TN-4900 Series User's Manual

Version 1.0, July 2021

www.moxa.com/product

TN-4900 Series User's Manual

Copyright Notice

Trademarks

Disclaimer

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

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

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

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

Technical Support Contact Information

www.moxa.com/support

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

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

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

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

1

Introduction

Welcome to the Moxa TN-4900 Series Industrial Secure Routers. These all-in-one Firewall/NAT/VPN secure routers are designed for connecting Ethernet-enabled devices with network IP security.

The following topics are covered in this chapter:

- **Overview**

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, an entirely new industry has sprung up to provide Ethernet products that comply with the requirements of demanding industrial applications.

Moxa's Industrial Secure Router series is a Gigabit speed, all-in-one Firewall/VPN/Router for Ethernet security applications in sensitive remote control and monitoring networks.

The Quick Automation Profile function of the Industrial Secure Router's firewall supports most common Fieldbus protocols, including EtherCAT, EtherNet/IP, FOUNDATION Fieldbus, Modbus/TCP, and PROFINET. Users can easily create a secure Ethernet Fieldbus network from a user-friendly web UI with a single click. In addition, wide temperature models are available that operate reliably in hazardous, -40 to 7-°C environments.

2

Getting Started

This chapter explains how to access the Industrial Secure 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 Industrial Secure Router to a PC's COM port, can be used if you do not know the Industrial Secure Router's IP address. The Telnet console and web browser connection methods can be used to access the Industrial Secure 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)**
- **Using Telnet to Access the Industrial Secure Router's Console**
- **Using a Web Browser to Configure the Industrial Secure Router**

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

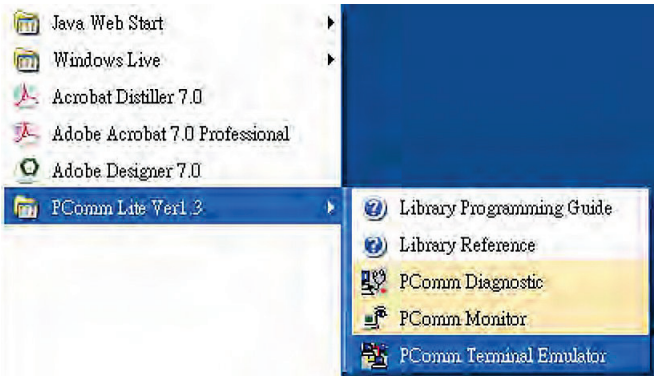
NOTE **Connection Caution!**
We strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your Industrial Secure Router

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

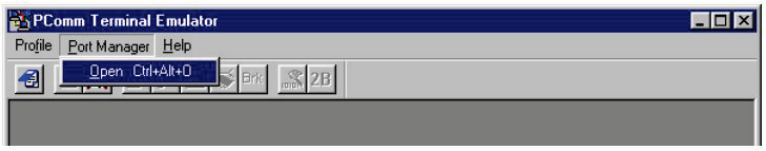
Before running PComm Terminal Emulator, use a USB-C-to-DB9-F (or USB-C-to-DB25-F) cable to connect the Industrial Secure Router's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

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

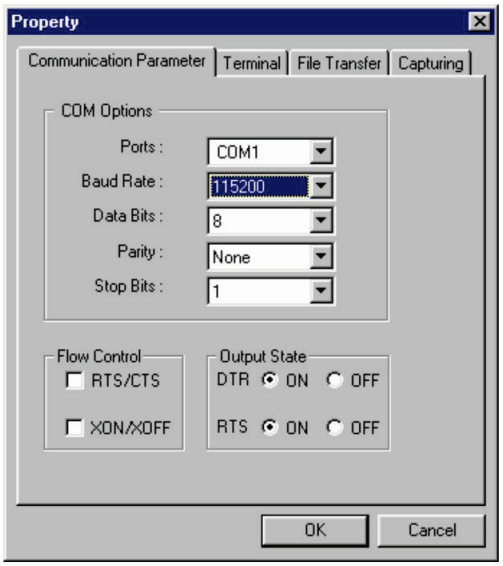
1. From the Windows desktop, click **Start** → **Programs** → **PCommLite1.3** → **Terminal Emulator**.



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.



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; enter the default password "moxa" into the Password field if a console password has not been set), and then press **Enter**.

```
login: admin
Password:

Please change default password in consideration of higher security level.

                    MOXA EDR-G9010-VPN-2MGSFP-T Series  V1.0   build 20120219.

--------------------------------------------------------------------------------
Firewall/VPN Router 00000#
```

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

```
Firewall/VPN Router 00000#
  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
  config-file           - configuration file
  no                    - Negate a command or set its defaults
  save                  - Save Running Configuration to Flash
  ping                  - Send Echo Messages
  tcpdump               - Dump traffic on a network
  clear                 - Clear Information
  show                  - Show System Information
  configure             - Enter Configuration Mode
  sslcertgen            - Generate SSL certificate.
  sshkeygen             - Generate SSH host key.
Firewall/VPN Router 00000#
```

The following table lists commands that can be used when the Industrial Secure 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
config-file	Configure file
no	Negate a command or set its defailts
save	Save Running Configuration to Flash
ping	Send Echo Messages
tcpdump	Dump traffic on a network
clear	Clear Information
show	Show System Information
configure	Enter Configuration Mode
sslcertgen	Generate a SSL certificate
sshkeygen	Generate a SSH host key

Using Telnet to Access the Industrial Secure Router's Console

You may use Telnet to access the Industrial Secure Router's console utility over a network. To access the TN router'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 Industrial Secure Router, you need to make sure that the PC host and the Industrial

Secure 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.

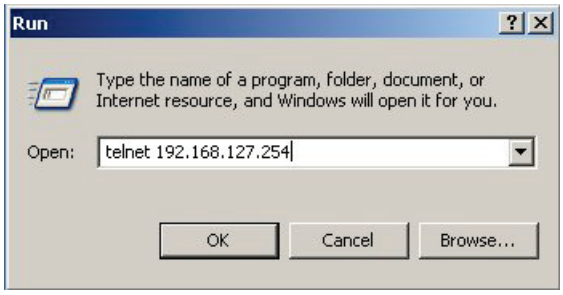
NOTE To use the Industrial Secure Router's management and monitoring functions from a PC host connected to the same LAN as the Industrial Secure Router, you must make sure that the PC host and the Industrial Secure Router are connected to the same logical subnet.

NOTE Before accessing the console utility via Telnet, first connect the Industrial Secure 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 Industrial Secure 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 Industrial Secure Router's IP address from the Windows Run window. (You may also issue the Telnet command from the MS-DOS prompt.)



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 Industrial Secure Router

The Industrial Secure 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 Industrial Secure Router's management and monitoring functions from a PC host connected to the same LAN as the Industrial Secure Router, you must make sure that the PC host and the Industrial Secure Router are connected to the same logical subnet.

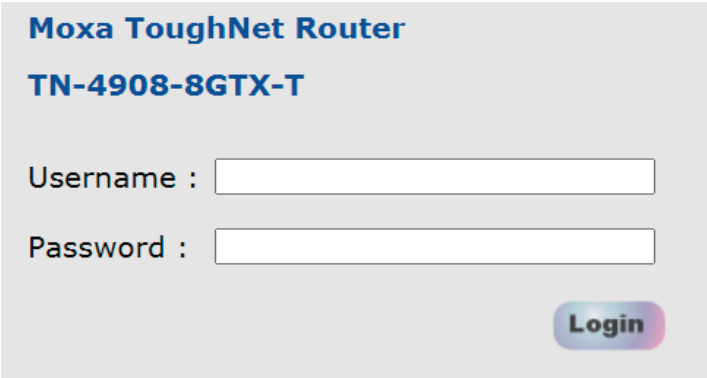
NOTE Before accessing the Industrial Secure Router's web browser, first connect the Industrial Secure Router's RJ45 Ethernet LAN ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can use either a straight-through or cross-over Ethernet cable.

NOTE The Industrial Secure Router's default LAN IP address is 192.168.127.254.

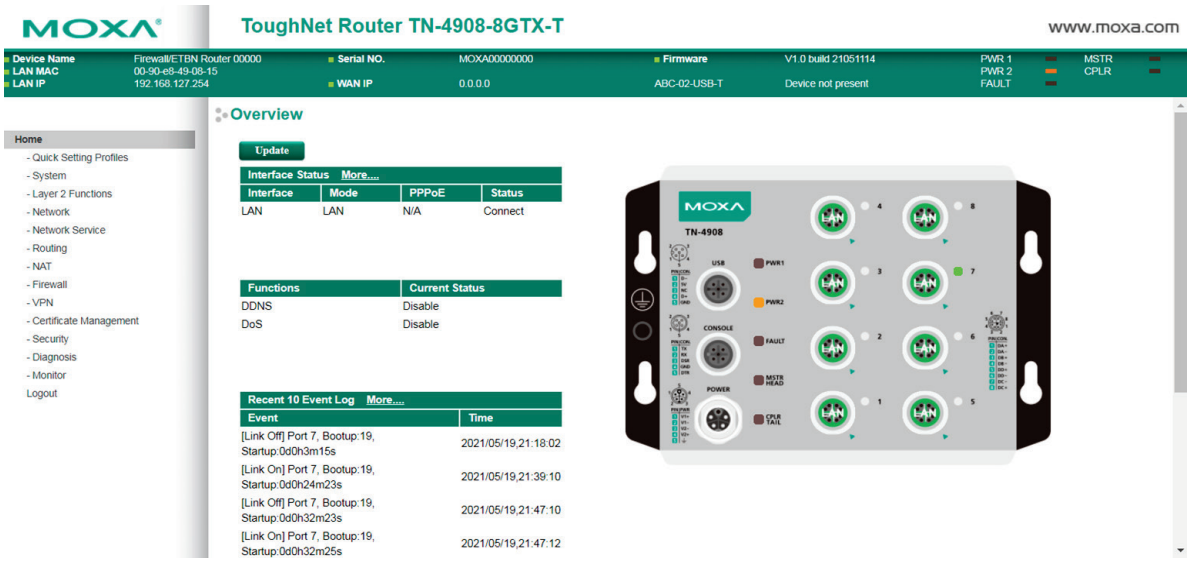
Perform the following steps to access the Industrial Secure Router's web browser interface.

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

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. Enter the default password "moxa" in the **Password** field if a password has not been set.



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.



3

Features and Functions

In this chapter, we explain how to access the Industrial Secure 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 Industrial Secure Router, since you can both monitor the Industrial Secure 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 Industrial Secure Router's configuration and monitoring functions.

The following topics are covered in this chapter:

- **Quick Setting Profile**
  - WAN Routing Quick Setting
  - Bridge Routing Quick Setting
- **System**
  - System Information
  - User Account
  - Password and Login Policy
  - Date and Time
  - Warning Notification
  - SettingCheck
  - System File Update—by Remote TFTP
  - System File Update—by Local Import/Export
  - System File Update –Import/Export the configurations stored on the ABC-02-USB
  - Restart
  - Reset to Factory Default
- **Port**
  - Port Settings
  - Port Status
  - 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 and Rate Control**
  - ToS/DSCP Mapping
- **MAC Address Table**
- **Interface**
  - WAN
  - LAN
  - Bridge Group Interface
- **Network Service**
  - DHCP Settings
  - SNMP Settings
  - Dynamic DNS
- **Security**
  - User Interface Management
  - Authentication Certificate
  - Trusted Access
  - RADIUS Server Settings
  - Port Access Control Setting
  - Security Notification Setting

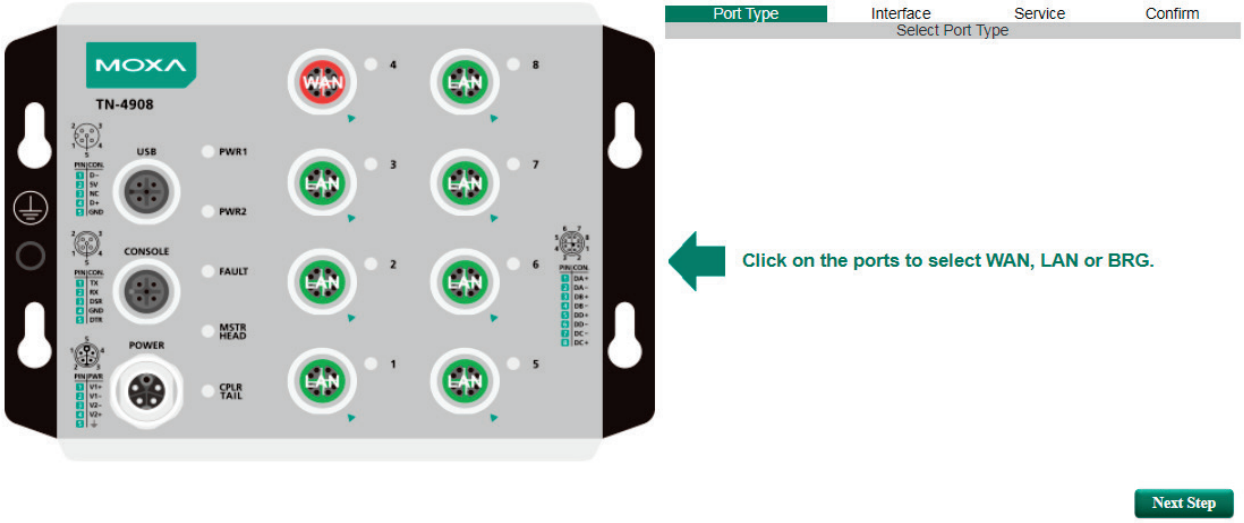
Quick Setting Profile

WAN Routing Quick Setting

The TN-4900 Series supports Interface Type Quick Settings, which creates a routing function between LAN ports and WAN ports defined by users. Follow the wizard's instructions to configuring the LAN and WAN ports.

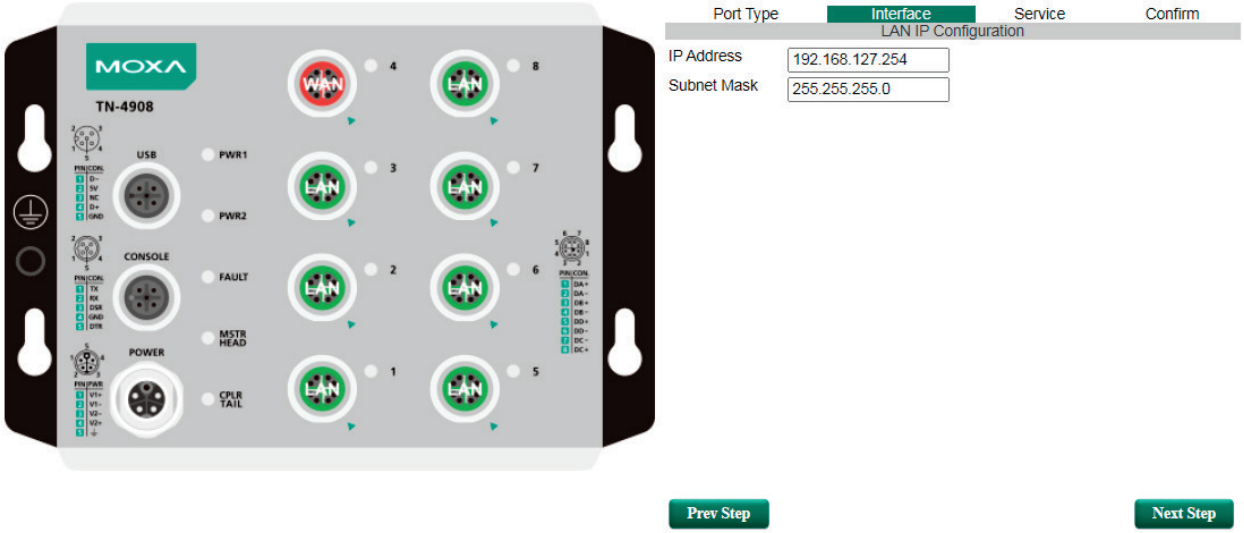
Step 1: Define the WAN ports and LAN ports

Click on the ports in the figure to define the WAN ports and LAN ports.



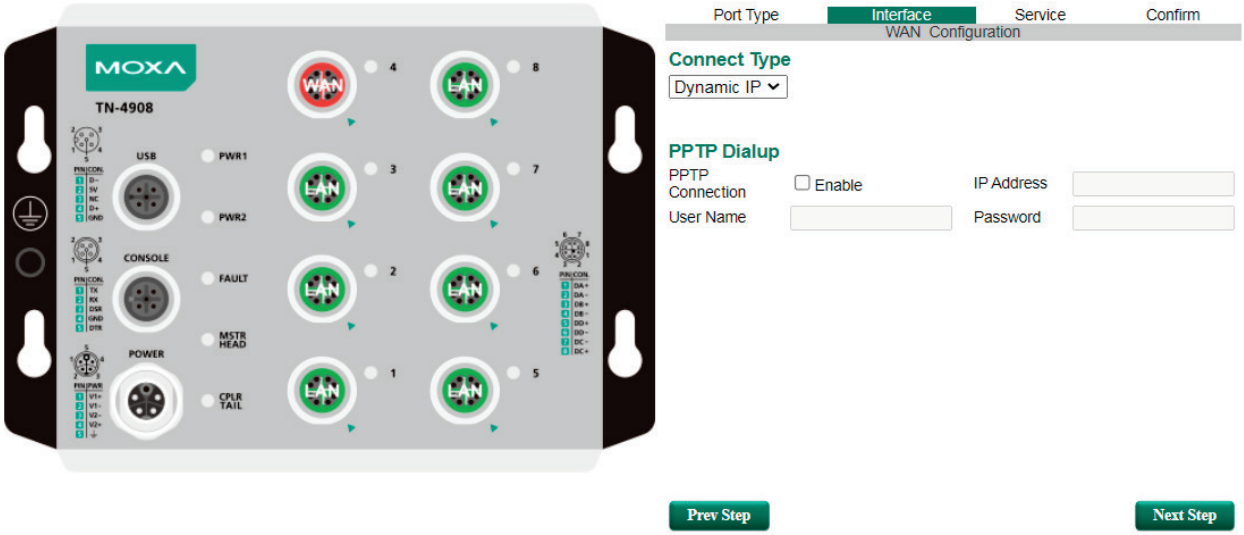
Step 2: Configure the LAN IP address and the subnet address of the LAN ports

Configure the LAN IP address to define the subnet of the LAN ports on the secure router. The default IP address on the LAN side is 192.168.127.254, and the default subnet address is 255.255.255.0.



Step 3: Configure the WAN port type

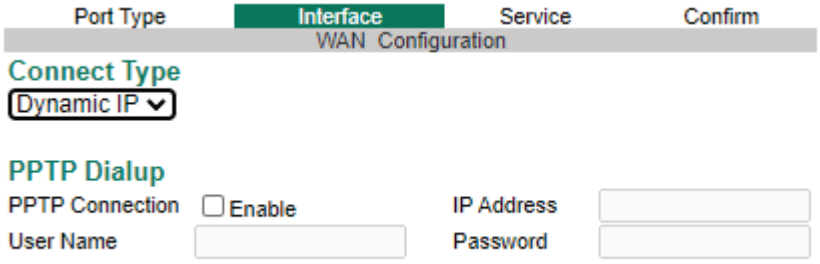
Configure the WAN port type to define how the secure router switch connects to the WAN.



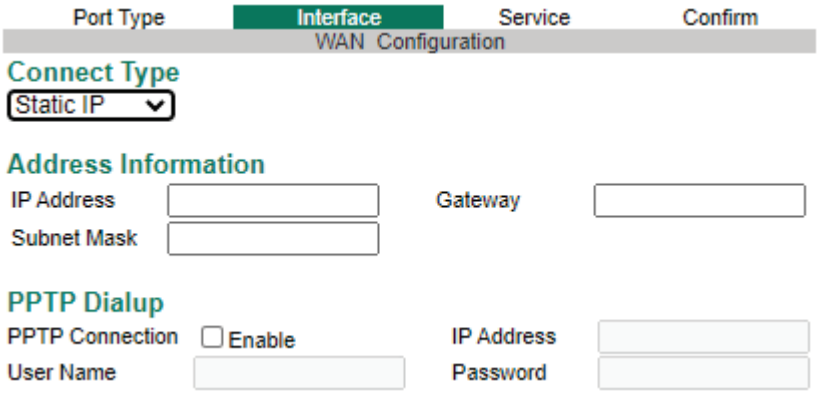
Connect Type

Setting	Description	Factory Default
Dynamic IP	Get the WAN IP address from a DHCP server or via a PPTP connection.	Dynamic IP
Static IP	Set a specific static WAN IP address or create a connection to a PPTP server with a specific IP address.	
PPPoE	Get the WAN IP address through PPPoE Dialup.	

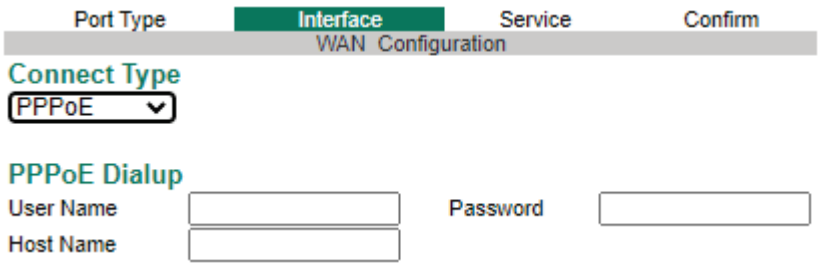
Dynamic IP



Static IP

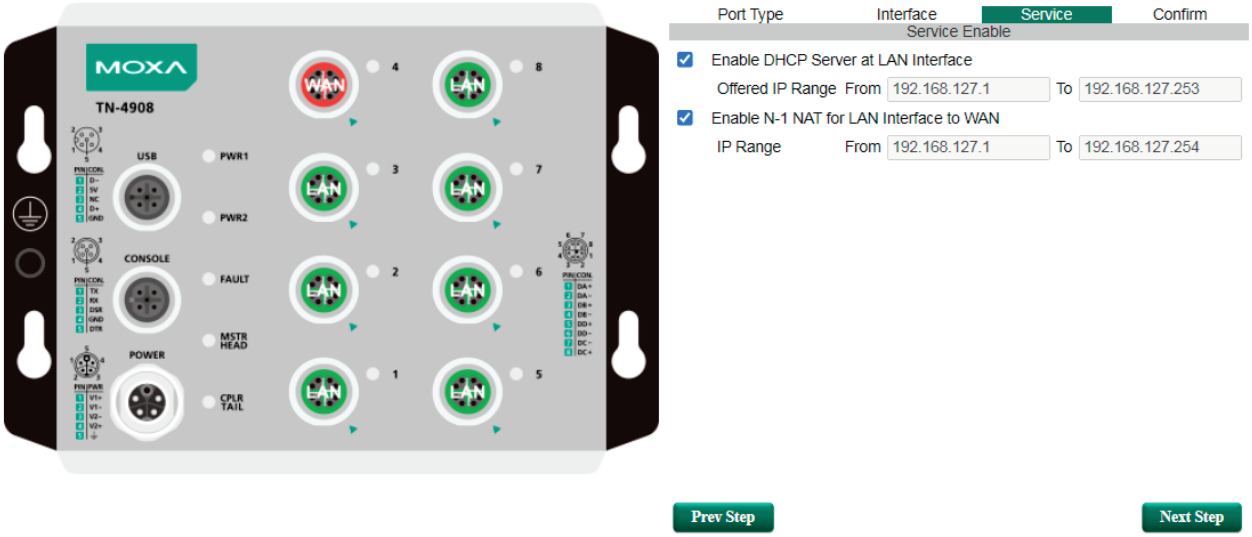


PPPoE



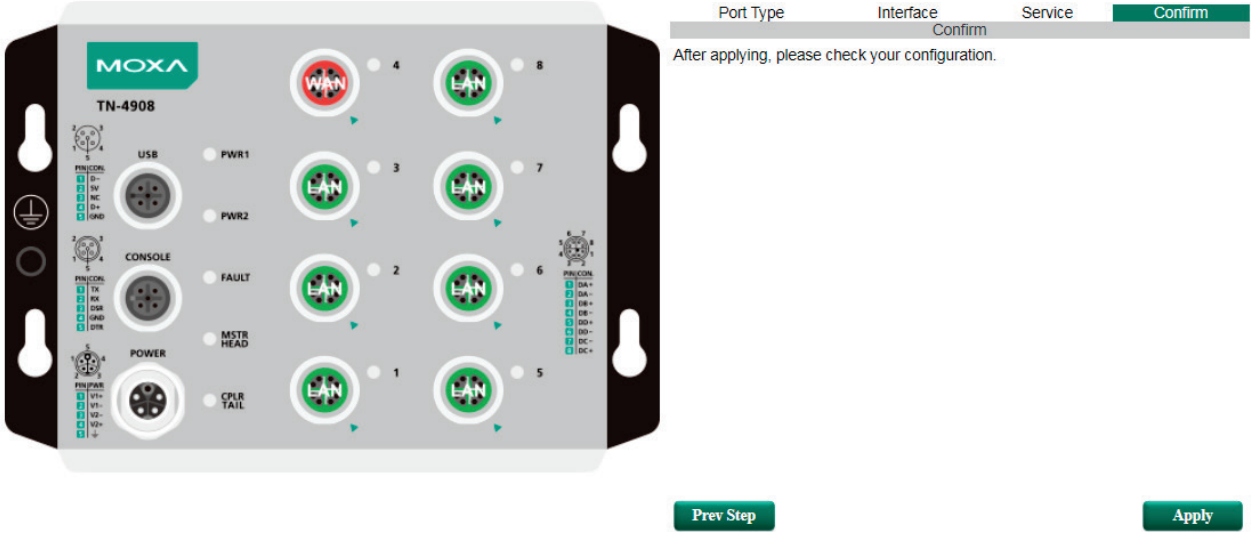
Step 4: Enable services

Check **Enable DHCP Server at LAN Interface** to enable the DHCP server for LAN devices. The default IP address range will be set automatically. To modify the IP range, go to the **DHCP Server** page. N-1 NAT will be also enabled by default.



Step 5: Apply the settings

Click the **Apply** button.



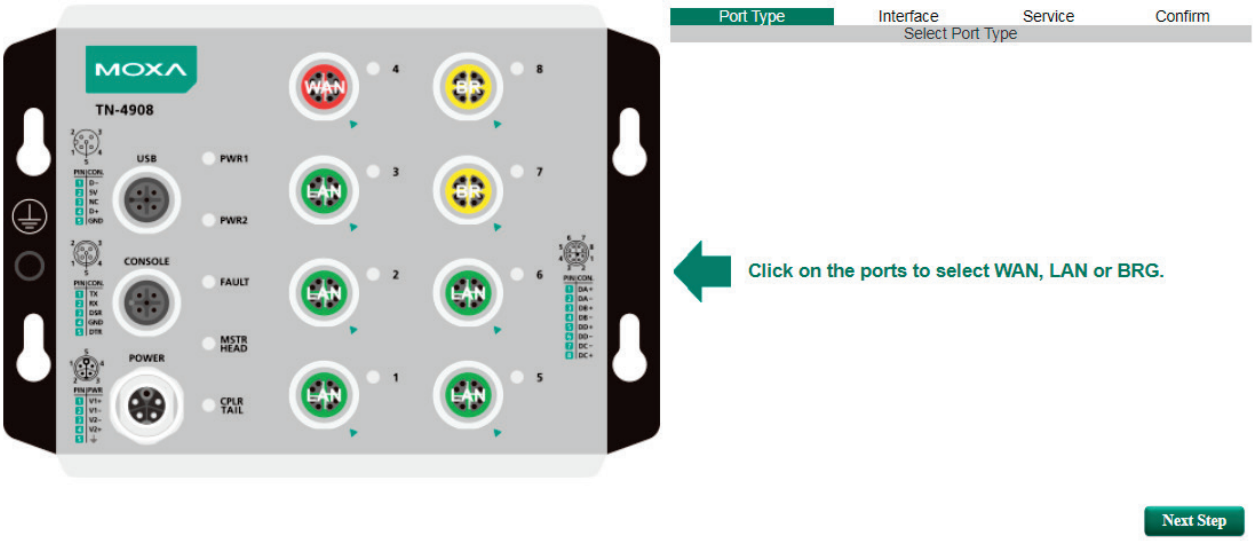
NOTE	Any existing configuration will be overwritten by the new settings when processing **Interface Type Quick Settings**.

Bridge Routing Quick Setting

The TN-4900 Series supports Interface Type Quick Settings, which creates a routing function between LAN ports and WAN ports defined by users. Follow the wizard's instructions to configuring the LAN and WAN ports.

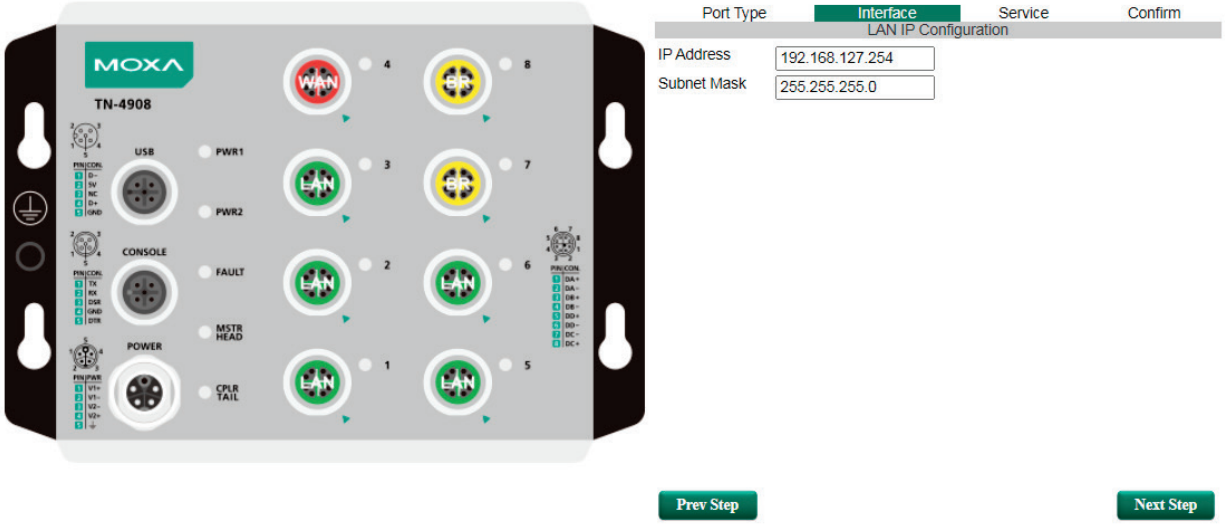
Step1: Define the WAN port and Bridge ports

Click on the ports in the figure to define the WAN ports and Bridge ports.



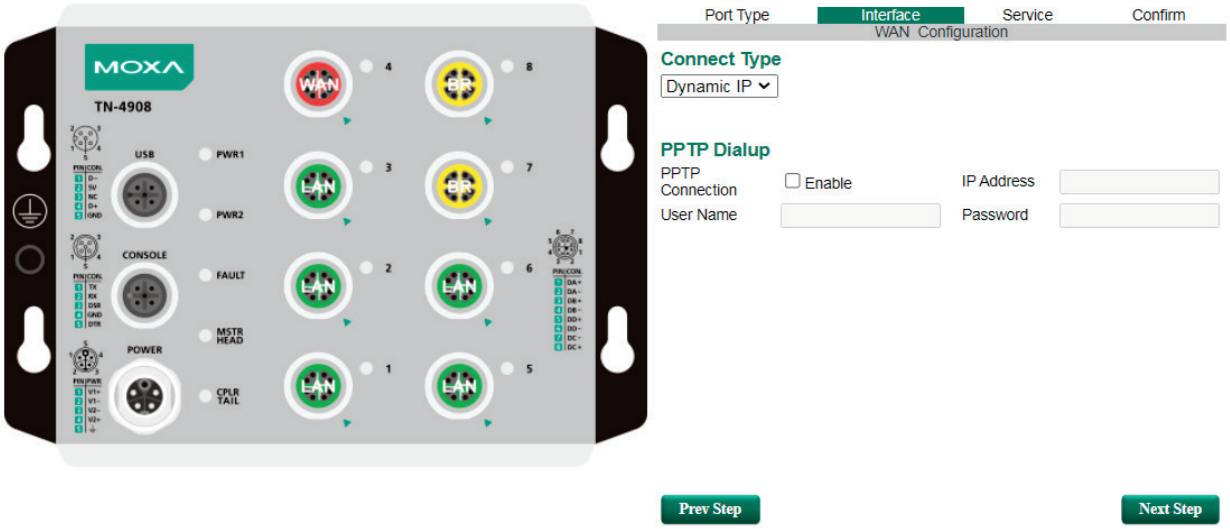
Step 2: Configure the Bridge LAN IP address and the subnet address of the Bridged ports

Configure the Bridge LAN Interface IP address to define the subnet of the Bridge LAN ports on the secure router. The default IP address on the Bridge LAN side is 192.168.126.254, and the default subnet address is 255.255.255.0.



Step 3: Configure the WAN port type

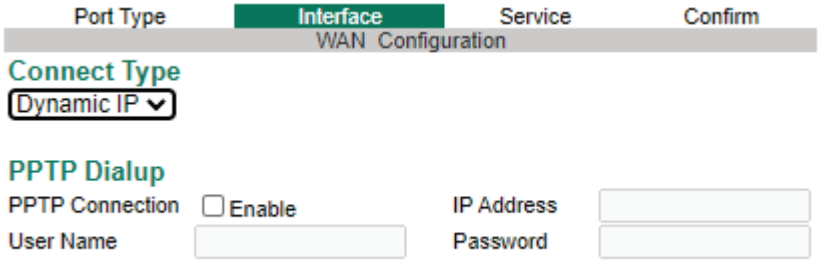
Configure the WAN port type to define how the secure router switch connects to the WAN.



