Industrial Secure Router User's Manual

Edition 4.0, April 2018

www.moxa.com/product

Industrial Secure Router User's Manual

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

Copyright Notice

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 Industrial Secure Router series, the EDR-G902, EDR-G902, and EDR-810. The 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**
- ❐ **Package Checklist**
- ❐ **Features**
  - ➢ Industrial Networking Capability
  - ➢ Designed for Industrial Applications
  - ➢ Useful Utility and Remote Configuration

Overview

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

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 Industrial Secure Router supports one WAN, one LAN, and a user-configurable WAN/DMZ interface (EDR-G903) that provides high flexibility for different applications, such as WAN redundancy or Data/FTP server security protection.

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 75°C environments.

Package Checklist

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

- 1 Moxa Industrial Secure Router
- RJ45 to DB9 console port cable
- Protective caps for unused ports
- DIN rail mounting kit (attached to the Industrial Secure Router's rear panel by default)
- Hardware installation guide (printed)
- CD-ROM with user's manual and Windows utility
- Warranty card

Features

Industrial Networking Capability

- Router/Firewall/VPN all in one
- 1 WAN, 1 LAN, and 1 user-configurable WAN or DMZ interface
- Network address translation (N-to-1, 1-to-1, and port forwarding)

Designed for Industrial Applications

- Dual WAN redundancy function
- Firewall with Quick Automation Profile for Fieldbus protocols
- Intelligent PolicyCheck and SettingCheck tools
- -40 to 75°C operating temperature (T models)
- Long-haul transmission distance of 40 km or 80 km (with optional mini-GBIC)
- Redundant, dual 12 to 48 VDC power inputs
- IP30, rugged high-strength metal case
- DIN rail or panel mounting ability

Useful Utility and Remote Configuration

- Configurable using a Web browser and Telnet/Serial console

- Send ping commands to identify network segment integrity

2

Getting Started

This chapter explains how to access the 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)

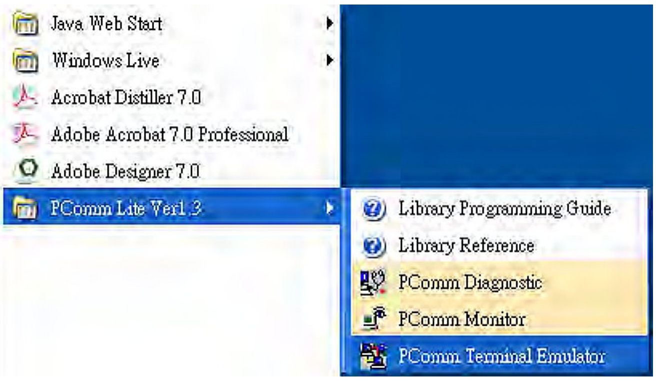
NOTE **Connection Caution!**
We strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your Industrial Secure Router

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

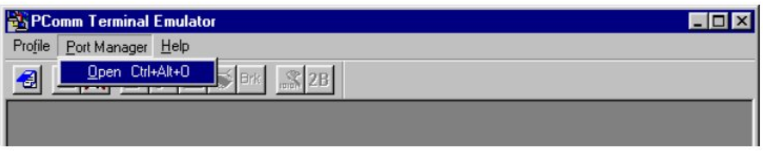
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the Industrial Secure Router’s RS-232 console port to your PC’s COM port (generally COM1 or COM2, depending on how your system is set up).

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

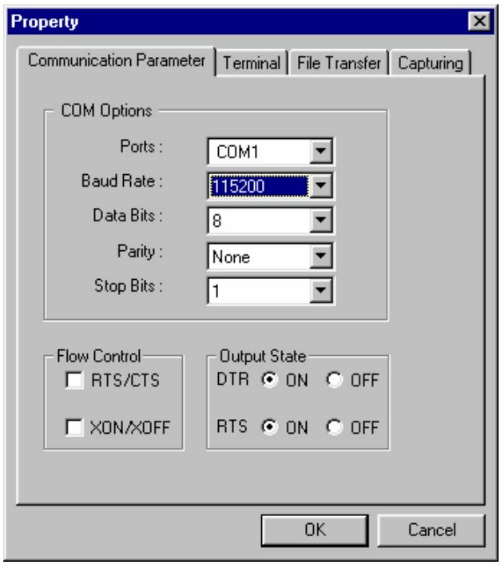
1. From the Windows desktop, click **Start** → **Programs** → **PCommLite1.3** → **Terminal Emulator**.



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.

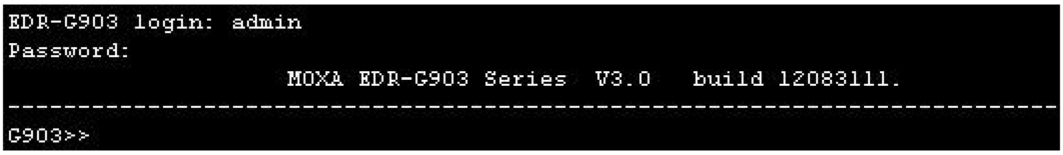


COM Options
Ports : COM1
Baud Rate : 115200
Data Bits : 8
Parity : None
Stop Bits : 1

Flow Control
□ RTS/CTS
□ XON/XOFF

Output State
DTR ● ON ○ OFF
RTS ● ON ○ OFF

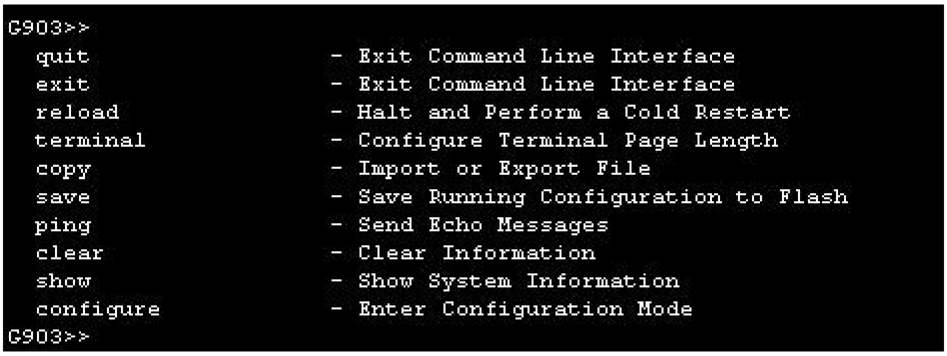
4. Click the **Terminal** tab, select VT100 for Terminal Type, and then click **OK** to continue.
5. The **Console** login screen will appear. Use the keyboard to enter the login account (**admin** or **user**), and then press **Enter** to jump to the **Password** field. Enter the console Password (the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



```
EDR-G903 login: admin
Password:
                    MOXA EDR-G903 Series  V3.0   build 12083111.
----------------------------------------------------------------------------
G903>>
```

NOTE The default password for the EDR series with firmware v3.0 and later is "moxa". For previous firmware versions, the default password is blank. For greater security, please change the default password after the first log in.

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



```
G903>>
  quit                     - Exit Command Line Interface
  exit                     - Exit Command Line Interface
  reload                   - Halt and Perform a Cold Restart
  terminal                 - Configure Terminal Page Length
  copy                     - Import or Export File
  save                     - Save Running Configuration to Flash
  ping                     - Send Echo Messages
  clear                    - Clear Information
  show                     - Show System Information
  configure                - Enter Configuration Mode
G903>>
```

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
save	Save Running Configuration to Flash
ping	Send Echo Messages
clear	Clear Information
show	Show System Information
configure	Enter Configuration Mode

Using Telnet to Access the Industrial Secure Router's Console

You may use Telnet to access the Industrial Secure Router's console utility over a network. To access the EDR'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.

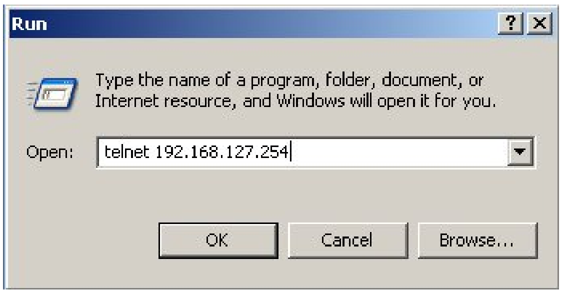
NOTE To use the Industrial Secure Router's management and monitoring functions from a PC host connected to the same LAN as the Industrial Secure Router, you must make sure that the PC host and the Industrial Secure Router are connected to the same logical subnet.

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.)



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 192.168.127.254

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

Using a Web Browser to Configure the 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.

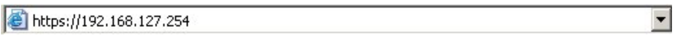
NOTE To use the Industrial Secure Router's management and monitoring functions from a PC host connected to the same LAN as the Industrial Secure Router, you must make sure that the PC host and the Industrial Secure Router are connected to the same logical subnet.

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.

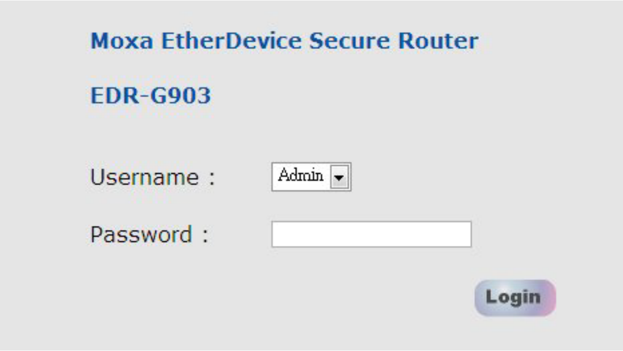
Perform the following steps to access the Industrial Secure Router's web browser interface.

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



https://192.168.127.254

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



Moxa EtherDevice Secure Router

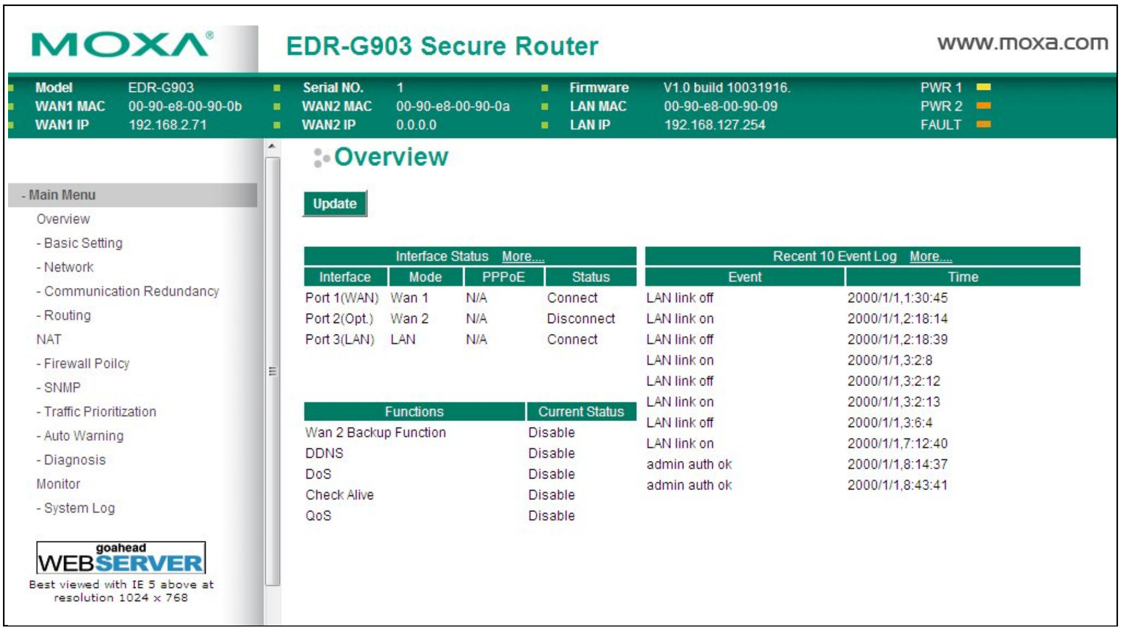
EDR-G903

Username : Admin

Password :

NOTE The default password for the EDR series with firmware v3.0 and later is "moxa". For previous firmware versions, the default password is blank. For greater security, please change the default password after the first log in.

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



EDR-G903 Secure Router

Model	EDR-G903	Serial NO.	1	Firmware	V1.0 build 10031916.	PWR 1	▬
WAN1 MAC	00-90-e8-00-90-0b	WAN2 MAC	00-90-e8-00-90-0a	LAN MAC	00-90-e8-00-90-09	PWR 2	▬
WAN1 IP	192.168.2.71	WAN2 IP	0.0.0.0	LAN IP	192.168.127.254	FAULT	▬

Overview

Interface Status More....

Interface	Mode	PPPoE	Status
Port 1(WAN)	Wan 1	N/A	Connect
Port 2(Opt.)	Wan 2	N/A	Disconnect
Port 3(LAN)	LAN	N/A	Connect

Functions	Current Status
Wan 2 Backup Function	Disable
DDNS	Disable
DoS	Disable
Check Alive	Disable
QoS	Disable

Recent 10 Event Log More....

Event	Time
LAN link off	2000/1/1,1:30:45
LAN link on	2000/1/1,2:18:14
LAN link off	2000/1/1,2:18:39
LAN link on	2000/1/1,3:2:8
LAN link off	2000/1/1,3:2:12
LAN link on	2000/1/1,3:2:13
LAN link off	2000/1/1,3:6:4
LAN link on	2000/1/1,7:12:40
admin auth ok	2000/1/1,8:14:37
admin auth ok	2000/1/1,8:43:41

3

EDR-810 Series 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**
  - Fast Bootup Setting
  - 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
    - SNMP Trap Setting
    - Dynamic DNS
- **Security**
    - User Interface Management
    - Authentication Certificate
    - Trusted Access
    - RADIUS Server Settings
    - Security Notification Setting
    - Diagnosis
    - Event Log
    - Connection Status

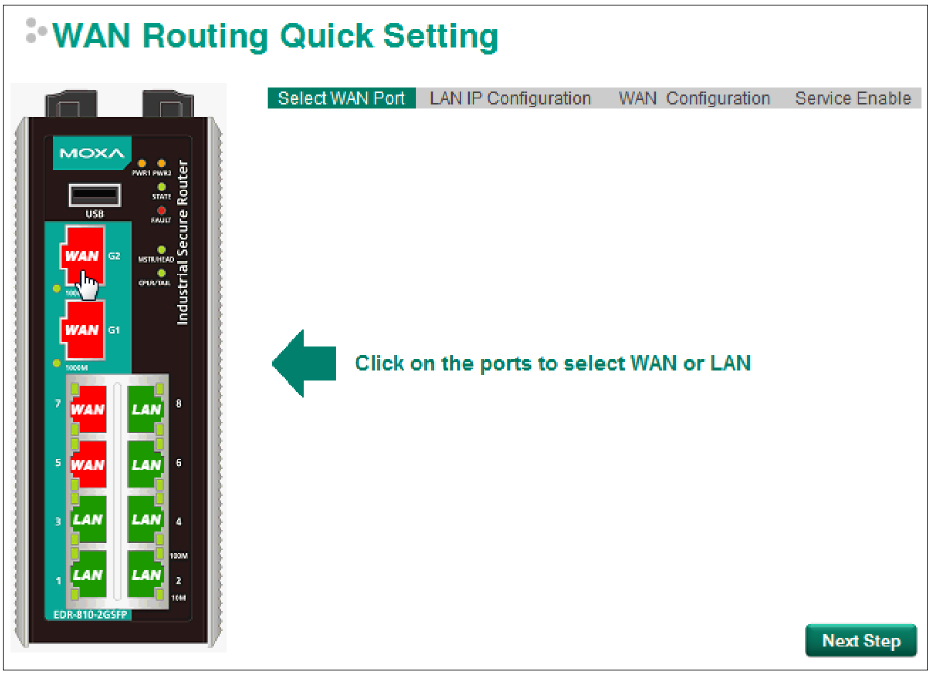
Quick Setting Profile

WAN Routing Quick Setting

The EDR-810 series supports WAN Routing Quick Setting, 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.

