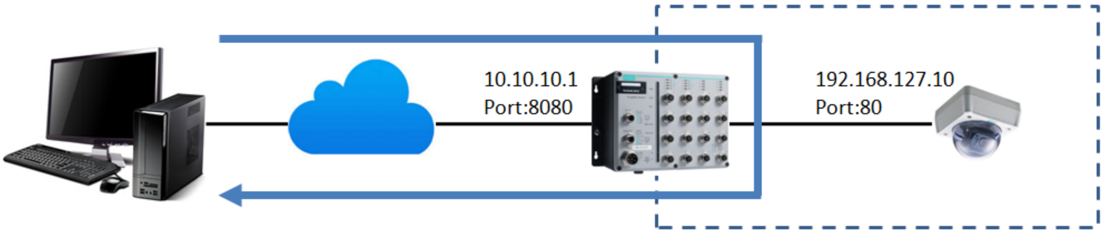
After adding/deleting/modifying any NAT Rules, be sure to Activate it.

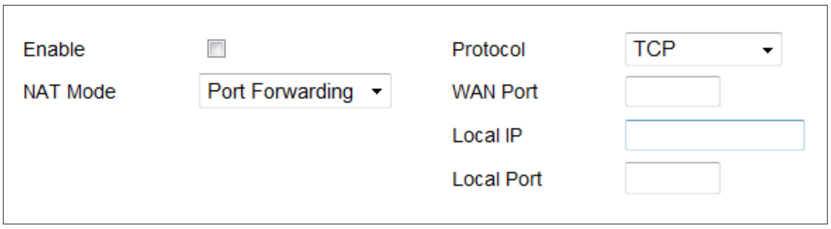
Port Forward

If the initial connection is from outside the LAN, but the user still wants to hide the Internal IP address, one way to do this is to use the Port Forwarding NAT function.

The user can specify the port number of an external IP address in the Port Forwarding policy list. For example, if the IP address of an IP camera on the internal network is 192.168.127.10 with port 80, the user can set up a port forwarding policy to let remote users connect to the internal IP camera from external IP address 10.10.10.10 through port 8080. The ToughNet NAT Router will transfer the packet to IP address 192.168.127.10 through port 80.

The Port Forwarding NAT function is one way of connecting from an external insecure area (WAN) to an internal secure area (LAN). The user can initiate the connection from the external network to the internal network, but will not able to initiate a connection from the internal network to the external network.





Enable	□	Protocol	TCP ▾
NAT Mode	Port Forwarding ▾	WAN Port	
		Local IP	
		Local Port	

Enable/Disable NAT policy

Setting	Description	Factory Default
Enable or Disable	Enable or disable the selected NAT policy	Enabled

NAT Mode

Setting	Description	Factory Default
N-1 1-1 Port Forward	Select the NAT types	N-1

Protocol (Port Forward mode)

Setting	Description	Factory Default
TCP UDP TCP & UDP	Select the Protocol for NAT Policy	TCP

WAN Port (Port Forward mode)

Setting	Description	Factory Default
1 to 65535	Select a specific WAN port number	None

LAN IP (Port Forward mode)

Setting	Description	Factory Default
IP Address	The translated IP address in the internal network	None

LAN Port (Port Forward mode)

Setting	Description	Factory Default
1 to 65535	The translated port number in the internal network	None

7

Diagnosis

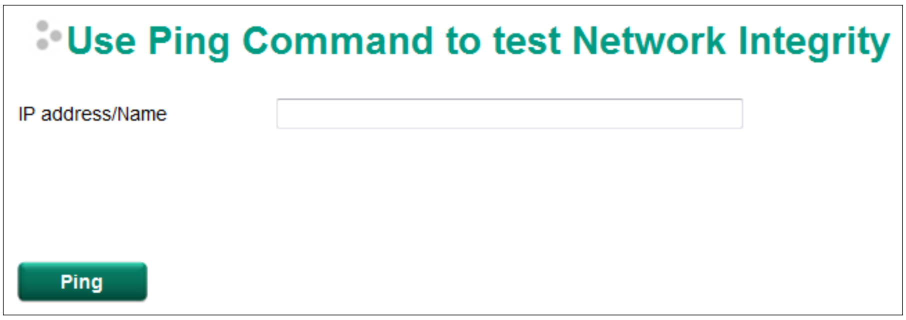
The ToughNet NAT Router provides **Ping** tools and **LLDP** for administrators to diagnose network systems.