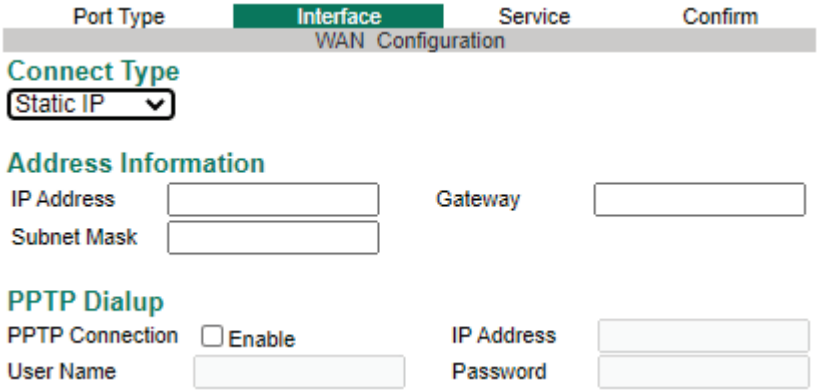
Connect Type

Setting	Description	Factory Default
Dynamic IP	Get the WAN IP address from a DHCP server or via a PPTP connection.	Dynamic IP
Static IP	Set a specific static WAN IP address or create a connection to a PPTP server with a specific IP address.	
PPPoE	Get the WAN IP address through PPPoE Dialup.	

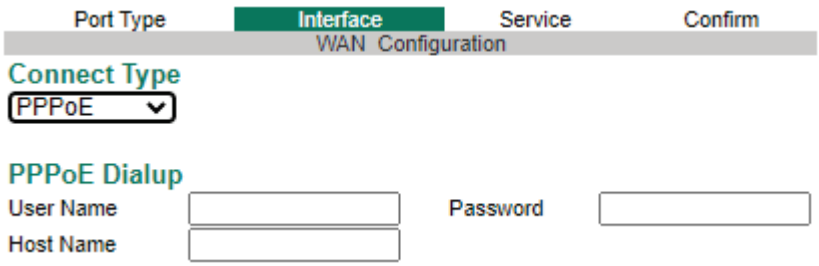
Dynamic IP



Static IP

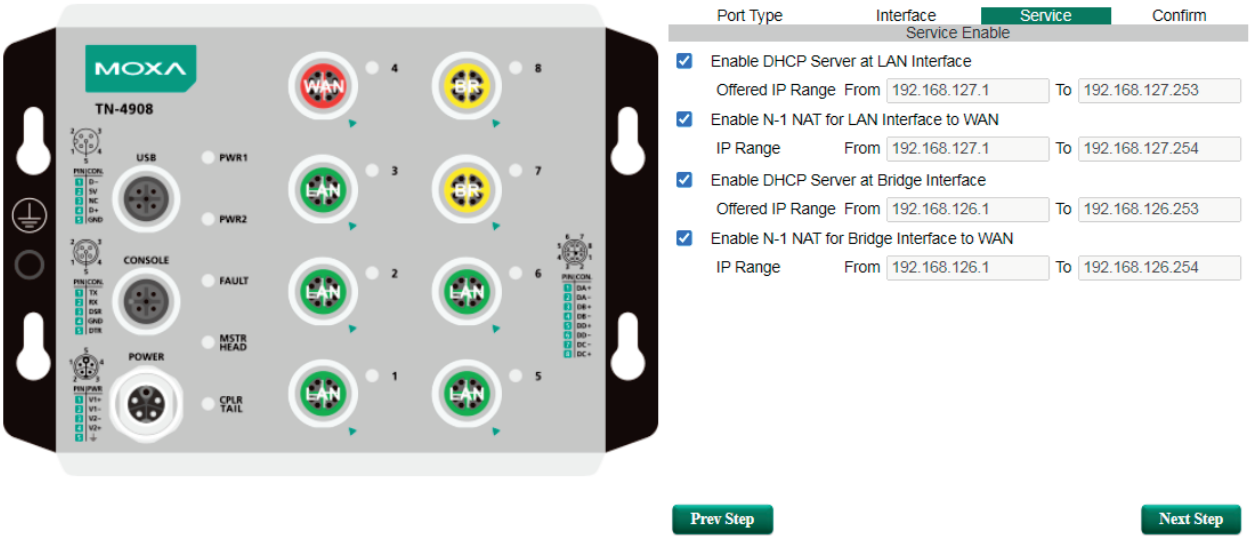


PPPoE



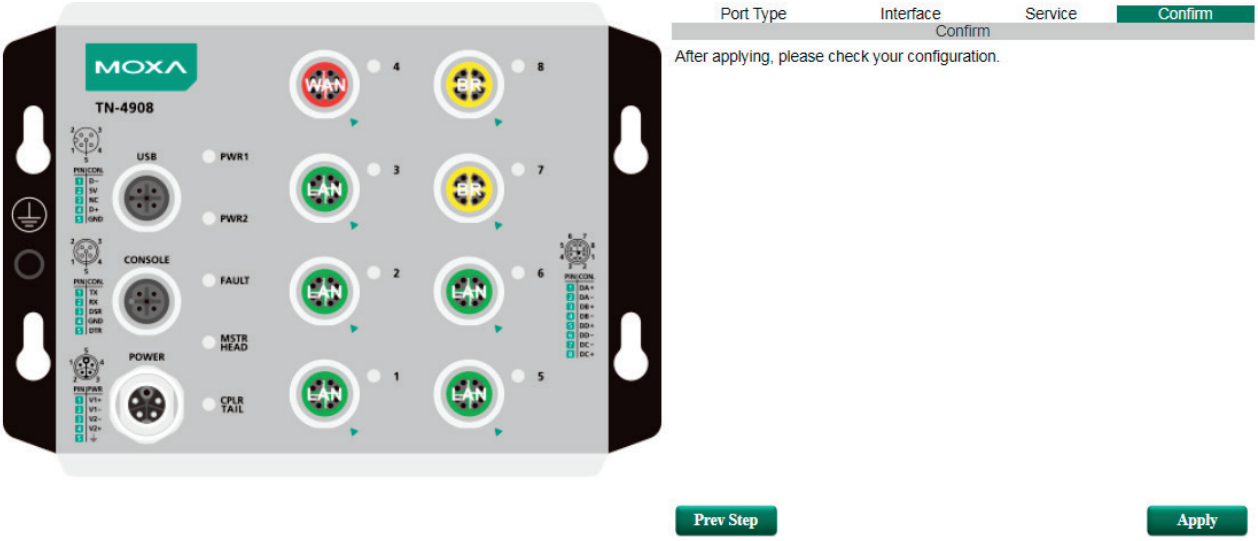
Step 4: Enable services

Check **Enable DHCP Server** to enable the DHCP server for LAN devices. The default IP address range will be set automatically. To modify the IP range, go to the **DHCP Server** page. N-1 NAT will be also enabled by default.



Step 5: Apply the settings

Click the **Apply** button.



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.

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/ETBN 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

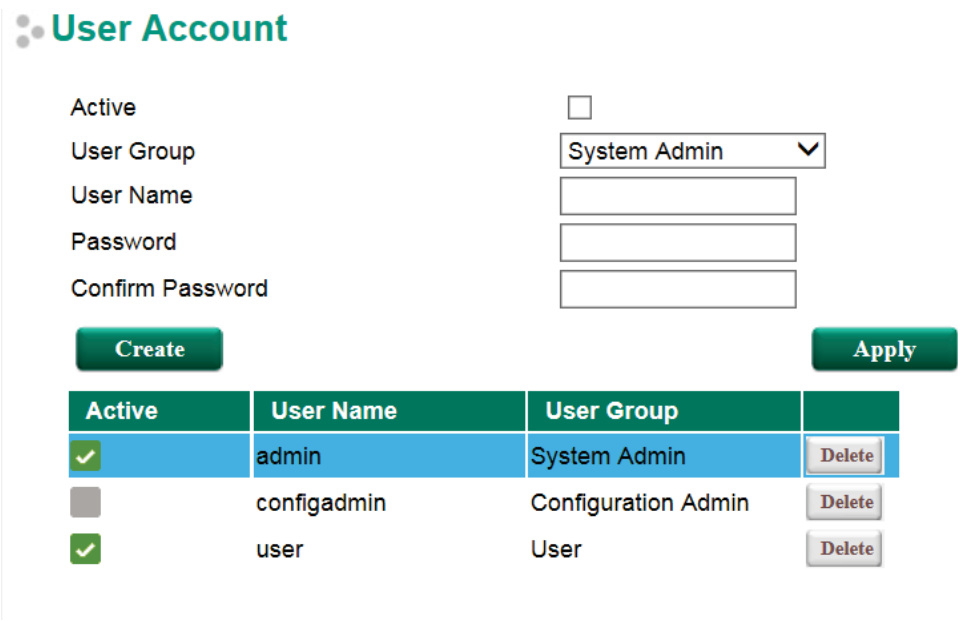
Setting	Description	Factory Default
Max. 30 characters	This option is useful for providing information about who is responsible for maintaining this unit and how to contact this person.	None

Users can define the message that will show up on the login page, and the message that will show up if login fails. The maximum length of each message is 512 bytes.

User Account

The Moxa industrial secure 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, we strongly suggest to change the default password after logging in for the time.
2. The user with 'admin' account name can't be deleted and is disabled by default.



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	

User Group

Setting	Description	Factory Default
System Admin	The account has read/write access of all configuration parameters.	System Admin
Configuration Admin	The account has read/write access of all configuration parameters except create, delete, and modify account.	
User	The account can only read configurations but cannot make any modifications.	

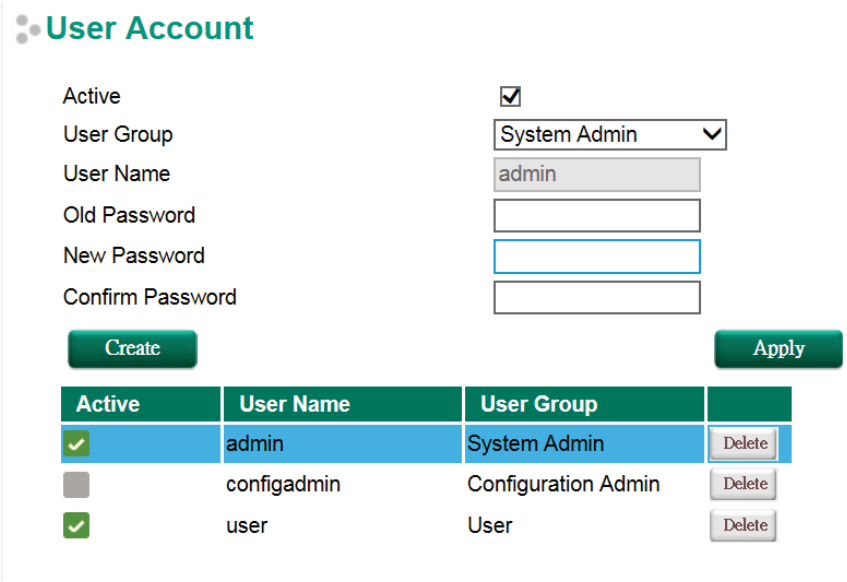
Create New Account

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

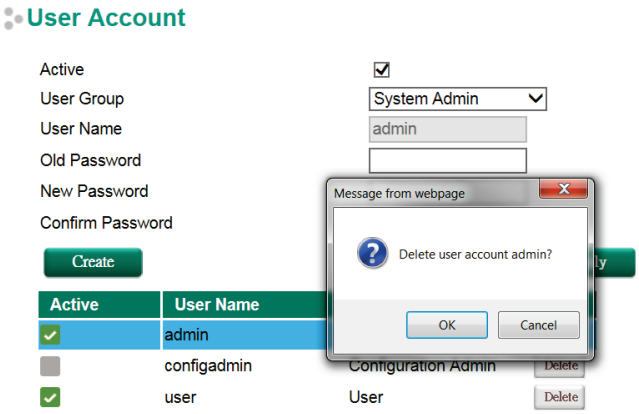
Modify Existing Account

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



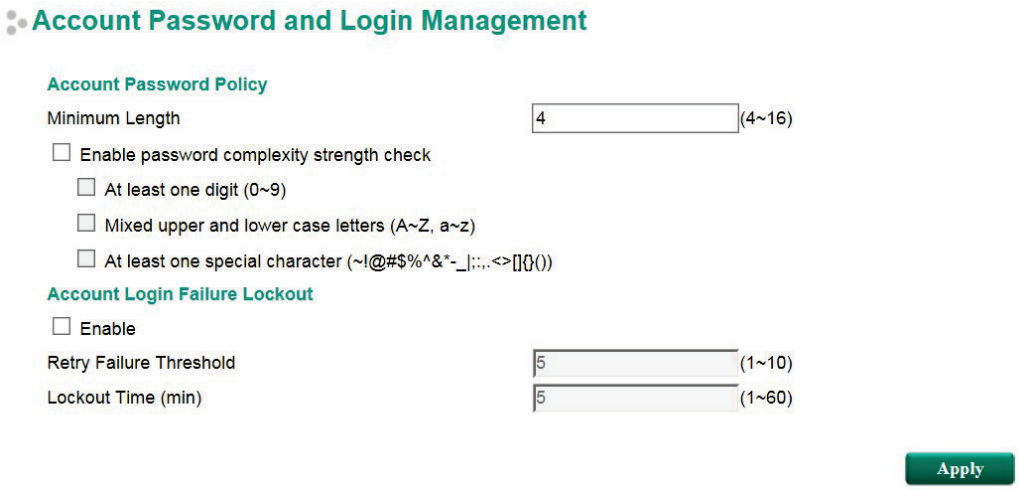
Delete Existing Account

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



Password and Login Policy

With password and login policy function enabled, administrators can set up complex login passwords to improve the security of the system. At the same time, administrators can set up an account login failure lockout time to avoid unauthorized users gaining access.



Account Password Policy

Setting	Description	Factory Default
Enable/Disable	Enable password complexity strength check	Disable

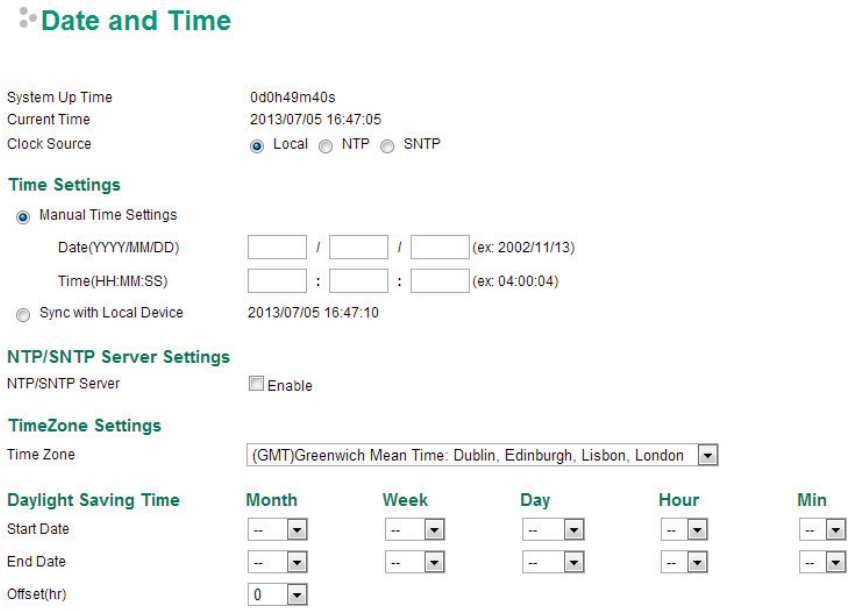
Account Login Failure Lockout

Setting	Description	Factory Default
Enable/Disable	Enable Account Login Failure Lockout	Disable

Date and Time

The Moxa industrial secure 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 industrial secure 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.



System Up Time

Indicates how long the Moxa industrial secure 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.

NTP Client Setting

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

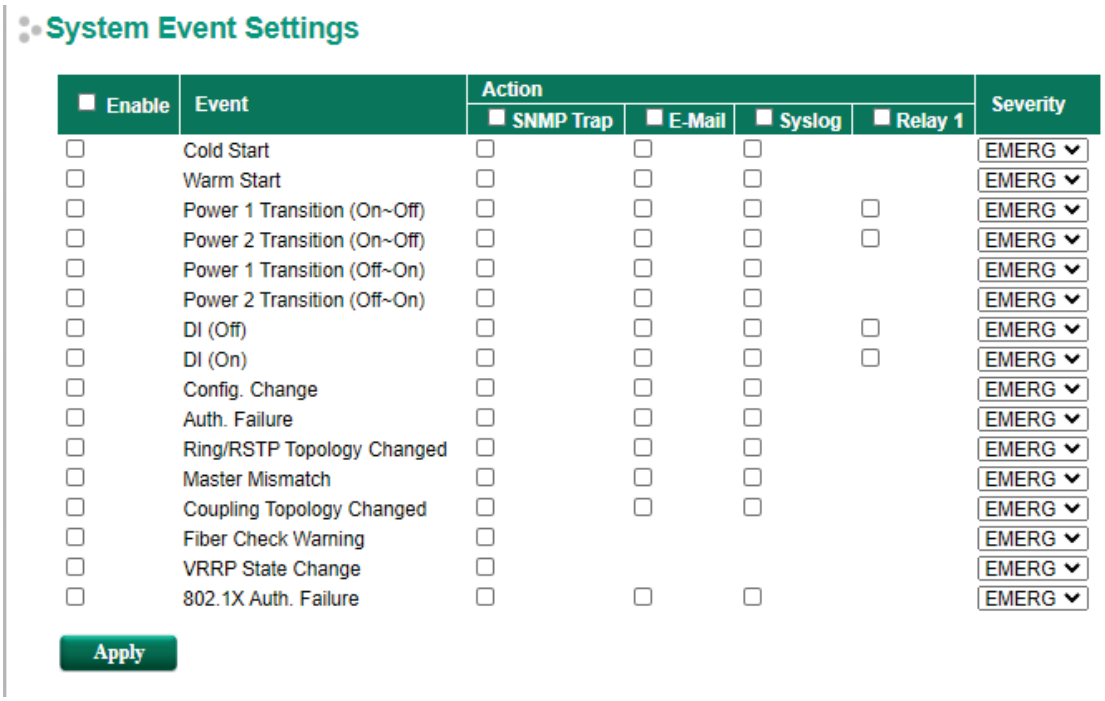
Setting	Description	Factory Default
Enable/Disable	Enables SNTP/NTP server functionality for clients	Disabled

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 industrial secure 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 industrial secure 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.



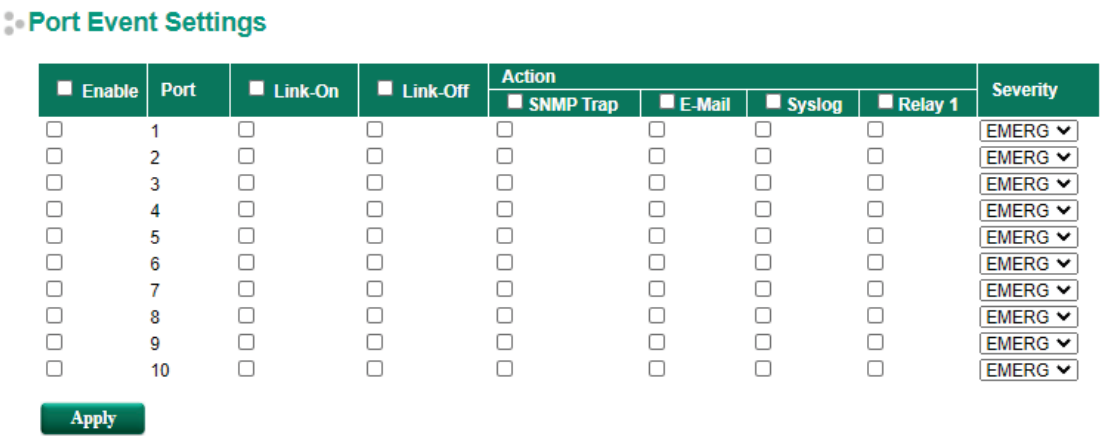
System Events	Description
Cold Start	Power is cut off and then reconnected.
Warm Start	Moxa industrial secure router is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	Moxa industrial secure router is powered down.
Power Transition (Off→On)	Moxa industrial secure router is powered up.
DI (Off)	Digital input state is "0"
DI (On)	Digital input state is "1"
Configuration Change	Any configuration item has been changed.
Authentication Failure	An incorrect password was entered.
Ring/RSTP Topology Changed	Ring/RSTP Topology has been changed.
Master Mismatch	Turbo Ring Master mismatch occurred
VRRP State Change	The VRRP state has been changed.
802.1X Auth. Failure	An 802.1X authentication failure occurred.

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

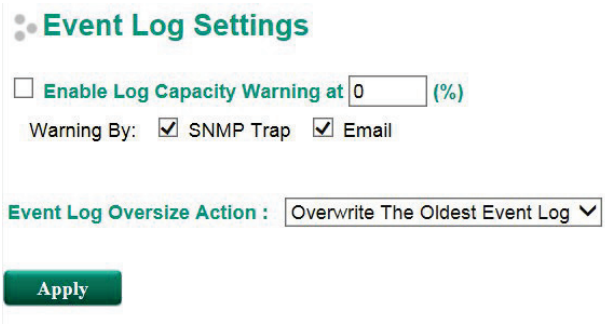
Port Events are related to the activity of a specific port.



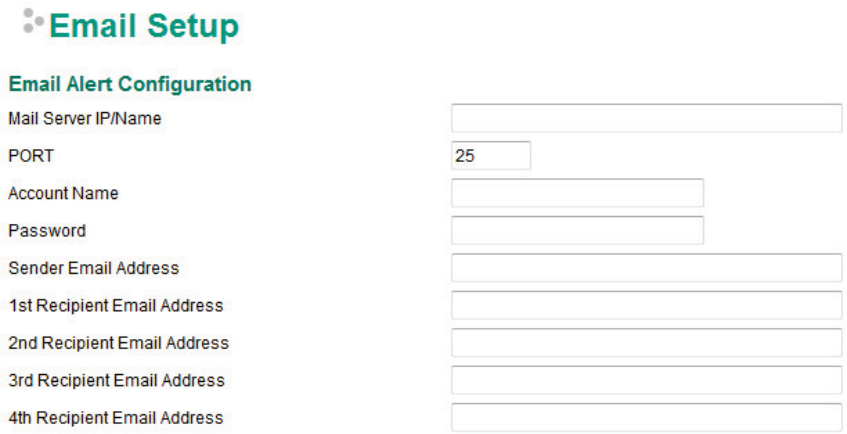
Port Events	Warning e-mail is sent when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).

Event Log Setting

In event log setting, administrators can set up a warning for when the capacity of the system log is not enough and how to deal with this. By utilizing this function, the administrator will not miss any system events.



Email Settings



Mail Server IP/Name

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

Port

Setting	Description	Factory Default
TCP port number	The TCP port of your email server.	25

Account Name

Setting	Description	Factory Default
Max. 45 characters	Your email account.	None

Password

Setting	Description	Factory Default
Password	The email account password.	None

Sender Email Address

Setting	Description	Factory Default
Max. 30 characters	The sender email address.	None

Email Address

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

Send Test Email

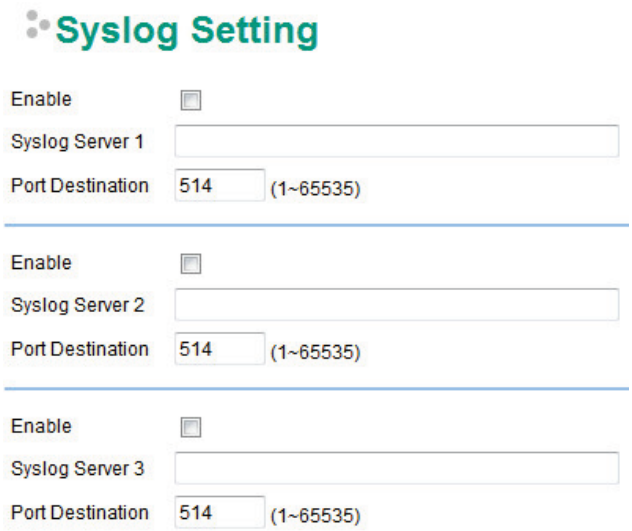
After you complete the email settings, you should first click **Apply** to activate those settings, and then press the **Test** button to verify that the settings are correct.

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.



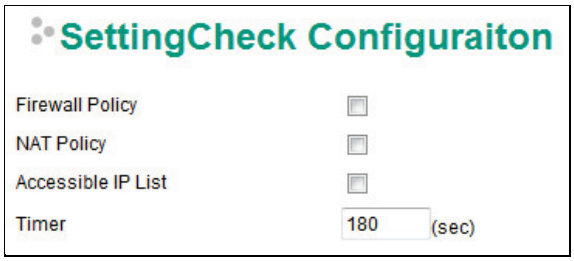
Syslog Server 1/2/3

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 industrial secure 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

SettingCheck



SettingCheck is a safety function for industrial users using a secure router. It provides a double confirmation mechanism for when a remote user changes the security policies, such as **Firewall filter**, **NAT**, and **Accessible IP list**. When a remote user changes these security polices, SettingCheck provides a means of blocking the connection from the remote user to the Firewall/VPN device. The only way to correct a wrong setting is to get help from the local operator, or go to the local site and connect to the device through the console port, which could take quite a bit of time and money. Enabling the SettingCheck function will execute these new policy changes temporarily until doubly confirmed by the user. If the user does not click the confirm button, the Industrial Secure Router will revert to the previous setting.

Firewall Policy

Enables or Disables the SettingCheck function when the Firewall policies change.

NAT Policy

Enables or Disables the SettingCheck function when the NAT policies change.

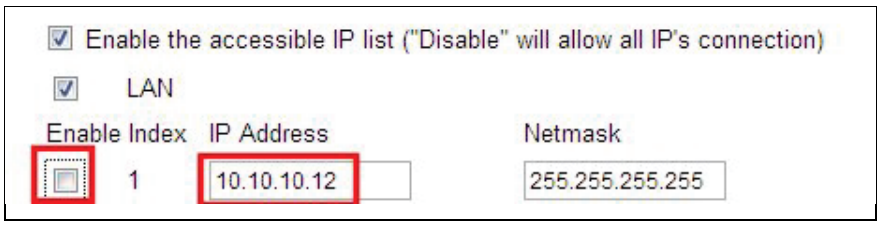
Accessible IP List

Enables or Disables the SettingCheck function when the Accessible IP List changes.

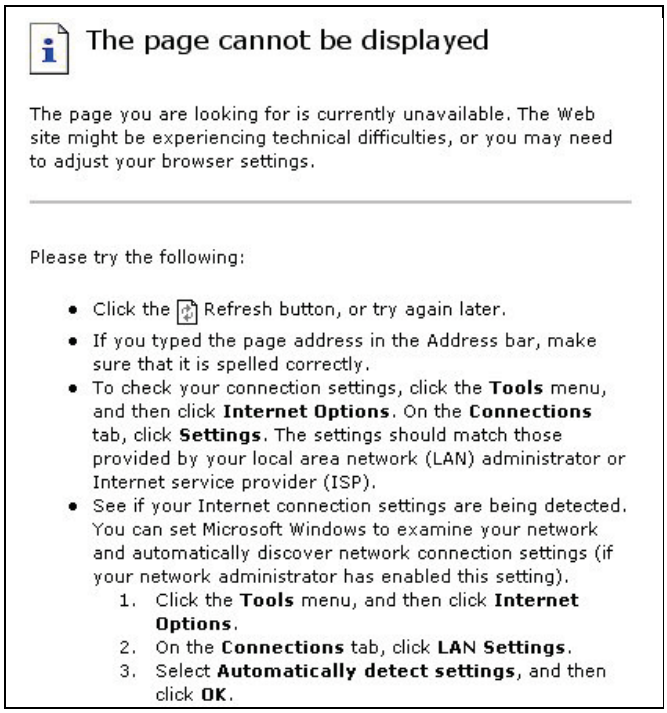
Timer

Setting	Description	Factory Default
10 to 3600 sec.	The timer waits this amount of time to double confirm when the user changes the policies	180 (sec.)

For example, if the remote user (IP: 10.10.10.10) connects to the Industrial Secure Router and changes the accessible IP address to 10.10.10.12, or deselects the Enable checkbox accidently after the remote user clicks the Activate button, connection to the Industrial Secure Router will be lost because the IP address is not in the Industrial Secure Router's Accessible IP list.



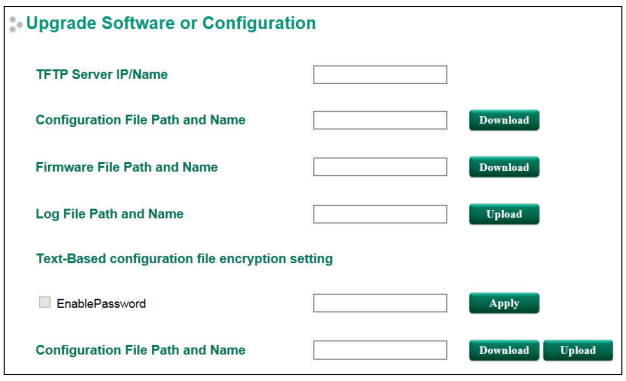
If the user enables the SettingCheck function with the Accessible IP list and the confirmer Timer is set to 15 seconds, then when the user clicks the Activate button on the accessible IP list page, the Industrial Secure Router will execute the configuration change and the web browser will try to jump to the SettingCheck Confirmed page automatically. Because the new IP list does not include the Remote user's IP address, the remote user cannot connect to the SettingCheck Confirmed page. After 15 seconds, the Industrial Secure Router will roll back to the original Accessible IP List setting, allowing the remote user to reconnect to the Industrial Secure Router and check what's wrong with the previous setting.



If the new configuration does not block the connection from the remote user to the Industrial Secure Router, the user will see the SettingCheck Confirmed page, shown in the following figure. Click **Confirm** to save the configuration updates.

System File Update—by Remote TFTP

The Industrial Secure Router supports saving your configuration file to a remote TFTP server or local host to allow other Industrial Secure 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 Industrial Secure Router.



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 Industrial Secure 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 Industrial Secure Router's firmware file.	None

Log File Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and filename of the Industrial Secure 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.

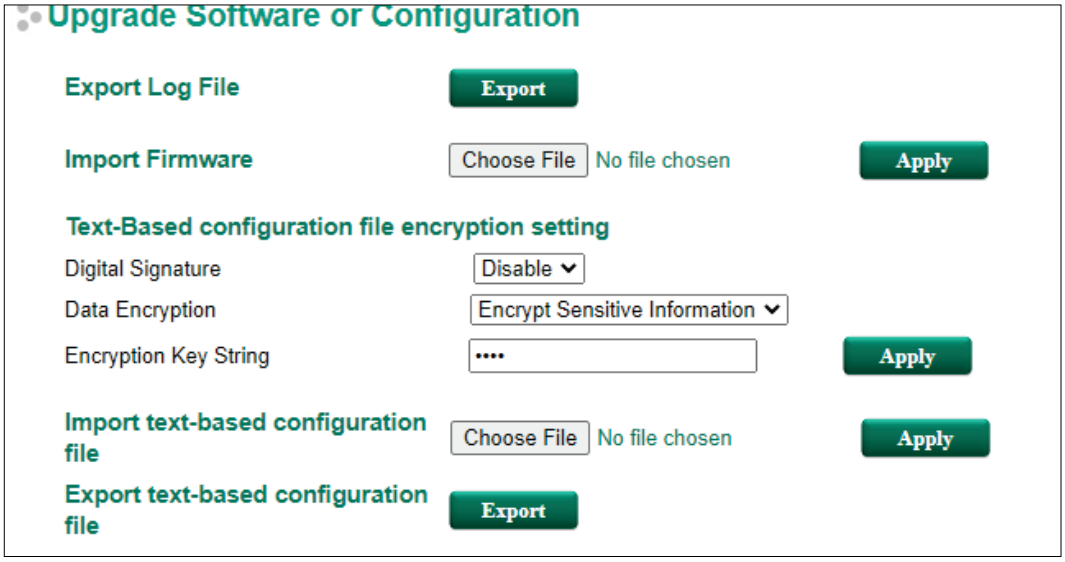
Text-Based configuration file encryption setting

Setting	Description	Factory Default
Enable Password	Type in the password for text-based configuration file encryption or decryption.	None

Configuration File Path and Name

Setting	Description	Factory Default
Enable Password	The path and filename of the Industrial Secure Router's configuration file is in the TFTP server. When the configuration file is downloaded from the TFTP server, it is exported from the TN-4900's system. The configuration file uses file extension .txt file.	None

System File Update—by Local Import/Export



Log File

Click **Export** to export the Log file of the Industrial Secure 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

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.

Text-Based configuration file encryption setting

To export the configuration as an encrypted text-based (command line type) configuration file, select the **Digital Signature** and **Data Encryption** options and an encryption key string, and then click **Apply**. The key string is also used for decrypting when importing an encrypted configuration file.

.

NOTE The default encryption key string is “moxa”.

Digital Signature

Setting	Description	Factory Default
Enable/disable	Enable or disable the use of a digital signature for checking the configuration file integrity.	Disable

Data Encryption

Setting	Description	Factory Default
Encrypt Sensitive Information	Only encrypt sensitive information in the exported configuration.	Encrypt Sensitive Information
Encrypt All Information	Encrypt all information in the exported configuration	

Upload Text-Based Configuration Data

To import a configuration file into the Industrial Secure Router, click **Browse** to select a configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking **Apply**.