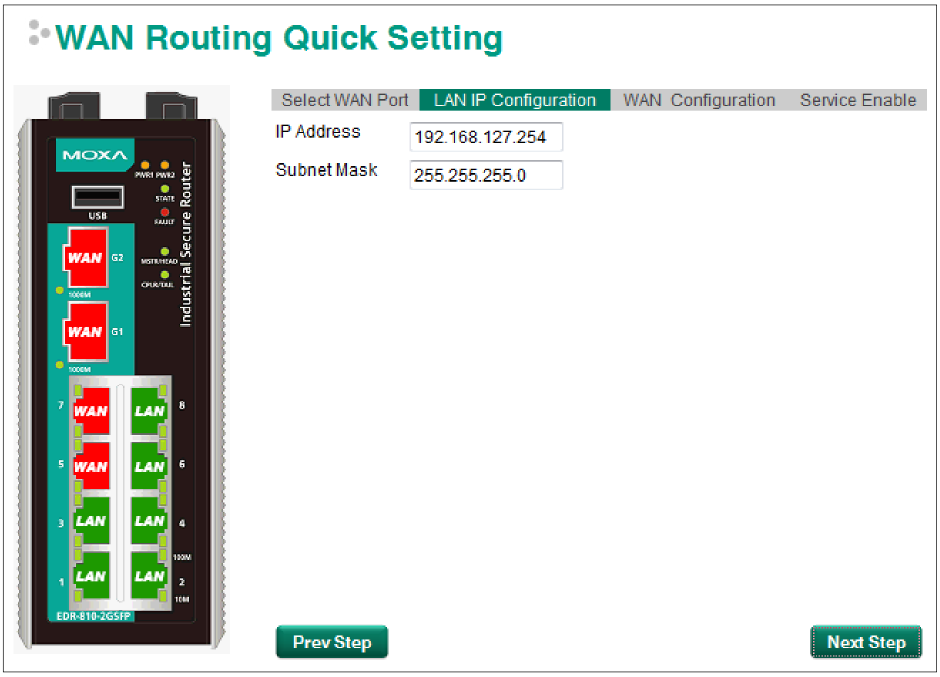
Step 1: Define the WAN ports and LAN ports

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



Step 2: Configure the LAN IP address of the EDR-810 and the subnet address of the LAN ports

Configure the LAN IP address of the EDR-810 to define the subnet of the LAN ports on the secure router. The default IP address of the EDR-810 on the LAN side is 192.168.127.254, and the default subnet address is 192.168.127.0/24.



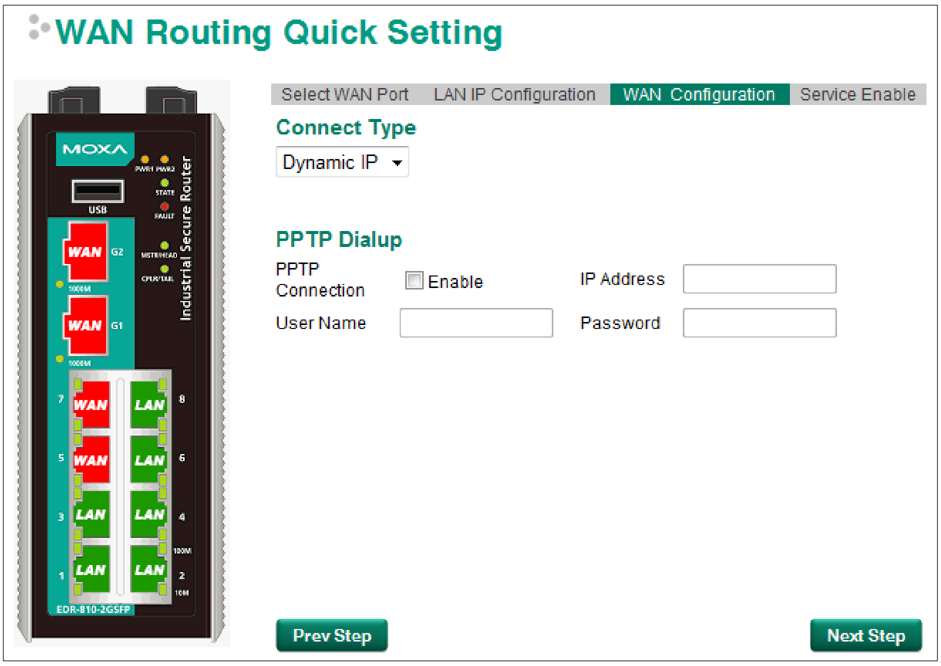
WAN Routing Quick Setting

IP Address 192.168.127.254

Subnet Mask 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.



WAN Routing Quick Setting

Connect Type

Dynamic IP

PPTP Dialup

PPTP Connection □ Enable

IP Address

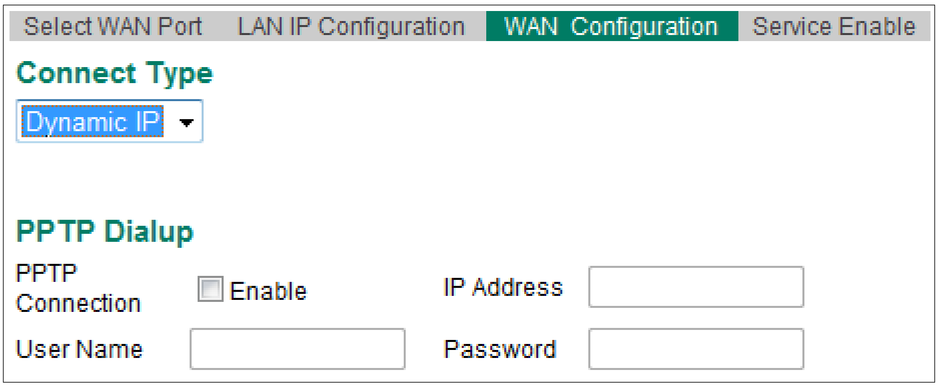
User Name

Password

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



Connect Type

Dynamic IP

PPTP Dialup

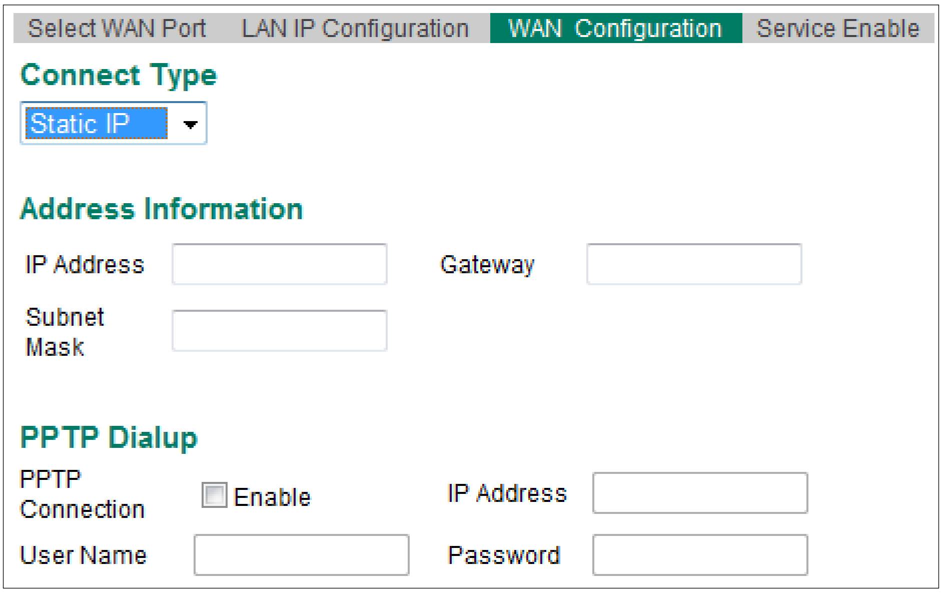
PPTP Connection □ Enable

IP Address

User Name

Password

Static IP



Connect Type

Static IP

Address Information

IP Address

Gateway

Subnet Mask

PPTP Dialup

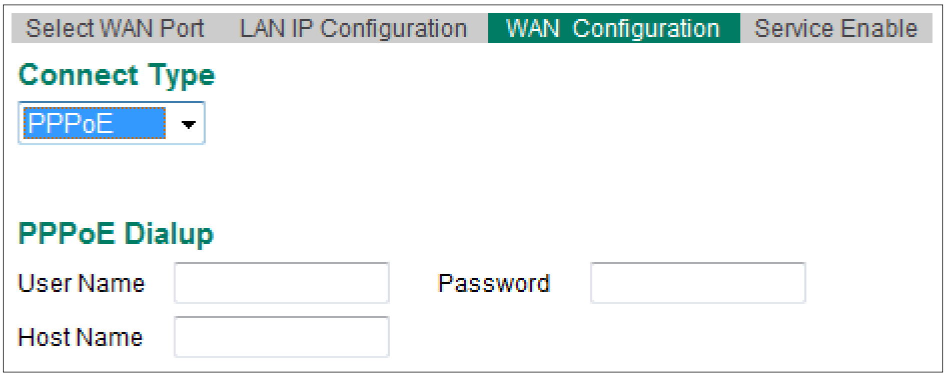
PPTP Connection □ Enable

IP Address

User Name

Password

PPPoE



Connect Type

PPPoE

PPPoE Dialup

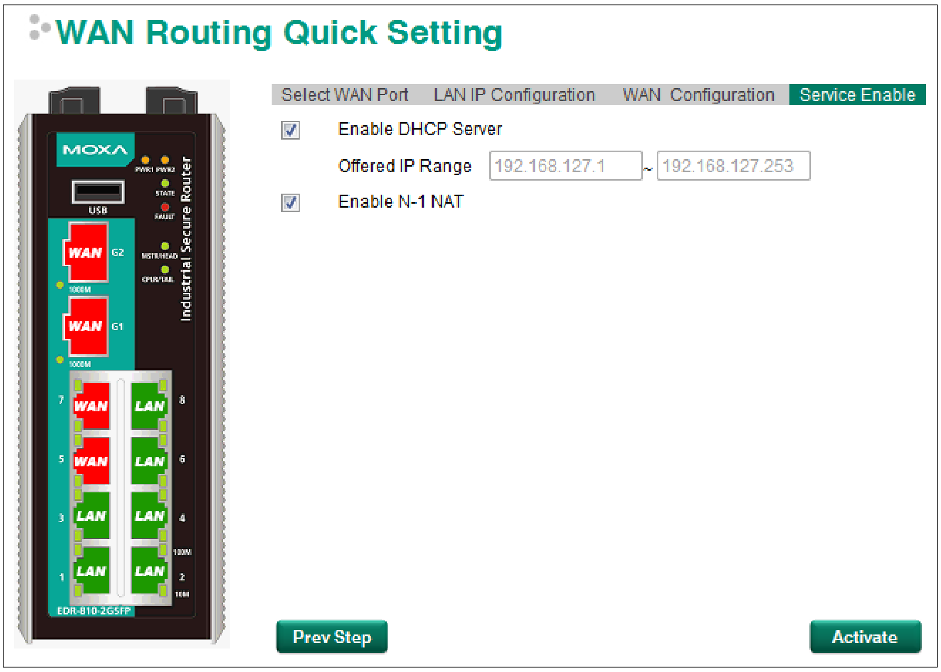
User Name

Password

Host Name

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.



WAN Routing Quick Setting

☑ Enable DHCP Server

Offered IP Range 192.168.127.1 ~ 192.168.127.253

☑ Enable N-1 NAT

Step 5: Activate the settings

Click the **Activate** button.

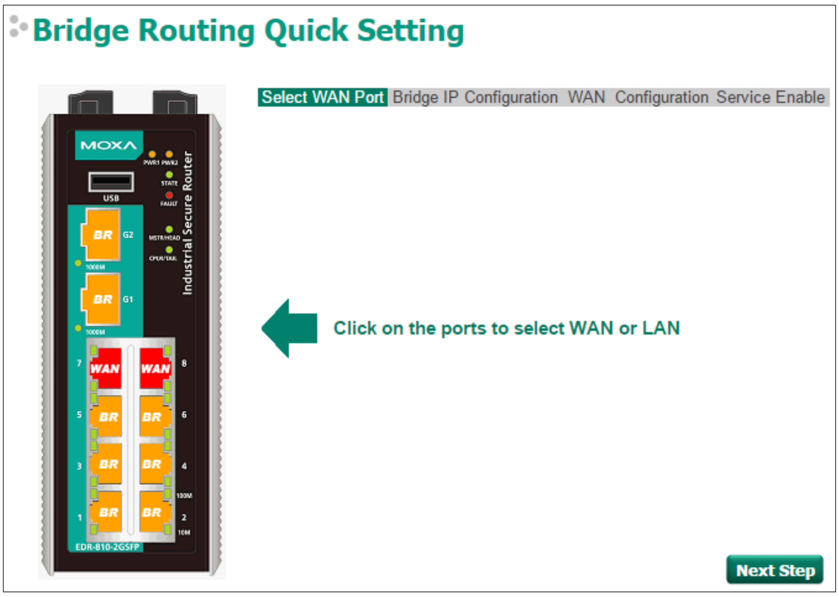
NOTE An existing configuration will be overwritten by new settings when processing **WAN Routing Quick Setting**.

Bridge Routing Quick Setting

The EDR-810 series supports WAN Routing Quick Setting, 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.

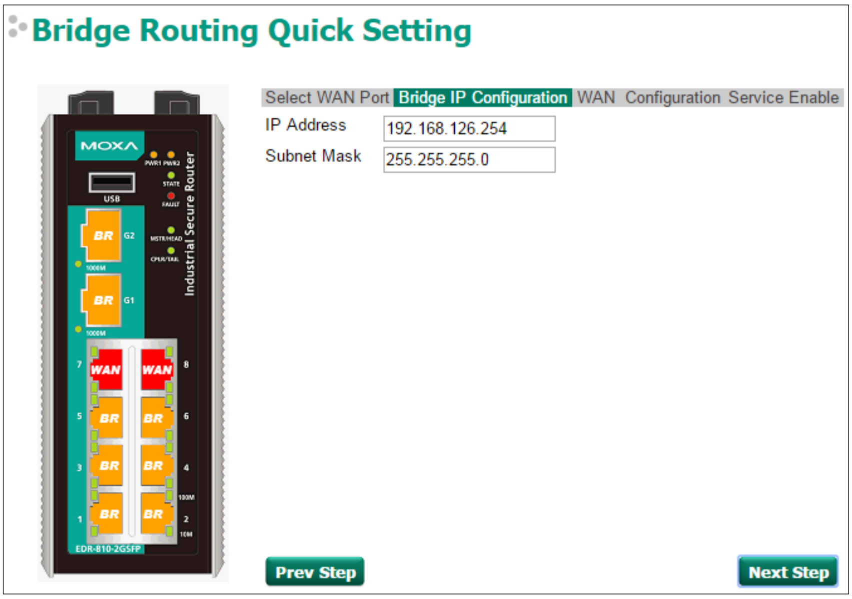


Bridge Routing Quick Setting

Click on the ports to select WAN or LAN

Step 2: Configure the Bridge LAN IP address of the EDR-810 and the subnet address of the Bridged ports

Configure the Bridge LAN Interface IP address of the EDR-810 to define the subnet of the Bridge LAN ports on the secure router. The default IP address of the EDR-810 on the Bridge LAN side is 192.168.126.254, and the default subnet address is 192.168.126.0/24.

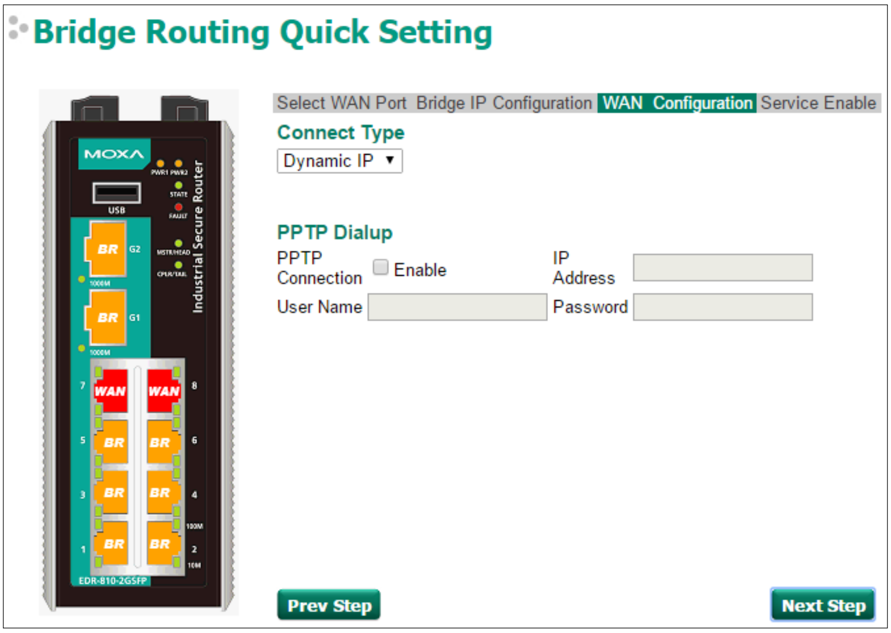

Bridge Routing Quick Setting

IP Address 192.168.126.254

Subnet Mask 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.