The following topics are covered in this chapter:

❒ **Ping**

❒ **LLDP**

Ping



Use Ping Command to test Network Integrity

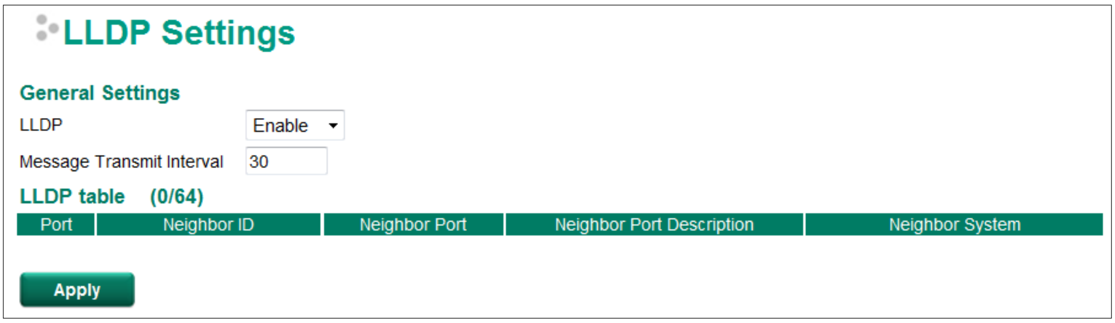
IP address/Name

The Ping function uses the ping command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the ToughNet NAT Router itself. In this way, the user can essentially control the ToughNet NAT Router and send ping commands out through its ports. Just type in the desired IP address and click **Ping**, the router will send out the ping command to test the integrity of the network.

LLDP

LLDP Function Overview

Defined by IEEE 802.11AB, Link Layer Discovery Protocol (LLDP) is an OSI Layer 2 Protocol that standardizes the methodology of self-identity advertisement. It allows each networking device, such as a Moxa managed switch/router, to periodically inform its neighbors about itself and its configuration. In this way, all devices will be aware of each other.



LLDP Settings

General Settings

LLDP: Enable

Message Transmit Interval: 30

LLDP table (0/64)

Port	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System

The router's web interface can be used to enable or disable LLDP, and to set the LLDP **Message Transmit Interval**. Users can view each switch's neighbor-list, which is reported by its network neighbors.

LLDP Setting

Enable LLDP

Setting	Description	Factory Default
Enable or Disable	Enable or disable LLDP function.	Enable

Message Transmit Interval

Setting	Description	Factory Default
5 to 32768 sec.	Set the transmit interval of LLDP messages. Unit is in seconds.	30 (sec.)

LLDT Table

Port: The port number that connects to the neighbor device.

Neighbor ID: A unique entity that identifies a neighbor device; this is typically the MAC address.

Neighbor Port: The port number of the neighbor device.

Neighbor Port Description: A textual description of the neighbor device’s interface.

Neighbor System: Hostname of the neighbor device.

A

MIB Groups

The ToughNet NAT Router comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold start trap, line up/down trap, and RFC 1213 MIB-II. The standard MIB groups that the ToughNet NAT Router series support are:

MIB II.1 – System Group

sysORTable

MIB II.2 – Interfaces Group

ifTable

MIB II.4 – IP Group

ipAddrTable
ipNetToMediaTable
IpGroup
IpBasicStatsGroup
IpStatsGroup

MIB II.5 – ICMP Group

IcmpGroup
IcmpInputStatus
IcmpOutputStats

MIB II.6 – TCP Group

tcpConnTable
TcpGroup
TcpStats

MIB II.7 – UDP Group

udpTable
UdpStats

MIB II.11 – SNMP Group

SnmpBasicGroup
SnmpInputStats
SnmpOutputStats

Public Traps

1. Cold Start
2. Link Up
3. Link Down
4. Authentication Failure

Private Traps:

1. Configuration Changed
2. Power On
3. Power Off

The ToughNet NAT Router also provides a MIB file, located in the file "Moxa-TN5916-MIB.my" on the ToughNet NAT Router Series utility CD-ROM for SNMP trap message interpretation.