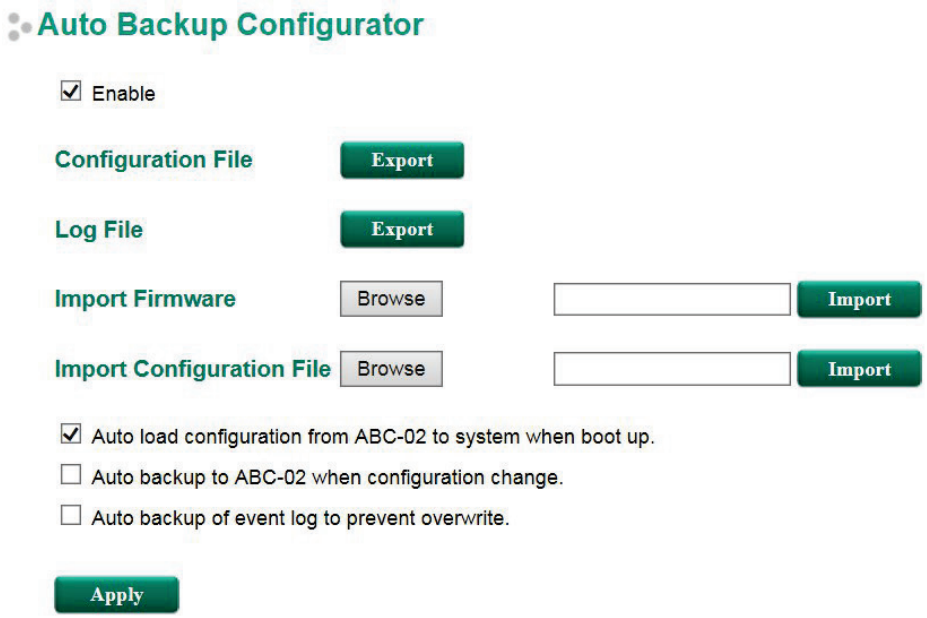
Download Text-Based Configuration Data

To export a configuration file, click **Export** to export the configuration file from the Industrial Secure Router to the local host.

System File Update –Import/Export the configurations stored on the ABC-02-USB

On large-scale networks, administrators need to configure many network devices. This is a time-consuming process and errors often occur. By using Moxa's Automatic Backup Configurator (ABC-02), the administrator can easily duplicate the system configurations across many systems in a short period of time.

Administrators only need to set up the configuration in a system once including the firewall rule and certificates, and then export the configuration file to the ABC-02. Then, the administrator can plug the ABC-02-USB into other systems, which allows other systems to sync using the configuration files stored in the ABC-02-USB.



Auto Backup Configurator

Setting	Description	Factory Default
Enable	Allows a system to import or export configuration files and firmware	Enable

Automatically load configurations from the ABC-02 to the new system on boot up

Setting	Description	Factory Default
Checked	Allows a system to load configuration files from the ABC-02 automatically on boot up	Checked
Unchecked	System will not load configuration files from the ABC-02 automatically on boot up	

Automatically backup to ABC-02 when configurations change

Setting	Description	Factory Default
Checked	Allows a system to back up configuration files to the ABC-02 automatically when configurations change	Checked

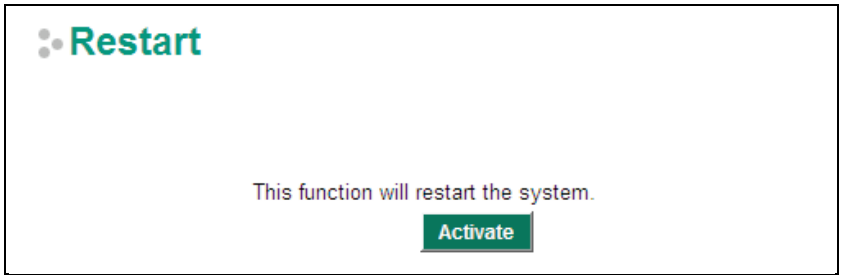
Unchecked	System will not backup configuration files to the ABC-02 automatically when configurations change	

Automatically back up event logs to prevent overwrite

Setting	Description	Factory Default
Checked	Allow systems to automatically backup logs to the ABC-02	Checked
Unchecked	System will not automatically back up logs to the ABC-02	

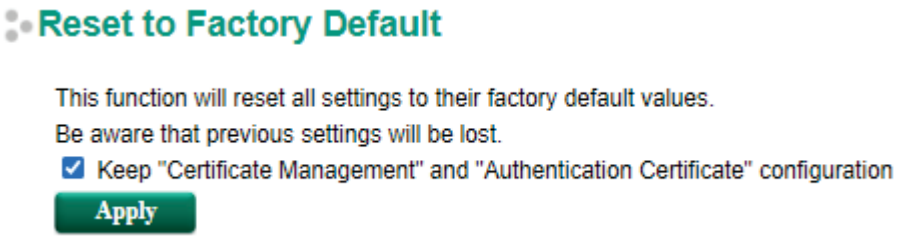
NOTE The ABC-02 USB is an optional accessory and has to be purchased separately.

Restart



This function is used to restart the Industrial Secure Router.

Reset to Factory Default



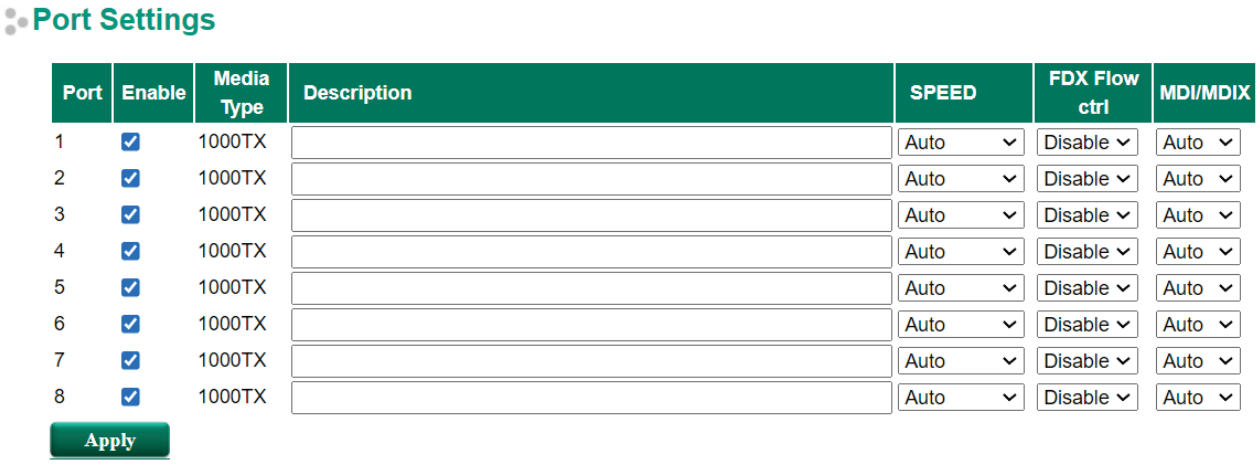
The **Reset to Factory Default** option gives users a quick way of restoring the Industrial Secure Router's configuration settings to the factory default values. This function is available in the console utility (serial or Telnet), and web browser interface.

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 Industrial Secure 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).



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	1000TX

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
1G-Full	Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	
100M-Full		
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		

Port Status

This page informs the users about the current status of all the ports including the port transmission speed, flow control, and port type (MDI or MDIX).

Port Status

Port	Media Type	Link Status	MDI/MDIX	FDX Flow ctrl	Port State
1/1	1000TX	--	--	--	---
1/2	1000TX	--	--	--	---
1/3	1000TX	--	--	--	---
1/4	1000TX	--	--	--	---
1/5	1000TX	--	--	--	---
1/6	1000TX	--	--	--	---
1/7	1000TX	--	--	--	---
1/8	1000TX	1G-Full	MDI	Off	Forwarding

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 industrial secure router's port trunking feature allows devices to communicate by aggregating up to 4 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 industrial secure routers. If all ports on both switches are configured as 1000BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 16 Gbps.

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 1000BaseTX and they are operating in full duplex mode, the potential bandwidth of the connection will be up to 16 Gbps. This means that users can double, triple, or quadruple the bandwidth of the connection by port trunking between two Moxa switches.

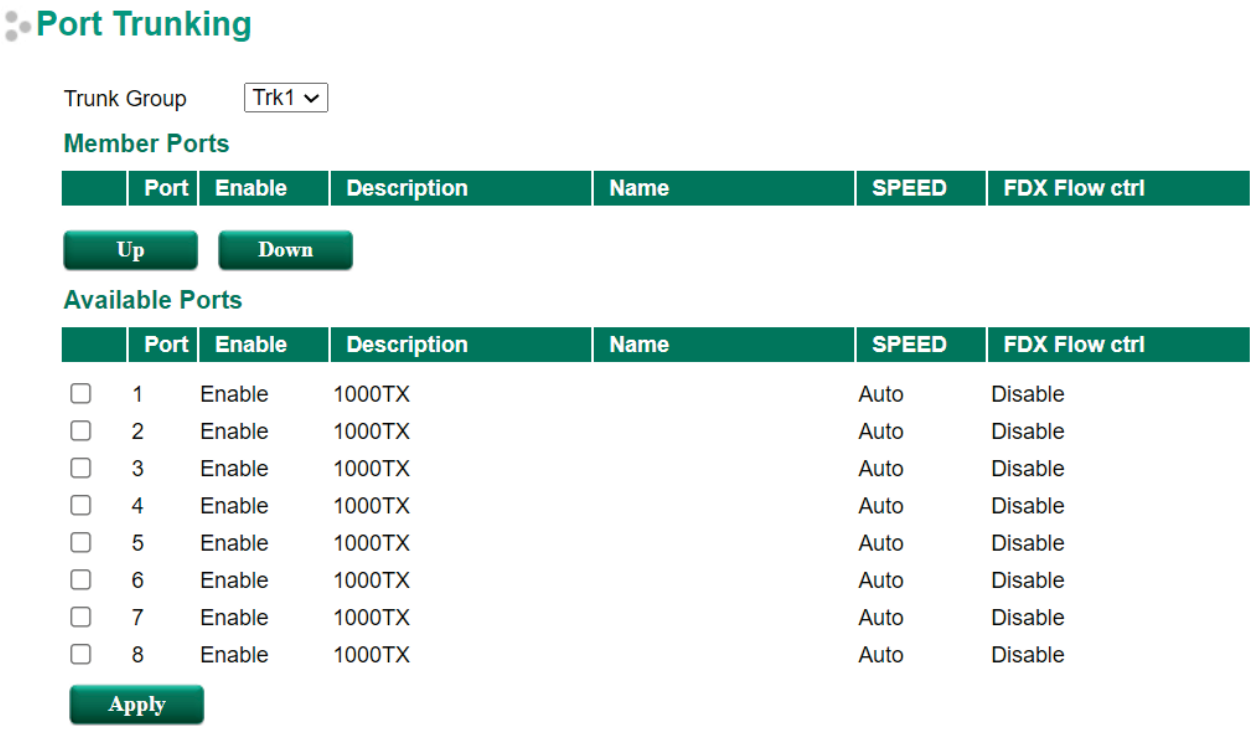
Each Moxa industrial secure router can set a maximum of 4 port trunking groups. When you activate port trunking, certain settings on each port will be reset to factory default values or disabled:

- 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.



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 4 trunk groups)

Setting	Description	Factory Default
Trk1, Trk2, Trk3, Trk4 (depends on switching chip capability; some products only support 3 trunk groups)	Specifies the current trunk group.	Trk1

Trunking Status

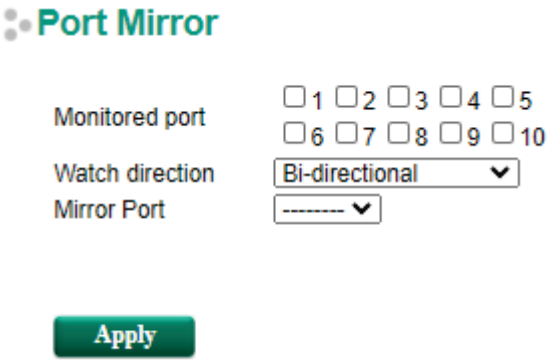
The **Trunking Status table** shows the Trunk Group configuration status.

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 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 industrial secure router's port. • Output data stream: Select this option to monitor only those data packets being sent out through the Moxa industrial secure router's port. • Bi-directional: Select this option to monitor data packets both coming into, and being sent out through, the Moxa industrial secure 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

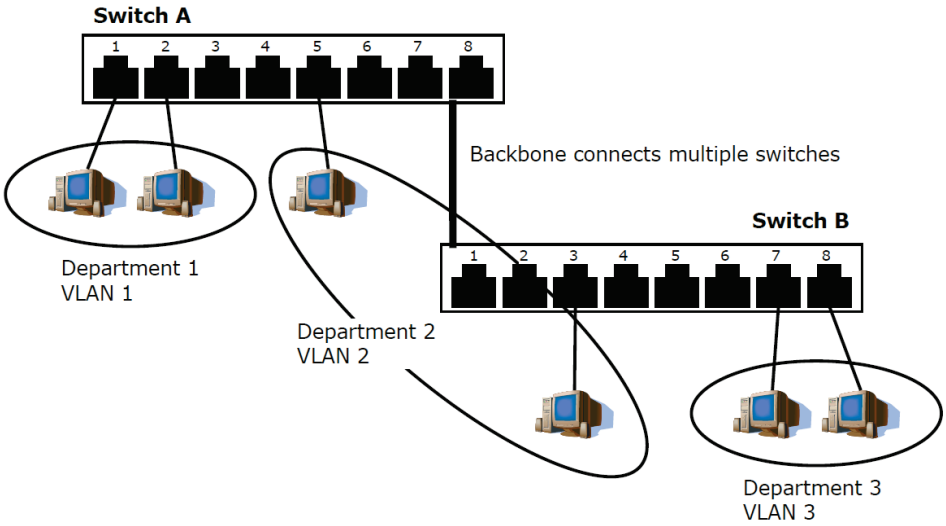
Setting up Virtual LANs (VLANs) on your Moxa industrial secure router increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

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 industrial secure router contains a single VLAN—the Default VLAN. This VLAN has the following definition:

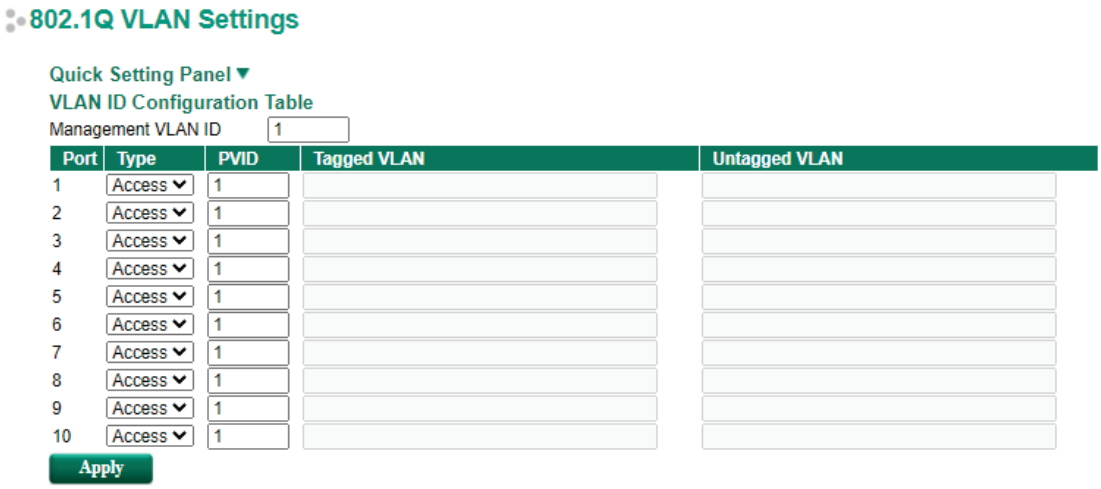
- **VLAN Name**—Management VLAN
- **802.1Q VLAN ID**—1 (if tagging is required)

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



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	Select the Access port type to connect single devices without tags.	Access
Trunk	Select the 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

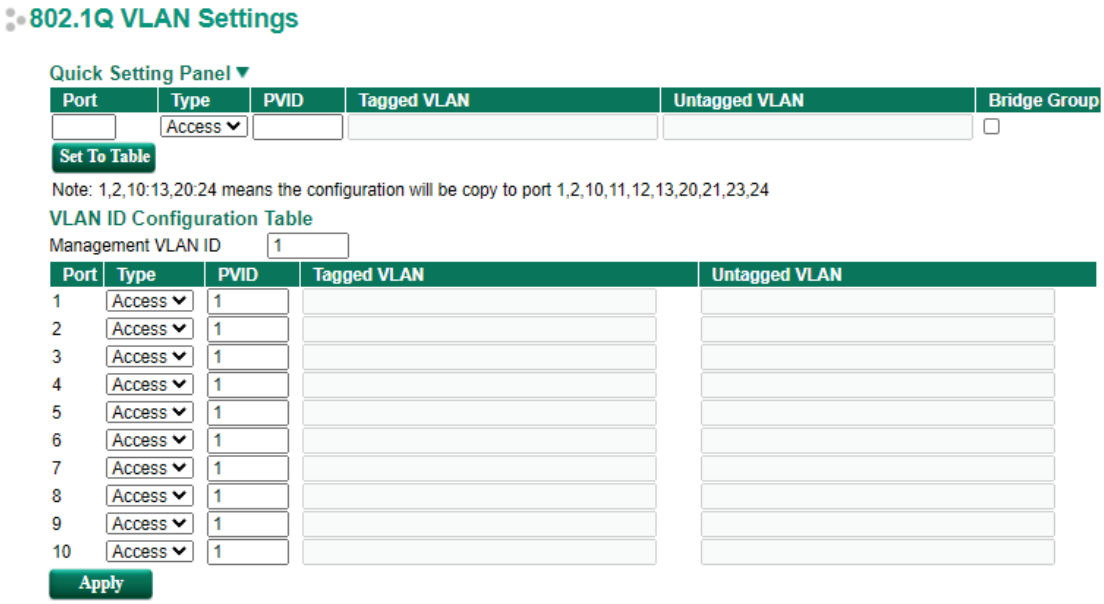
Setting	Description	Factory Default
VLAN ID from 1-4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	None

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

Quick Setting Panel

Click the triangle to open the **Quick Setting Panel**. Use this panel for quick and easy configuration of VLAN settings for multiple ports at once.



Input the port numbers in the Port column, and set the Port Type, Tagged VLAN ID, and untagged VLAN ID. Next, click the **Set to Table** button to create the VLAN ID configuration table.

VLAN Table

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 industrial secure 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:

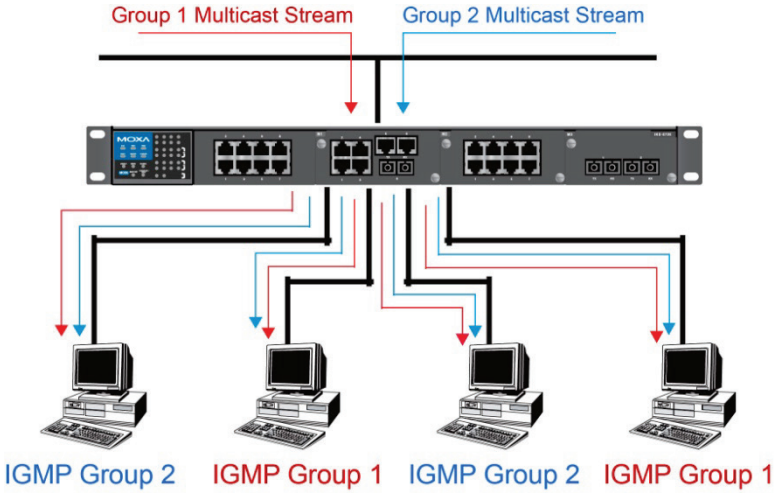
- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and 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

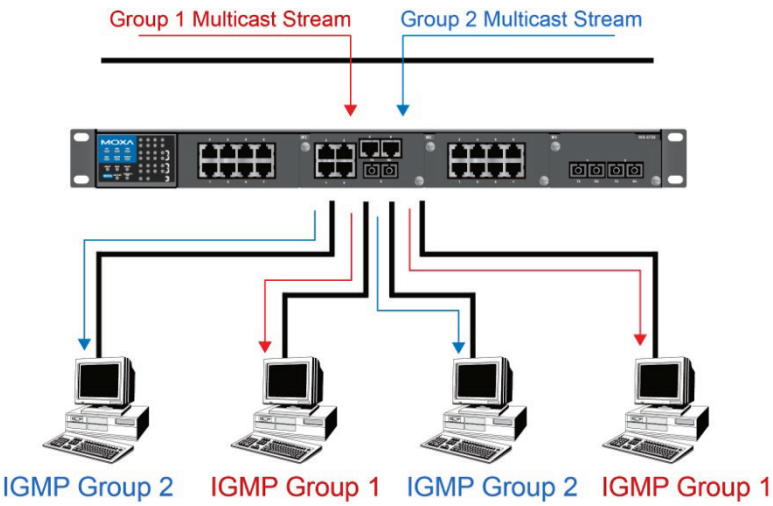
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves 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 Industrial Secure Routers

The Moxa industrial secure 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 industrial secure 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 industrial secure router support IGMP snooping version 1, version 2 and version 3. 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, 2 and 3. 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 3 supports "source filtering," which allows the system to define how to treat packets from specified source addresses. The system can either white-list or black-list specified sources.

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
V3	Compatible with V1, V2 and adds: a. Source filtering - accept multicast traffic from specified source - accept multicast traffic from any source except the specified source	RFC-3376

Static Multicast MAC

Some devices may only support multicast packets, but not support either IGMP Snooping. The Moxa industrial secure router supports adding multicast groups manually to enable multicast filtering.

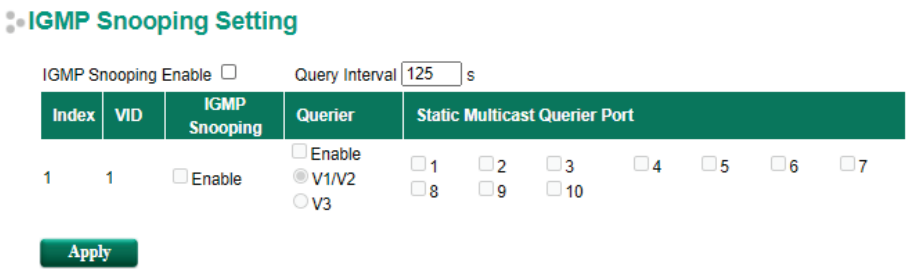
Enabling Multicast Filtering

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



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 Industrial Secure Router's querier function.	Disabled
V1/V2 and V3 Checkbox	V1/V2: Enables the Moxa Industrial Secure Router to send IGMP snooping version 1 and 2 queries V3: Enables the Moxa Industrial Secure Router to send IGMP snooping version 3 queries	V1/V2

Static Multicast Querier Port

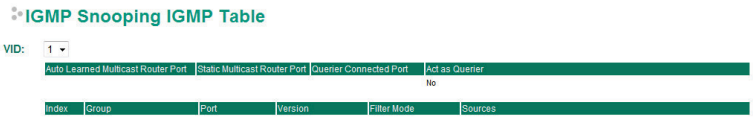
Setting	Description	Factory Default
Select/Deselect	Select the ports that will connect to the multicast routers. These ports will receive all multicast packets from the source. This option is only active when IGMP Snooping is enabled.	Disabled

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 industrial secure router displays the current active IGMP groups that were detected. View IGMP group setting per VLAN ID on this page.



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 this 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
- Filter Mode: Indicates the multicast source address is included or excluded. Displays Include or Exclude when IGMP v3 is enabled
- Sources: Displays the multicast source address when IGMP v3 is enabled

Stream Table

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

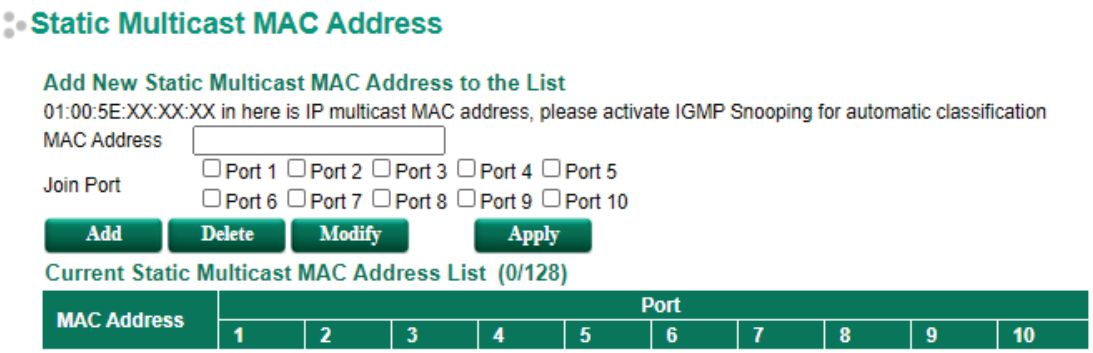
Stream Group: Multicast group IP address

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



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

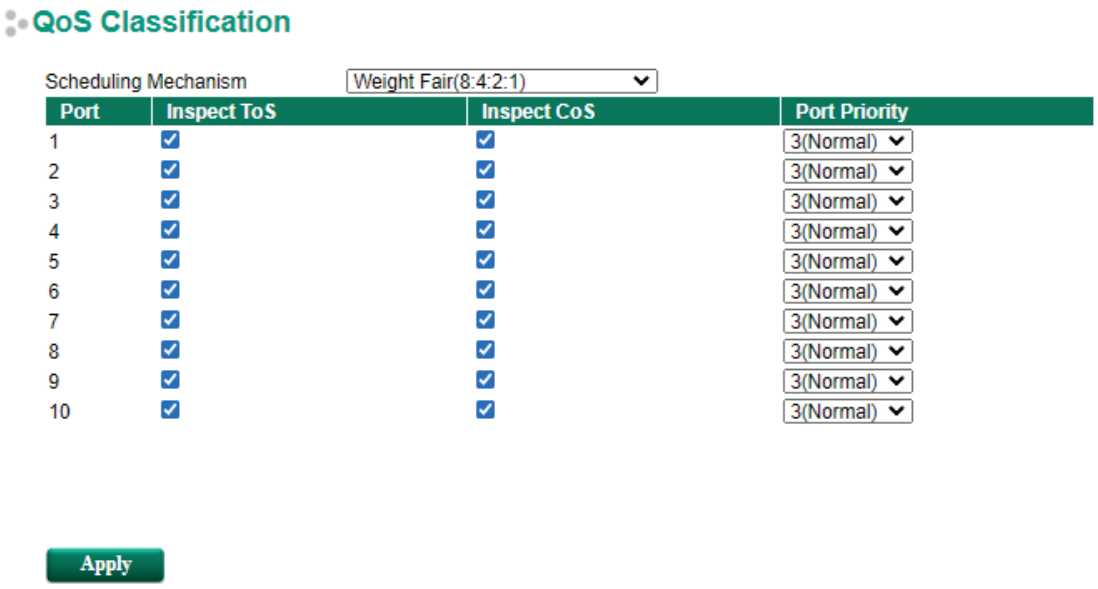
Setting	Description	Factory Default
Integer	Input the number of the VLAN that the host with this MAC address belongs to.	None

Join Port

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

QoS and Rate Control

QoS Classification



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 industrial secure 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 industrial secure 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 industrial secure router for inspecting 802.1p CoS tags in the MAC frame to determine the priority of each frame.	Enabled

Port Priority

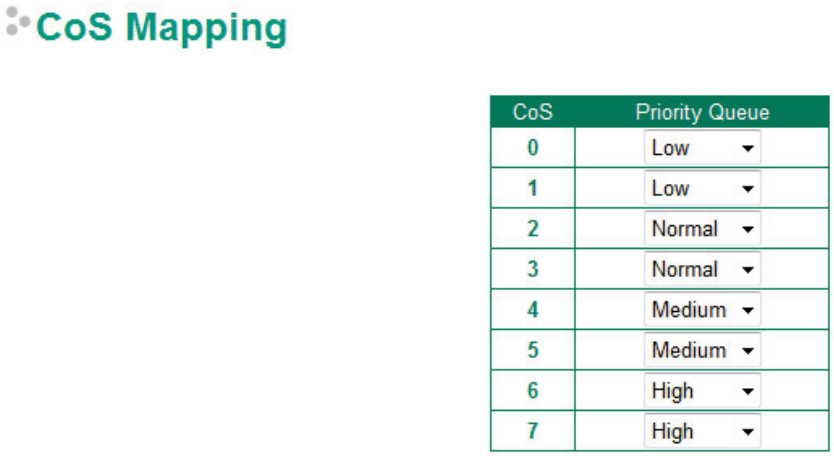
Setting	Description	Factory Default
Port priority	The port priority has 4 priority queues. Low, normal, medium, high priority queue option is applied to each port.	3(Normal)

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.

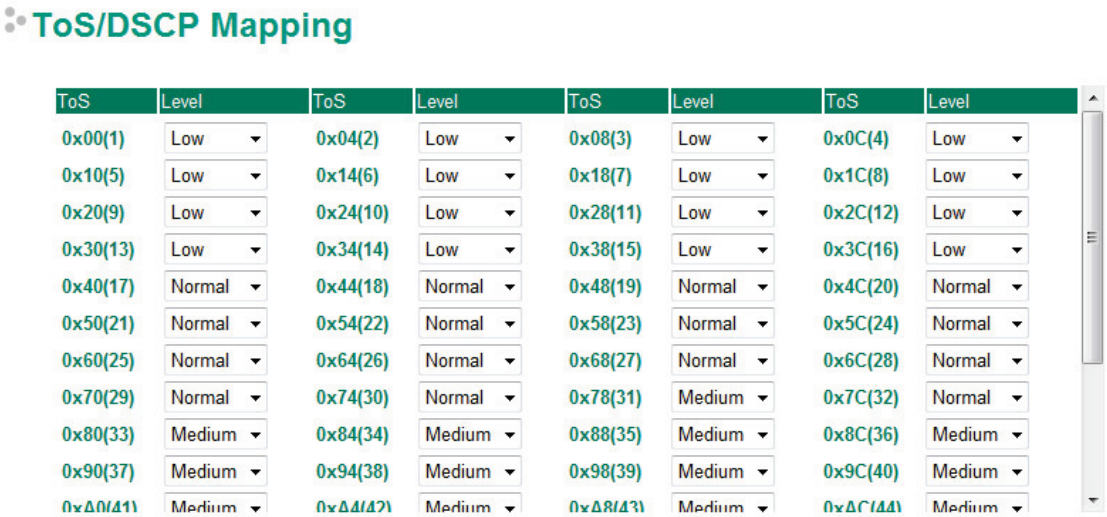
CoS Mapping



CoS 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



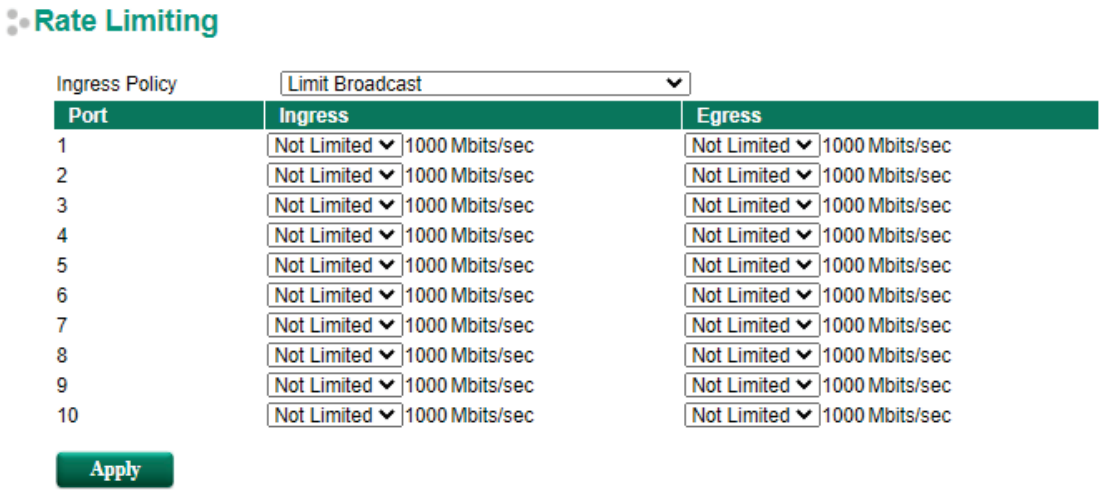
ToS (DSCP) Value and Priority Queues

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

Rate Limiting

In general, one host should not be allowed to occupy unlimited bandwidth, particularly when the device malfunctions. For example, so-called “broadcast storms” could be caused by an incorrectly configured topology, or a malfunctioning device. Moxa industrial secure routers not only prevent broadcast storms, but

can also be configured to a different ingress rate for all packets, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.



Ingress Policy

Setting	Description	Factory Default
Limit All	Select the ingress rate limit for different packet types	Limit Broadcast
Limit Broadcast, Multicast, Flooded Unicast		
Limit Broadcast, Multicast		
Limit Broadcast		

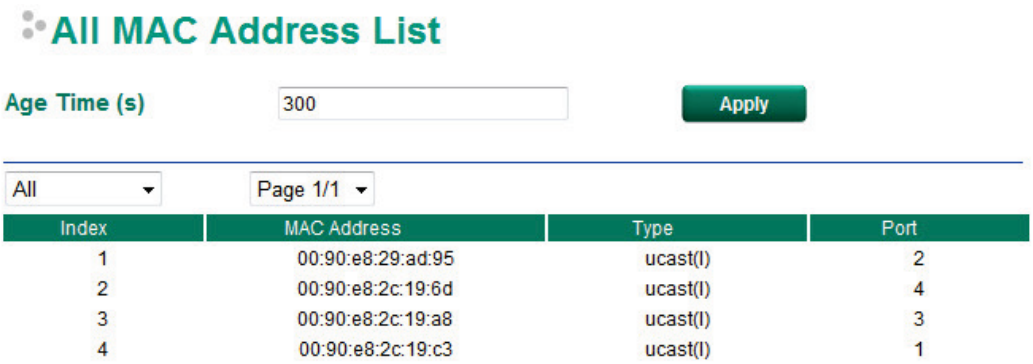
Ingress/Egress Rate

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

MAC Address Table

The MAC address table shows the MAC address list pass through Moxa industrial secure 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 industrial secure router MAC address groups, which are selected from the drop-down list.



Drop Down List

ALL	Select this item to show all of the Moxa industrial secure router's MAC addresses.
ALL Learned	Select this item to show all of the Moxa industrial secure router's Learned MAC addresses.
ALL Static	Select this item to show all of the Moxa industrial secure router's Static, Static Lock, and Static Multicast MAC addresses.
ALL Multicast	Select this item to show all of the Moxa industrial secure 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

VLAN ID

Moxa Industrial Secure Router's WAN interface is configured by VLAN group. The ports with the same VLAN can be configured as one WAN interface.