Bridge Routing Quick Setting

Connect Type

Dynamic IP ▼

PPTP Dialup

PPTP Connection □ Enable

IP Address

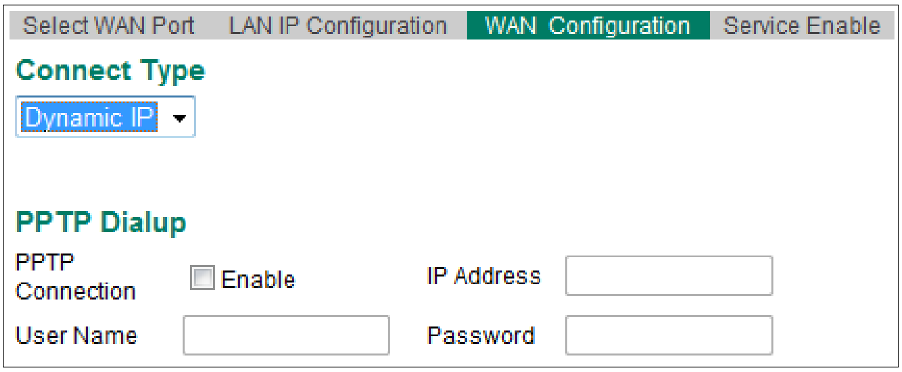
User Name

Password

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



Connect Type

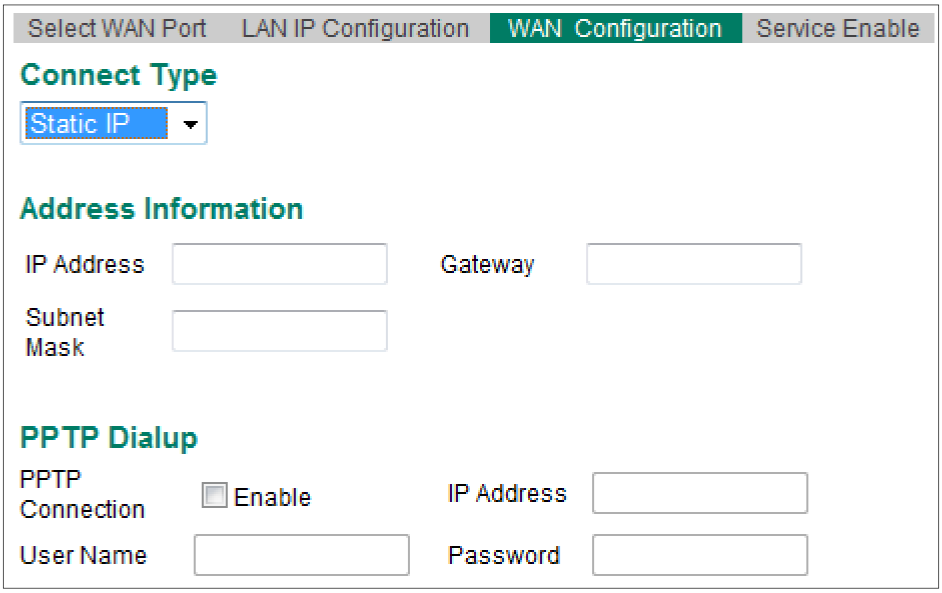
Dynamic IP

PPTP Dialup

PPTP Connection □ Enable IP Address

User Name Password

Static IP



Connect Type

Static IP

Address Information

IP Address Gateway

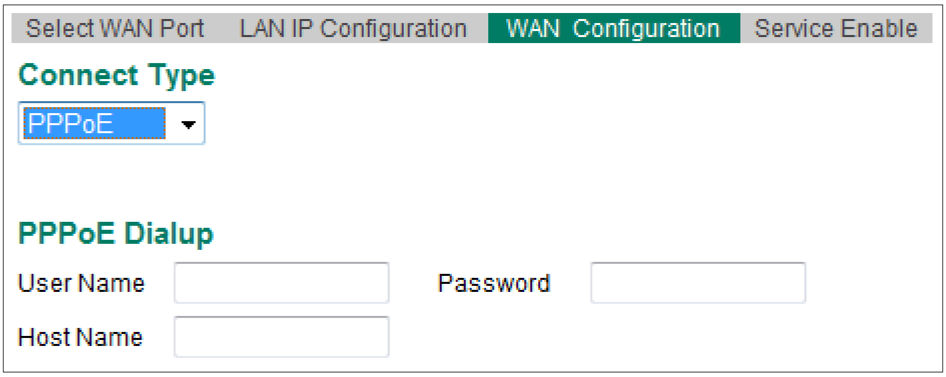
Subnet Mask

PPTP Dialup

PPTP Connection □ Enable IP Address

User Name Password

PPPoE



Connect Type

PPPoE

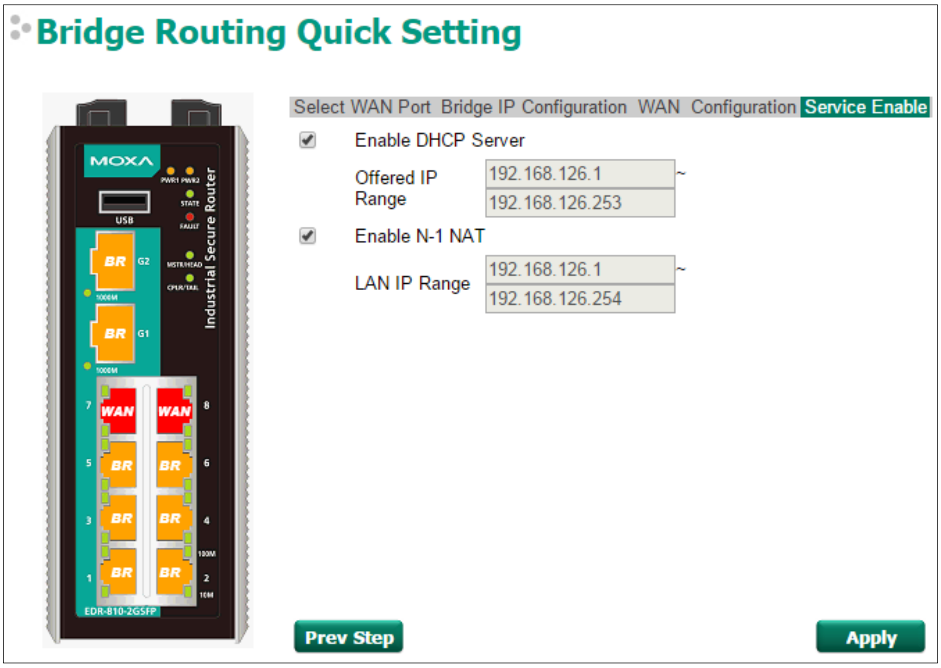
PPPoE Dialup

User Name Password

Host Name

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.



Bridge Routing Quick Setting

☑ Enable DHCP Server

Offered IP Range: 192.168.126.1 ~ 192.168.126.253

☑ Enable N-1 NAT

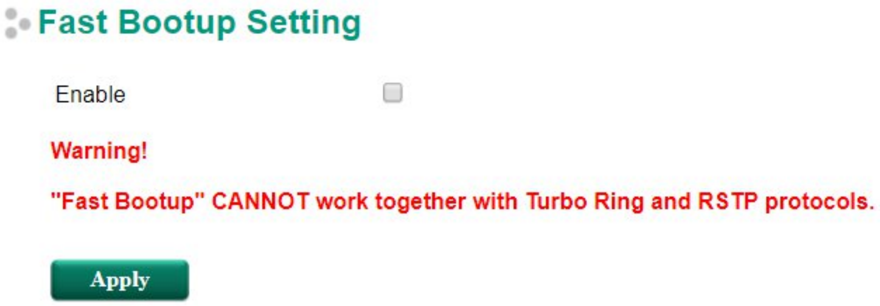
LAN IP Range: 192.168.126.1 ~ 192.168.126.254

System

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

Fast Bootup Setting

When booting up a normal security router it generally takes about 3 minutes to complete all the system settings including firewall, NAT, and VPN. However, three minutes is too long for some users who require the network connection earlier. When the fast boot up function is enabled, the EDR-810's VLAN settings, DHCP server, and WAN/LAN interface will be ready within 30 seconds. This allows end devices connected to the EDR-810 to communicate with each other and get the IP address from the DHCP server much quicker.



Fast Bootup Setting

Enable □

Warning!

"Fast Bootup" CANNOT work together with Turbo Ring and RSTP protocols.

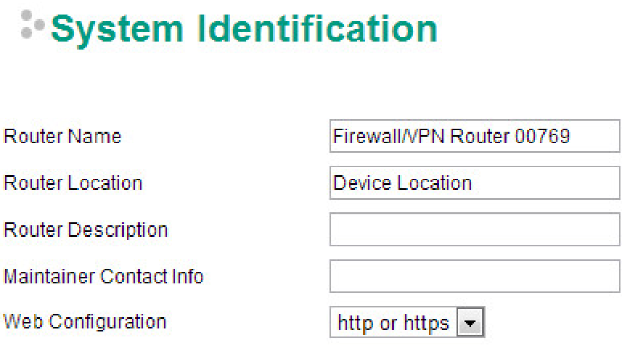
Enable Fast Bootup Setting

Setting	Description	Factory Default
Enable/Disable	Enable or disable Fast Bootup	Disable

NOTE Fast Bootup CANNNOT work together with Turbo Ring and RSTP protocols.

System Information

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



System Identification

Router Name	Firewall/VPN Router 00769
Router Location	Device Location
Router Description	
Maintainer Contact Info	
Web Configuration	http or https

Router Name

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

Router Location

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

Router Description

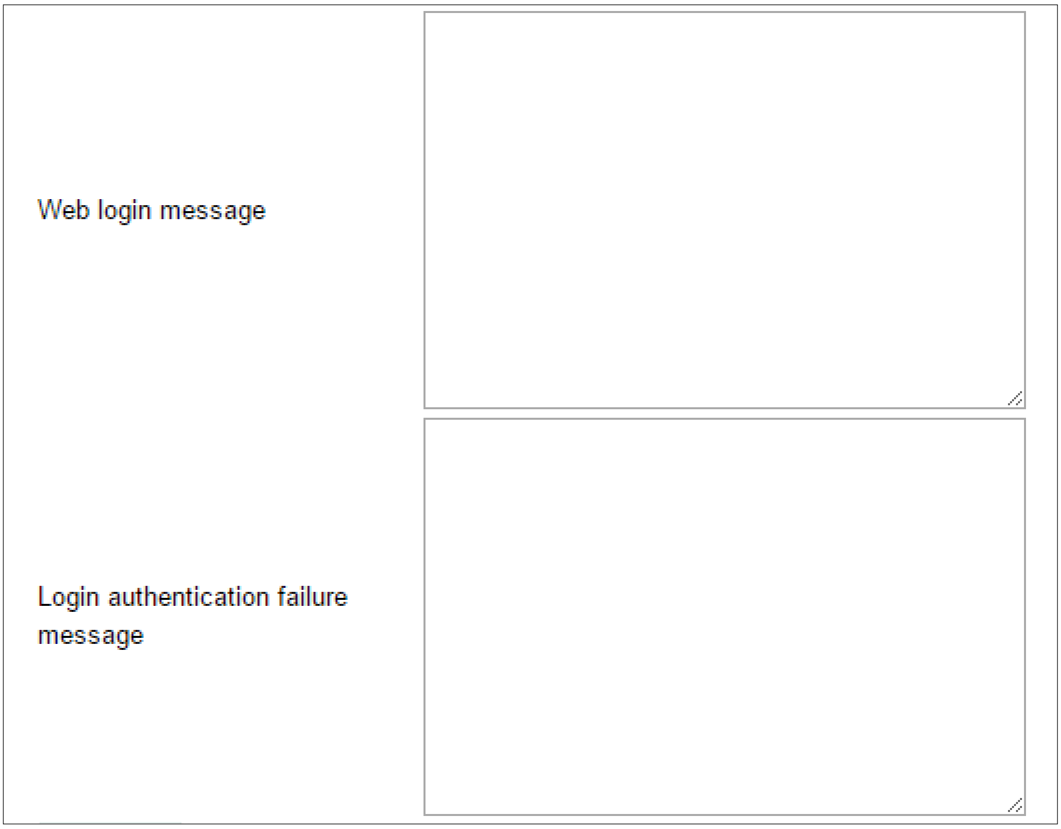
Setting	Description	Factory Default
Max. 30 characters	This option is useful for recording a more detailed description of the unit.	None

Maintainer Contact Info

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

Web Configuration

Setting	Description	Factory Default
http or https	Enable HTTP and HTTPS	http or https
https only	Enable HTTPS only	



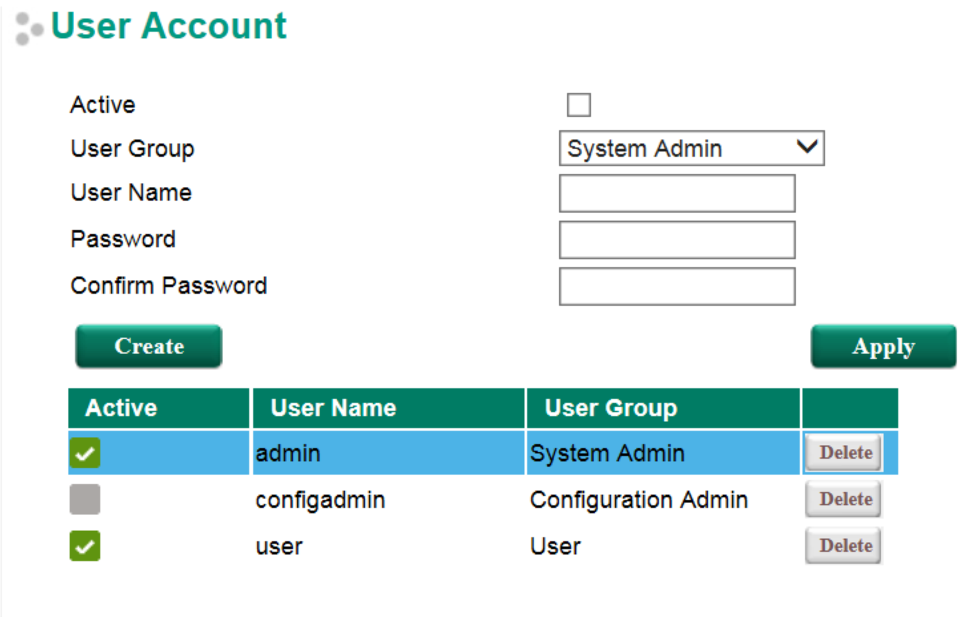
Users can define the message that will show up on the login page, and the message that will show up if login fails. The maximum length of each message is 512 bytes.

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, strongly suggest to change the default password after first log in
2. The user with ‘admin’ account name can’t be deleted and disabled by default



User Account

Active	□
User Group	System Admin
User Name	
Password	
Confirm Password	

Active	User Name	User Group	
✓	admin	System Admin	Delete
□	configadmin	Configuration Admin	Delete
✓	user	User	Delete

Active

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

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.	

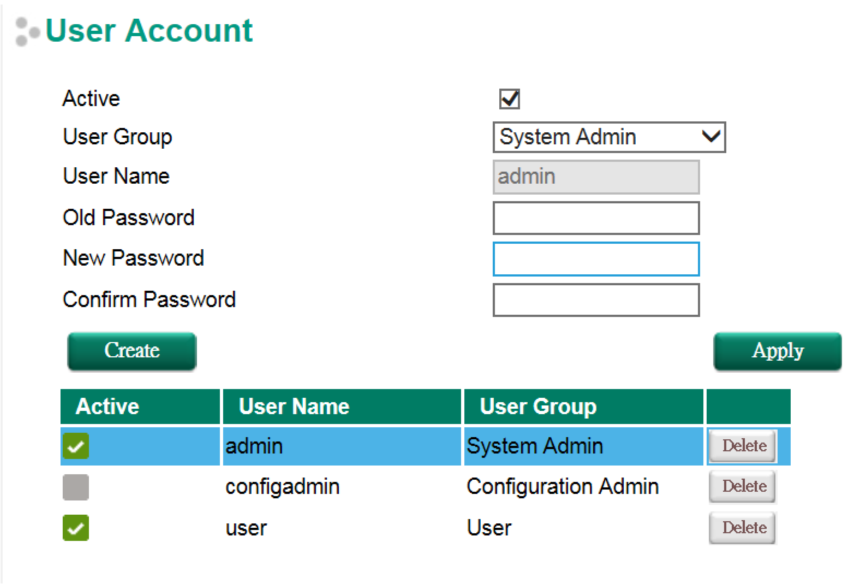
Create New Account

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.