Connection

Note that there are three different connection types for the WAN interface: Dynamic IP, Static IP, and PPPoE. A detailed explanation of the configuration settings for each type is given below.

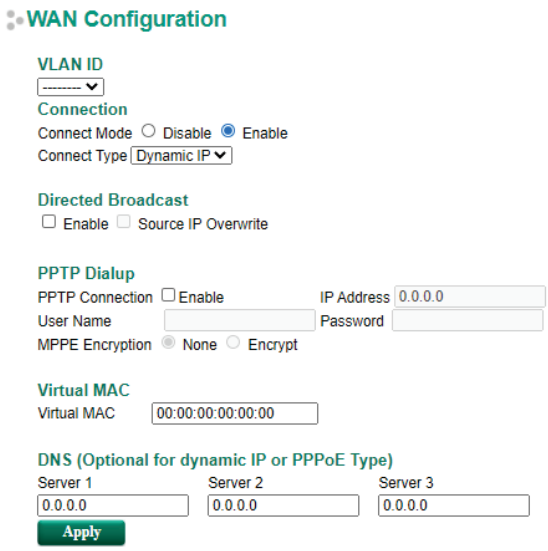
Connection Mode

Setting	Description	Factory Default
Enable or Disable	Enable or Disable the WAN interface	Enable

Connection Type

Setting	Description	Factory Default
Static IP, Dynamic IP, PPPoE	Setup the connection type	Dynamic IP

Detailed Explanation of Dynamic IP Type



Directed Broadcast

Setting	Description	Factory Default
Enable or Disable	Enable or disable directed broadcasting	None
Source IP Overwrite	Check to overwrite the source IP	None

PPTP Dialup

Point-to-Point Tunneling Protocol is used for Virtual Private Networks (VPN). Remote users can use PPTP to connect to private networks from public networks.

PPTP Connection

Setting	Description	Factory Default
Enable or Disable	Enable or Disable the PPTP connection	None

IP Address

Setting	Description	Factory Default
IP Address	The PPTP service IP address	None

User Name

Setting	Description	Factory Default
Max. 30 Characters	The Login username when dialing up to PPTP service	None

Password

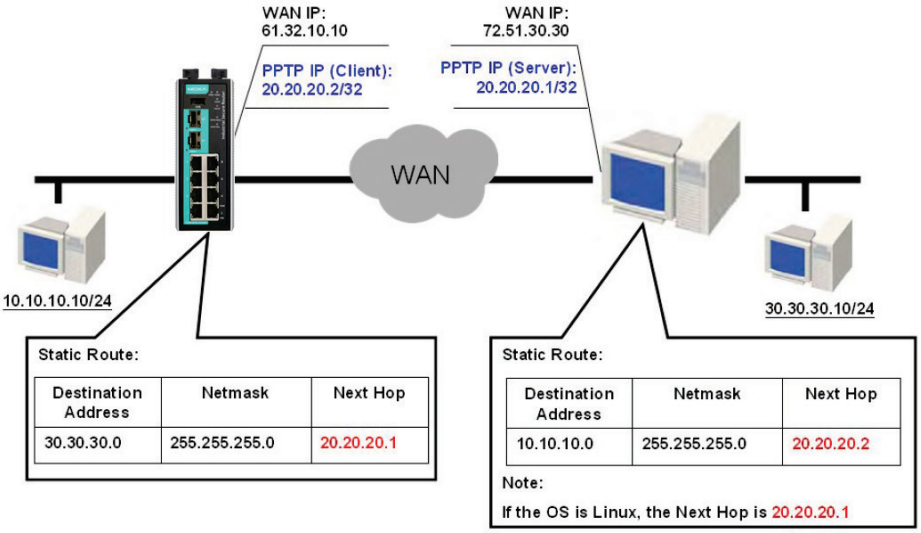
Setting	Description	Factory Default
Max. 30 characters	The password for dialing the PPTP service	None

MPPE Encryption

Setting	Description	Factory Default
None/Encrypt	Enable or disable the MPPE encryption	None

Example

Suppose a remote user (IP: 10.10.10.10) wants to connect to the internal server (private IP: 30.30.30.10) via the PPTP protocol. The IP address for the PPTP server is 20.20.20.1. The necessary configuration settings are shown in the following figure.



Virtual MAC

Setting	Description	Factory Default
Virtual MAC Address	The virtual MAC address	None

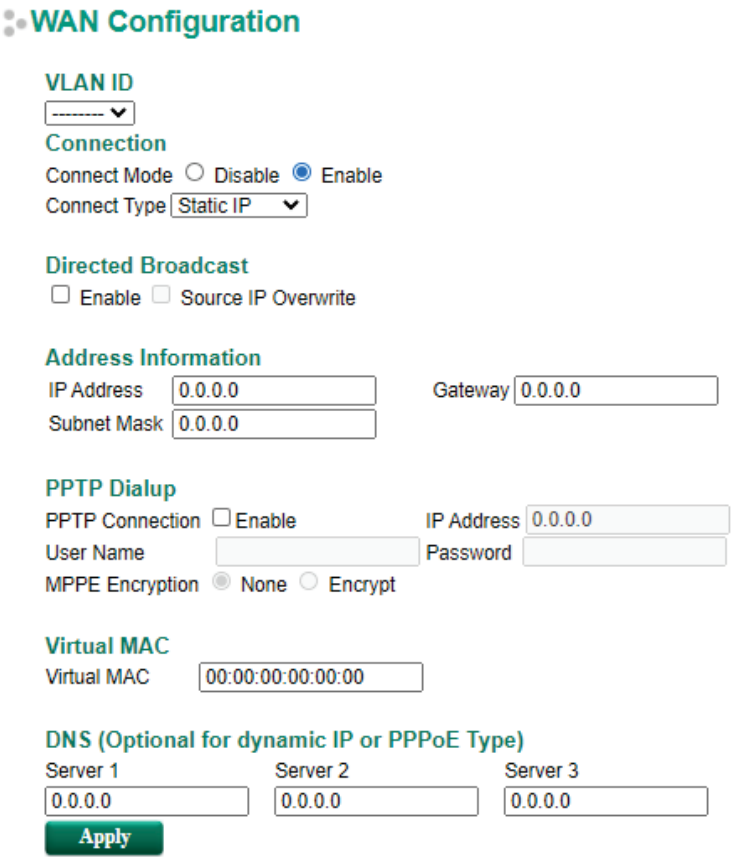
DNS (Domain Name Server; optional setting for Dynamic IP and PPPoE types)

Server 1/2/3

Setting	Description	Factory Default
IP Address	The DNS IP address	None

NOTE The priority of a manually configured DNS will be higher than the DNS from the PPPoE or DHCP server.

Detailed Explanation of Static IP Type



Address Information

IP Address

Setting	Description	Factory Default
IP Address	The interface IP address	None

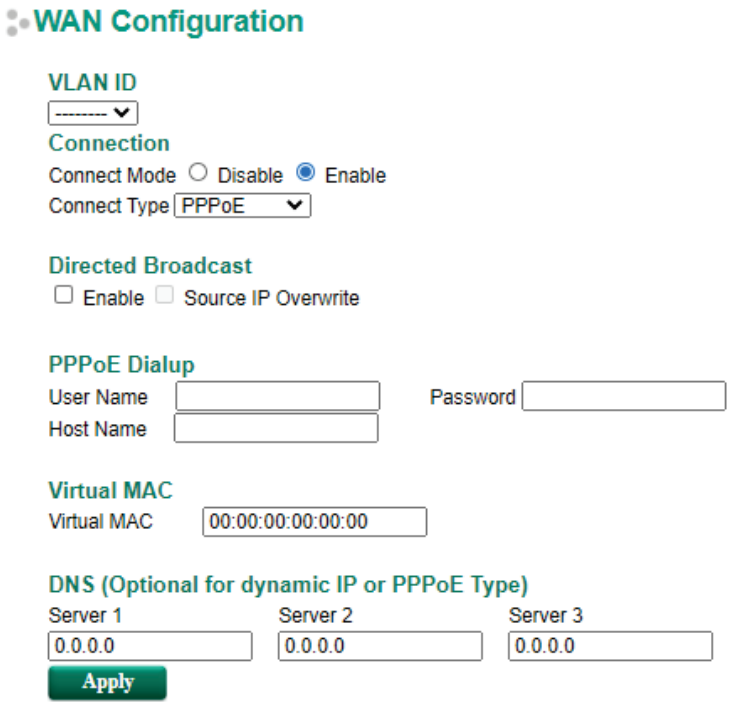
Subnet Mask

Setting	Description	Factory Default
IP Address	The subnet mask	None

Gateway

Setting	Description	Factory Default
IP Address	The Gateway IP address	None

Detailed Explanation of PPPoE Type



PPPoE Dialup

User Name

Setting	Description	Factory Default
Max. 30 characters	The User Name for logging in to the PPPoE server	None

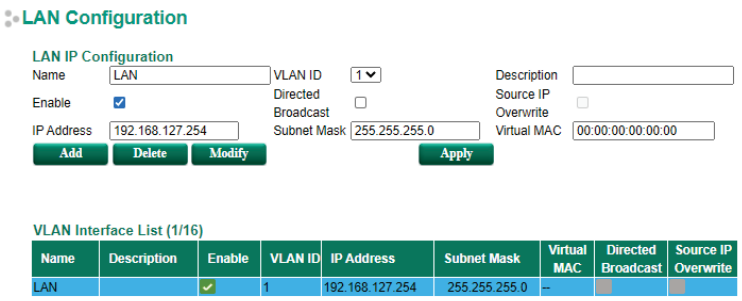
Host Name

Setting	Description	Factory Default
Max. 30 characters	User-defined Host Name of this PPPoE server	None

Password

Setting	Description	Factory Default
Max. 30 characters	The login password for the PPPoE server	None

LAN



Create a VLAN Interface

Input the 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/Virtual MAC Address 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

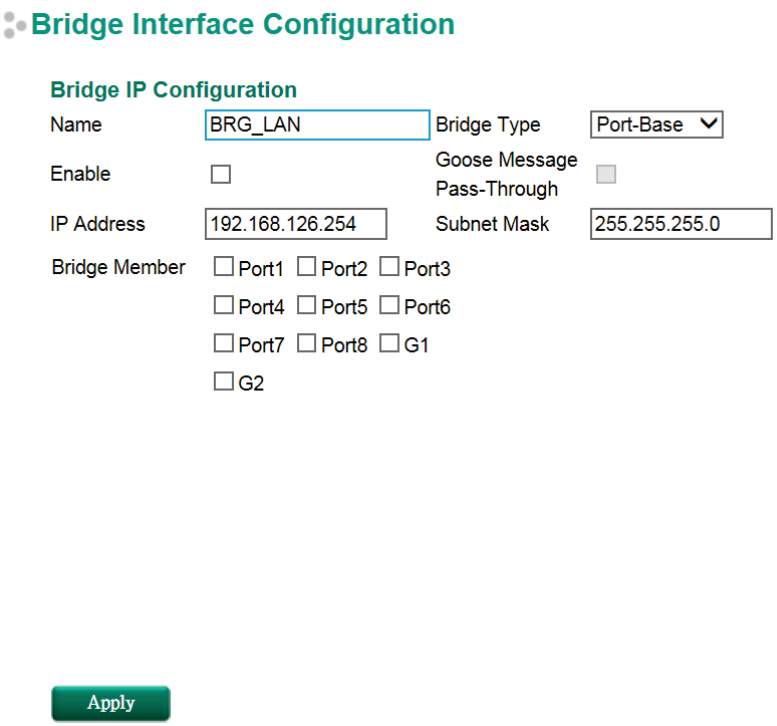
After adding/deleting/modifying any LAN interface, be sure to click **Activate**.

NOTE You can create up to 16 LAN interfaces by configuring each port with unique VLAN ID numbers.

Bridge Group Interface

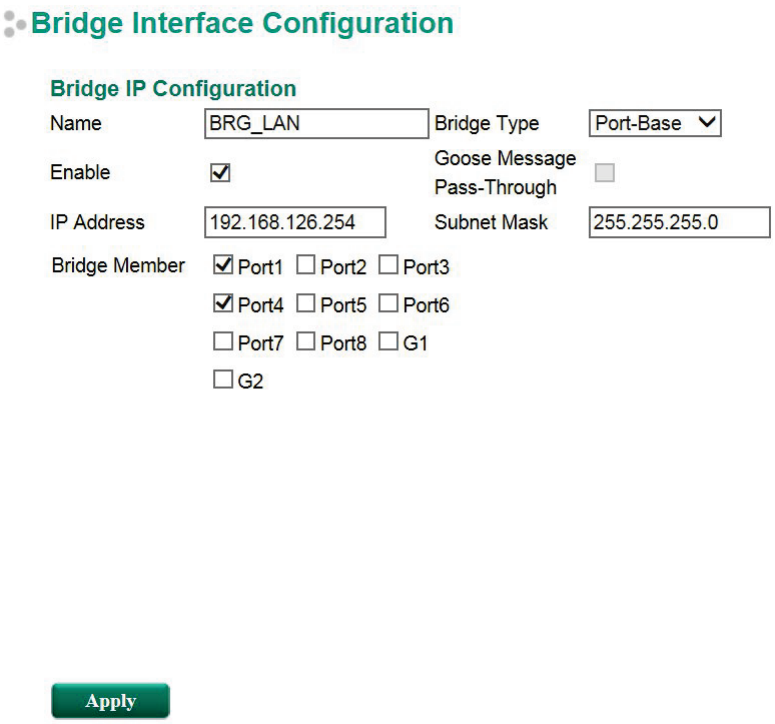
When ports are set in the VLAN, the packets transmitted within these ports will be forwarded by the switching chip without being filtered by the firewall. However, in some scenarios, it is required to filter specific packets transmitted within the VLAN. By selecting ports as Bridge port, the packets transmitted between these ports will be checked by the firewall.

In addition, when ports are set in different VLANs, the packets transmitted within these VLANs will be routed by the switching chip locally, without being inspected by the firewall. However in some scenarios, it is required to filter specific packets transmitted within VLANs. By selecting VLAN to join Bridge Zone, the packets transmitted between these two zones will be checked by the firewall.



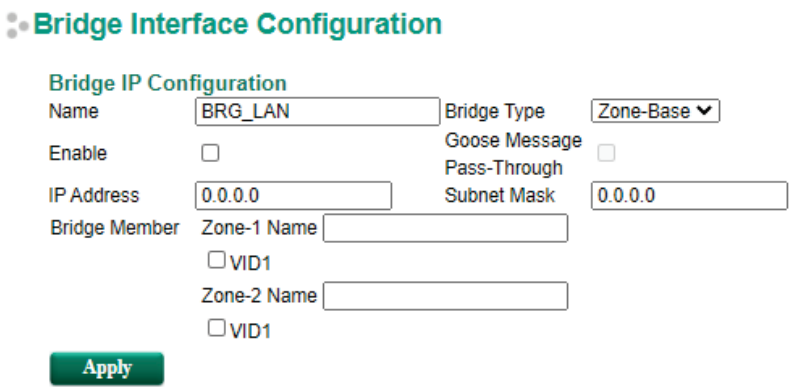
Adding Ports/VLANs into the Bridge Interface

Port Base



First, select **Port-Base** in Bridge Type. Then input a name for the Bridge interface and assign an IP address/Subnet Mask for the interface. In order to enable this feature, checkmark the Enable checkbox. Finally, please select the port that will be set as the bridge port and check Apply.

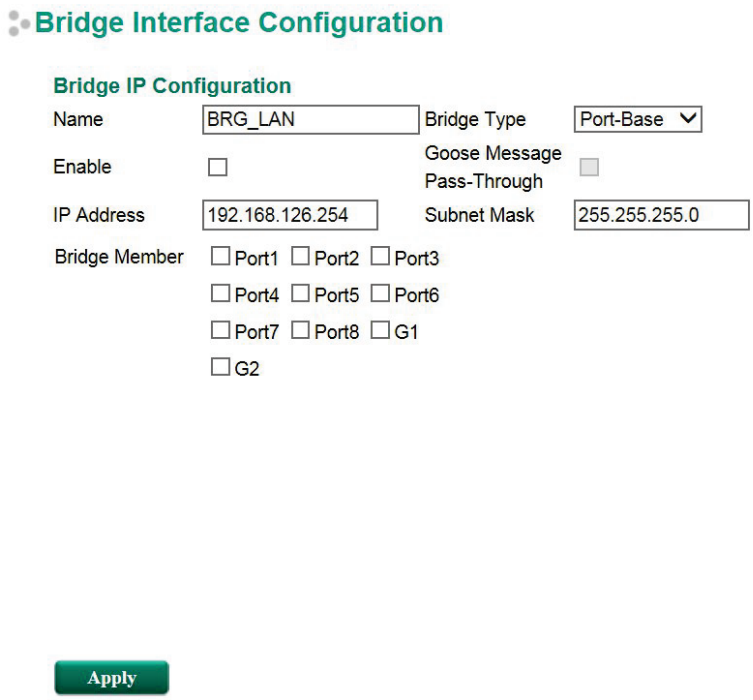
Zone base



First, select **Zone-Base** in Bridge Type. Next, input a name of the Bridge Zone interface and assign an IP address/Subnet Mask for the interface. In order to enable this feature, checkmark the Enable checkbox. Then, Zone-1 and Zone-2 will display on the page. Finally, please select which VLAN should join Zone-1 and which VLAN should join Zone-2 and then check Apply.

Modify and Cancel the Bridge Group Interface

In order to modify which Bridge member has been selected, users can simply check new ports/VLANs under the bridge member section, and uncheck ports/VLANs they no longer want to be a member of the bridge LAN. Finally, they should click Apply.



NOTE When bridge setting is canceled, for example removing all ports or VLANs from bridge inter, the bridge interface will still be alive. Even though there is no port in bridge interface, user can see VLAN ID of bridge interface in VLAN table, e.g.4040, 4041. To remove bride interface, please modify PVID in VLAN Settings.

Network Service

DHCP Settings

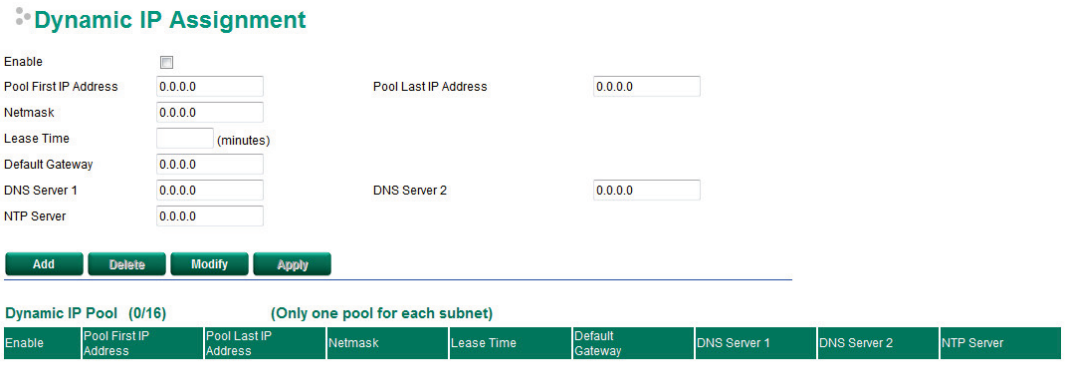
Global Settings

DHCP Server Mode

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

DHCP Server

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



<u>Dynamic IP Assignment</u>

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

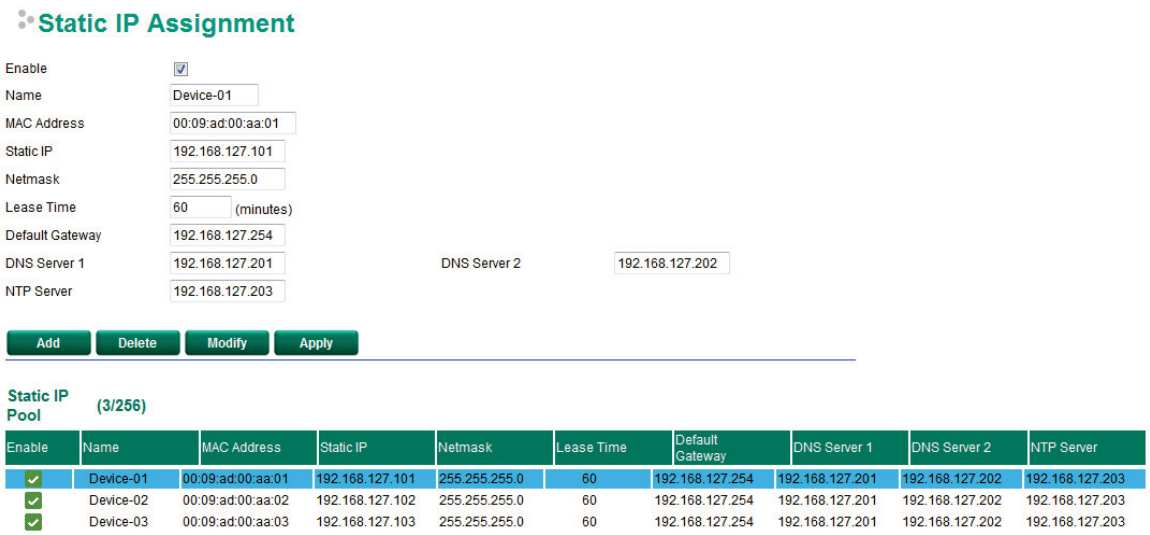
NTP Server

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 Industrial Secure Router always use the same IP address. The static DHCP list matches IP addresses to MAC addresses.



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 Industrial Secure Router, the Industrial Secure 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	1440

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.

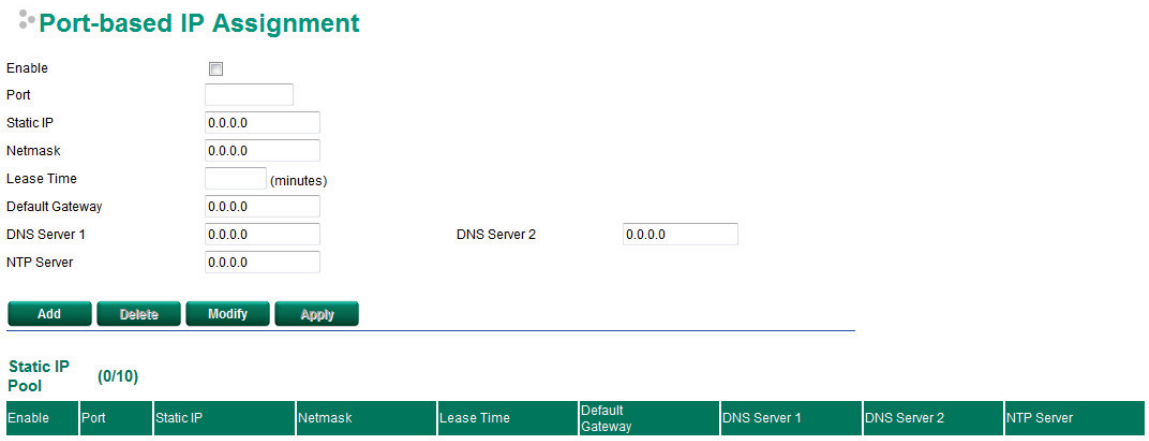
Delete

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



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	1440

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.

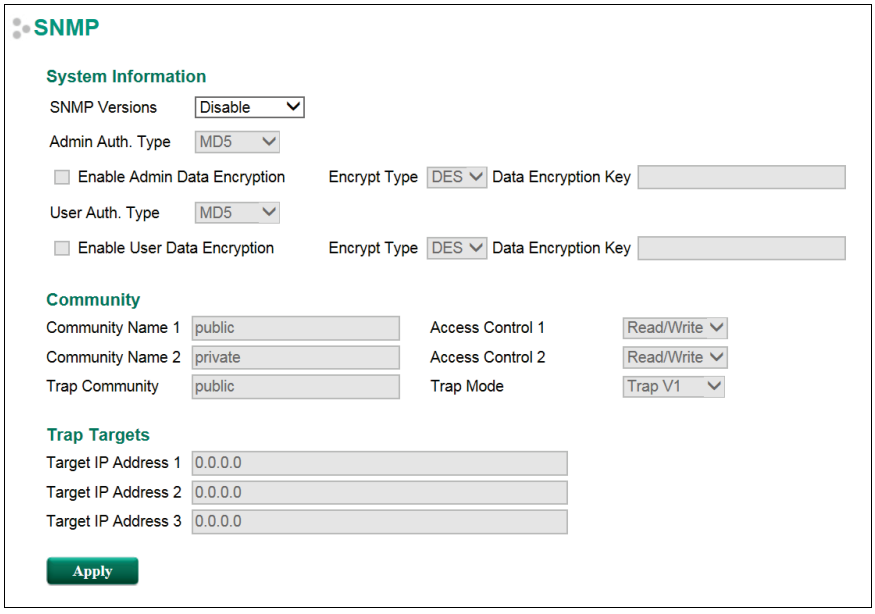
Name	MAC Address	IP Address	Time Left
Server	00-0E-A6-09-7A-9E	192.168.127.1	32m:36s

SNMP Settings

The Industrial Secure 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 Industrial Secure 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 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

Encrypt type

Setting	Description	Factory Default
DES/AES	Select encryption mechanism	DES

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

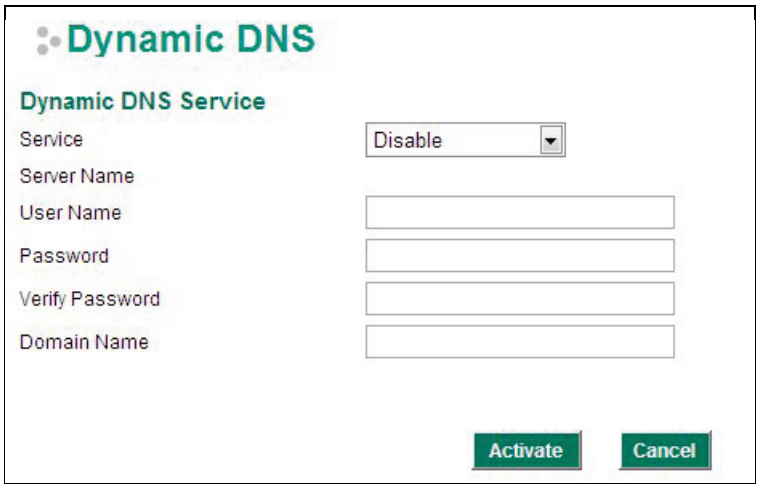
Setting	Description	Factory Default
Read/Write	Access control type after matching the community string	Read/Write
Read only (Public MIB only)		
No Access		

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.

Dynamic DNS

Dynamic DNS (Domain Name Server) allows you to use a domain name to connect to the Industrial Secure Router. The Industrial Secure Router can connect to 4 free DNS servers and register the user configurable Domain name in these servers.



Service

Setting	Description	Factory Default
> Disable > freedns.afraid.org > www.3322.org > members.dyndns.org > dynupdate.no-ip.com	Disable or select the DNS server	Disable

User Name

Setting	Description	Factory Default
Max. 30 characters	The DNS server's user name	None

Password

Setting	Description	Factory Default
Max. 30 characters	The DNS server's password	None

Verify Password

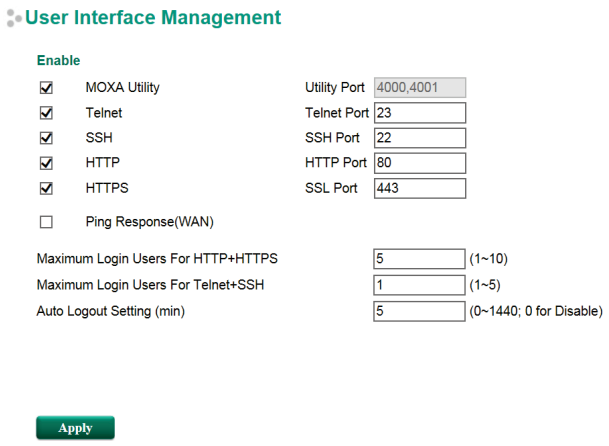
Setting	Description	Factory Default
Max. 30 characters	Verifies the DNS server password	None

Domain name

Setting	Description	Factory Default
Max. 30 characters	The DNS server's domain name	None

Security

User Interface Management



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

Enable Ping Response (WAN)

Setting	Description	Factory Default
Select/Deselect	When the WAN connection has been established, if the WAN port is pinged it will send a response.	Deselect

Maximum Login Users For HTTP+HTTTPS

Setting	Description	Factory Default
Maximum Login Users For HTTP+HTTPS	Set a limit for the amount of users who can be logged in to the TN-4900 using HTTP and HTTPS. The maximum number of users using HTTP and HTTPS is 10.	5

Maximum Login Users For Telnet+SSH

Setting	Description	Factory Default
Maximum Login Users For Telnet+SSH	Set a limit for the amount of users who can be logged in to the TN-4900 using HTTP and HTTPS. The maximum supported user numbers of Telnet+SSH is 5.	5

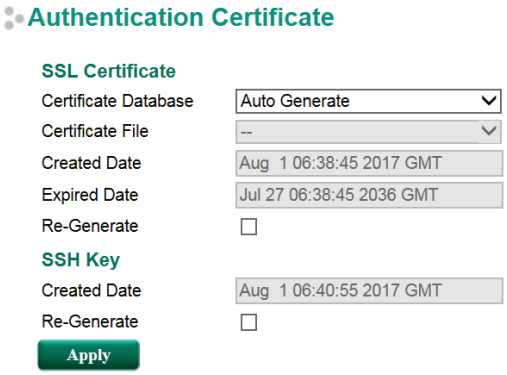
Auto Logout Setting (min)

Setting	Description	Factory Default
Auto Logout Setting (min)	When the user does not touch the TN-4900 management interface for a defined period of time, the management interface will logout automatically. The TN-4900 default setting is 5 minutes.	5

NOTE To ping WAN port successfully, please make sure "Ping Response (WAN)" is checked, and ping sender IP is in "Trusted Access" list or "Accept all connection from LAN port" in Trusted Access is checked.

Authentication Certificate

Authentication certificate refers to certificates that use HTTPS. The web console certificate can be generated by the TN-4900 automatically or users can choose the certificate imported in Local certificate.



Certificate Database

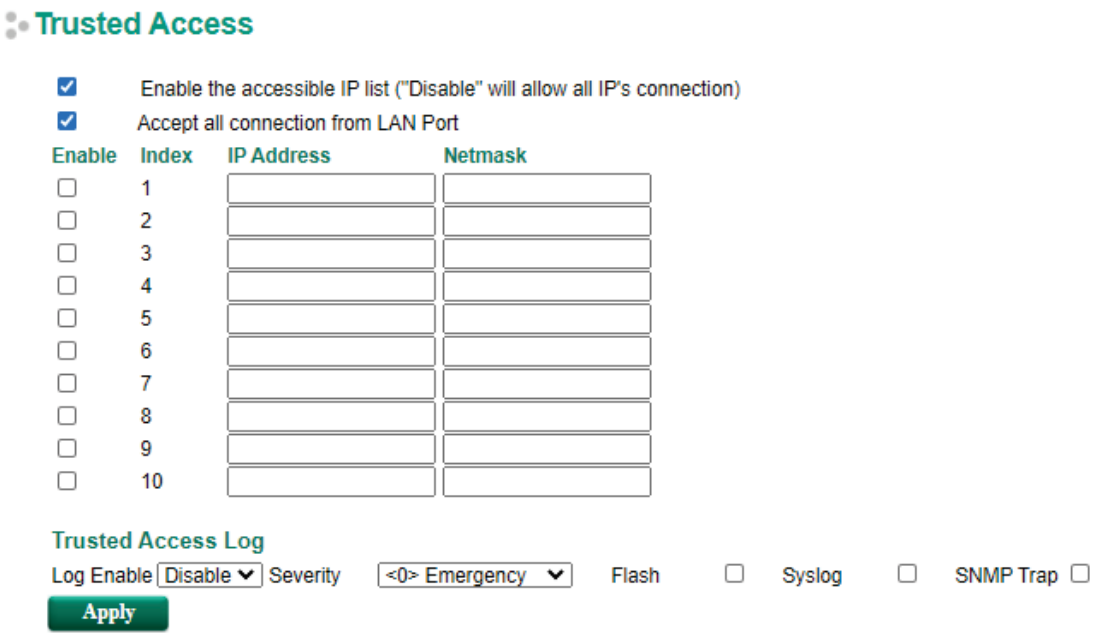
Setting	Description	Factory Default
Auto Generate	The TN-4900 will generate a certificate automatically. If not, please select "Re-Generate" to generate a certificate. Auto Generate is the default setting.	Auto Generate

SSH Key Re-generate

Setting	Description	Factory Default
Select/Deselect	Enable the SSH Key Re-generate	Deselect

Trusted Access

The TN-4900 uses an IP address-based filtering method to control access.



You may add or remove IP addresses to limit access to the Moxa industrial secure router. When the accessible IP list is enabled, only addresses on the list will be allowed access to the Moxa industrial secure 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:

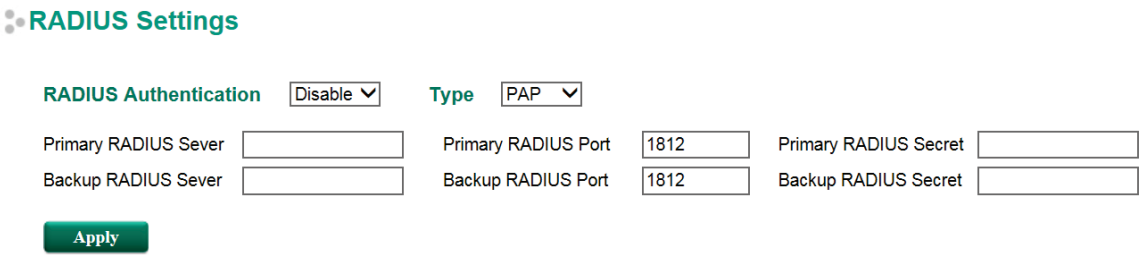
Hosts That Need Access	Input Format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254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

Enable Logging Trusted Access Events

To enable the Trusted Access event log function, select the **Enable** option in Log Enable and click Flash, Syslog, or SNMP Trap. You may also define the severity of the Trusted Access types and record it in the event.

RADIUS Server Settings

For the entire network, users can set up two RADIUS servers. One functions as the primary and the other one as the backup server. When the primary RADIUS server fails, the TN-4900 will switch the connection to the backup RADIUS server.



Radius Status

Setting	Description	Factory Default
Enable/Disable	Enable to use the same setting as Auth Server	Disable

Type

Setting	Description	Factory Default
PAP	Authentication type of Radius server	PAP
CHAP		

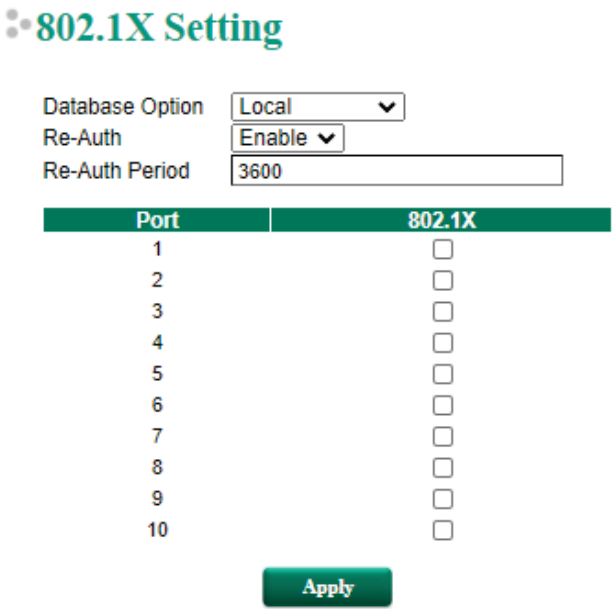
Primary/Backup Server Setting

Setting	Description	Factory Default
RADIUS Server	Specifies the IP/name of the server	None
RADIUS Port	Specifies the port of the server	1812
RADIUS Secret	Specifies the shared key of the server	None

Port Access Control Setting

PAC (Port-based Access Control) provides an authentication mechanism to prevent unauthorized access to the LAN. Without this mechanism, users can access the LAN by simply physically connecting to any LAN device on the network. PAC enhances network security by providing a procedure to authenticate and authorize users who attempt to access the network.

802.1X



802.1X Setting

Setting	Description	Factory Default
Database Option	Select the authentication server user account database	Local

Re-Auth	Enable or disable the re-authentication function	Enable
Re-Auth Period	If Re-Auth is enabled, specify the re-authentication period (in seconds)	3600
Port Enable	Enable or disable 802.1X port access control on the port	Disable

802.1X Information

The following table shows the 802.1X authentication status information.

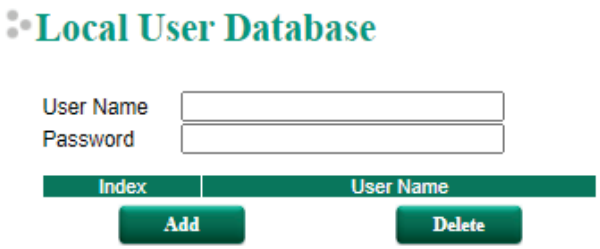
Authentication Status	Description
INITIALIZE	The initial state of the 802.1X-enabled port shown when the device is rebooting, when a supplicant sends an EAPOL start packet, or when the port link is down
CONNECTING	Establishing a connection with the supplicant
DISCONNECTED	This state is entered from the CONNECTING, AUTHENTICATED, and ABORTING state if an explicit logoff request is received from the supplicant, and from the CONNECTING state if the number of allowed re-authentication attempts has been exceeded
AUTHENTICATING	The supplicant is being authenticated
AUTHENTICATED	The supplicant was successfully authenticated
ABORTING	The authentication is prematurely terminated due to a re-authentication request, an EAPOL-Start frame, an EAPOL-Logoff frame, or an authTimeout
HELD	Failed to authenticate the supplicant

RADIUS Server Setting

Radius Server Setting

Setting	Description	Factory Default
Server IP address	Specify the first and second RADIUS authentication IP address or server name	None
Port number	Specify the first and second RADIUS server port number	1812
Shared key	Specify the shared key for the first and second RADIUS server	None

Local User Database

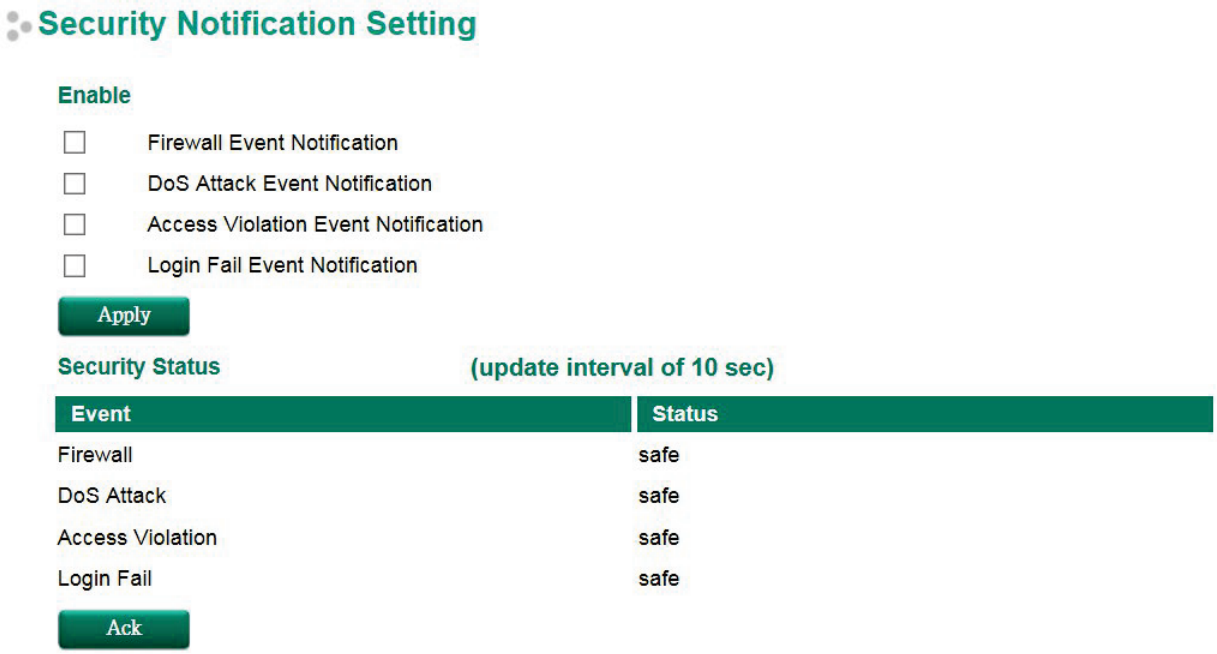


Local User Database

Setting	Description	Factory Default
User name	Specify the user account user name	None
Password	Specify the user account password	None

Security Notification Setting

When the events below are displayed, the TN-4900 will send an SNMP trap to notify the server.



4

Routing

The following topics are covered in this chapter:

- **Unicast Route**
  - Static Routing
  - RIP (Routing Information Protocol)
  - Dynamic Routing with Open Shortest Path First (OSPF)
  - Routing Table
- **Multicast Route**
  - Static Multicast
  - Distance Vector Multicast Routing Protocol (DVMRP)
  - Protocol Independent Multicast Sparse Mode (PIM-SM)
- **VRRP Setting**

Unicast Route

The Industrial Secure Router supports two routing methods: static routing and dynamic routing. Dynamic routing makes use of RIP V1/V1c/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 Industrial Secure Router forwards data for a specific subnet. The settings of the Static Route will be added to the routing table and stored in the Industrial Secure Router.

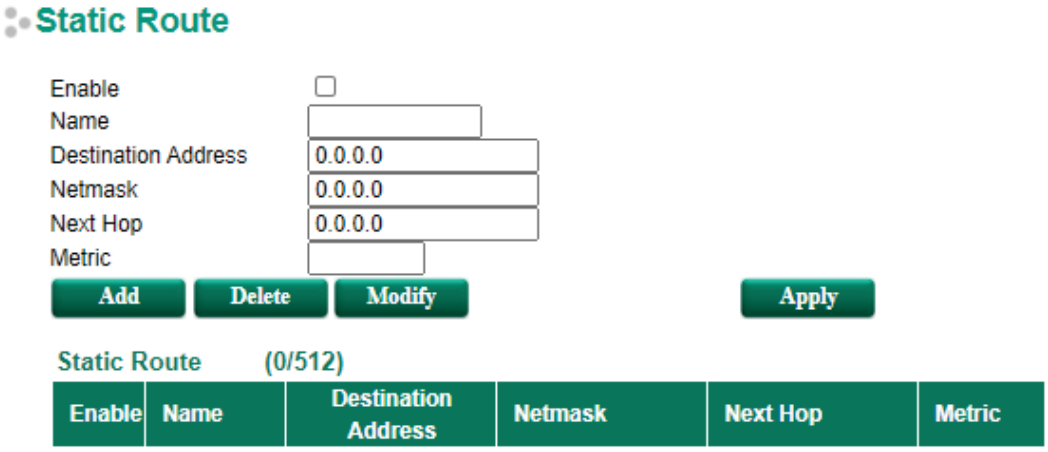
RIP (Routing Information Protocol)

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

The Industrial Secure 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 Industrial Secure Router's static routing table.



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

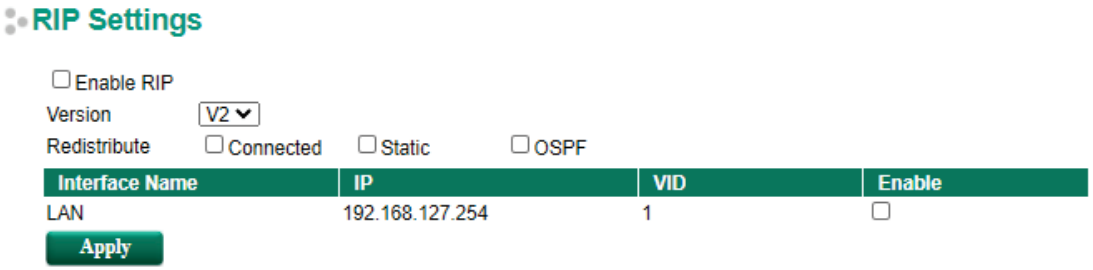
For modifying the content of a selected entry in the Static Routing Table.

NOTE The entries in the Static Routing Table will not be added to the Industrial Secure Router's routing table until you click the **Apply** 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	Description	Factory Default
Enable/Disable	Enable or Disable RIP protocol	Disable

Version

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

Redistribute

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
Connected	Check the checkbox to enable the Redistributed Connected function.	Unchecked
OSPF	Check the checkbox to enable the Redistributed OSPF function.	Unchecked

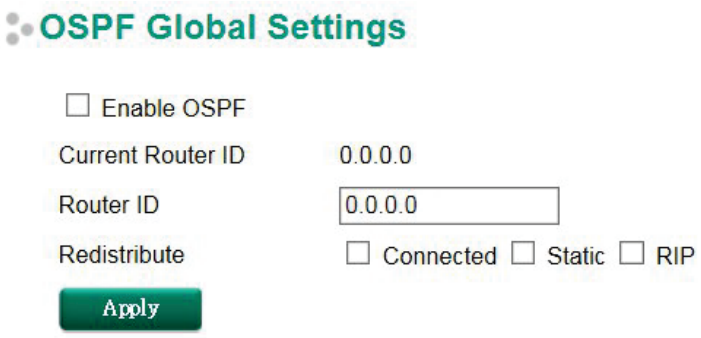
RIP Interface Table

Setting	Description	Factory Default
Enable/Disable	Check the checkbox to enable RIP for each interface.	Unchecked

Dynamic Routing with Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a dynamic routing protocol for use on Internet Protocol (IP) networks. Specifically, it is a link-state routing protocol, and falls into the group of interior gateway protocols, operating within a single autonomous system. As a link-state routing protocol, OSPF establishes and maintains neighbor
relationships in order to exchange routing updates with other routers. The neighbor relationship table is called an adjacency database in OSPF. OSPF forms neighbor relationships only with the routers directly connected to it. In order to form a neighbor relationship between two routers, the interfaces used to form the relationship must be in the same area. An interface can only belong to a single area. With OSPF enabled, Industrial Secure router is able to exchange routing information with other L3 switches or routers more efficiently in a large system.

OSPF Global Settings



Industrial Secure router has an OSPF router ID, customarily written in the dotted decimal format (e.g., 1.2.3.4) of an IP address. This ID must be established for every OSPF instance. If not explicitly configured, the default ID (0.0.0.0) will be regarded as the router ID. Since the router ID is an IP address, it does not need to be a part of any routable subnet on the network.

Enable OSPF

Setting	Description	Factory Default
Enable/Disable	This option is used to enable or disable the OSPF function globally.	Disable

Current Router ID

Setting	Description	Factory Default
Current Router ID	Shows the current ID of the Industrial Secure Router.	0.0.0.0

Router ID

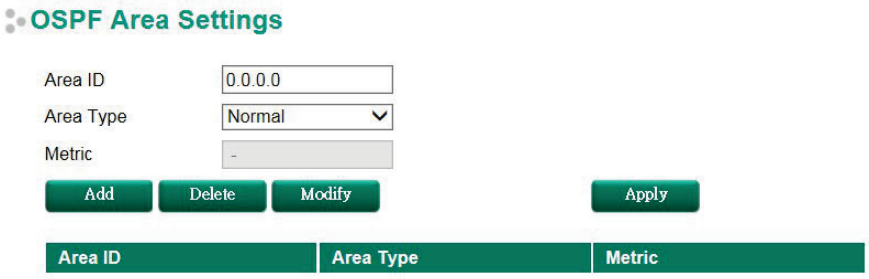
Setting	Description	Factory Default
Router ID	Sets each Industrial Secure Router's Router ID.	0.0.0.0

Redistributed

Setting	Description	Factory Default
Connected	Entries learned from the directly connected interfaces will be re-distributed if this option is enabled.	Unchecked (disable)
Static	Entries set in a static route will be re-distributed if this option is enabled.	Unchecked (disable)
RIP	Entries learned from the RIP will be re-distributed if this option is enabled.	Unchecked (disable)

OSPF Area Settings

An OSPF domain is divided into areas that are labeled with 32-bit area identifiers, commonly written in the dot-decimal notation of an IPv4 address. Areas are used to divide a large network into smaller network areas.
They are logical groupings of hosts and networks, including the routers connected to a particular area. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Thus, the topology of an area is unknown outside of the area. This reduces
the amount of routing traffic between parts of an autonomous system.



Area ID

Setting	Description	Factory Default
Area ID	Defines the areas that this Industrial Secure Router connects to.	0.0.0.0

Area Type

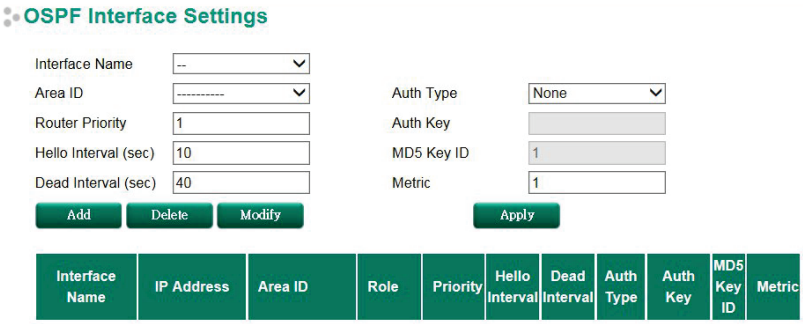
Setting	Description	Factory Default
Normal/Stub/NSSA	Defines the area type.	Normal

Metric

Setting	Description	Factory Default
Metric	Defines the metric value.	N/A

OSPF Interface Setting

Before using OSPF, you need to assign an interface for each area. Detailed information related to the interface is defined in this section.



Interface Name

Setting	Description	Factory Default
Interface Name	Defines the interface name.	LAN

Area ID

Setting	Description	Factory Default

Area ID	Defines the Area ID.	N/A

Router Priority

Setting	Description	Factory Default
Router Priority	Defines Industrial Secure Router's priority.	1

Hello Interval (sec)

Setting	Description	Factory Default
Hello Interval	Hello packets are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors. The hello packets are sent at a configurable interval (in seconds). The value of all hello intervals must be the same within a network.	10

Dead Interval (sec)

Setting	Description	Factory Default
Dead Interval	The dead interval is also a configurable interval (in seconds), and defaults to four times the value of the hello interval.	40

Auth Type

Setting	Description	Factory Default
None/Simple/MD5	OSPF authentication provides the flexibility of authenticating OSPF neighbors. Users can enable authentication to exchange routing update information in a secure manner. OSPF authentication can either be none, simple, or MD5. However, authentication does not need to be configured. If it is configured, all Industrial Secure Router on the same segment must have the same password and authentication method.	None

Auth Key

Setting	Description	Factory Default
Auth Key	• pure-text password if Auth Type = Simple • encrypted password if Auth Type = MD5	N/A

MD5 Key ID

Setting	Description	Factory Default
MD5 Key ID	MD5 authentication provides higher security than plain text authentication. This method uses the MD5 to calculate a hash value from the contents of the OSPF packet and the authentication key. This hash value is transmitted in the packet, along with a key ID.	1

Metric

Setting	Description	Factory Default
Metric	Manually set Metric/Cost of OSPF.	1

OSPF Virtual Link Settings

All areas in an OSPF autonomous system must be physically connected to the backbone area (Area 0.0.0.0). However, this is impossible in some cases. For those cases, users can create a virtual link to connect to the backbone through a non-backbone area and also use virtual links to connect two parts of a partitioned backbone through a non-backbone area.

Transit Area ID

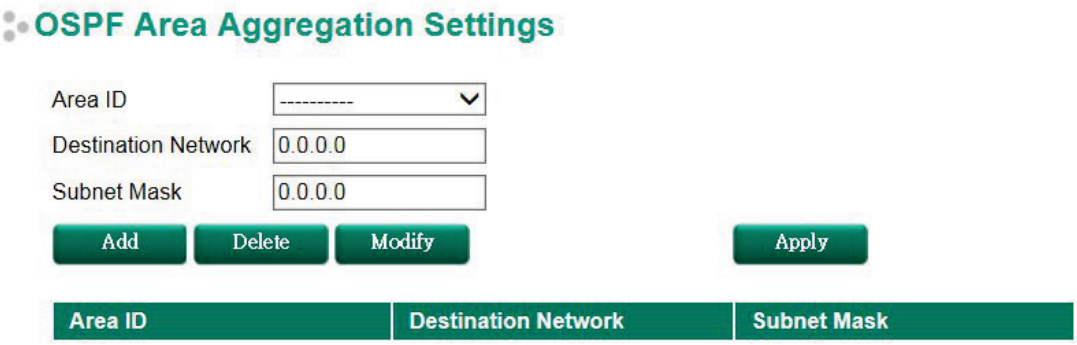
Setting	Description	Factory Default
Transit Area ID	Defines the areas that this Industrial Secure Router connect to.	N/A

Neighbor Router ID

Setting	Description	Factory Default
Neighbor Router ID	Defines the neighbor Industrial Secure Router's ID.	0.0.0.0

OSPF Area Aggregation Settings

Each OSPF area, which consists of a set of interconnected subnets and traffic, is handled by routers attached to two or more areas, known as Area Border Routers (ABRs). With the OSPF aggregation function, users can combine groups of routes with common addresses into a single routing table entry. The function is used to
reduce the size of routing tables.



Area ID

Setting	Description	Factory Default
Area ID	Select the Area ID that you want to configure.	N/A

Destination Network

Setting	Description	Factory Default
Destination Network	Fill in the network address in the area.	0.0.0.0

Subnet Mask

Setting	Description	Factory Default
4(240.0.0.0) to 30(255.255.255.252)	Select the network mask.	0.0.0.0

OSPF Neighbor Table

This is a table showing the current OSPF Neighbor table.

OSPF Neighbor Table

Page 1/1

Index	Neighbor Router ID	Priority	State	Neighbor IP Address	Interface Name

OSPF LSA Table

This is a table showing the current OSPF LSA information.

OSPF LSA Table

Page 1/1

Index	Area ID	LSA Type	Link State ID	Advertising Router	Aging Time	Route

Routing Table

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

Page 1/1 All

Index	Type	Destination Address	Next Hop	Interface Name	Metric
1	default	0.0.0.0/0	192.168.2.254	wan1	0
2	connected	100.100.100.0/24	100.100.100.254	lan	0
3	connected	192.168.2.0/24	192.168.2.74	wan1	0

Routing Entry List Settings

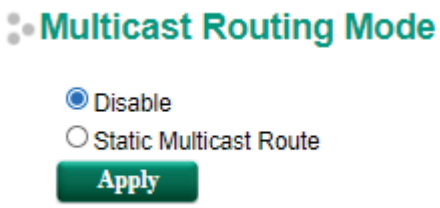
Setting	Description	Factory Default
All	Show all routing entries	N/A
Connected	Show connected routing entries	N/A
Static	Show Static routing entries	N/A
RIP	Show RIP routing entries	N/A
OSPF	Show OSPF routing entries	N/A

Multicast Route

The industrial secure router supports one multicast routing protocol: Static Multicast Route.

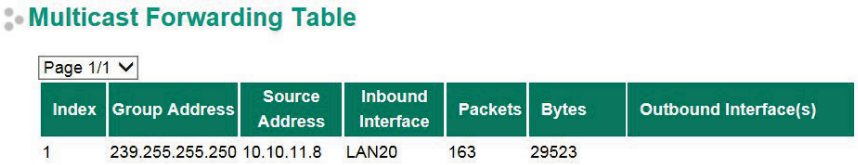
Global setting

Only one multicast routing protocol can be enabled in one industrial secure router. Please select the multicast protocol that suits your application best.

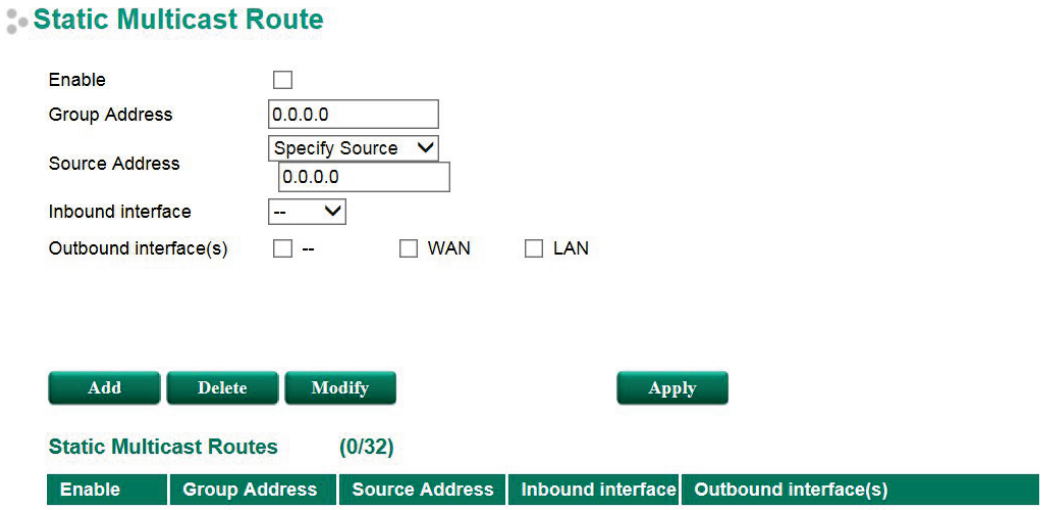


Setting	Description	Factory Default
Check/Uncheck	Disable multicast routing mode or select which multicast routing protocol is used (Static multicast route)	Disable

This is a table showing the current Multicast Forwarding table.



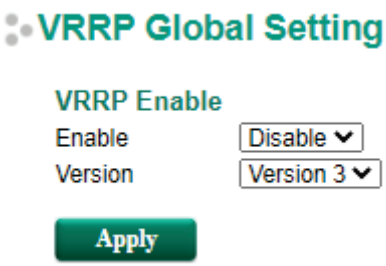
Static Multicast



VRRP Setting

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.

Global Setting



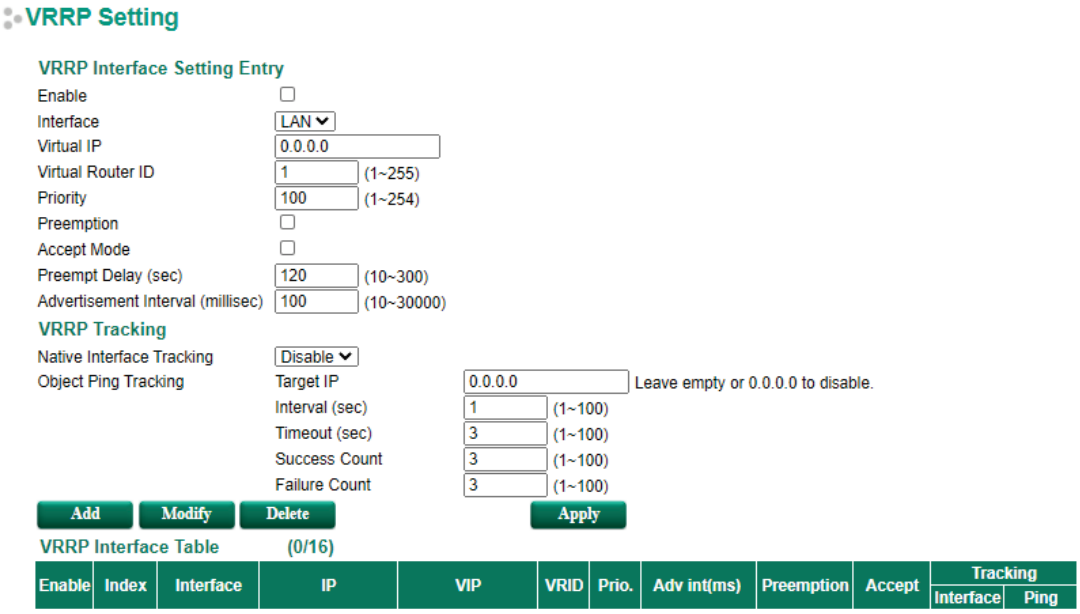
Enable

Setting	Description	Factory Default
Enable	Enables all VRRP interface	Disable

Version

Setting	Description	Factory Default
Version	Choose the VRRP version	Version 3

VRRP Setting



VRRP Interface Setting Entry

Setting	Description	Factory Default
Enable	Enables VRRP.	Uncheck
Interface	Select the interface where you want to enable VRRP, LAN or WAN interface.	LAN
Virtual IP (VIP)	Industrial secure routers in the same VRRP group have to be in the same subnet. Please note the virtual IP has to be the same subnet with real IP address.	0.0.0.0
Virtual Router ID (VRID)	Virtual Router ID is used to assign a VRRP group. The Industrial secure routers, which operate as master / backup, should have the same ID. Industrial secure routers support	1

	one virtual router ID for each interface. IDs can range from 1 to 255.	
Priority (Prio.)	Determines priority in a VRRP group. The priority value range is 1 to 255 and 255 is the highest priority. If several Industrial secure routers have the same priority, the router with the higher IP address has the higher priority. The usable range is "1 to 255".	100
Preemption	When the master is back alive, it determines whether the master will take the authority back or not.	Checked
Accept Mode	When Accept Mode is enabled, the virtual router with the role of Master allows others to access its own virtual IP address	Checked
Preemption Delay (sec)	When Preemption Delay is enabled, in order to prevent the master taking back authority before the network connection is ready, it is suggested for the master to wait for a defined period of time before taking authority back.	120
Advertisement Interval (sec)	For every defined period of time, the master will send packets to all slave devices to inform who the master is.	100

VRRP Tracking Enable

Setting	Description	Factory Default
Native Interface Tracking	Verify if master's next hub is still alive.	Disable

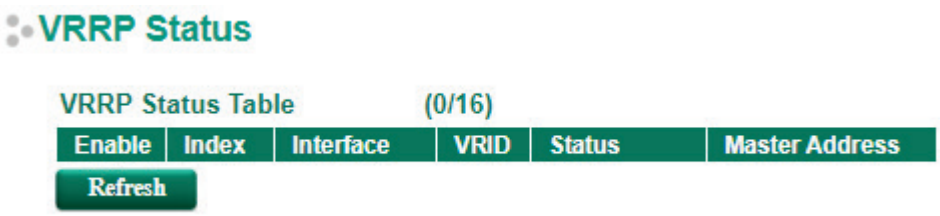
NOTE Before enabling the function "Native Interface Tracking", please make sure the WAN interface IP is set.

Object Ping Tracking

Setting	Description	Factory Default
Target IP	Verify if the connection to destination, e.g. control center, is workable.	0.0.0.0
Interval (sec)	How many seconds to ping destination to verify connection.	1
TimeOut (sec)	See how many seconds it takes for the ping response before timeout	3
Success Count	Know how many times the ping responds in order to know the connection is working.	3
Failure Count	Know how long until the ping does not respond in order to know the connection is not working.	3

VRRP Status

This is a table showing the current VRRP status.



5

Network Redundancy

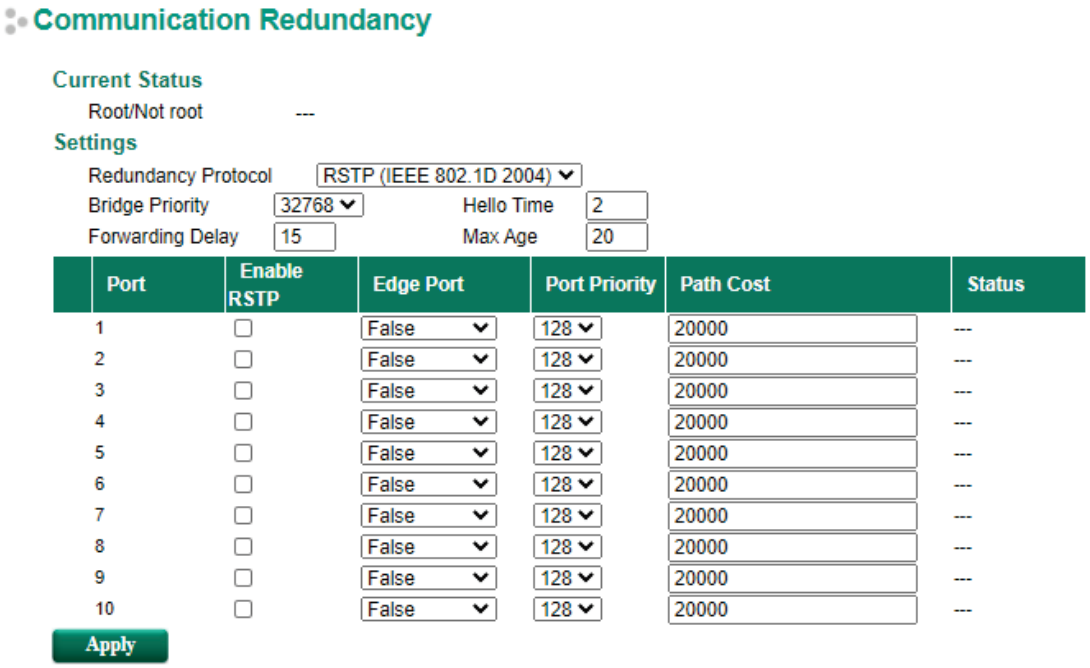
The following topics are covered in this chapter:

- **Layer 2 Redundant Protocols**
  - Configuring RSTP
  - Configuring Turbo Ring V2

Layer 2 Redundant Protocols

Configuring RSTP

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



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

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 Spanning Tree topology.	Disabled

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

Edge Port

Setting	Description	Factory Default
Force Edge	The port is fixed as an edge port and will always be in the forwarding state	Force edge
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

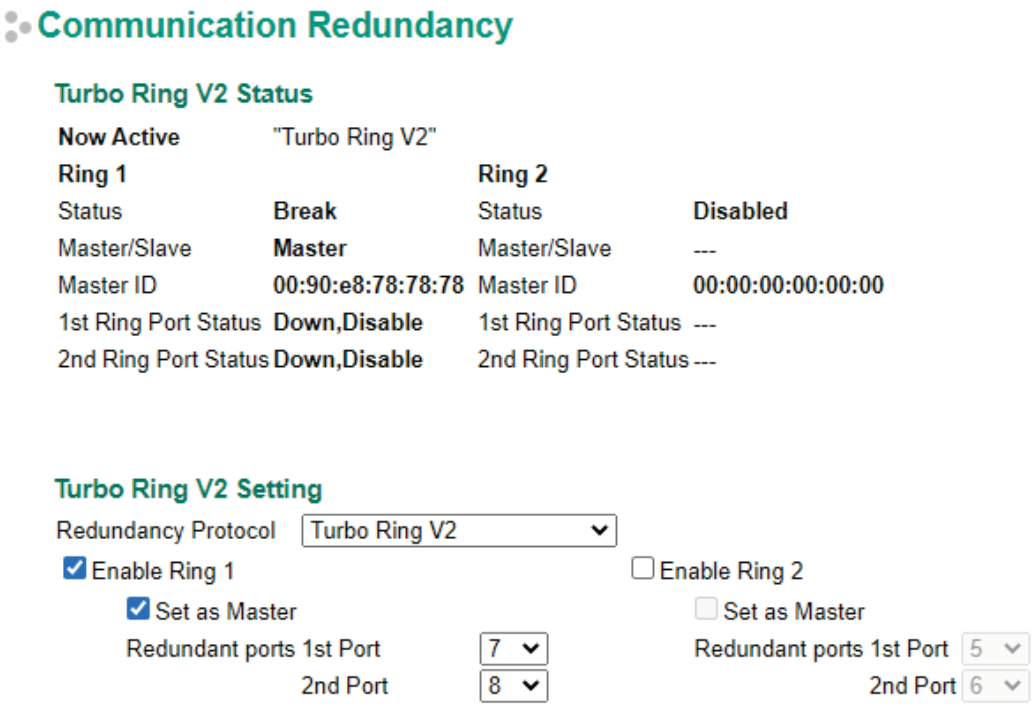
Port Cost

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



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

Explanation of "Current Status" Items

Now Active

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

Ring 1/2—Status

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

Ring 1/2—Master/Slave

It indicates whether or not this TN 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 1/2—1st Ring Port Status

Ring 1/2—2nd 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.	RSTP
RSTP (IEEE 802.1W/ 802.1D-2004)	Select this item to change to the RSTP configuration page.	