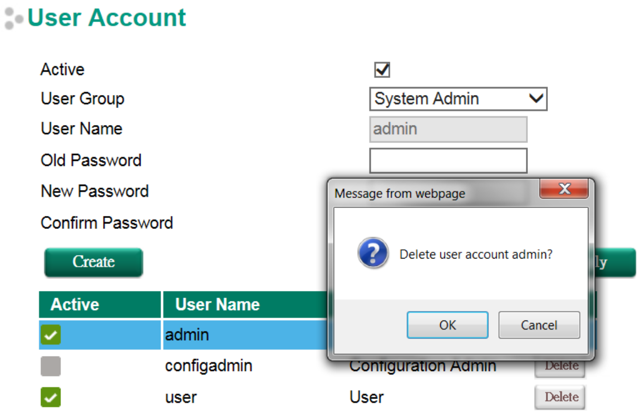
User Account

Active	☑
User Group	System Admin
User Name	admin
Old Password	
New Password	
Confirm Password	

Active	User Name	User Group	
✓	admin	System Admin	Delete
☐	configadmin	Configuration Admin	Delete
✓	user	User	Delete

Delete Existing Account

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



User Account

Active	☑
User Group	System Admin
User Name	admin
Old Password	
New Password	
Confirm Password	

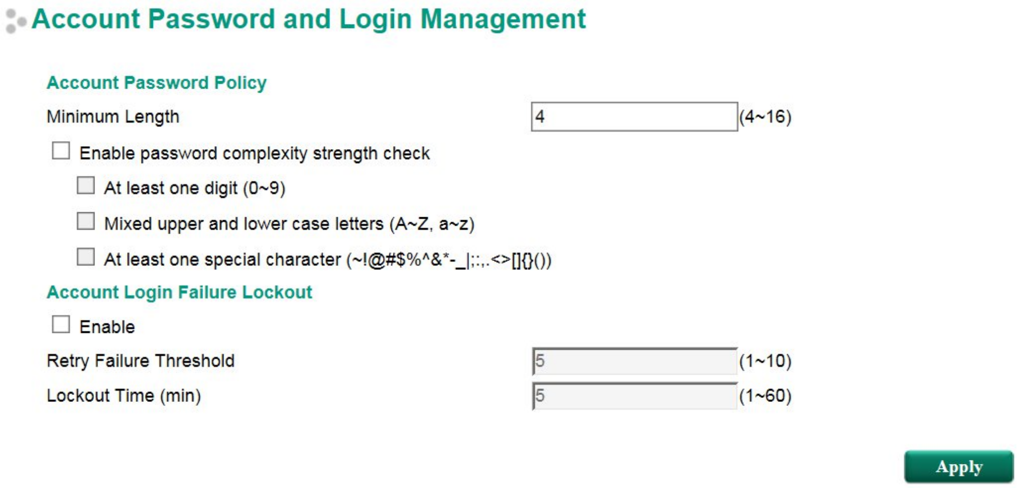
Message from webpage

Delete user account admin?

Active	User Name		
✓	admin		
☐	configadmin	Configuration Admin	Delete
✓	user	User	Delete

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 and Login Management

Account Password Policy

Minimum Length 4 (4~16)

□ Enable password complexity strength check

□ At least one digit (0~9)

□ Mixed upper and lower case letters (A~Z, a~z)

□ At least one special character (~!@#$%^&*-_|;:,.<>[]{}())

Account Login Failure Lockout

□ Enable

Retry Failure Threshold 5 (1~10)

Lockout Time (min) 5 (1~60)

Account Password Policy

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

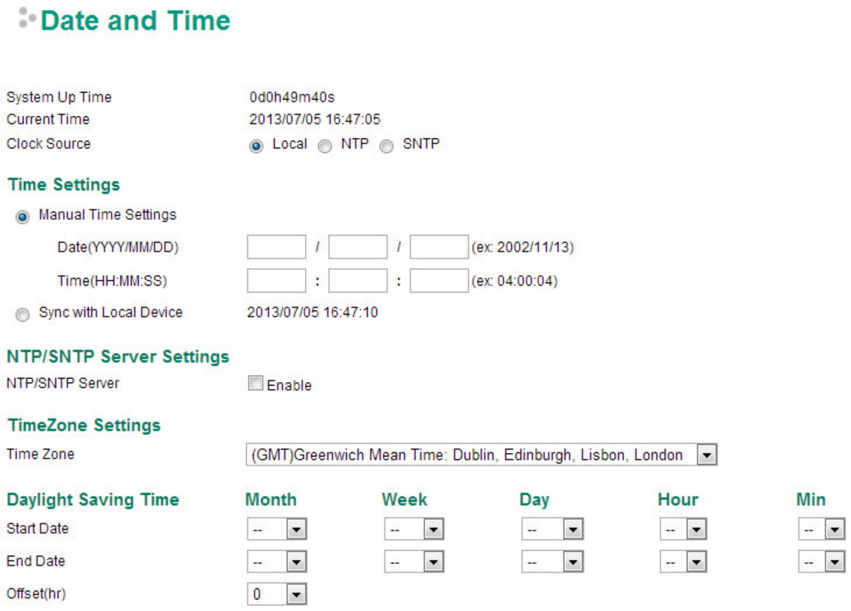
Account Login Failure Lockout

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.



Date and Time

System Up Time 0d0h49m40s

Current Time 2013/07/05 16:47:05

Clock Source ● Local ○ NTP ○ SNTP

Time Settings

● Manual Time Settings

Date(YYYY/MM/DD) / / (ex: 2002/11/13)

Time(HH:MM:SS) : : (ex: 04:00:04)

○ Sync with Local Device 2013/07/05 16:47:10

NTP/SNTP Server Settings

NTP/SNTP Server □ Enable

TimeZone Settings

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

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

System Up Time

Indicates how long the Moxa 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.

Time Server IP/Name

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

Enable NTP/SNTP Server

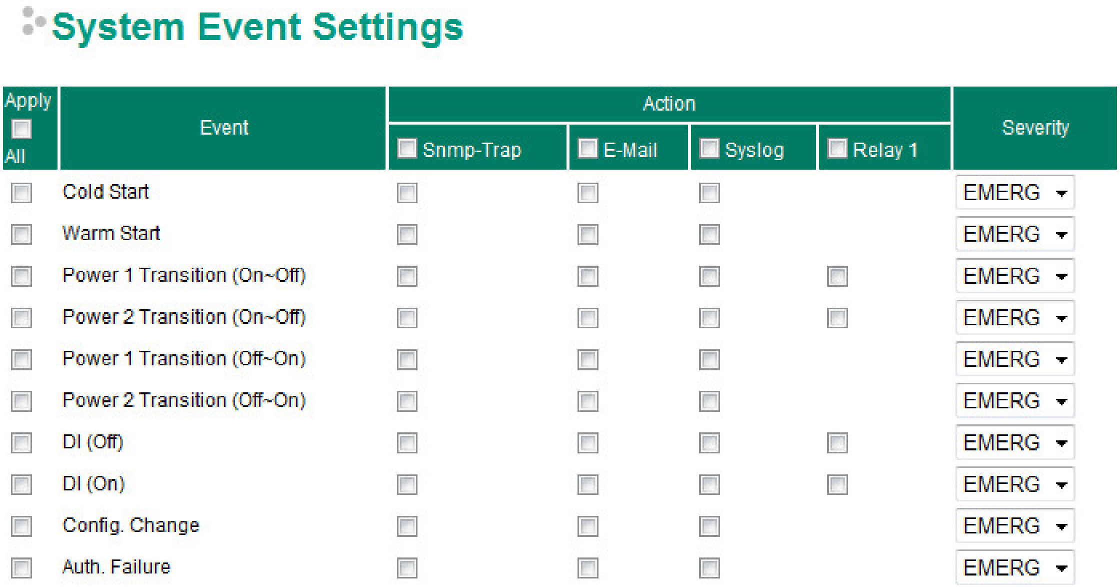
Setting	Description	Factory Default
Enable/Disable	Enables SNTP/NTP server functionality for clients	Disabled

Warning Notification

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an 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 for EDR-810

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



System Event Settings

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

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.

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

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

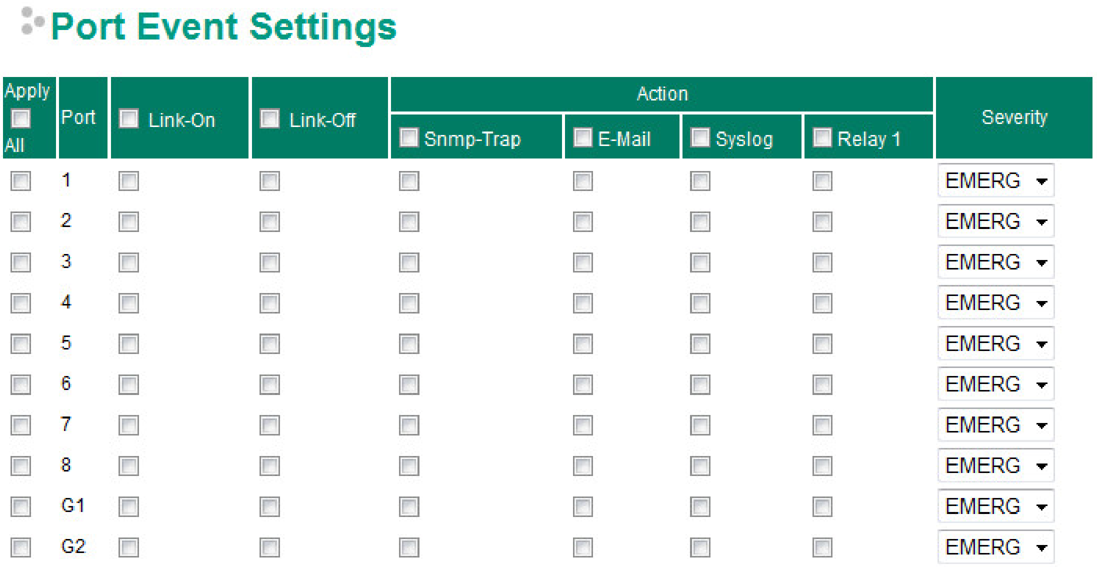
Severity

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

Debug	Debug-level messages

Port Event Settings

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



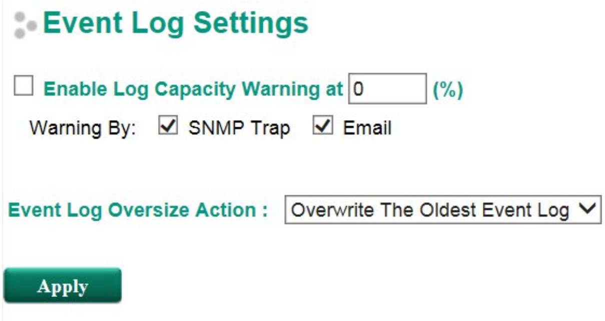
Port Event Settings

Apply ☐ All	Port	☐ Link-On	☐ Link-Off	Action				Severity
				☐ Snmp-Trap	☐ E-Mail	☐ Syslog	☐ Relay 1	
☐	1	☐	☐	☐	☐	☐	☐	EMERG
☐	2	☐	☐	☐	☐	☐	☐	EMERG
☐	3	☐	☐	☐	☐	☐	☐	EMERG
☐	4	☐	☐	☐	☐	☐	☐	EMERG
☐	5	☐	☐	☐	☐	☐	☐	EMERG
☐	6	☐	☐	☐	☐	☐	☐	EMERG
☐	7	☐	☐	☐	☐	☐	☐	EMERG
☐	8	☐	☐	☐	☐	☐	☐	EMERG
☐	G1	☐	☐	☐	☐	☐	☐	EMERG
☐	G2	☐	☐	☐	☐	☐	☐	EMERG

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

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.



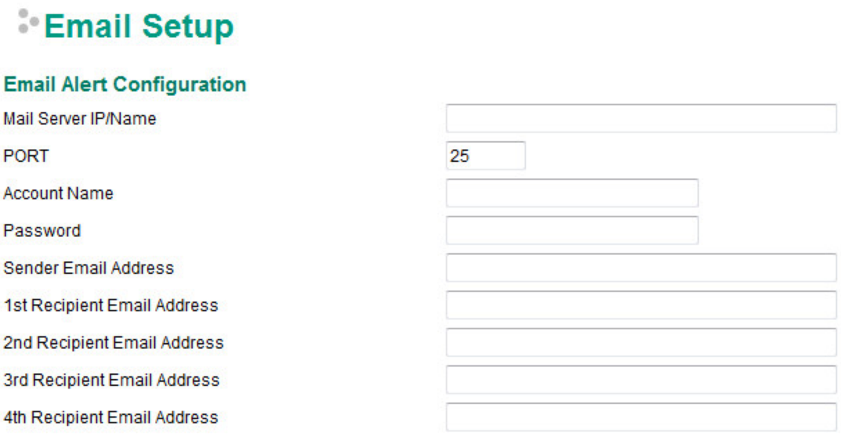
Event Log Settings

☐ Enable Log Capacity Warning at 0 (%)

Warning By: ☑ SNMP Trap ☑ Email

Event Log Oversize Action : Overwrite The Oldest Event Log

Email Settings



Email Setup

Email Alert Configuration

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

Mail Server IP/Name

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

Account Name

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

Password Setting

Setting	Description	Factory Default
Password	The email account password.	None

Email Address

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

Send Test Email

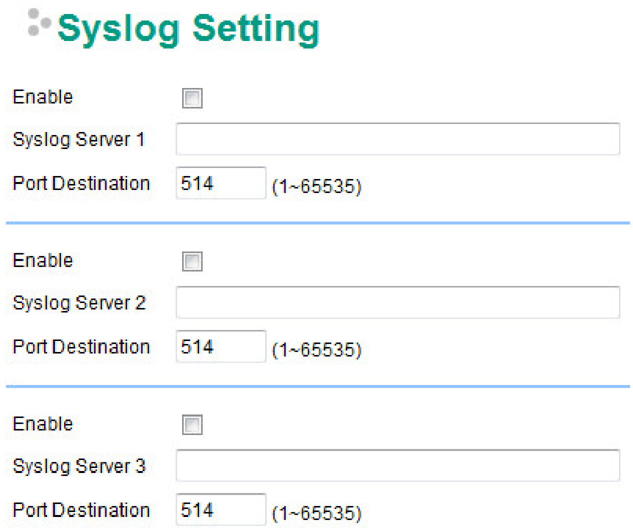
After you complete the email settings, you should first click **Apply** to activate those settings, and then press the **Test** button to verify that the settings are correct.

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

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

Syslog Server Settings

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



Syslog Setting

Enable □

Syslog Server 1

Port Destination 514 (1~65535)

Enable □

Syslog Server 2

Port Destination 514 (1~65535)

Enable □

Syslog Server 3

Port Destination 514 (1~65535)

Syslog Server 1/2/3

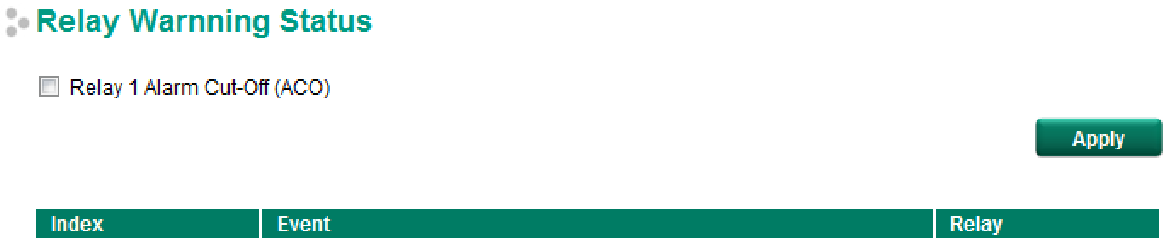
Setting	Description	Factory Default
IP Address	Enter the IP address of Syslog server 1/2/3, used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of Syslog server 1/2/3.	514

NOTE The following events will be recorded into the Moxa 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

Relay Warning Status

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

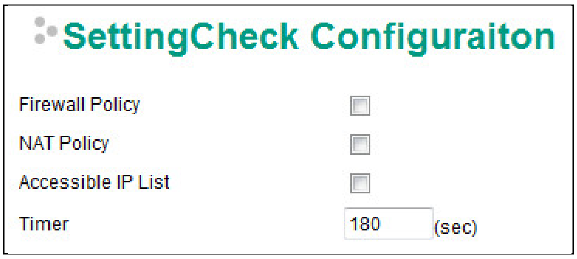


Relay Warnning Status

□ Relay 1 Alarm Cut-Off (ACO)

Index	Event	Relay

SettingCheck



SettingCheck Configuraiton

Firewall Policy □

NAT Policy □

Accessible IP List □

Timer 180 (sec)

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.

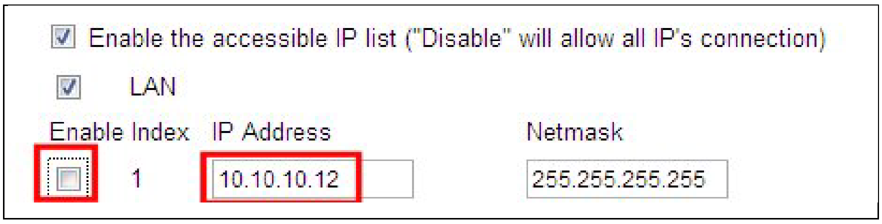
Accessible IP List

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.

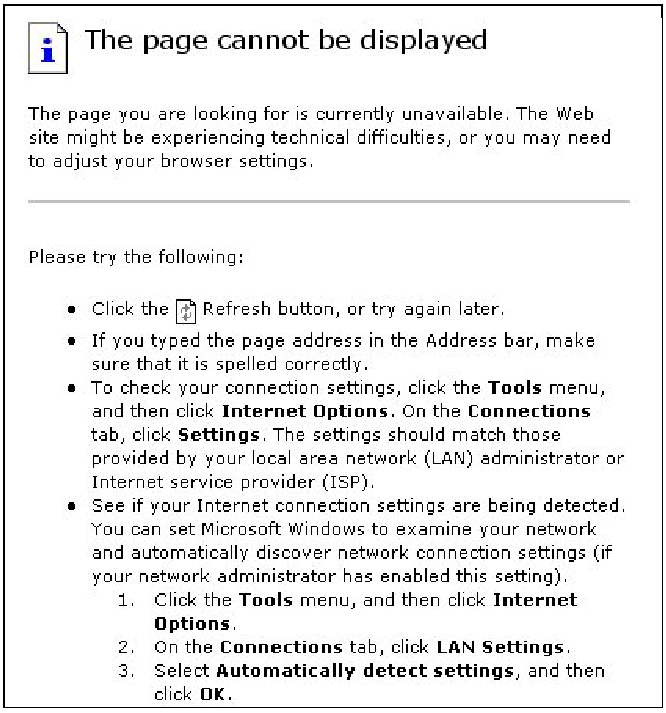


☑ Enable the accessible IP list ("Disable" will allow all IP's connection)

☑ LAN

Enable	Index	IP Address	Netmask
□	1	10.10.10.12	255.255.255.255

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.



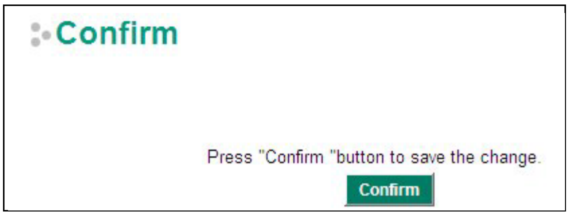
The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
  1. Click the **Tools** menu, and then click **Internet Options**.
  2. On the **Connections** tab, click **LAN Settings**.
  3. Select **Automatically detect settings**, and then click **OK**.

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.

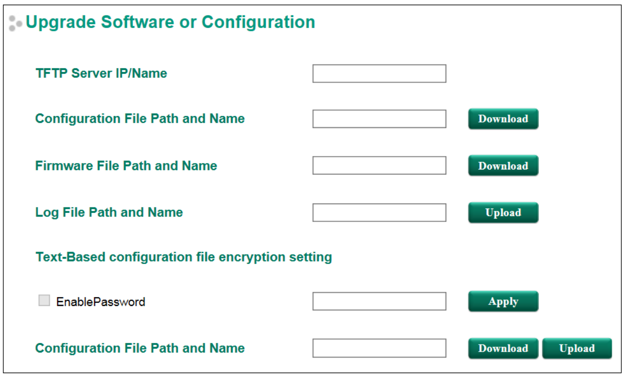


Confirm

Press "Confirm "button to save the change.

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.



Upgrade Software or Configuration

TFTP Server IP/Name

Configuration File Path and Name

Firmware File Path and Name

Log File Path and Name

Text-Based configuration file encryption setting

□ EnablePassword

Configuration File Path and Name

TFTP Server IP/Name

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

Configuration File Path and Name

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

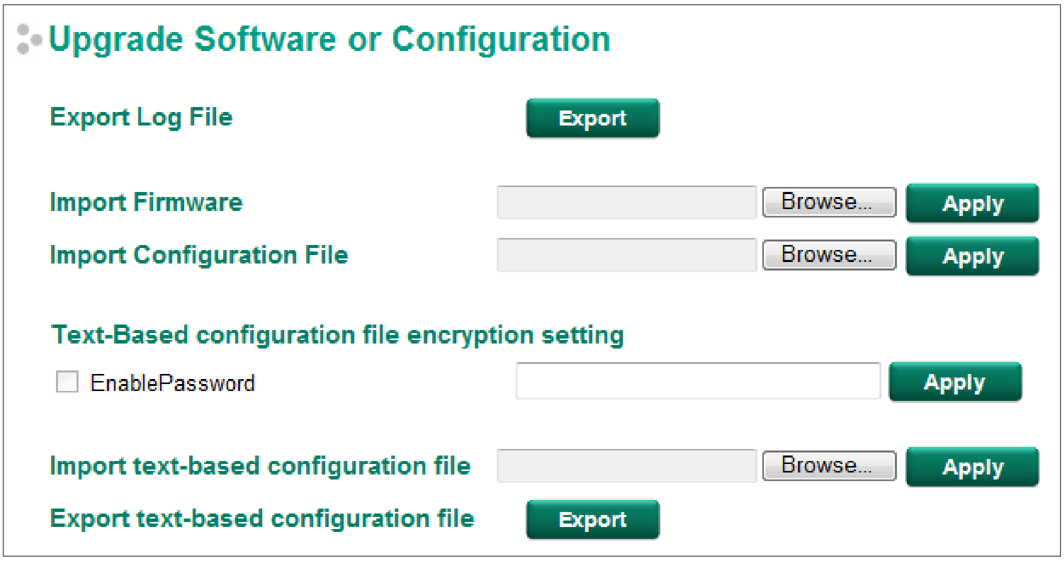
Text_Based configuration file encryption setting

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 EDR-810's system with firmware version 3.4 or later. The configuration file uses file extension .txt file.	None

System File Update—by Local Import/Export


Upgrade Software or Configuration
Export Log File
Export
Import Firmware
Browse...
Apply
Import Configuration File
Browse...
Apply
Text-Based configuration file encryption setting
☐ EnablePassword
Apply
Import text-based configuration file
Browse...
Apply
Export text-based configuration file
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

To import a firmware file that is exported from firmware V3.3 or previous versions into the Industrial Secure Router, click **Browse** to select a firmware file already saved on your computer. The upgrade procedure will proceed automatically after clicking Import. This upgrade procedure will take a couple of minutes to complete, including the boot-up time.

Upload Configuration Data

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

Text-Based configuration file encryption setting

To export the configuration as an encrypted text-based (command line type) configuration file, click the **Enable Password** checkbox and fill in the user-defined password, and then click **Apply**. The password is also used for decrypting when importing an encrypted configuration file.

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.

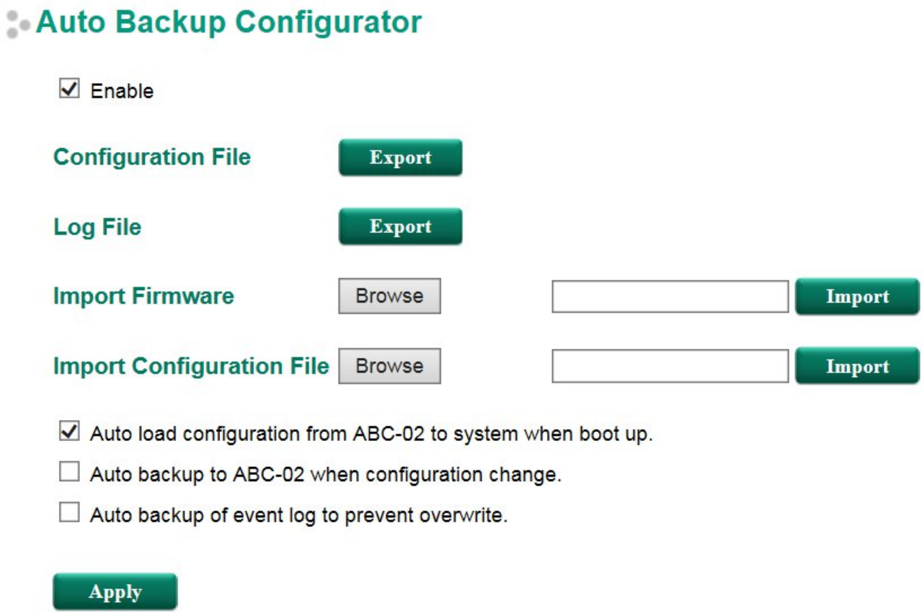
System File Update –Import/Export the configurations stored on the ABC-02-USB

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. For more details about the ABC-02-USB, please visit:

https://www.moxa.com/product/Automatic_Backup_Configurator_ABC-02-USB.htm

Moxa’s Automatic Backup Configurator (ABC-02)



Auto Backup Configurator

☑ Enable

Configuration File Export

Log File Export

Import Firmware Browse Import

Import Configuration File Browse Import

☑ Auto load configuration from ABC-02 to system when boot up.

□ Auto backup to ABC-02 when configuration change.

□ Auto backup of event log to prevent overwrite.

Apply

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

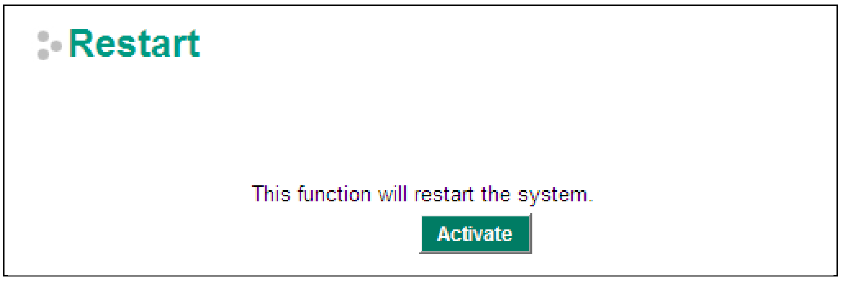
Setting	Description	Factory Default
Checked	Allows a system to back up configuration files to the ABC-02 automatically when configurations change	Checked
Unchecked	System will not backup configuration files to the ABC-02 automatically when configurations change	

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.

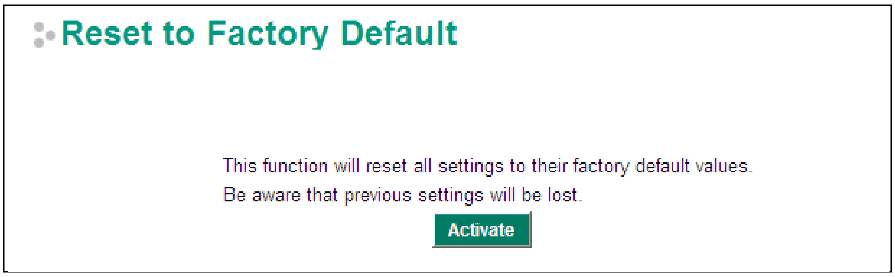
Restart



This function will restart the system.

This function is used to restart the Industrial Secure Router.

Reset to Factory Default



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

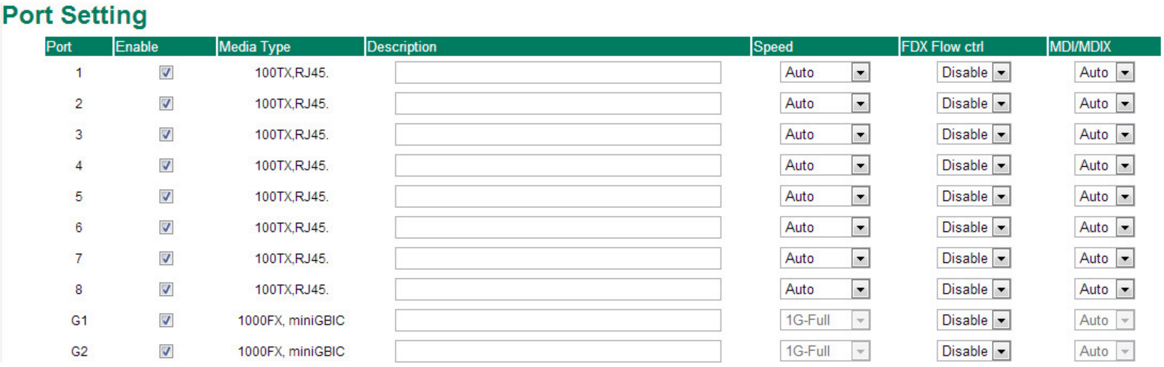
The **Reset to Factory Default** option gives users a quick way of restoring the Industrial Secure Router's configuration settings to the factory default values. This function is available in the console utility (serial or Telnet), and web browser interface.

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).



Port	Enable	Media Type	Description	Speed	FDX Flow ctrl	MDI/MDIX
1	☑	100TX,RJ45.		Auto	Disable	Auto
2	☑	100TX,RJ45.		Auto	Disable	Auto
3	☑	100TX,RJ45.		Auto	Disable	Auto
4	☑	100TX,RJ45.		Auto	Disable	Auto
5	☑	100TX,RJ45.		Auto	Disable	Auto
6	☑	100TX,RJ45.		Auto	Disable	Auto
7	☑	100TX,RJ45.		Auto	Disable	Auto
8	☑	100TX,RJ45.		Auto	Disable	Auto
G1	☑	1000FX, miniGBIC		1G-Full	Disable	Auto
G2	☑	1000FX, miniGBIC		1G-Full	Disable	Auto

Enable

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

Media Type

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

Description

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

Speed

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
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.

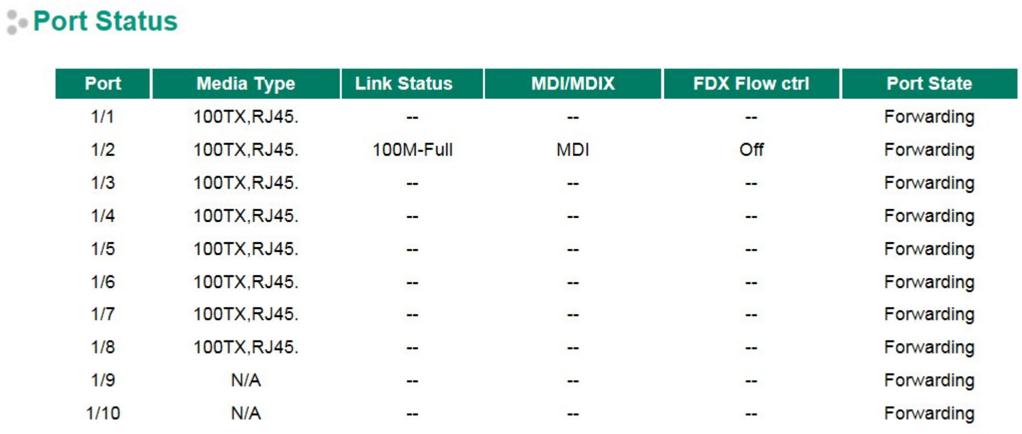
Setting	Description	Factory Default
Enable	Enables flow control for this port when the port's Speed is set to Auto.	Disabled
Disable	Disables flow control for this port when the port's Speed is set to Auto.	

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	100TX,RJ45.	--	--	--	Forwarding
1/2	100TX,RJ45.	100M-Full	MDI	Off	Forwarding
1/3	100TX,RJ45.	--	--	--	Forwarding
1/4	100TX,RJ45.	--	--	--	Forwarding
1/5	100TX,RJ45.	--	--	--	Forwarding
1/6	100TX,RJ45.	--	--	--	Forwarding
1/7	100TX,RJ45.	--	--	--	Forwarding
1/8	100TX,RJ45.	--	--	--	Forwarding
1/9	N/A	--	--	--	Forwarding
1/10	N/A	--	--	--	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 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 1600 Mbps.