Enable Ring 1

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

Enable Ring 2*

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

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

Set as Master

Setting	Description	Factory Default
Enabled	Select this 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.	

6

Network Address Translation

The following topics are covered in this chapter:

- **Network Address Translation (NAT)**
  - NAT Concept
  - 1-to-1 NAT Overview
  - 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:

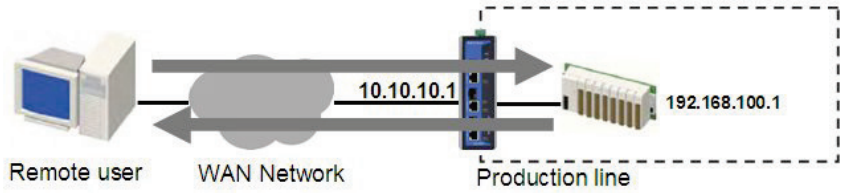
- Uses the N-1 or Port forwarding Nat function to hide the Internal IP address of a critical network or device to increase the level of security of industrial network applications.
- Uses the same private IP address for different, but identical, groups of Ethernet devices. For example, 1-to-1 NAT makes 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 Industrial Secure 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 Industrial Secure Router is 512.

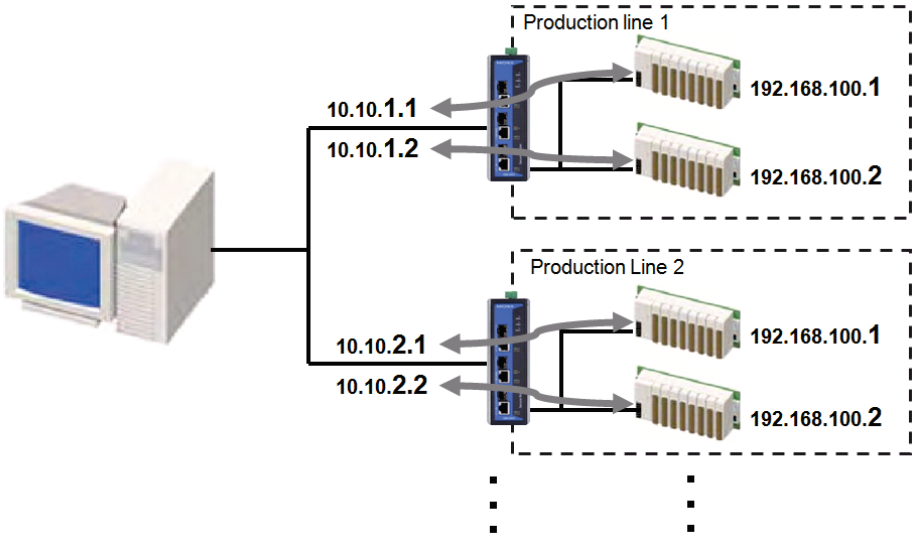
1-to-1 NAT Overview

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 Production Line 1

NAT List (2/512)

Status	Description	Index	Mode	Protocol	Original Packet (Condition)			Translated Packet (Action)		
					Incoming Interface	Src. IP : Port	Dst. IP : Port	Outgoing Interface	Src. IP : Port	Dst. IP : Port
✓	1-to-1_production_line_1-1	1	1-to-1	Any	WAN	Any:Any	10.10.1.1:Any	Any	Any:Any	192.168.100.1:Any
✓	1-to-1_production_line_1-2	2	1-to-1	Any	WAN	Any:Any	10.10.1.2:Any	Any	Any:Any	192.168.100.2:Any

1-to-1 NAT Setting in Production Line 2

NAT List (2/512)

Status	Description	Index	Mode	Protocol	Original Packet (Condition)			Translated Packet (Action)		
					Incoming Interface	Src. IP : Port	Dst. IP : Port	Outgoing Interface	Src. IP : Port	Dst. IP : Port
✓	1-to-1_production_line_2-1	1	1-to-1	Any	WAN	Any:Any	10.10.2.1:Any	Any	Any:Any	192.168.100.1:Any
✓	1-to-1_production_line_2-2	2	1-to-1	Any	WAN	Any:Any	10.10.2.2:Any	Any	Any:Any	192.168.100.2:Any

Network Address Translation

Enable ☑
Description
Index 1
NAT Mode 1-to-1
VRRP Binding --

Original Packet (Condition)
Incoming Interface LAN
Dstination IP 0.0.0.0

Translated Packet (Action)
Dstination IP 0.0.0.0

1-to-1 NAT

Enable

Setting	Description	Factory Default
Enable	Enable or disable the selected NAT policy	Checked

Description

Setting	Description	Factory Default
Description	Enter the name of the NAT rule	None

NAT Mode

Setting	Description	Factory Default
N-to-1 1-to-1 PAT	Select the NAT types	1-to-1

VRRP Binding

Setting	Description	Factory Default
VRRP Index No	Select which VRRP setting 1-to-1 NAT rule should work with	None

NOTE VRRP Binding function is only supported in 1-to-1 NAT. With selected VRRP setting, 1-to-1 NAT rule is valid when the system is the master. If no VRRP index is selected, 1-to-1 NAT rule will be valid regardless if the system is using master or backup.

Incoming Interface

Setting	Description	Factory Default
WAN, BRG_LAN, LAN	In the TN-4900, select WAN/LAN/BRG_LAN interface for NAT rule.	LAN

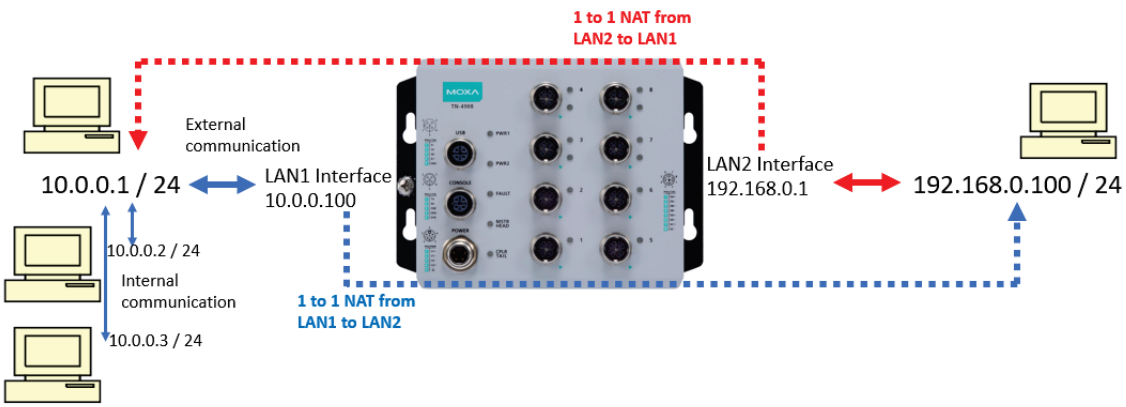
Destination IP (Original)

Setting	Description	Factory Default
IP Address	Set the public IP address which the internal IP will be translated into.	0.0.0.0

Destination IP (Translated)

Setting	Description	Factory Default
IP Address	Select the Internal IP address in LAN network area	0.0.0.0

Bidirectional 1-to-1 NAT



NAT List (2/512)

Status	Description	Index	Mode	Protocol	Original Packet (Condition)			Translated Packet (Action)		
					Incoming Interface	Src. IP : Port	Dst. IP : Port	Outgoing Interface	Src. IP : Port	Dst. IP : Port
✓		1	1-to-1	Any	LAN	Any:Any	192.168.0.1:Any	Any	Any:Any	10.0.0.1:Any
✓		2	1-to-1	Any	WAN	Any:Any	10.0.0.100:Any	Any	Any:Any	192.168.0.100:Any

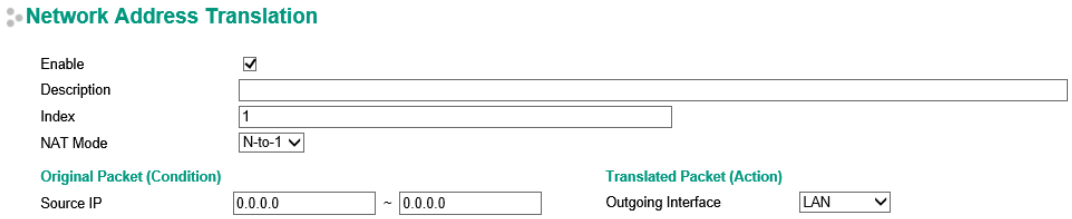
For some applications, devices need to talk to both internal devices and external devices without using a gateway. Bidirectional 1-to-1 NAT can do Network Address Translation in both directions without a gateway.

NOTE The Industrial Secure 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

Setting	Description	Factory Default
Enable	Enable or disable the selected NAT policy	Checked

Description

Setting	Description	Factory Default
Description	Enter the name of the NAT rule	None

NAT Mode

Setting	Description	Factory Default
N-to-1 1-to-1 PAT	Select the NAT types	N-to-1

Outgoing Interface

Setting	Description	Factory Default
WAN, LAN, BRG_LAN,	In the TN-4900, select WAN/LAN/BRG_LAN interface for NAT rule.	LAN

Source IP

Setting	Description	Factory Default
IP address	Select the Internal IP range for IP translation to WAN IP address	0.0.0.0

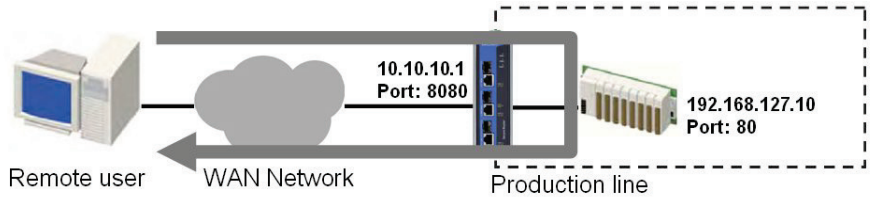
Port Forward

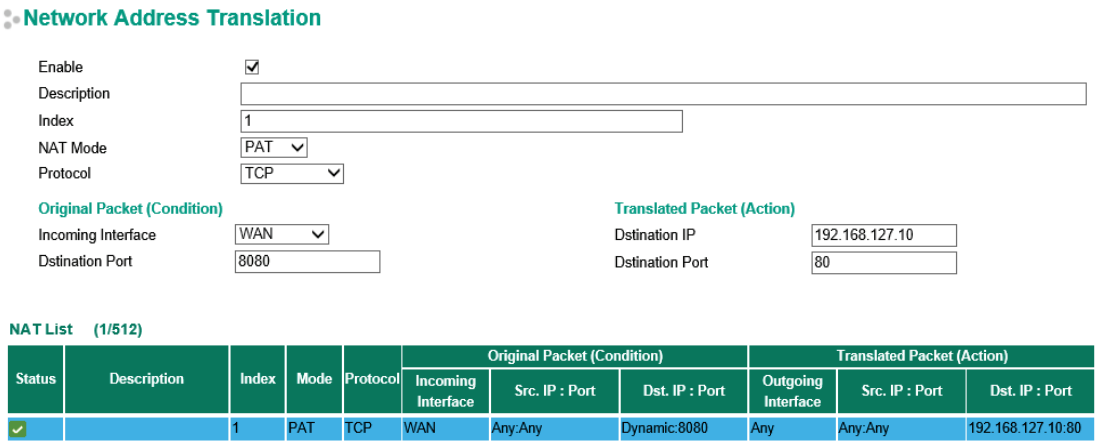
If the initial connection is from outside the LAN, but the user still wants to hide the Internal IP address, one way to do this is to use the Port Forwarding NAT function.

The user can specify the port number of an external IP address (WAN1 or WAN2) in the Port Forwarding policy list. For example, if the IP address of a web server in 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 web server

from external IP address 10.10.10.10 through port 8080. The Industrial Secure 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

Setting	Description	Factory Default
Enable	Enable or disable the selected NAT policy	Checked

Description

Setting	Description	Factory Default
Description	Enter the name of the NAT rule	None

NAT Mode

Setting	Description	Factory Default
N-to-1 1-to-1 PAT	Select the NAT types	PAT

Incoming Interface

Setting	Description	Factory Default
WAN, LAN, BRG_LAN,	Select the Interface for this NAT Policy	LAN

Protocol

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

Destination Port (Original)

Setting	Description	Factory Default
1 to 65535	Select a specific destination port number	0

Destination IP

Setting	Description	Factory Default
IP Address	The translated IP address in the internal network	0.0.0.0

Destination IP (Translated)

Setting	Description	Factory Default
1 to 65535	The translated port number in the internal network	0

7

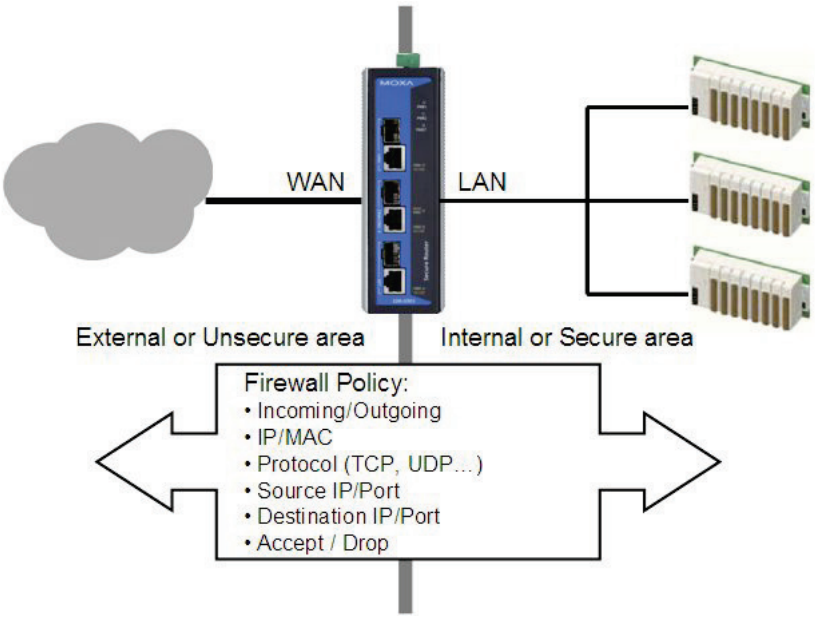
Firewall

The following topics are covered in this chapter:

- **Policy Concept**
- **Policy Overview**
- **Firewall**
  - Layer 2 policy
  - Layer 3 policy
  - Quick Automation Profile
  - Policy Check
- **Denial of Service (DoS) Defense**

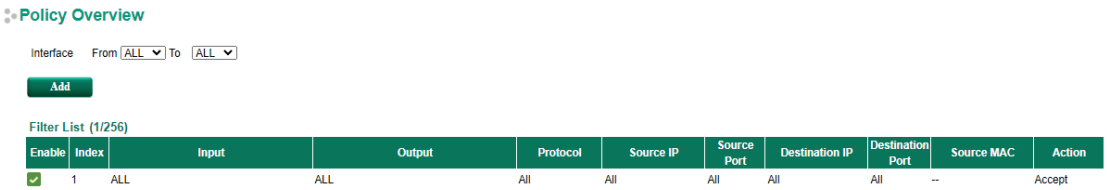
Policy Concept

A firewall device is commonly used to provide secure traffic control over an Ethernet network, as illustrated in the following figure. Firewall devices are deployed at critical points between an external network (the non-secure part) and an internal network (the secure part).



Policy Overview

The Industrial Secure Router provides a Firewall Policy Overview that lists firewall policies by interface direction.



Select the **From** interface and **To** interface and then click the **Show** button. The Policy list table will show the policies that match the **From-To** interface.

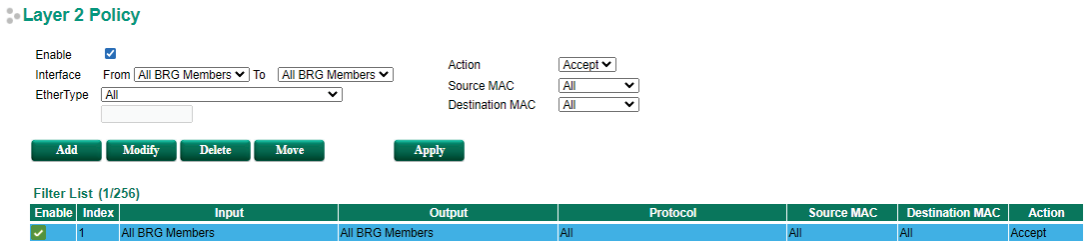
Interface From/To

Setting	Description	Factory Default
All (WAN/LAN)	Select the From Interface and To interface	From All to All
WAN		
LAN		

Firewall

Layer 2 policy

The TN-4900 firewall models provides an advanced Layer 2 firewall policy for secure traffic control, which depends on the following parameters. Layer 2 firewall policy can filter packets from bridge ports. Layer 2 policy priority is higher than L3 policy.



Interface From/To

Setting	Description	Factory Default
All (WAN/LAN)	Select the From Interface and To interface	From All to All
WAN		
LAN		

EtherType

Setting	Description	Factory Default
0x0600 to 0xFFFF	Select the Layer 2 protocol for this Firewall Policy. When Protocol is set to "Manual" you can set up EtherType manually	All

Action

Setting	Description	Factory Default
Accept	The packet will pass the Firewall when it matches the policy	Accept
Drop	The packet will not pass the Firewall when it matches this Firewall policy	

Source MAC

Setting	Description	Factory Default
All	This Firewall Policy will check all Source MAC addresses of the packet	N/A
Single	This Firewall Policy will check only check the specified Source MAC addresses of the packet	00:00:00:00:00:00

Destination MAC

Setting	Description	Factory Default
All	This Firewall Policy will check all Destination MAC addresses of the packet	N/A
Single	This Firewall Policy will check only check the specified Destination MAC addresses of the packet	00:00:00:00:00:00

The following table shows the Layer 2 protocol types commonly used in Ethernet frames.

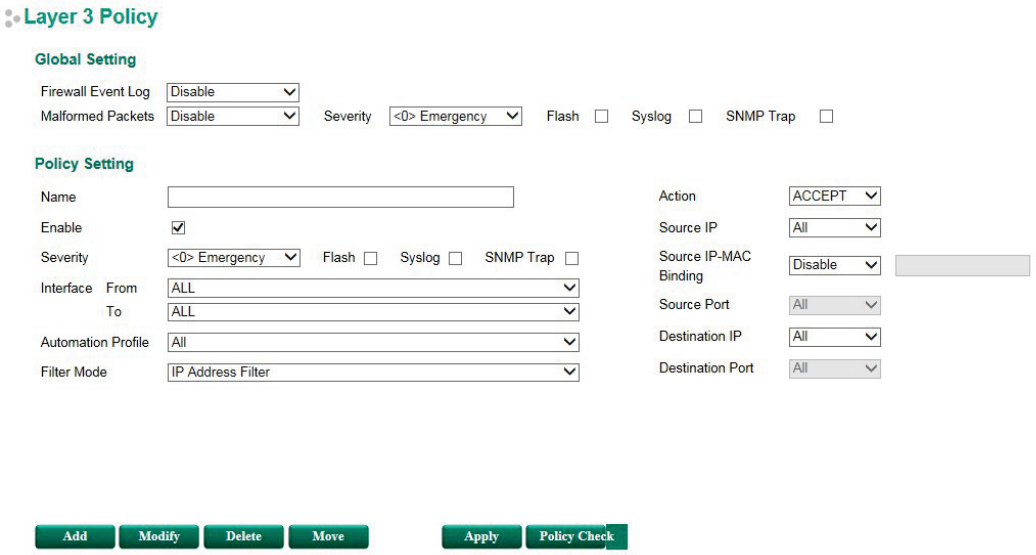
EtherType for Layer 2 Protocol

Type	Layer 2 Protocol
0x0800	IPv4 (Internet Protocol version 4)
0x0805	X.25
0x0806	ARP (Address Resolution Protocol)
0x0808	Frame Relay ARP
0x08FF	G8BPQ AX.25 Ethernet Packet
0x6000	DEC Assigned proto
0x6001	DEC DNA Dump/Load
0x6002	DEC DNA Remote Console
0x6003	DEC DNA Routing
0x6004	DEC LAT
0x6005	DEC Diagnostics

0x6006	DEC Customer use
0x6007	DEC Systems Comms Arch
0x6558	Trans Ether Bridging
0x6559	Raw Frame Relay
0x80F3	Appletalk AARP
0x809B	Appletalk
0x8100	8021Q VLAN tagged frame
0x8137	Novell IPX
0x8191	NetBEUI
0x86DD	IPv6 (Internet Protocol version 6)
0x880B	PPP
0x884C	MultiProtocol over ATM
0x8863	PPPoE discovery messages
0x8864	PPPoE session messages
0x8884	Frame-based ATM Transport over Ethernet
0x9000	Loopback

Layer 3 policy

The Industrial Secure Router's Firewall policy provides secure traffic control, allowing users to control network traffic based on the following parameters.



Global Setting

The Industrial Secure Router supports real-time event logs for Firewall, DoS, and VPN events. You can configure the system to save these logs locally in the flash or send them to the Syslog server and SNMP Trap server.

Enable Logging Firewall Events

Select **Enable** for the Firewall Event Log option to enable logging firewall events including dropped malformed packets and firewall allow/deny rule events. For firewall allow/deny rule event logs, users can select where to store these logs in the Policy Setting section.

Enable Malformed Packets

Enabling the **Malformed Packets** function will cause the firewall to drop malformed packets and store the event logs in the flash memory, send them to the syslog server, or to the SNMP trap server. It is possible to select multiple log storage options. Users can also set the severity of drop malformed packet logs.

Policy Setting

Name

Setting	Description	Factory Default
Description	Enter a name for the firewall rule	None

Enable

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

Severity

Setting	Description	Factory Default
<0> Emergency <1> Alert <2> Critical <3> Error <4> Warning <5> Notice <6> Informational <7> Debug	The severity of firewall event	<0> Emergency

Flash

Setting	Description	Factory Default
Check/Uncheck	Firewall white/black rules event logs is stored in flash, and will show in "Event Log "Table	Unchecked

Syslog/ SNMP trap

Setting	Description	Factory Default
Check/Uncheck	Industrial Secure Router send firewall white/ black rules event logs through syslog or SNMP trap	Unchecked

Interface From/To

Setting	Description	Factory Default
All (WAN/LAN)	Select the From Interface and To interface	From All to All
WAN		
LAN		

Automation Profile

Setting	Description	Factory Default
Refer to the "Quick Automation Profile" section.	Select the Protocol parameters in this Firewall Policy	All

Filter Mode

Setting	Description	Factory Default
IP Address Filter	This Firewall policy will filter by IP address	IP Address Filter
Source MAC Filter	This Firewall policy will filter by MAC address and source	

Action

Setting	Description	Factory Default
Accept	The packet will penetrate the firewall when it matches this firewall policy	Drop
Drop	The packet will not penetrate the firewall when it does not match this firewall policy	

Source IP

Setting	Description	Factory Default
All (IP Address)	This Firewall Policy will check all Source IP addresses in the packet	All
Single (IP Address)	This Firewall Policy will check single Source IP addresses in the packet	
Range (IP Address)	This Firewall Policy will check multiple Source IP addresses in the packet	

Source IP-MAC Binding

Setting	Description	Factory Default
Disable/Enable	The firewall policy will check source MAC address in the packet. Via this way, the IP Spoofing attack can be decreased	Disable

Source Port

Setting	Description	Factory Default
All (Port number)	This Firewall Policy will check all Source port numbers in the packet	All
Single (Port number)	This Firewall Policy will check single Source Port numbers in the packet	
Range (Port number)	This Firewall Policy will check multiple Source port numbers in the packet	

Destination IP

Setting	Description	Factory Default
All (IP Address)	This Firewall Policy will check all Destination IP addresses in the packet	All
Single (IP Address)	This Firewall Policy will check single Destination IP addresses in the packet	
Range (IP Address)	This Firewall Policy will check multiple Destination IP addresses in the packet	

Destination Port

Setting	Description	Factory Default
All (Port number)	This Firewall Policy will check all Destination port numbers in the packet	All
Single (Port number)	This Firewall Policy will check single Destination Port numbers in the packet	

Range (Port number)	This Firewall Policy will check multiple Destination port numbers in the packet	

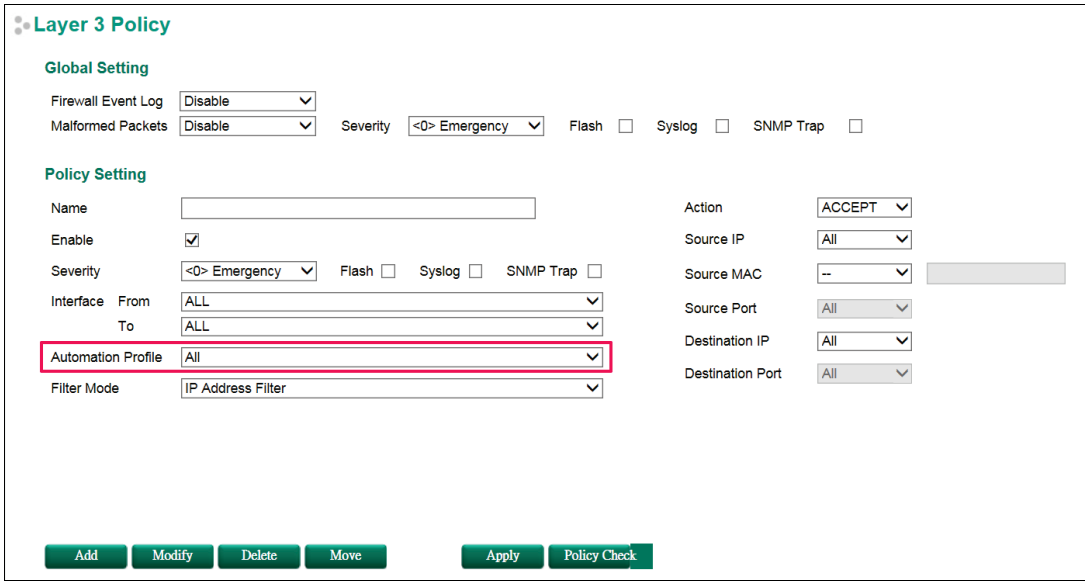
NOTE The Industrial Secure Router's firewall function will check if incoming or outgoing packets match the firewall policy. It starts by checking the packet with the first policy (Index=1); if the packet matches this policy, it will accept the packet immediately and then check the next packet. If the packet does not match this policy it will check with the next policy.

NOTE The maximum number of Firewall policies for the TN-4900 is 1024.

Quick Automation Profile

Ethernet Fieldbus protocols are popular in industrial automation applications. In fact, many Fieldbus protocols (e.g., EtherNet/IP and Modbus TCP/IP) can operate on an industrial Ethernet network, with the Ethernet port number defined by IANA (Internet Assigned Numbers Authority). The Industrial Secure Router provides an easy to use function called **Quick Automation Profile** that includes 45 different pre-defined profiles (Modbus TCP/IP, Ethernet/IP, etc.), allowing users to create an industrial Ethernet Fieldbus firewall policy with a single click.

For example, if the user wants to create a Modbus TCP/IP firewall policy for an internal network, the user just needs to select the **Modbus TCP/IP(TCP)** or **Modbus TCP/IP(UDP)** protocol from the **Protocol** drop-down menu on the **Firewall Policy Setting** page.



The following table shows the Quick Automation Profile for Ethernet Fieldbus Protocol and the corresponding port number

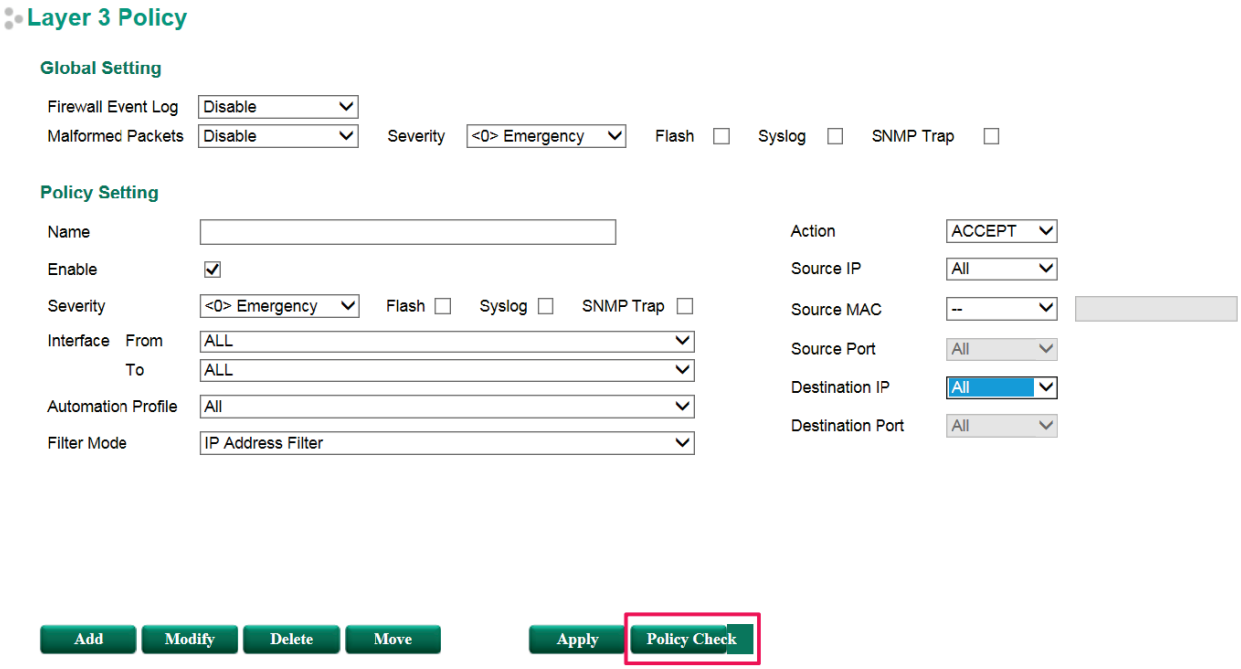
Ethernet Fieldbus Protocol	Port Number
EtherCat port (TCP)	34980
EtherCat port (UDP)	34980
EtherNet/IP I/O (TCP)	2222
EtherNet/IP I/O (UDP)	2222
EtherNet/IP Messaging (TCP)	44818
EtherNet/IP Messaging (UDP)	44818
FF Annunciation (TCP)	1089
FF Annunciation (UDP)	1089
FF Fieldbus Message (TCP)	1090

FF Fieldbus Message (UDP)	1090
FF System Management (TCP)	1091
FF System Management (UDP)	1091
FF LAN Redundancy Port (TCP)	3622
FF LAN Redundancy Port (UDP)	3622
LonWorks (TCP)	2540
LonWorks (UDP)	2540
LonWorks2 (TCP)	2541
LonWorks2 (UDP)	2541
Modbus TCP/IP (TCP)	502
Modbus TCP/IP (UDP)	502
PROFInet RT Unicast (TCP)	34962
PROFInet RT Unicast (UDP)	34962
PROFInet RT Multicast (TCP)	34963
PROFInet RT Multicast (UDP)	34963
PROFInet Context Manager (TCP)	34964
PROFInet Context Manager (UDP)	34964
IEC 60870-5-104 (TCP)	2404
IEC 60870-5-104 (UDP)	2404
DNP (TCP)	20000
DNP (UDP)	20000

The Quick Automation Profile also includes the commonly used Ethernet protocols listed in the following table:

Ethernet Protocol	**Port Number**
IPsec NAT Traversal (UDP)	4500
IPsec NAT traversal (TCP)	4500
FTP-data (TCP)	20
FTP-data (UDP)	20
FTP-control (TCP)	21
FTP-control (UDP)	21
SSH (TCP)	22
SSH (UDP)	22
Telnet (TCP)	23
Telnet (UDP)	23
HTTP (TCP)	80
HTTP (UDP)	80
IPsec (TCP)	1293
IPsec (UDP)	1293
L2F & L2TP (TCP)	1701
L2F & L2TP (UDP)	1701
PPTP (TCP)	1723
PPTP (UDP)	1723
Radius authentication (TCP)	1812
Radius authentication (UDP)	1812
RADIUS accounting (TCP)	1813
RADIUS accounting (UDP)	1813

Policy Check



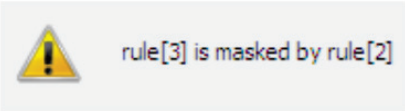
The Industrial Secure Router supports a **PolicyCheck** function for maintaining the firewall policy list. The **PolicyCheck** function detects firewall policies that may be configured incorrectly. **PolicyCheck** provides an auto detection function for detecting common configuration errors in the Firewall policy (e.g., **Mask**, **Include**, and **Cross conflict)**. When adding a new firewall policy, the user just needs to click the PolicyCheck button to check each policy; warning messages will be generated that can be used for further analysis. If the user decides to ignore a warning message, the Industrial Secure Router firewall will run on the configuration provided by the user. The three most common types of configuration errors are related to **Mask**, **Include**, and **Cross Conflict**. The Source/Destination IP range or Source/Destination port number of policy [X] is smaller or equal to policy[Y] but the action target (Accept/Drop) is different. For example, two firewall policies are shown below:

Index	Input	Output	Protocol	Source IP	Destination IP	Target
1	WAN1	LAN	ALL	10.10.10.10	192.168.127.10	ACCEPT
2	WAN2	LAN	ALL	20.20.20.10 to 20.20.20.30	192.168.127.20	ACCEPT

Suppose the user next adds a new policy with the following configuration:

Index	Input	Output	Protocol	Source IP	Destination IP	Target
3	WAN2	LAN	ALL	20.20.20.20	192.168.127.20	DROP

After clicking the **PolicyCheck** button, the Industrial Secure Router will issue a message informing the user that policy [3] is **masked** by policy [2] because the IP range of policy [3] is smaller than the IP range of policy [2], and the Target action is different.