The Port Trunking Concept

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

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

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

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

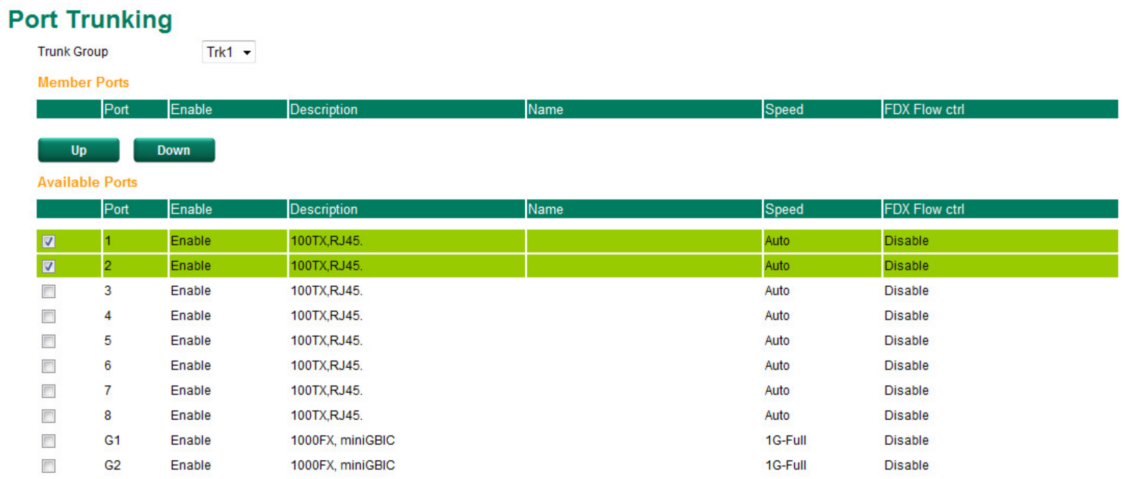
Each Moxa industrial secure router can set a maximum of 4 port trunking groups. When you activate port trunking, certain settings on each port will be reset to factory default values or disabled:

- 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.



Port Trunking

Trunk Group [Trk1 ▾]

Member Ports

	Port	Enable	Description	Name	Speed	FDX Flow ctrl

Available Ports

	Port	Enable	Description	Name	Speed	FDX Flow ctrl
☑	1	Enable	100TX,RJ45.		Auto	Disable
☑	2	Enable	100TX,RJ45.		Auto	Disable
□	3	Enable	100TX,RJ45.		Auto	Disable
□	4	Enable	100TX,RJ45.		Auto	Disable
□	5	Enable	100TX,RJ45.		Auto	Disable
□	6	Enable	100TX,RJ45.		Auto	Disable
□	7	Enable	100TX,RJ45.		Auto	Disable
□	8	Enable	100TX,RJ45.		Auto	Disable
□	G1	Enable	1000FX, miniGBIC		1G-Full	Disable
□	G2	Enable	1000FX, miniGBIC		1G-Full	Disable

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

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

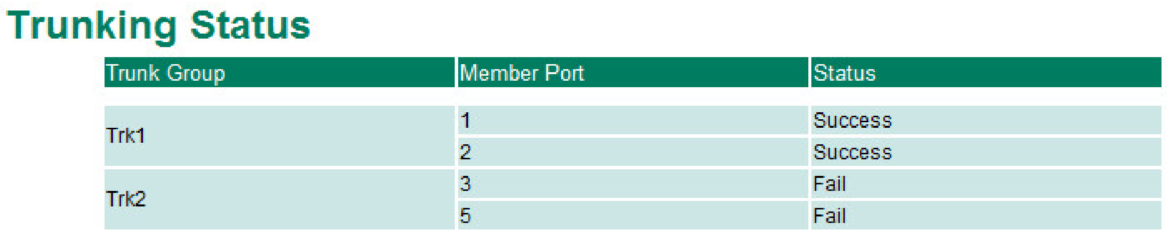
Step 3: Use **Up** and **Down** to modify the Group Members

Trunk Group (maximum of 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.

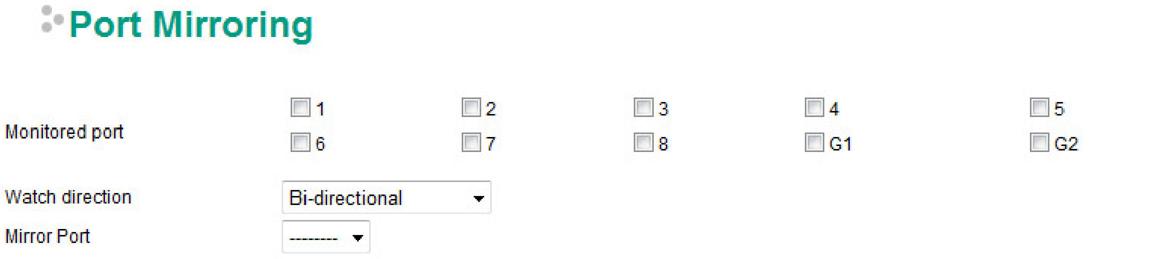


Trunking Status

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

Monitored port □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ G1 □ G2

Watch direction [Bi-directional ▾]

Mirror Port [-------- ▾]

Port Mirroring Settings

Setting	Description
Monitored Port	Select the number of the ports whose network activity will be monitored. Multiple port selection is acceptable.
Watch Direction	Select one of the following two watch direction options: • Input data stream: Select this option to monitor only those data packets coming into the Moxa 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

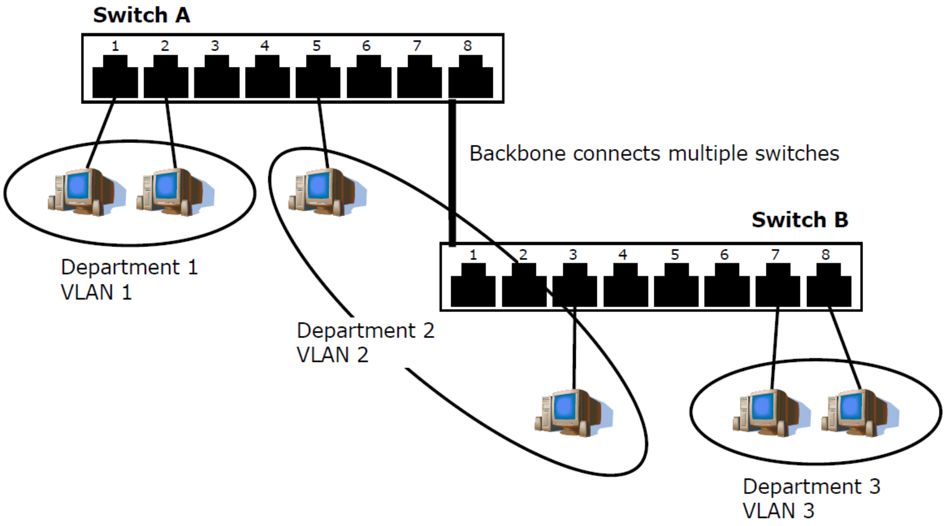
Setting up Virtual LANs (VLANs) on your Moxa industrial secure router increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

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:

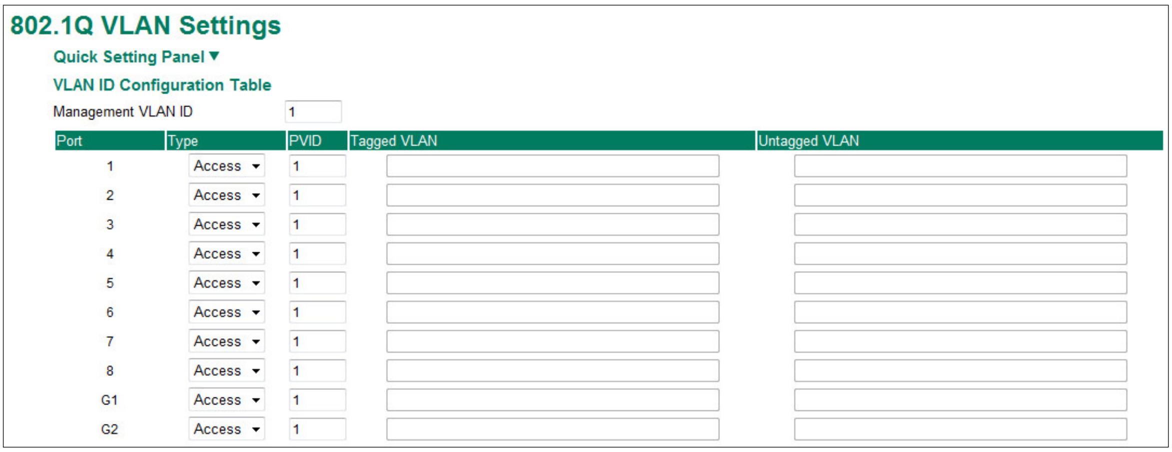
- **VLAN Name**—Management VLAN
- **802.1Q VLAN ID**—1 (if tagging is required)

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



802.1Q VLAN Settings

Quick Setting Panel ▼

VLAN ID Configuration Table

Management VLAN ID: 1

Port	Type	PVID	Tagged VLAN	Untagged VLAN
1	Access	1		
2	Access	1		
3	Access	1		
4	Access	1		
5	Access	1		
6	Access	1		
7	Access	1		
8	Access	1		
G1	Access	1		
G2	Access	1		

Management VLAN ID

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

Port Type

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

PVID

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

Tagged VLAN

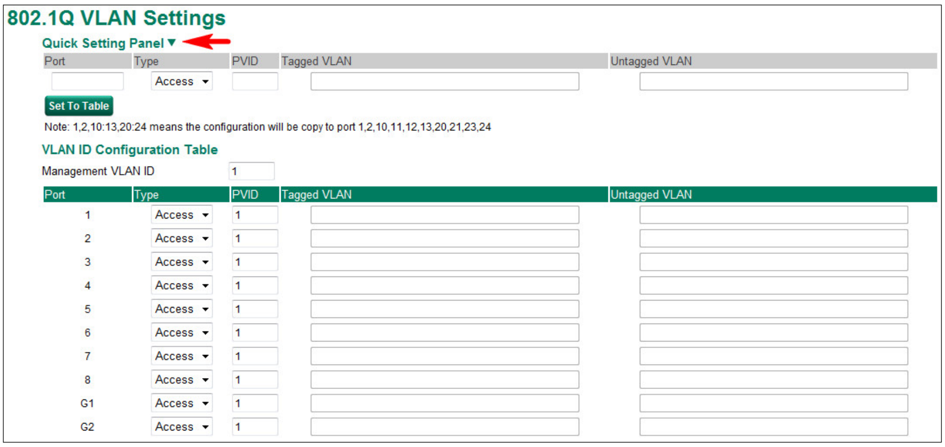
Setting	Description	Factory Default
VLAN ID from 1-4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	None

Untagged VLAN

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

Quick Setting Panel

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



802.1Q VLAN Settings

Quick Setting Panel ▼

Port	Type	PVID	Tagged VLAN	Untagged VLAN
	Access			

Note: 1,2,10:13,20:24 means the configuration will be copy to port 1,2,10,11,12,13,20,21,23,24

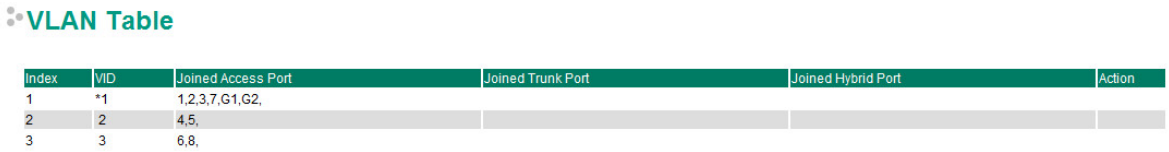
VLAN ID Configuration Table

Management VLAN ID: 1

Port	Type	PVID	Tagged VLAN	Untagged VLAN
1	Access	1		
2	Access	1		
3	Access	1		
4	Access	1		
5	Access	1		
6	Access	1		
7	Access	1		
8	Access	1		
G1	Access	1		
G2	Access	1		

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

VLAN Table



VLAN Table

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

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

Multicast

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

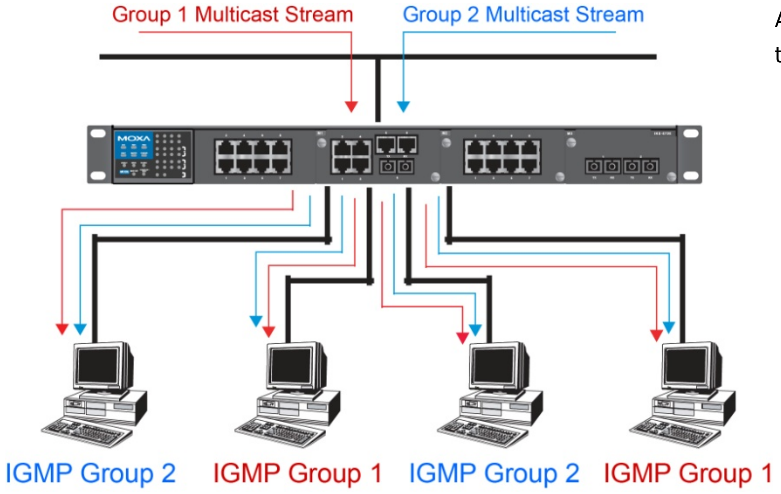
- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and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

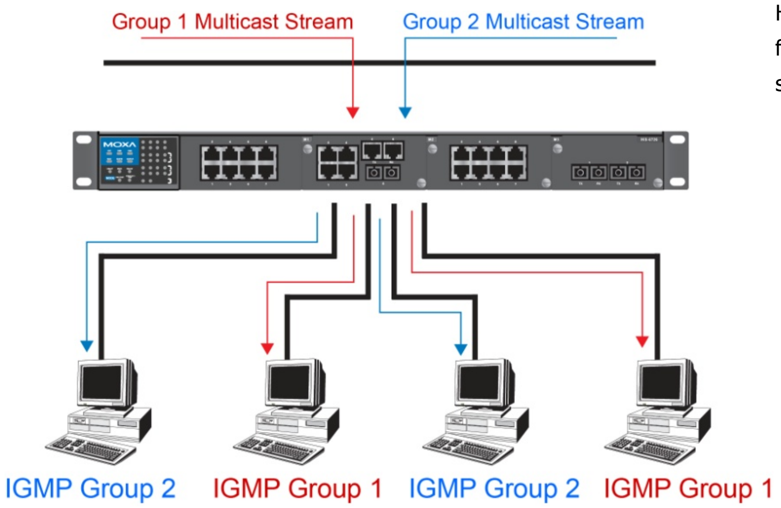
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves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

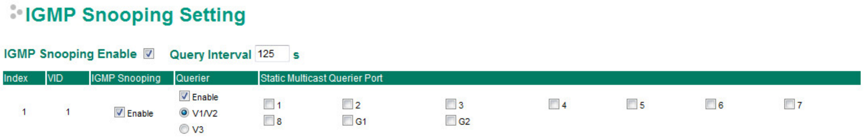
Enabling Multicast Filtering

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



IGMP Snooping Setting

IGMP Snooping Enable ☑ Query Interval 125 s

Index	VID	IGMP Snooping	Querier	Static Multicast Querier Port
1	1	☑ Enable	☑ Enable ● V1/V2 ○ V3	□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ G1 □ G2

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

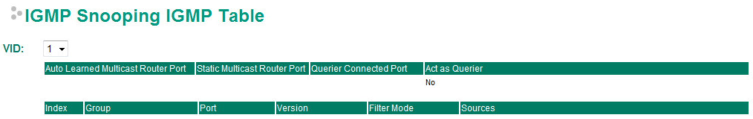
Setting	Description	Factory Default
Select/Deselect	Select the ports that will connect to the multicast routers. These ports will receive all multicast packets from the source. This option is only active when IGMP Snooping is enabled.	Disabled

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.