Include: Policy [X] is included in Policy [Y]

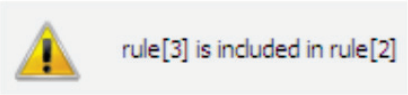
The Source/Destination IP range or Source/Destination port number of policy [X] is less than or equal to policy [Y], and the action target (Accept/Drop) is the same. In this case policy [X] will increase the loading of the Industrial Secure Router and lower its performance. For example, two firewall policies are shown in the following table:

Index	Input	Output	Protocol	Source IP	Destination IP	Target
1	WAN1	LAN	ALL	10.10.10.10	192.168.127.10	ACCEPT
2	WAN2	LAN	ALL	20.20.20.10 to 20.20.20.30	192.168.127.20	ACCEPT

Suppose the user next adds a new policy with the following configuration:

Index	Input	Output	Protocol	Source IP	Destination IP	Target
3	WAN2	LAN	ALL	20.20.20.20	192.168.127.20	ACCEPT

After clicking the PolicyCheck button, the Industrial Secure Router will issue a message informing the user that policy [3] is included in policy [2] because the IP range of policy [3] is smaller than the IP range of policy
[2], and the Target action is the same.



Cross Conflict: Policy [X] cross conflicts with Policy [Y]

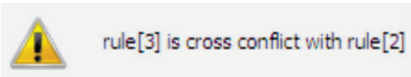
Two firewall policy configurations, such as Source IP, Destination IP, Source port, and Destination port, in policy [X] and policy [Y] are masked, and the action target (Accept/Drop) is different. For example, two firewall policies are shown in the following table:

Index	Input	Output	Protocol	Source IP	Destination IP	Target
1	WAN1	LAN	ALL	10.10.10.10	192.168.127.10	ACCEPT
2	WAN2	LAN	ALL	20.20.20.10 to 20.20.20.30	192.168.127.20	ACCEPT

Suppose the user next adds a new policy with the following configuration:

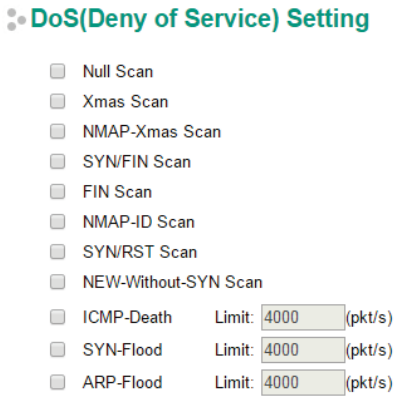
Index	Input	Output	Protocol	Source IP	Destination IP	Target
3	WAN2	LAN	ALL	20.20.20.25	192.168.127.20 to 192.168.127.30	DROP

The source IP range in policy 3 is smaller than policy 2, but the destination IP of policy 2 is smaller than policy 3, and the target actions (Accept/Drop) of these two policies are different. If the user clicks the **PolicyCheck** button, the Industrial Secure Router will issue a message informing the user that policy [3] is in **Cross Conflict** with policy [2].



Denial of Service (DoS) Defense

The Industrial Secure Router provides 9 different DoS functions for detecting or defining abnormal packet format or traffic flow. The Industrial Secure Router will drop the packets when it detects an abnormal packet format. The Industrial Secure Router will also monitor some traffic flow parameters and activate the defense process when abnormal traffic conditions are detected.



Null Scan

Setting	Description	Factory Default
Enable or Disable	Enable or disable the Null Scan	None

Xmas Scan

Setting	Description	Factory Default
Enable or Disable	Enable or disable the Xmas Scan	None

NMAP-Xmas Scan

Setting	Description	Factory Default
Enable or Disable	Enable or disable the NMAP-Xmas	None

SYN/FIN Scan

Setting	Description	Factory Default
Enable or Disable	Enable or disable the SYN/FIN Scan	None

FIN Scan

Setting	Description	Factory Default
Enable or Disable	Enable or disable the FIN Scan	None

NMAP-ID Scan

Setting	Description	Factory Default
Enable or Disable	Enable or disable the NMAP-ID Scan	None

SYN/RST Scan

Setting	Description	Factory Default
Enable or Disable	Enable or disable the SYN/RST Scan	None

EW-Without-SYN Scan

Setting	Description	Factory Default
Enable or Disable	Enable or disable the NEW-Without-SYN Scan protection	None

ICMP-Death

Setting	Description	Factory Default
Enable or Disable	Enable or disable the ICMP-Death defense	None
Limit (Packets/Second)	The limit value to activate ICMP-Death defense	None

SYN-Flood

Setting	Description	Factory Default
Enable or Disable	Enable or disable the Null Scan function	None
Limit (Packets/Second)	The limit value to activate SYN-Flood defense	None

ARP-Flood

Setting	Description	Factory Default
Enable or Disable	Enable or disable the ARP-Flood protection	None
Limit (Packets/Second)	The limit value to activate ARP-Flood protection	None

8

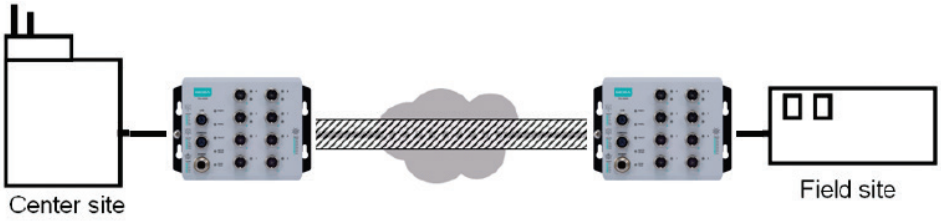
Virtual Private Network (VPN)

The following topics are covered in this chapter:

- **Overview**
- **IPsec Configuration**
  - Global Settings
  - IPsec Settings
  - IPsec Use Case Demonstration
  - IPsec Status
- **L2TP Server (Layer 2 Tunnel Protocol)**
  - L2TP Configuration
- **Examples for Typical VPN Applications**
  - Site-to-site IPsec VPN tunnel with Pre-Shared Key
  - Site to Site IPsec VPN tunnel with Jupiter System
  - L2TP for Remote User Maintenance

Overview

In this section we describe how to use the Industrial Secure Router to build a secure Remote Automation network with the VPN (Virtual Private Network) feature. A VPN provides a highly cost-effective solution of establishing secure tunnels, so that data can be exchanged in a secure manner.



There are two common applications for secure remote communication in an industrial automation network:

IPsec (Internet Protocol Security) VPN for LAN to LAN Security: Data communication only in a pre-defined IP range between two different LANs.

L2TP (Layer 2 Tunnel Protocol) VPN for Remote roaming User: It is for a remote roaming user with a dynamic IP to create a VPN. L2TP is a popular choice for remote roaming users for VPN applications because the L2TP VPN protocol is already built in to the Microsoft Windows operating system.

IPsec uses IKE (Internet Key Exchange) protocol for Authentication, Key exchange and provides a way for the VPN gateway data to be protected by different encryption methods.

There are 2 phases for IKE for negotiating the IPsec connections between 2 VPN gateways:

Key Exchange (IPsec Phase 1): The 2 VPN gateways will negotiate how IKE should be protected. Phase 1 will also authenticate the two VPN gateways by the matched Pre-Shared Key or X.509 Certificate.

Data Exchange (IPsec Phase 2): In Phase 2, the VPN gateways negotiate to determine additional IPsec connection details, which include the data encryption algorithm.

IPsec Configuration

IPsec configuration includes 5 parts:

- **Global Setting:** Enable or disable all IPsec Tunnels and NAT-Traversal functions
- **Tunnel Setting:** Set up the VPN Connection type and the VPN network plan
- **Key Exchange:** Authentication for 2 VPN gateways
- **Data Exchange:** Data encryption between VPN gateways
- **Dead Peer Detection:** The mechanism for VPN Tunnel maintenance

Global Settings

The Industrial Secure Router provides 3 Global Settings for IPsec VPN applications.

All IPsec Connection

Users can Enable or Disable all IPsec VPN services with this configuration.

NOTE The factory default setting is Disable, so when the user wants to use IPsec VPN function, make sure the setting is enabled.

IPsec NAT-T Enable

If there is an external NAT device between VPN tunnels, the user must enable the NAT-T (NAT-Traversal) function.

VPN Event Log

To enable the VPN event log function, select the **Enable** option in **Log Enable** and click **Flash**, **Syslog**, or **SNMP Trap**. You may also define the severity and record it in the event.

IPsec Settings

IPsec Quick Setting

The Industrial Secure Router's **Quick Setting** mode can be used to easily set up a site-to-site VPN tunnel for two Industrial Secure Router units.

When choosing the Quick setting mode, the user just needs to configure the following:

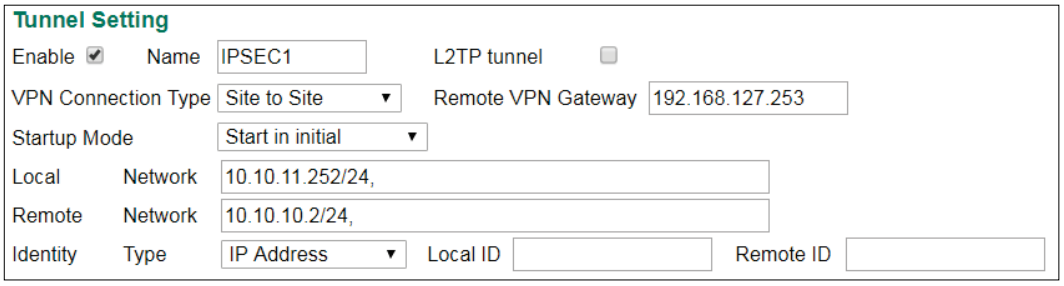
- Tunnel Setting
- Security Setting
  - Encryption Strength: Simple (AES-128), Standard (AES-192), Strong (AES-256)
  - Password of Pre-Shared Key
  - IKE Version: V1, V2

NOTE The Encryption strength, IKE Version, and Pre-Shared key should be configured identically for both Industrial Secure Router units.

IPsec Advanced Setting

Click **Advanced Setting** to configure detailed VPN settings.

Tunnel Setting



Enable or Disable VPN Tunnel

Setting	Description	Factory Default
Enable or Disable	Enable or Disable this VPN Tunnel	Disable

Name of VPN Tunnel

Setting	Description	Factory Default
Max. of 16 characters	User defined name of this VPN Tunnel.	None

NOTE The first character cannot be a number.

L2TP over IPsec Enable or Disable

Setting	Description	Factory Default
Enable or Disable	Enable or Disable L2TP over IPsec	None

VPN Connection Type

Setting	Description	Factory Default
Site to Site	VPN tunnel for Local and Remote subnets are fixed	Site to Site
Site to Site (Any)	VPN tunnel for Remote subnet area is dynamic and Local subnet is fixed	

Remote VPN Gateway

Setting	Description	Factory Default
IP Address	Remote VPN Gateway's IP Address	0.0.0.0

Startup Mode

Setting	Description	Factory Default
Start in Initial	This VPN tunnel will actively initiate the connection with the Remote VPN Gateway.	Start in Initial
Wait for Connecting	This VPN tunnel will wait remote VPN gateway to initiate the connection	

NOTE The maximum number of **Starts** in the initial VPN tunnel is 30. The maximum number of **Waits** for connecting to a VPN tunnel is 100.

Local Network

Setting	Description	Factory Default
Network	IP address of local VPN network/Subnet mask of local VPN network. Users can enter multiple local networks that build IPsec connections here. If there are two local networks, the user can enter their addresses 192.168.127.254/24,192.168.126.254/24 and then these two networks will build an IPsec connection with remote network.	192.168.127.0/24

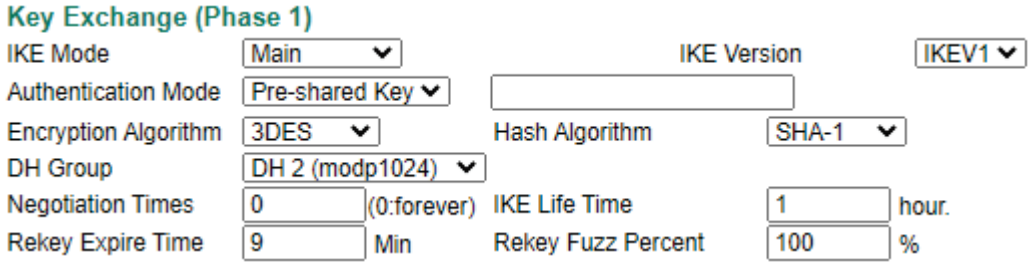
Remote Network

Setting	Description	Factory Default
Network	IP address of remote VPN network/Subnet mask of remote VPN network. Users can enter multiple remote networks that build IPsec connections here. If there are two remote networks, the user can enter their addresses (10.10.100.254/24, 10.10.110.254/24) and then these two networks will build an IPsec connection with local network.	None

Identity

Setting	Description	Factory Default
Type	There are four ID types for users to choose from: IP address, FQDN, Key ID, and Auto. Key ID is a string, which users can create by themselves. Auto (with Cisco) is for building connections for use with Cisco's systems.	Type: IP address Local ID: None Remote ID: None
Local ID	ID for identifying the VPN tunnel connection. The Local ID must be equal to the Remote ID of the connected VPN Gateway. Otherwise, the VPN tunnel cannot be established successfully	
Remote ID	ID for identifying the VPN tunnel connection. The Local ID must be equal to the Remote ID of the connected VPN Gateway. Otherwise, the VPN tunnel cannot be established successfully	

Key Exchange (IPsec phase I)



IKE Mode

Setting	Description	Factory Default
Main	In 'Main' IKE Mode, both the Remote and Local VPN gateway will negotiate which Encryption/Hash algorithm and DH groups can be used in this VPN tunnel; both VPN gateways must use the same algorithm to communicate	Main
Aggressive	In "Aggressive" Mode, the Remote and Local VPN gateway will not negotiate the algorithm; it will use the user's configuration only	

IKE Version

Setting	Description	Factory Default
IKEV1	Use the IKE Version 1 protocol	IKEV2
IKEV2	Use the IKE Version 2 protocol	

Authentication Mode

Setting	Description	Factory Default
Pre-Shared Key	When two systems use a Pre-Shared Key which users define as an authentication tool to build an IPsec VPN connection.	Pre-Shared Key
X.509	In this mode, two systems use certificates that users imported in advance in "Local Certificate" as an authentication tool to build an IPsec VPN connection. For the detailed workflow, please refer to User Scenario 1 and 2 later in this chapter.	N/A
X.509 With CA	In this mode, two systems use certificates that users imported in advance in "Local Certificate", and the CA that users imported in advance in "Trusted CA Certificate" as an authentication tool to build an IPsec VPN connection. For the	N/A

	detailed workflow, please refer to User Scenario 3, 4, and 5 later in this chapter.	

For the detailed workflow of X.509 and X.509 with CA, please refer to the user scenarios 1 to 5 below later in this chapter.

NOTE Certificates are a time related form of authentication. Before processing certificates, please ensure that the industrial secure router is synced with the local device. For more information about time sync, please refer to the Date and Time section.

Encryption Algorithm

Setting	Description	Factory Default
DES 3DES AES-128 AES-192 AES-256	Encryption Algorithm in key exchange	AES-256

Hash Algorithm

Setting	Description	Factory Default
Any MD5 SHA1 SHA-256	Hash Algorithm in key exchange	SHA-256

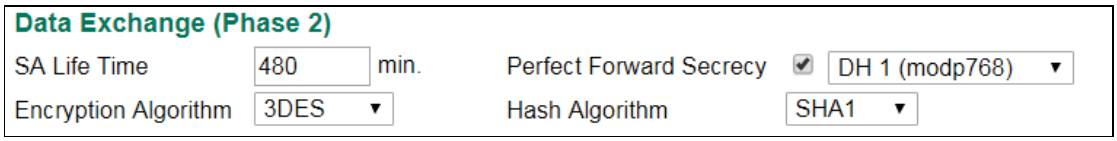
DH Group

Setting	Description	Factory Default
DH1(modp 768) DH2(modp 1024) DH5(modp 1536) DH14(modp 2048)	Diffie-Hellman groups (the Key Exchange group between the Remote and VPN Gateways)	DH2(modp 2048)

IKE Lifetime

Setting	Description	Factory Default
IKE lifetime (hours)	Lifetime for IKE SA	720 (hr)/43200 (min)

Data Exchange (IPsec phase II)



Perfect Forward Secrecy

Setting	Description	Factory Default
Enable or Disable	Uses different security keys for different IPsec phases in order to enhance security	Disable
DH1 (modp768) DH2 (modp1024) DH5 (modp1536) DH14 (modp2048)	Diffie-Hellman groups (the Key Exchange group between the Remote and VPN Gateways)	DH1 (modp2048)

SA Lifetime

Setting	Description	Factory Default
SA lifetime (minutes)	Lifetime for SA in Phase 2	43200 (min)

Encryption Algorithm

Setting	Description	Factory Default
DES 3DES AES-128 AES-192 AES-256	Encryption Algorithm in data exchange	AES-256

Hash Algorithm

Setting	Description	Factory Default
Any MD5 SHA1 SHA-256	Hash Algorithm in data exchange	SHA-256

Dead Peer Detection

Dead Peer Detection is a mechanism to detect whether or not the connection between a local secure router and a remote IPsec tunnel has been lost.

Action

Action when a dead peer is detected.

Setting	Description	Factory Default
Hold	Hold this VPN tunnel	Restart
Restart	Reconnect this VPN tunnel	
Clear	Clear this VPN tunnel	
Disable	Disable Dead Peer Detection	

Retry Interval

Setting	Description	Factory Default
Retry interval (seconds)	The period of dead peer detection messages	30 (sec)

Confidence Interval

Setting	Description	Factory Default
Confidence interval (seconds)	Timeout to check if the connection is alive or not	120 (sec)

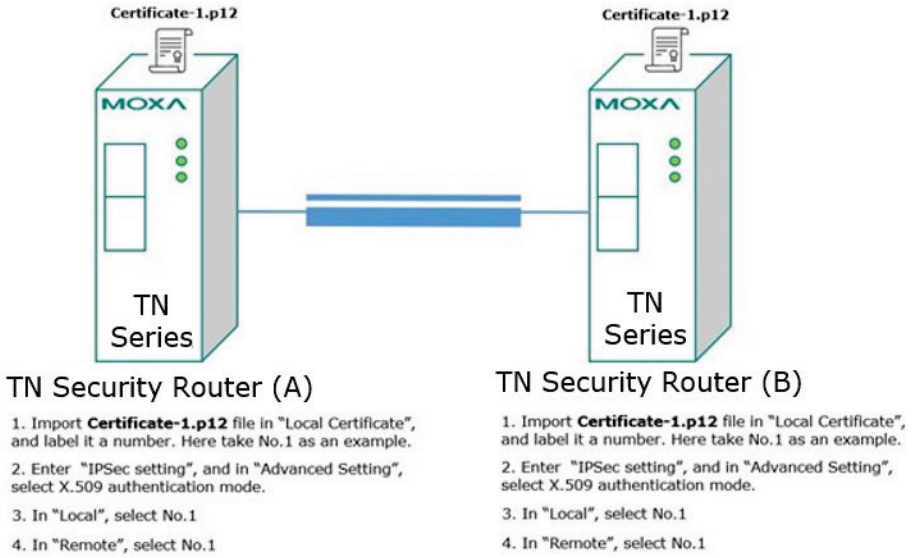
IPsec Use Case Demonstration

In the following section, we will consider five common user scenarios. The purpose of each example is to give a clearer understanding of two authentication modes 'X.509' and 'X.509 with CA'.

NOTE Certificates are a time related form of authentication. Before processing certificates, please ensure that the industrial secure router is synced with the local device. For more information about time sync, please refer to the Date and Time section.

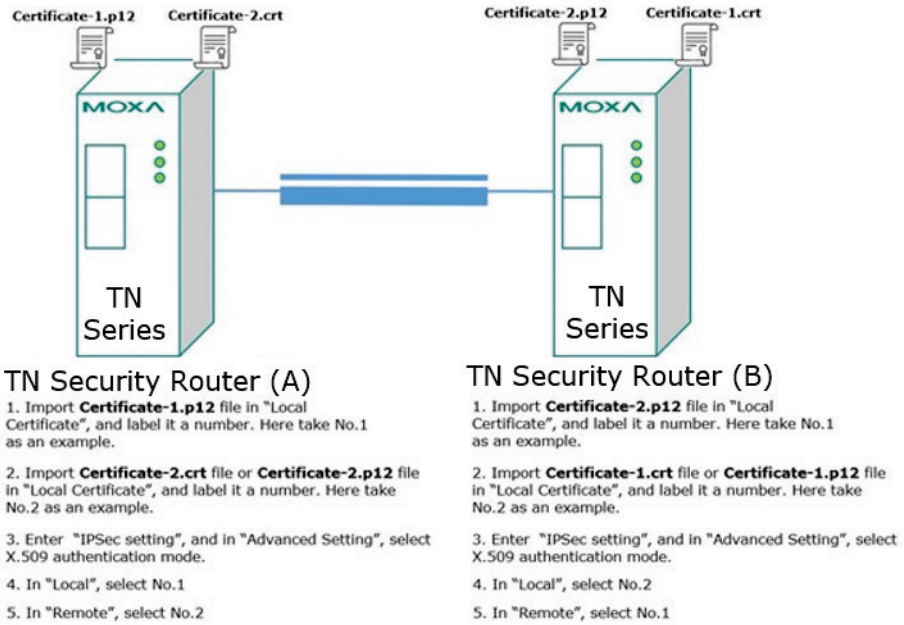
Scenario 1: X.509 Mode-One Certificate

Users will sometimes use certificates generated from a server or from the Internet. If users only get one certificate, they can import this certificate into a system. This system can then use the same certificate to identify other certificates and then build a VPN connection. In this case, users have to import certificates (.p12) into both sides. Please follow the steps in the diagram below to learn how to install certificates and build an IPsec VPN connection.



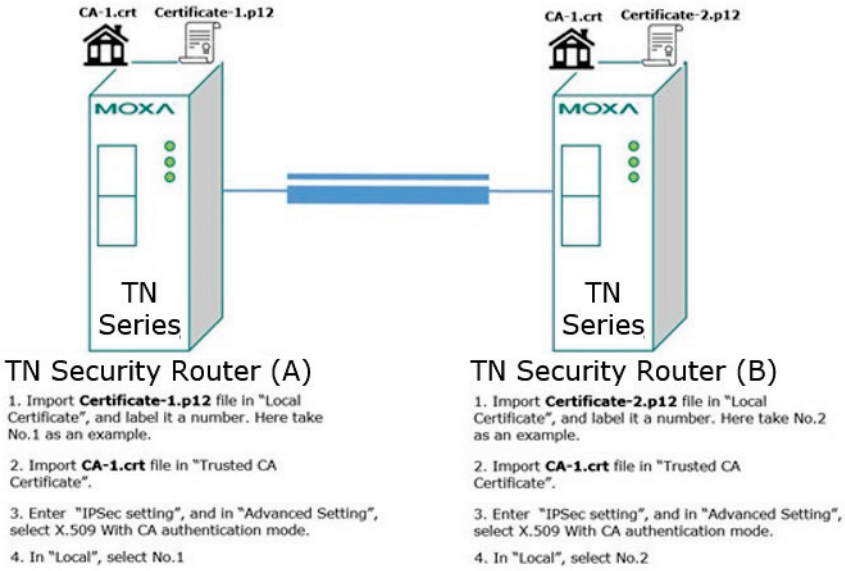
Scenario 2: X.509 Mode-Two Certificates

Users will sometimes use certificates generated from a server or from the Internet. If users get different certificates for different systems, users can import these certificates into systems accordingly. However, systems require all of these certificates to identify trusted systems before building an IPsec VPN connection. Taking two systems as an example: System A has certificate-1 (.p12) and System B has certificate-2 (.p12). To build an IPsec VPN connection, System A and B have to exchange certificates (.crt) with each other. And then Systems A and B need to install certificates (.crt) into their systems. Please follow the steps in the diagram below to learn how to install certificates and build an IPsec VPN connection.



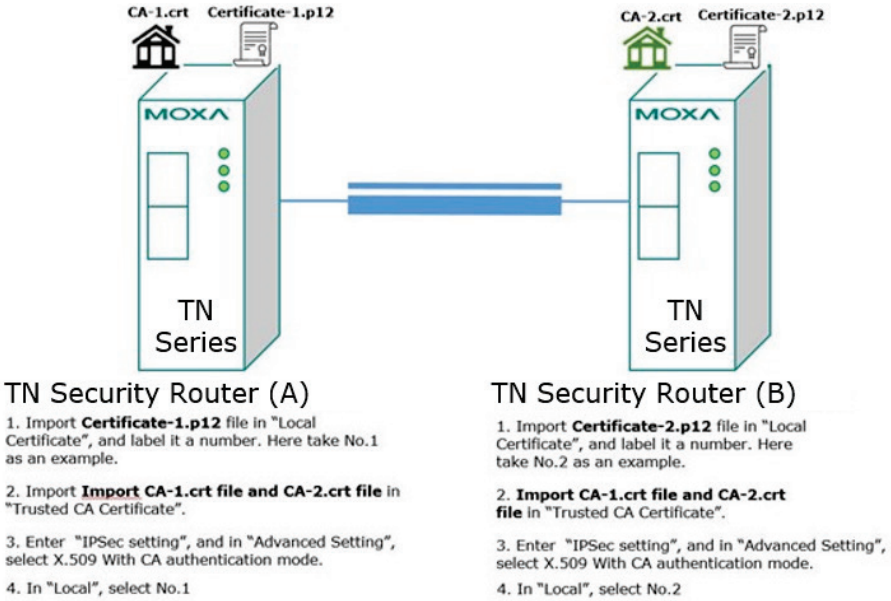
Scenario 3: X.509 with CA Mode-One CA

In X.509 mode, users have to install all certificates in all systems, which takes a lot of time and effort. To decrease users' effort, they can get the certificate from the CA (Certificate Authority). When using certificates from the CA, each system needs to install the same CA (.crt) to allow each system to identify different certificates from different systems. One condition is that every certificate should be issued by the same CA. Please follow the steps in the diagram below to learn how to install CA (.crt) and build an IPsec or OpenVPN connection.



Scenario 4: X.509 with CA Mode-Two CAs

In some large-scale systems, users may find it difficult to get certificates from one CA and therefore need to get certificates from different CAs. This scenario applies to the X.509 CA mode. The users have to install all CAs (.crt) into all systems. This means that every system can recognize certificates from different CAs, which allows identification of all the different systems. Please follow the steps in the diagram below to learn how to install CA (.crt) and certificate (.p12) in order to build an IPsec or OpenVPN connection.

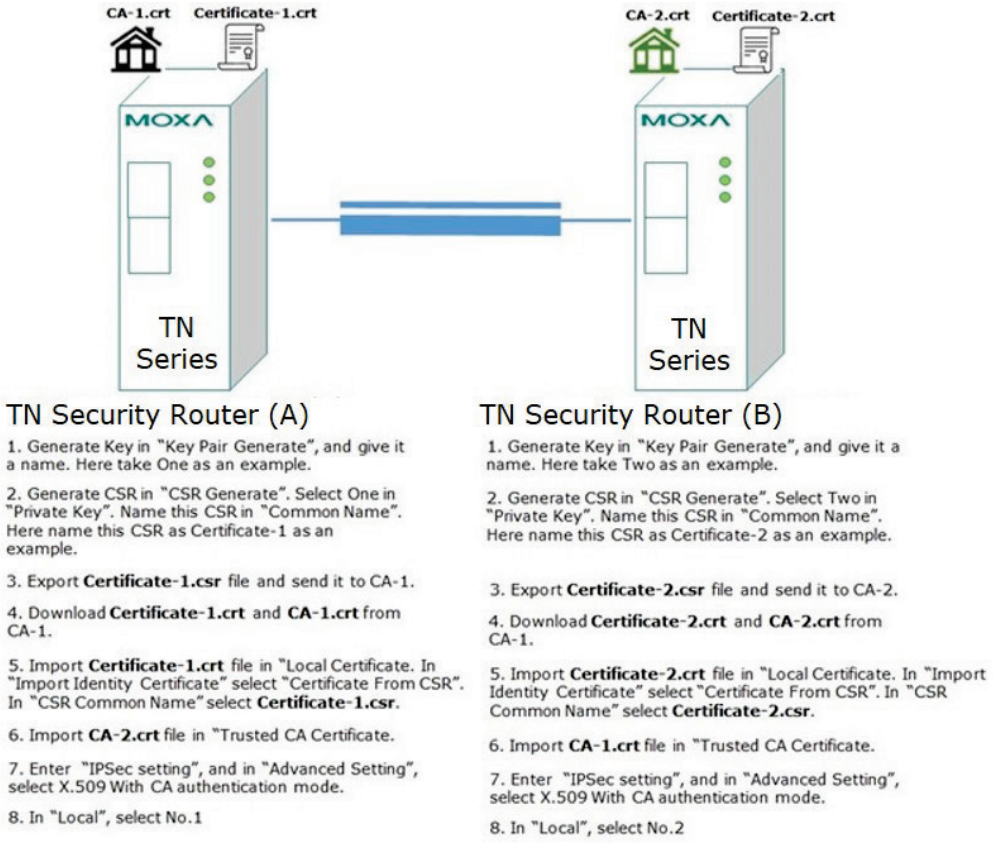


Scenario 5: X.509 with CA Mode-Certificate from CSR

For the previous four user scenarios, even when systems use certificates to identify each other before building a VPN connection, there is still a risk that someone can steal the certificate and pretend to be part of the trusted system.

To minimize this risk, there is a function called Certificate Signing Request (CSR) in X.509 with CA mode. CSR is a request issued by a single system for certificates issued by the CA. Through CSR, the certificate belongs only to one system and cannot be installed in other systems. By following this method, CSR significantly reduces the risk of certificates being used illegitimately.

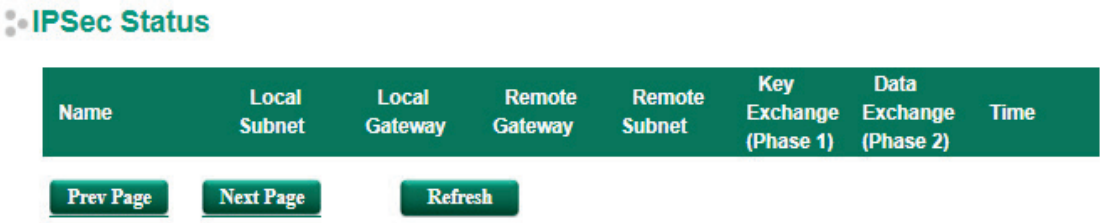
We will now consider an example using System A and System B. The CSR working model is System A or B issues a CSR (.csr) to the CA and then the CA updates the system with the certificate (.crt) and the CA file (.crt). Then, system A or B updates the other system with the CA file (.crt). System A or B installs certificates and the CA file in the system in order to build a VPN connection. Please follow the steps in the diagram below to learn how to install a CA file (.crt) and certificate (.crt) in order to build IPsec or OpenVPN connections.



IPsec Status

The user can check the VPN tunnel status in the **IPsec Status Table**.

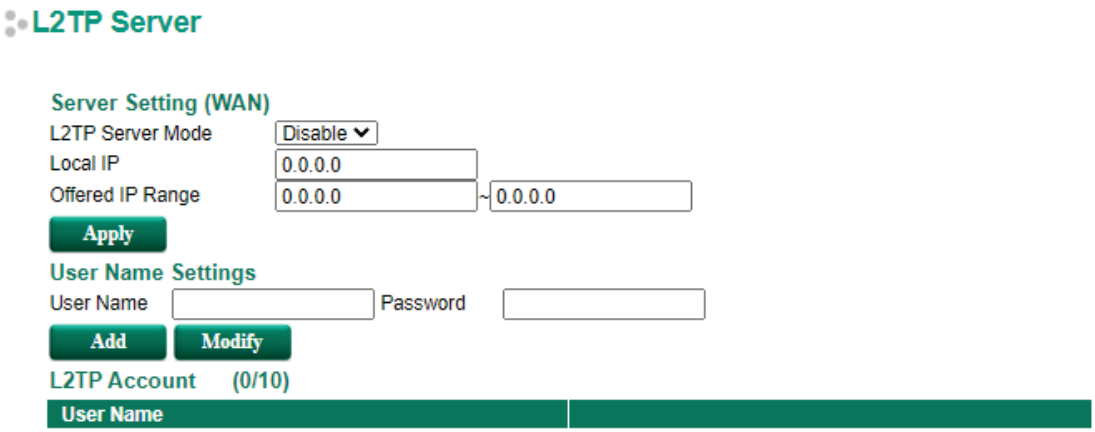
This list shows the name of the IPsec tunnel, IP address of the Local and Remote Subnet/Gateway, and the established status of the Key exchange phase and Data exchange phase.



L2TP Server (Layer 2 Tunnel Protocol)

L2TP is a popular choice for remote roaming users for VPN applications since an L2TP client is built in to the Microsoft Windows operating system. Since L2TP does not provide an encryption function, it is usually combined with IPsec to provide data encryption.

L2TP Configuration



The Industrial Secure Router supports up to 10 accounts with different user names and passwords.

L2TP Server Mode

Setting	Description	Factory Default
Enable / Disable	Enable or Disable the L2TP function on the WAN1 or WAN 2 interface	Disable

Local IP

Setting	Description	Factory Default
IP Address	The IP address of the Local Subnet	0.0.0.0

Offered IP Range

Setting	Description	Factory Default
IP Address	Offered IP range is for the L2TP clients	0.0.0.0

Login User Name

Setting	Description	Factory Default
Max. 32 characters.	User Name for L2TP connection	None

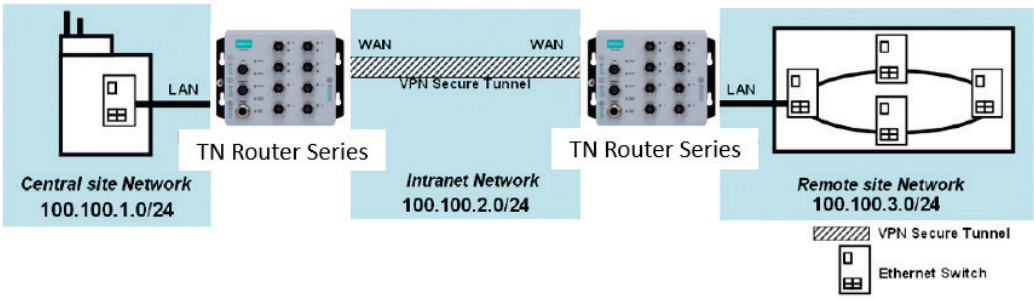
Login Password

Setting	Description	Factory Default
Max. 32 characters.	Password for L2TP connection	None

Examples for Typical VPN Applications

Site-to-site IPsec VPN tunnel with Pre-Shared Key

The following example shows how to create a secure LAN to LAN VPN tunnel between the Central site and Remote site via an Intranet network.



VPN Plan

- All communication from the Central site network (100.100.1.0/24) to the Remote site Network (100.100.3.0/24) needs to pass through the VPN tunnel.
- Intranet Network is 100.100.2.0/24
- The configuration of the WAN/LAN interface for 2 Industrial Secure Routers is shown in the following table.

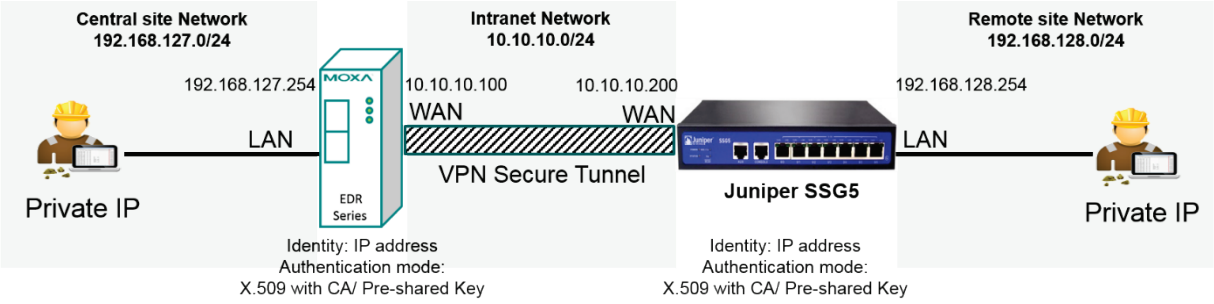
	Configuration	Industrial Secure Router (1)	Industrial Secure Router (2)
Interface Setting	WAN IP	100.100.2.1	100.100.2.2
	LAN IP	100.100.1.1	100.100.3.1

Based on the requirement and VPN plan, the recommended configuration for VPN IPsec is shown in the following table

	Configuration	Industrial Secure Router (1)	Industrial Secure Router (2)
Tunnel Setting	Connection Type	Site to Site	Site to Site
	Remote VPN gateway	100.100.2.2	100.100.2.1
	Startup mode	Wait for Connection	Start in Initial
	Local Network / Netmask	100.100.1.0 / 255.255.255.0	100.100.3.0 / 25.255.255.0
	Remote Network / Netmask	100.100.3.0 / 25.255.255.0	100.100.1.0 / 255.255.255.0
Key Exchange	Pre-Shared Key	12345	12345
Data Exchange	Encryption / Harsh	3DES / SHA1	3DES / SHA1

Site to Site IPsec VPN tunnel with Jupiter System

To build up a VPN tunnel, the central site router and remote site router have to know the identity of each other and use the same authentication mechanism to verify each other. Here we take Juniper SSG5 as an example to elaborate how the Industrial Secure Router can build an IPsec VPN connection with Juniper systems.



VPN Plan

All communication from the Central site network (192.168.127.0/24) to the Remote site Network (192.168.128.0/24) needs to pass through the VPN tunnel.
Intranet Network is 10.10.10.0/24

The configuration of the WAN/LAN interface for the Industrial Secure Routers and Juniper SSG5 is shown in the following table.

	Configuration	TN Series	Juniper SSG5
Router Setting	WAN IP	10.10.10.100	10.10.10.200
	LAN IP	192.168.127.254	192.168.128.254

Based on the requirement and VPN plan, the recommended configuration for VPN IPsec is shown in the following table:

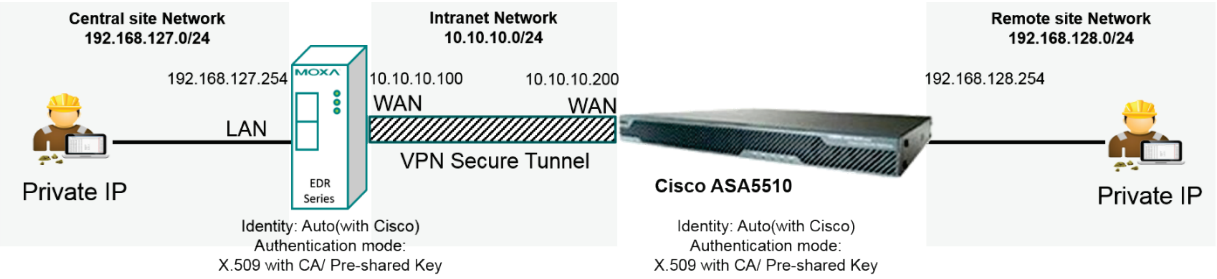
	Configuration	TN Series	Juniper SSG5
Tunnel Setting	Connection Type	Site to Site	Site to Site
	Remote VPN gateway	10.10.10.200	10.10.10.100
	Startup mode	Wait for Connection	Start in Initial
	Local Network / Netmask	192.168.127.0 / 255.255.255.0	192.168.128.0 / 25.255.255.0
	Remote Network / Netmask	192.168.128.0 / 25.255.255.0	192.168.127.0 / 255.255.255.0
	Identity	IP address Local ID: 10.10.10.100 Remote ID: 10.10.10.200	IP address Local ID: 10.10.10.200 Remote ID: 10.10.10.100
Key Exchange	Authentication mode	Pre-Shared Key or X.509 with CA	Pre-Shared Key or X.509 with CA
Data Exchange	Encryption / Harsh	3DES / SHA1	3DES / SHA1

Please note to build up a connection with Juniper systems, the identity should set as "**IP Address**" and authentication mode should set as "Pre-Shared Key or X.509 with CA". In the TN series compliance test with Juniper SSG5, identity except IP Address and authentication mode X.509 does not work in Juniper SSG5.
The Industrial Secure Router with Juniper compliance matrix is shown below:

TN Series VPN Setting to comply with Juniper System		Authentication mode		
		Pre-shared Key	X.509	X.509 With CA
Identity	IP Address	Comply	Not comply	Comply
	FQDN	Not Comply		
	Key ID			
	Auto (with Cisco)			

Site to Site IPsec VPN tunnel with Cisco system

To build up a VPN tunnel, the central site router and remote site router have to know the identity of each other and use the same authentication mechanism to verify each other. Here we take Cisco's ASA5510 as example to elaborate how the Industrial Secure Router builds an IPsec VPN connection with Cisco systems.



VPN Plan

All communication from the Central site network (192.168.127.0/24) to the Remote site Network (192.168.128.0/24) needs to pass through the VPN tunnel.
Intranet Network is 10.10.10.0/24
The configuration of the WAN/LAN interface for the Industrial Secure Routers and Cisco ASA5510 is shown in the following table:

	Configuration	TN Series	Cisco ASA5510
Router Setting	WAN IP	10.10.10.100	10.10.10.200
	LAN IP	192.168.127.254	192.168.128.254

Based on the requirement and VPN plan, the recommended configuration for VPN IPsec is shown in the following table

	Configuration	TN Series	Cisco ASA5510
Tunnel Setting	Connection Type	Site to Site	Site to Site
	Remote VPN gateway	10.10.10.200	10.10.10.100
	Startup mode	Wait for Connection	Start in Initial
	Local Network / Netmask	192.168.127.0 / 255.255.255.0	192.168.128.0 / 25.255.255.0
	Remote Network / Netmask	192.168.128.0 / 25.255.255.0	192.168.127.0 / 255.255.255.0
	Identity	Auto(with Cisco)	
Key Exchange	Authentication mode	Pre-Shared Key or X.509 with CA	Pre-Shared Key or X.509 with CA
Data Exchange	Encryption / Harsh	3DES / SHA1	3DES / SHA1

Please note to build up connection with Cisco systems, please base on your preferred authentication mode to decide which identity you prefer. Authentication modes including Pre-shared Key and X.509 with CA are supported when the Industrial Secure Router works with Cisco systems. However, X.509 is not supported in this case.

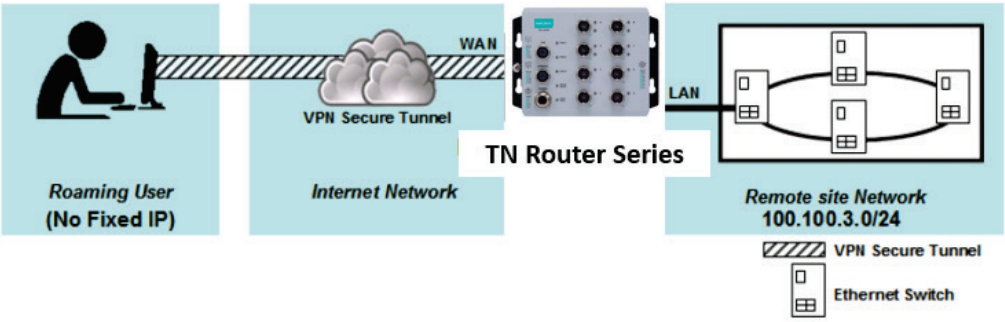
If you prefer Pre-shared Key, the identity can be set as "**IP Address**", "**FQDN**", "**Key ID**", or "**Auto (with Cisco)**". If you X.509 with CA, the identity should be set as "**Auto (with Cisco)**". The Industrial Secure Router with Cisco compliance matrix is shown below:

To simplify the setup process, the Industrial Secure Router supports an identity, called **"Auto(with Cisco)"**. No matter if Pre-shared Key or X.509 with CA is preferred, you can just select **"Auto(with Cisco)"** as identity.

TN Series VPN Setting to comply with Cisco System		**Authentication mode**		
		Pre-shared Key	X.509	X.509 With CA
Identity	IP Address	Comply	Not comply	Not comply
	FQDN	Comply		
	Key ID	Comply		
	Auto (with Cisco)	Comply		Comply

L2TP for Remote User Maintenance

The following example shows how a Roaming user uses L2TP over IPsec to connect to the remote site network.



VPN Plan

- All communication from the Roaming user (no fixed IP) to the Remote site Network (100.100.3.0/24) needs to pass through the VPN tunnel.
- Communication goes through the Internet.
- The configuration of the WAN/LAN interface for the Industrial Secure Router is shown in the following table.

	Configuration	**Industrial Secure Router (1)**
Interface Setting	WAN IP	100.100.2.1
	LAN IP	100.100.3.1

Based on the requirement and VPN plan, the recommended configuration for L2TP over IPsec is shown in the following table:

	Configuration	**Industrial Secure Router (1)**
L2TP Server Setting	L2TP Server Mode (WAN1)	Enable

	Local IP (L2TP Server IP)	100.100.4.1
	Offer IP Range	100.100.4.1 ~100.100.4.100
	Login User / Password	User01 / 12345
Tunnel Setting	Connection Type	Site to Site (Any)
	L2TP Tunnel	Enable
	Local Network	100.100.3.1 / 24 (Same as LAN Interface)
	Startup mode	Wait for Connection
Key Exchange	Pre-Shared Key	12345
Data Exchange	Encryption Algorithm Harsh Algorithm	3DES SHA1

9

Certificate Management

For the purposes of this document, certificate management refers to the X.509 SSL certificate. X.509 is a digital certificate method commonly used for IPsec, OpenVPN, and HTTPS authentication. The Industrial Secure Router can act as a Root CA (Certificate Authority) and issue a trusted Root Certificate. Alternatively, users can import certificates from other CAs into the Industrial Secure Router.

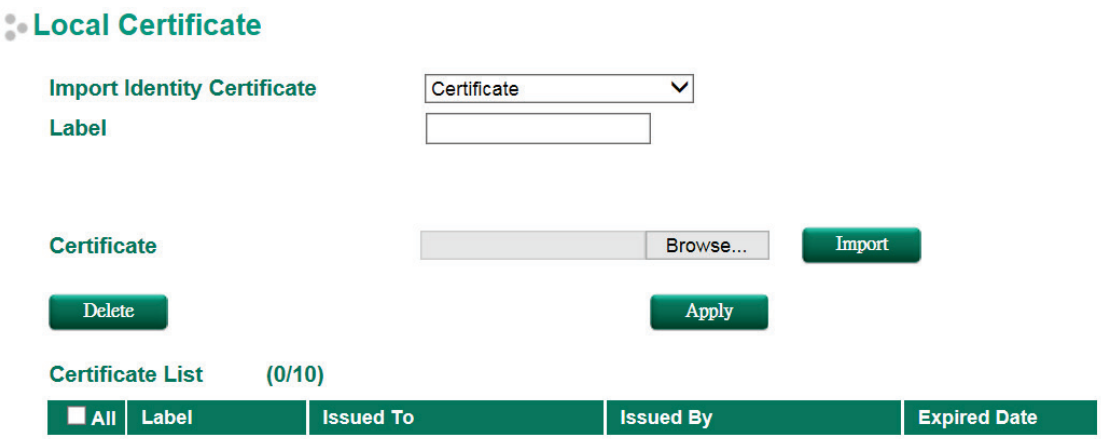
Certificates are a time related authentication mechanism. Before processing certificate management, please make ensure the industrial secure router is synced with the local device. For more details regarding time sync, please refer to section Date and Time

The following topics are covered in this chapter:

- **Local Certificate**
- **Trusted CA Certificates**
- **Certificate Signing Request**

Local Certificate

For Local Certificates, users can import certificates issued by the CA into the Industrial Secure Router.



Local Certificate

Import Identity Certificate

Setting	Description	Factory Default
Certificate/ Certificate from CSR/ Certificate from PKCS#12	Select the type of certificate the user has. Certificate uses the file extension .crt The certificate from CSR is a certificate issued by other CA Certificate from PKCS#12 uses the file extension .p12	Certificate

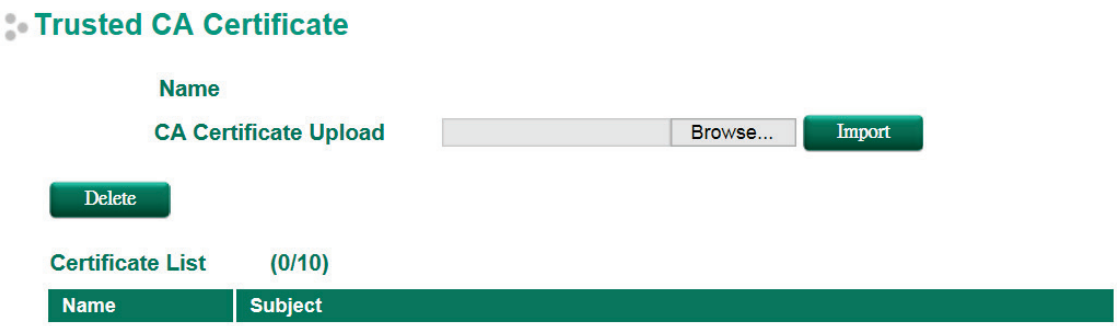
Label

Setting	Description	Factory Default
Label	No. of certificates	N/A

NOTE When importing the Certificate from PKCS#12, the user has to browse the certificate before typing Import Password.

Trusted CA Certificates

In Trusted CA Certificates, users can import a CA that the user trusts into the Industrial Secure Router. It is recommended that the user imports a trusted CA in advance. Otherwise, the Industrial Secure Router may not recognize the certificate and reject the connection.

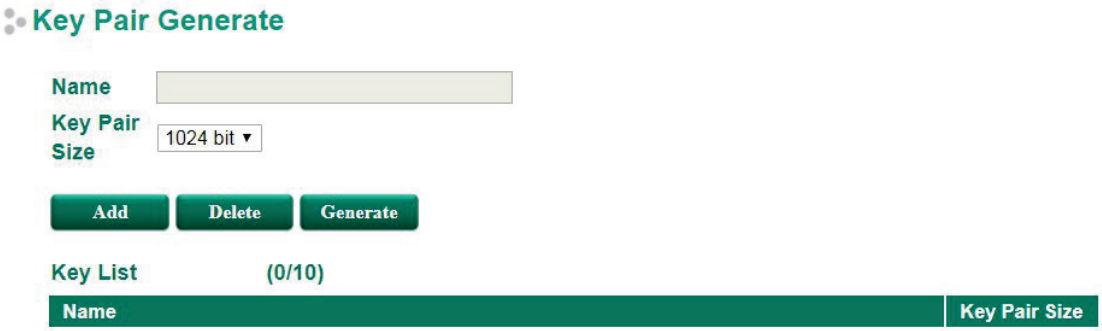


Certificate Signing Request

If the user wants to get a certificate from the CA for connection purposes, then the two steps below need to be followed in order to generate a private key and certificate signing request.

Step1: Generate Private Key

Before sending the Certificate Signing Request (CSR) to the CA, the CSR must include a public key that can be generated with a private key simultaneously. The user can use a private key to encrypt data and the receiver can use a public key to decrypt the data.



Key Pair Generate

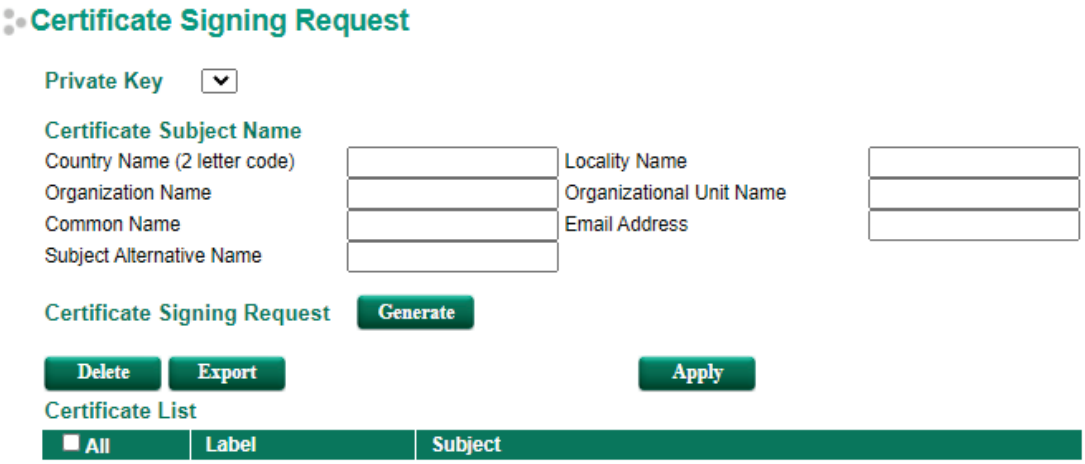
Name

Setting	Description	Factory Default
Name	Naming each private key	None

NOTE The user has to click **Add** before entering the name of each key.

Step2: Generate CSR

After generating the private key, the user can choose the key in Private Key and then must fill in all the information under **Certificate Subject Name**. After that, the user can click **Generate** to create the CSR and the CSR will be displayed in the **Certificate List**. To export the CSR, the user can simply choose the CSR in **Certificate List** and click **Export**.



Certificate Signing Request

Private Key

Setting	Description	Factory Default
Private Key	Choose the key generated in Key Pair Generate	None

10

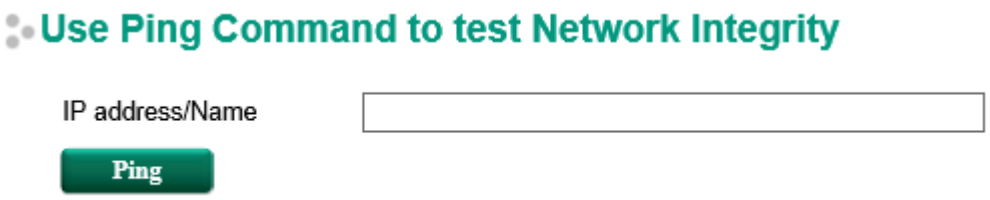
Diagnosis

The Industrial Secure Router provides **Ping** tools, **LLDP**, and **ARP** for administrators to diagnose network systems.

The following topics are covered in this chapter:

- **Ping**
- **LLDP**
- **ARP Table**

Ping



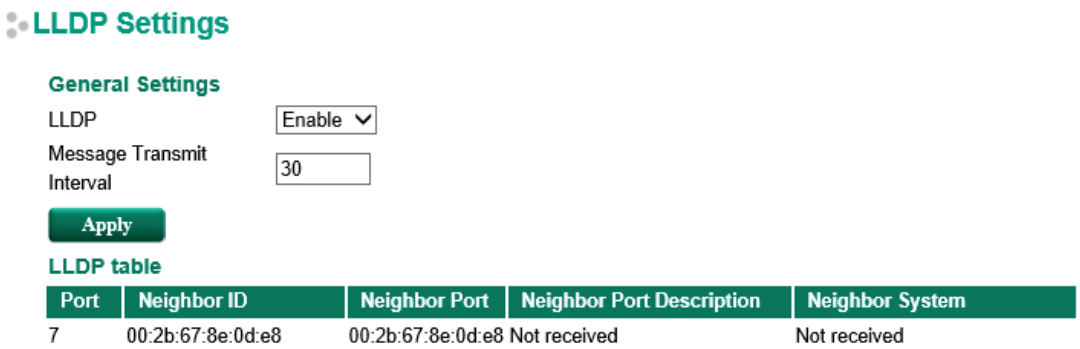
The Ping function uses the ping command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the Industrial Secure Router itself. In this way, the user can essentially control the Industrial Secure Router and send ping commands out through its ports. There one basic step required to set up the Ping command to test network integrity:

1. Type in the desired IP address, and click **Ping**.

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.



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.)

LLDP Table

The LLDP table displays the following information:

Field	Description
Port	The port number that connects to the neighbor device
Neighbor ID	A unique identifier (typically the MAC address) that identifies the neighbor device
Neighbor Port	The port number of the connecting neighbor device
Neighbor Port Description	The description of the neighbor device's interface
Neighbor System	The hostname of the neighbor device

ARP Table

The ARP table shows the device's Address Resolution Protocol (ARP) information.

11

Monitor

Through the Monitor section, you can keep track of the system and network performance, consult event logs.

The following topics are covered in this chapter:

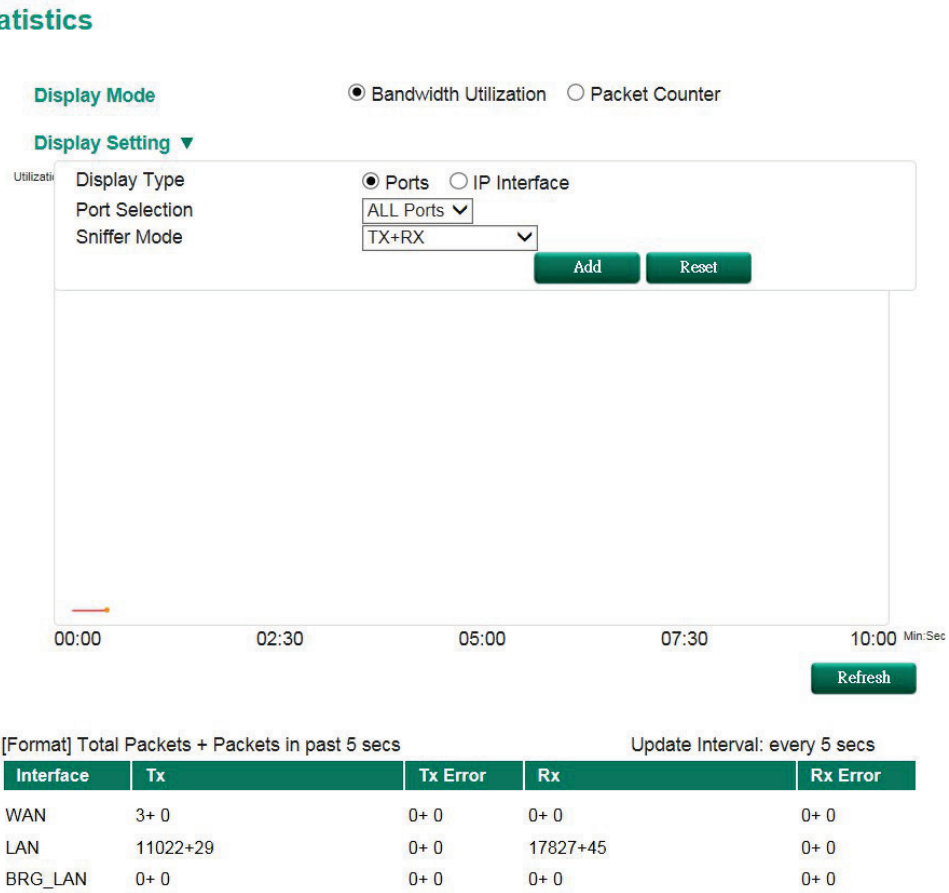
- **Statistics**
  - Bandwidth Utilization
  - Display Setting
  - Display Setting
- **Event Log**

Statistics

Users can monitor the data transmission activity of all the Industrial Secure Router ports from two perspectives, **Bandwidth Utilization** and **Packet Counter**. The graph displays data transmission activity by showing Utilization/Sec or Packet/Sec (i.e., packets per second, or pps) versus Min:Sec. (Minutes: Seconds). The graph is updated every 5 seconds, allowing the user to analyze data transmission activity in real-time.

Bandwidth Utilization

In **Bandwidth Utilization** mode, users can monitor total bandwidth in each interface (**IP Interface)**, each port or port group (**Ports**). In addition to display type, users can configure which packet flow is monitored, **TX Packets**, **RX Packets** or both (**TX/RX**). **TX Packets** are packets sent out from the Industrial Secure Router, and **RX Packets** are packets received from connected devices.



Display Mode

Setting	Description	Factory Default
Bandwidth Utilization/ Packet Counter	Graph display traffic bandwidth/Graph display total packet amount per second	Packet Counter

Display Setting

Display Type

Setting	Description	Factory Default
Port	Monitor total traffic per port or group port (FE Ports/ GE Ports)	IP Interface

IP Interface	Monitor total traffic per interface, e.g. LAN, WAN, Bridge	

Port Selection

Setting	Description	Factory Default
ALL Ports/FE Ports/GE Ports/Port1/Port2/Port3/Port4/Port5/Port6/Port7/Port8/Port16	Users can select which port or port group they want to monitor traffic from	ALL Ports

Interface Selection

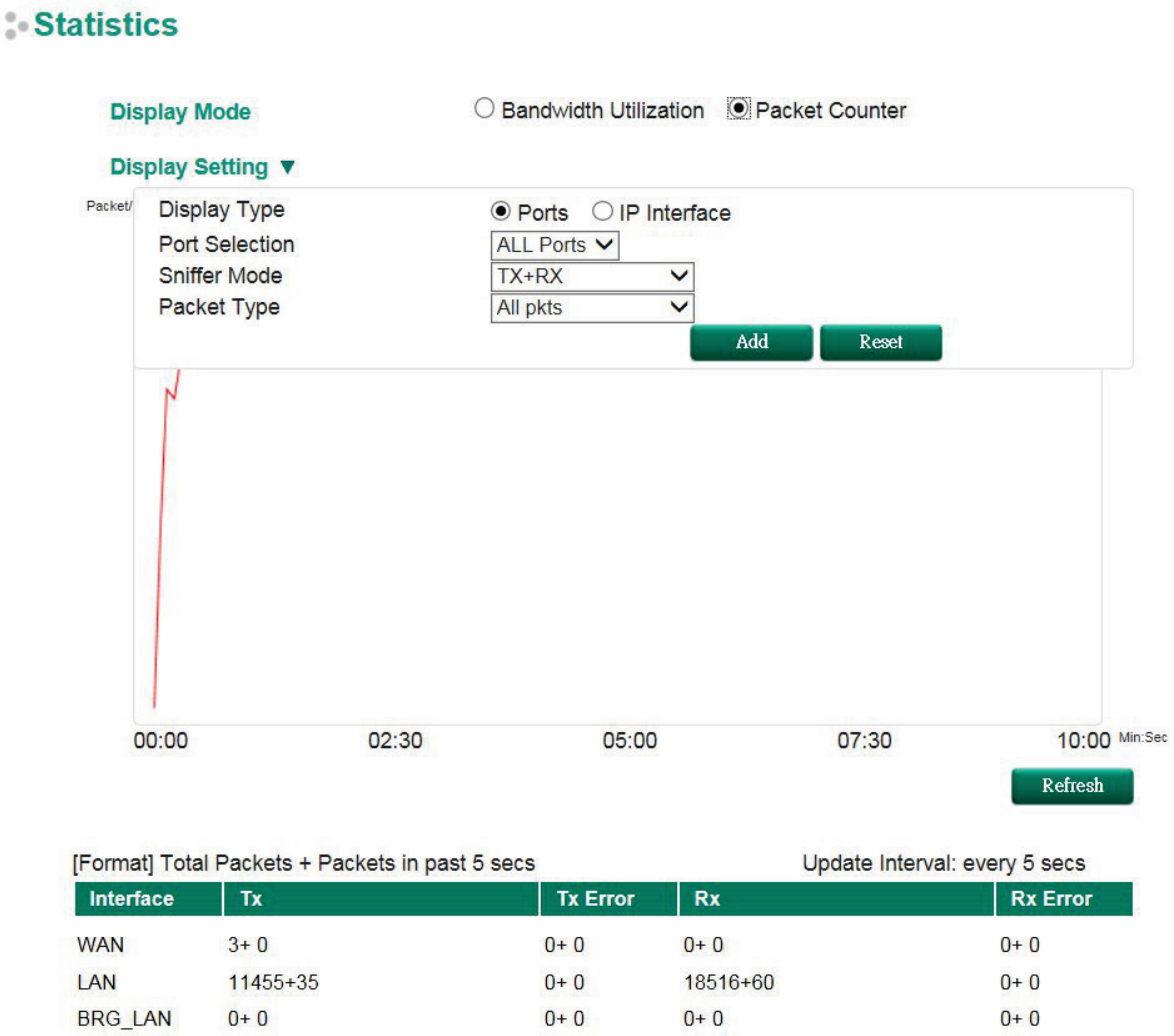
Setting	Description	Factory Default
All/LAN/WAN/Bridge_LAN	Select which interface user want to monitor traffic	All

Sniffer Mode

Setting	Description	Factory Default
(TX/RX)/TX/RX	Select which packet flow is monitored	TX/RX

Packet Counter

In **Packet Counter** mode, users can monitor total packet amount per second in each interface (**IP Interface)**, each port or port group (**Ports**). In addition to display type, users can configure which packet flow is monitored, **TX Packets**, **RX Packets** or both (**TX/RX**). **TX Packets** are packets sent out from the Industrial Secure Router, and **RX Packets** are packets received from connected devices. At the same time, users can choose to monitor different packet types, e.g. unicast, broadcast, multicast and error.



Display Mode

Setting	Description	Factory Default
Bandwidth Utilization/ Packet Counter	Graph display traffic bandwidth/ Graph display total packet amount per second	Packet Counter

Display Setting

Display Type

Setting	Description	Factory Default
Port/ IP Interface	Monitor total traffic per port or group port (FE Ports/ GE Ports)/ Monitor total traffic per interface, e.g. LAN, WAN, Bridge	IP Interface

Port Selection

Setting	Description	Factory Default
ALL Ports/FE Ports/GE Ports/Port1/Port2/ Port3/Port4/Port5/ Port6/Port7/Port8/ Port16	Users can select which port or port group they want to monitor traffic from	ALL Ports

Interface Selection

Setting	Description	Factory Default
All/WAN/LAN/ /Bridge_LAN	Select which interface user want to monitor traffic	All

Sniffer Mode

Setting	Description	Factory Default
(TX/RX)/TX/RX	Select which packet flow is monitored	TX/RX

Packet Type

Setting	Description	Factory Default
All/ Error	Select which packet type is monitored	All

Event Log

Event Log Table

All | <= | <7> Debug | Page 1/40

Index	Date	Time	Functions	Severity	Event
1	0000/00/00	00:00:00	Firewall	<4> Warning	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=1.0.0.0, SRC_IP=1.0.0.0, IN=LAN, DST_IP=0.0.0.0, DST_IP=0.0.0.0, OUT=LAN
2	0114/11/23	09:26:34	Firewall	<4> Warning	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.126.1, SRC_PORT=57768, IN=BRG, DST_IP=192.168.50.137, DST_PORT=8082, OUT=WAN
3	2015/01/14	16:27:33	System	<0> Emergency	[Link On] Port 1, Bootup:153, Startup:1d2h52m10s
4	2015/01/14	16:18:59	System	<0> Emergency	[Link Off] Port 1, Bootup:153, Startup:1d2h43m36s
5	2015/01/14	16:16:39	Firewall	<4> Warning	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.126.1, SRC_PORT=41066, IN=BRG, DST_IP=192.168.1.72, DST_PORT=445, OUT=WAN
6	2015/01/14	16:16:37	Firewall	<4> Warning	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.126.1, SRC_PORT=41066, IN=BRG, DST_IP=192.168.1.72, DST_PORT=445, OUT=WAN has repeated 6 times in past 10 seconds
7	2015/01/14	16:16:27	Firewall	<4> Warning	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.126.1, SRC_PORT=41066, IN=BRG, DST_IP=192.168.1.72, DST_PORT=445, OUT=WAN
8	2015/01/14	16:03:31	System	<0> Emergency	[Link On] Port 1, Bootup:153, Startup:1d2h28m8s
9	2015/01/14	14:58:36	System	<0> Emergency	[Link Off] Port 1, Bootup:153, Startup:1d1h23m13s
10	2015/01/14	14:57:14	Firewall	<4> Warning	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.126.1, SRC_PORT=49302, IN=BRG, DST_IP=192.168.50.137, DST_PORT=8082, OUT=WAN has repeated 5 times in past 10 seconds

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

A

MIB Groups

The Industrial Secure 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 Industrial Secure 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