IGMP Snooping IGMP Table

VID: 1

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

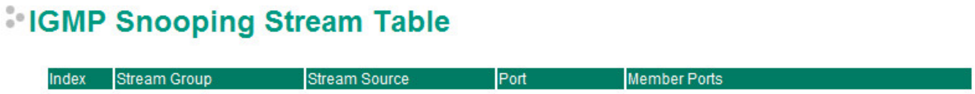
Index	Group	Port	Version	Filter Mode	Sources

The information shown in the table includes:

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



IGMP Snooping Stream Table

Index	Stream Group	Stream Source	Port	Member Ports

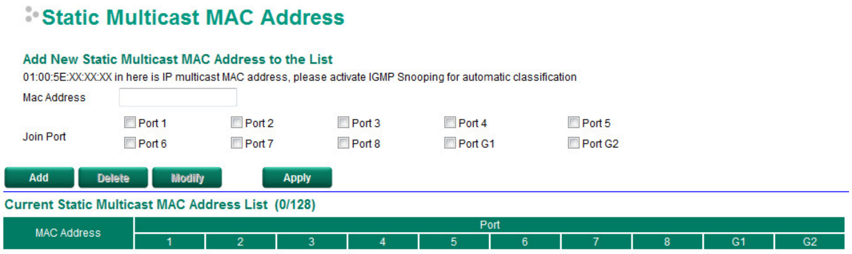
Stream Group: Multicast group IP address

Stream Source: Multicast source IP address

Port: Which port receives the multicast stream

Member ports: Ports the multicast stream is forwarded to

Static Multicast MAC



Static Multicast MAC Address

Add New Static Multicast MAC Address to the List

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

Mac Address

Join Port □ Port 1 □ Port 2 □ Port 3 □ Port 4 □ Port 5 □ Port 6 □ Port 7 □ Port 8 □ Port G1 □ Port G2

Current Static Multicast MAC Address List (0/128)

MAC Address	Port									
	1	2	3	4	5	6	7	8	G1	G2

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

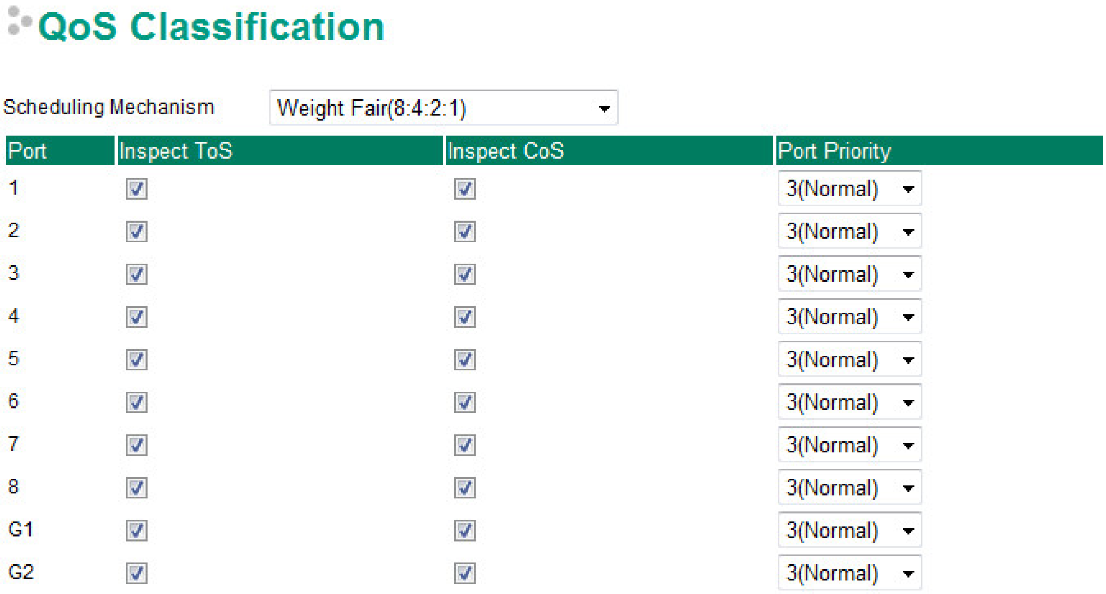
Setting	Description	Factory Default
Integer	Input the number of the VLAN that the host with this MAC address belongs to.	None

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



QoS Classification

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

Port	Inspect ToS	Inspect CoS	Port Priority
1	☑	☑	3(Normal)
2	☑	☑	3(Normal)
3	☑	☑	3(Normal)
4	☑	☑	3(Normal)
5	☑	☑	3(Normal)
6	☑	☑	3(Normal)
7	☑	☑	3(Normal)
8	☑	☑	3(Normal)
G1	☑	☑	3(Normal)
G2	☑	☑	3(Normal)

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

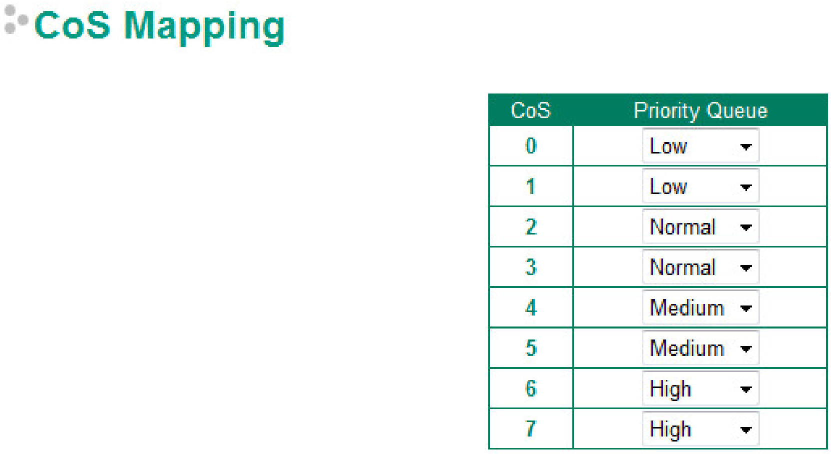
Setting	Description	Factory Default
Port priority	The port priority has 4 priority queues. Low, normal, medium, high priority queue option is applied to each port.	3(Normal)

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



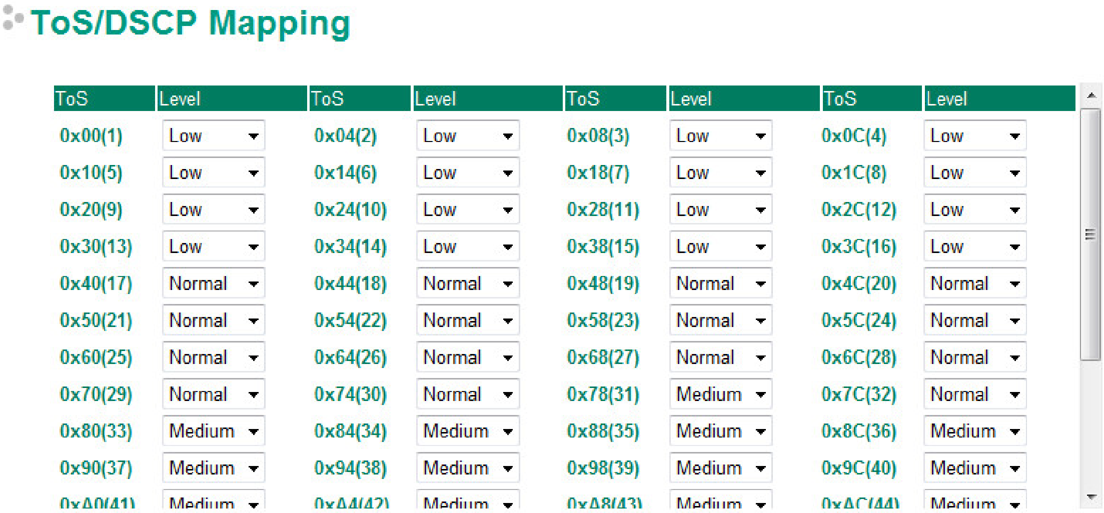
CoS Mapping

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

CoS Value and Priority Queues

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

ToS/DSCP Mapping



ToS/DSCP Mapping

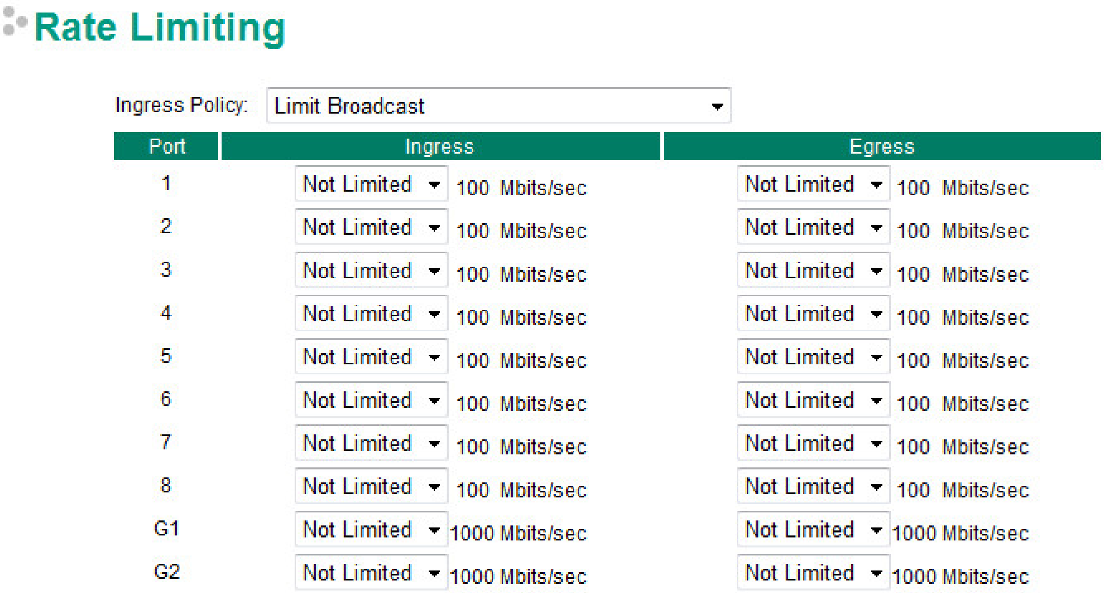
ToS	Level	ToS	Level	ToS	Level	ToS	Level
0x00(1)	Low	0x04(2)	Low	0x08(3)	Low	0x0C(4)	Low
0x10(5)	Low	0x14(6)	Low	0x18(7)	Low	0x1C(8)	Low
0x20(9)	Low	0x24(10)	Low	0x28(11)	Low	0x2C(12)	Low
0x30(13)	Low	0x34(14)	Low	0x38(15)	Low	0x3C(16)	Low
0x40(17)	Normal	0x44(18)	Normal	0x48(19)	Normal	0x4C(20)	Normal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

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.



Rate Limiting

Ingress Policy: Limit Broadcast

Port	Ingress		Egress	
1	Not Limited	100 Mbits/sec	Not Limited	100 Mbits/sec
2	Not Limited	100 Mbits/sec	Not Limited	100 Mbits/sec
3	Not Limited	100 Mbits/sec	Not Limited	100 Mbits/sec
4	Not Limited	100 Mbits/sec	Not Limited	100 Mbits/sec
5	Not Limited	100 Mbits/sec	Not Limited	100 Mbits/sec
6	Not Limited	100 Mbits/sec	Not Limited	100 Mbits/sec
7	Not Limited	100 Mbits/sec	Not Limited	100 Mbits/sec
8	Not Limited	100 Mbits/sec	Not Limited	100 Mbits/sec
G1	Not Limited	1000 Mbits/sec	Not Limited	1000 Mbits/sec
G2	Not Limited	1000 Mbits/sec	Not Limited	1000 Mbits/sec

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		

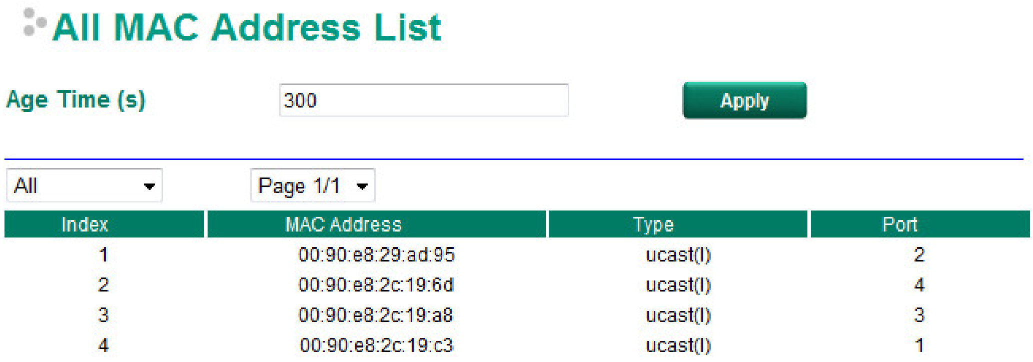
Ingress/Egress Rate

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.



All MAC Address List

Age Time (s): 300

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

Drop Down List

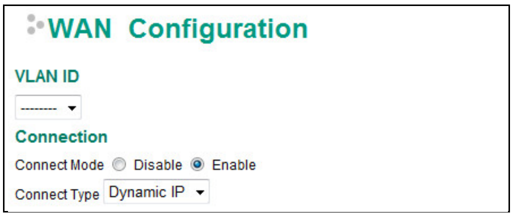
ALL	Select this item to show all of the Moxa industrial secure router's MAC addresses.
ALL Learned	Select this item to show all of the Moxa industrial secure router's Learned MAC addresses.
ALL Static	Select this item to show all of the Moxa industrial secure router's Static, Static Lock, and Static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


WAN Configuration

VLAN ID

Connection

Connect Mode ○ Disable ● Enable

Connect Type Dynamic IP

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.

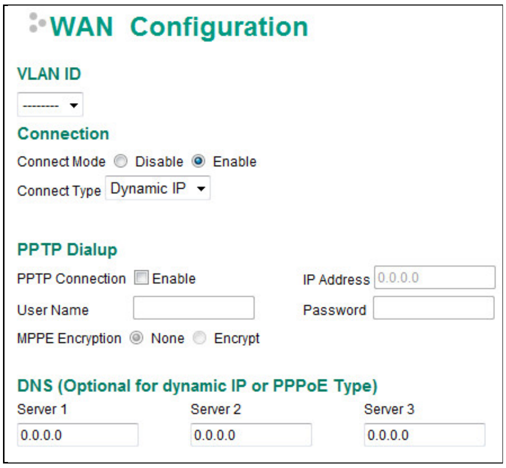
Connection Mode

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


WAN Configuration

VLAN ID

Connection

Connect Mode ○ Disable ● Enable

Connect Type Dynamic IP

PPTP Dialup

PPTP Connection □ Enable

IP Address 0.0.0.0

User Name

Password

MPPE Encryption ● None ○ Encrypt

DNS (Optional for dynamic IP or PPPoE Type)

Server 1 0.0.0.0

Server 2 0.0.0.0

Server 3 0.0.0.0

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

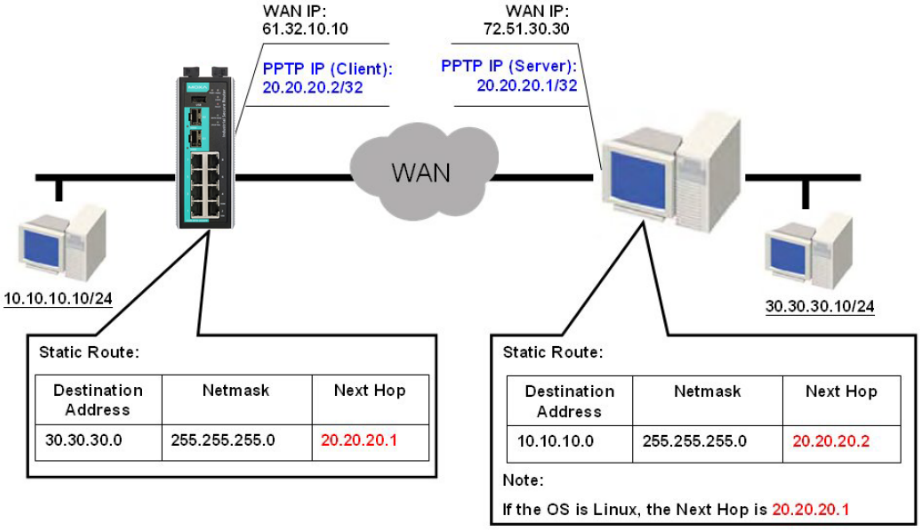
Setting	**Description**	**Factory Default**
Max. 30 characters	The password for dialing the PPTP service	None

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.



Static Route:

Destination Address	Netmask	Next Hop
30.30.30.0	255.255.255.0	20.20.20.1

Static Route:

Destination Address	Netmask	Next Hop
10.10.10.0	255.255.255.0	20.20.20.2

Note:

If the OS is Linux, the Next Hop is 20.20.20.1

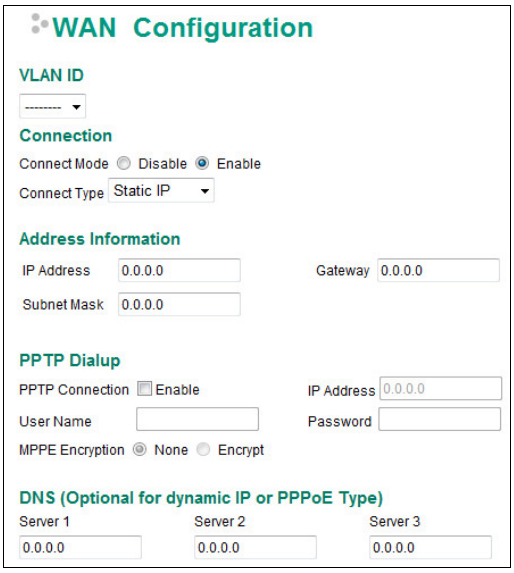
DNS (Doman Name Server; optional setting for Dynamic IP and PPPoE types)

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



WAN Configuration

VLAN ID

Connection

Connect Mode ○ Disable ● Enable

Connect Type Static IP

Address Information

IP Address 0.0.0.0 Gateway 0.0.0.0

Subnet Mask 0.0.0.0

PPTP Dialup

PPTP Connection □ Enable IP Address 0.0.0.0

User Name Password

MPPE Encryption ● None ○ Encrypt

DNS (Optional for dynamic IP or PPPoE Type)

Server 1 0.0.0.0 Server 2 0.0.0.0 Server 3 0.0.0.0

Address Information

IP Address

Setting	Description	Factory Default
IP Address	The interface IP address	None

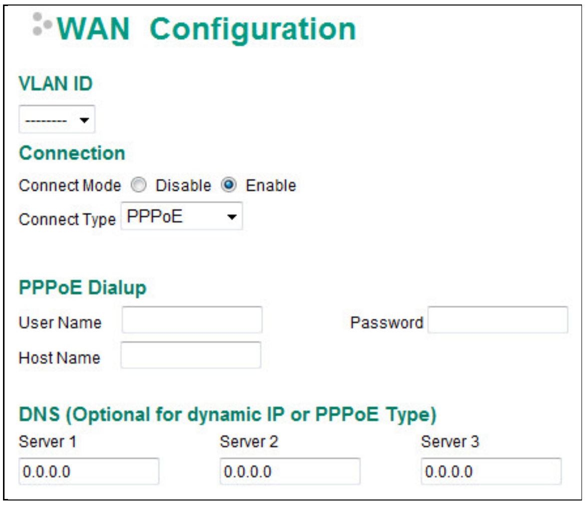
Subnet Mask

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



WAN Configuration

VLAN ID

Connection

Connect Mode ○ Disable ● Enable

Connect Type PPPoE

PPPoE Dialup

User Name Password

Host Name

DNS (Optional for dynamic IP or PPPoE Type)

Server 1 0.0.0.0 Server 2 0.0.0.0 Server 3 0.0.0.0

PPPoE Dialup

User Name

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

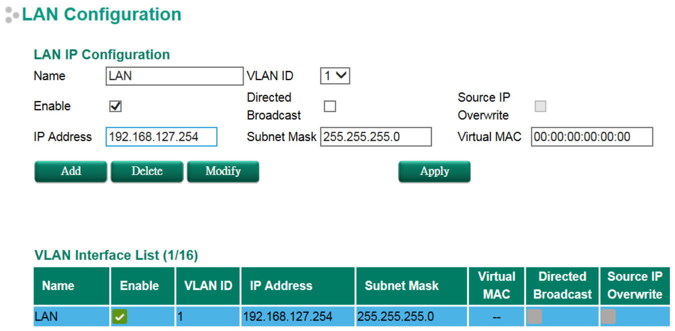
Host Name

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



LAN Configuration

LAN IP Configuration

Name	LAN	VLAN ID	1		
Enable	☑	Directed Broadcast	☐	Source IP Overwrite	☐
IP Address	192.168.127.254	Subnet Mask	255.255.255.0	Virtual MAC	00:00:00:00:00:00

VLAN Interface List (1/16)

Name	Enable	VLAN ID	IP Address	Subnet Mask	Virtual MAC	Directed Broadcast	Source IP Overwrite
LAN	☑	1	192.168.127.254	255.255.255.0	--	☐	☐

Create aVLAN Interface

Input a name of the LAN interface, select a VLAN ID that is already configured in VLAN Setting under the Layer 2 Function, and assign an IP address/Subnet Mask/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

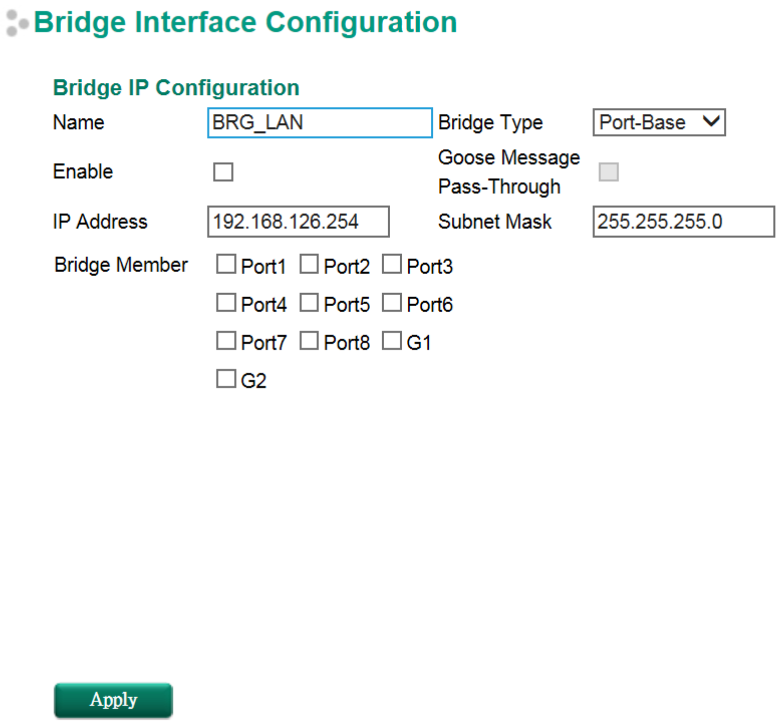
After adding/deleting/modifying any LAN interface, be sure to click **Activate**.

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.



Bridge Interface Configuration

Bridge IP Configuration

Name: BRG_LAN Bridge Type: Port-Base

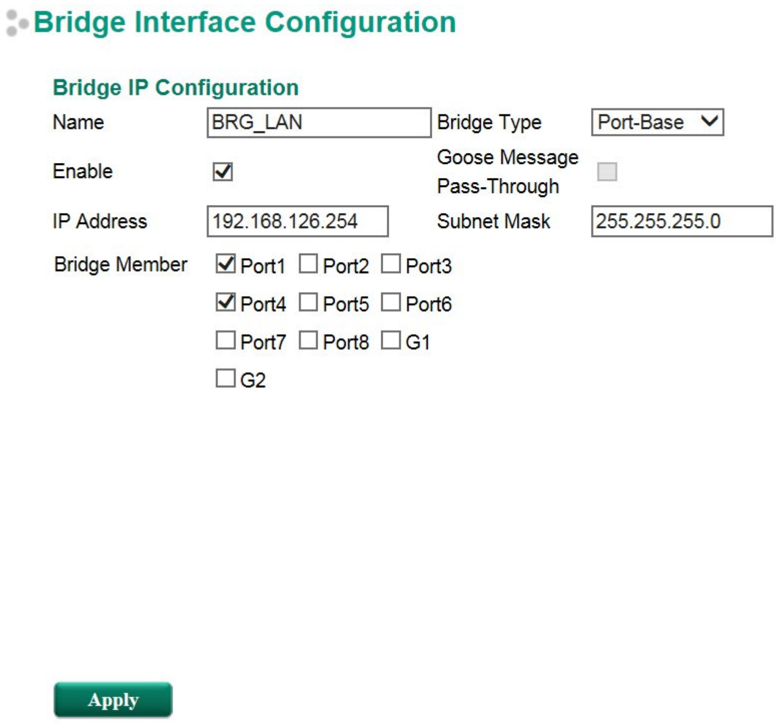
Enable: □ Goose Message Pass-Through: □

IP Address: 192.168.126.254 Subnet Mask: 255.255.255.0

Bridge Member: □ Port1 □ Port2 □ Port3 □ Port4 □ Port5 □ Port6 □ Port7 □ Port8 □ G1 □ G2

Adding Ports/VLANs into the Bridge Interface

Port Base



Bridge Interface Configuration

Bridge IP Configuration

Name: BRG_LAN Bridge Type: Port-Base

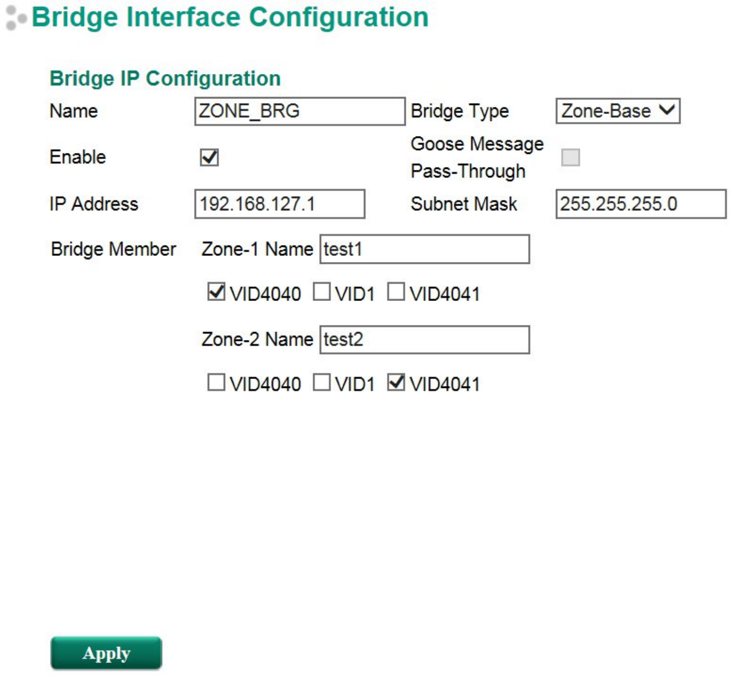
Enable: ☑ Goose Message Pass-Through: □

IP Address: 192.168.126.254 Subnet Mask: 255.255.255.0

Bridge Member: ☑ Port1 □ Port2 □ Port3 ☑ Port4 □ Port5 □ Port6 □ Port7 □ Port8 □ G1 □ G2

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



Bridge Interface Configuration

Bridge IP Configuration

Name: ZONE_BRG   Bridge Type: Zone-Base

Enable: ☑   Goose Message Pass-Through: □

IP Address: 192.168.127.1   Subnet Mask: 255.255.255.0

Bridge Member: Zone-1 Name: test1

☑ VID4040 □ VID1 □ VID4041

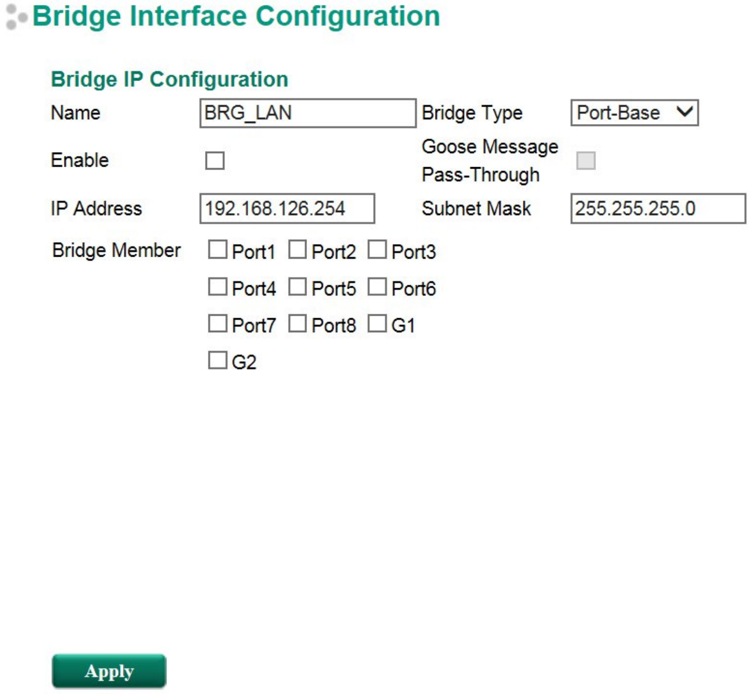
Zone-2 Name: test2

□ VID4040 □ VID1 ☑ VID4041

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.



Bridge Interface Configuration

Bridge IP Configuration

Name: BRG_LAN   Bridge Type: Port-Base

Enable: □   Goose Message Pass-Through: □

IP Address: 192.168.126.254   Subnet Mask: 255.255.255.0

Bridge Member: □ Port1 □ Port2 □ Port3

□ Port4 □ Port5 □ Port6

□ Port7 □ Port8 □ G1

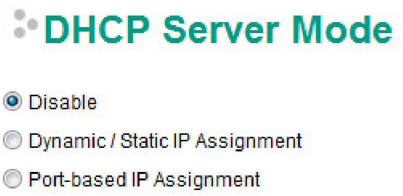
□ G2

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

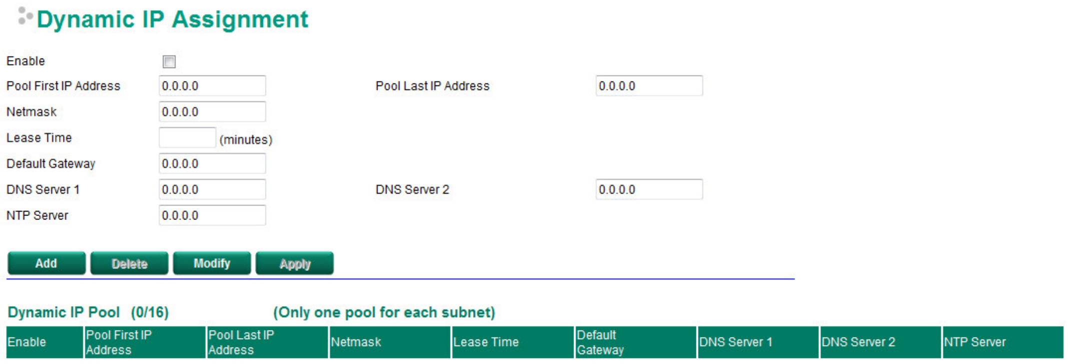
● Disable
○ Dynamic / Static IP Assignment
○ Port-based IP Assignment

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.



Dynamic IP Assignment

Enable □
Pool First IP Address 0.0.0.0 Pool Last IP Address 0.0.0.0
Netmask 0.0.0.0
Lease Time (minutes)
Default Gateway 0.0.0.0
DNS Server 1 0.0.0.0 DNS Server 2 0.0.0.0
NTP Server 0.0.0.0

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

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

<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

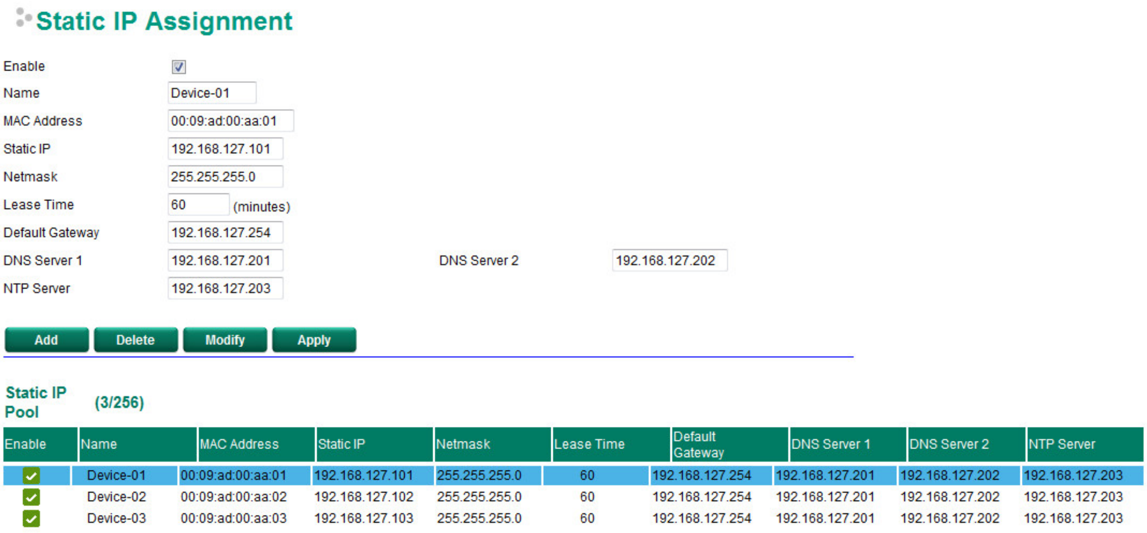
Setting	Description	Factory Default
IP Address	The NTP server for DHCP clients	0.0.0.0

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.



Static IP Assignment

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

Static IP Pool (3/256)

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

In the above example, a device named “Device-01” was added to the Static DHCP list, with a static IP address set to 192.168.127.101 and MAC address set to 00:09:ad:00:aa:01. When a device with a MAC address of 00:09:ad:00:aa:01 is connected to the 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	None

Default Gateway

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

DNS Server

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

NTP Server

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

Clickable Buttons

Add

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

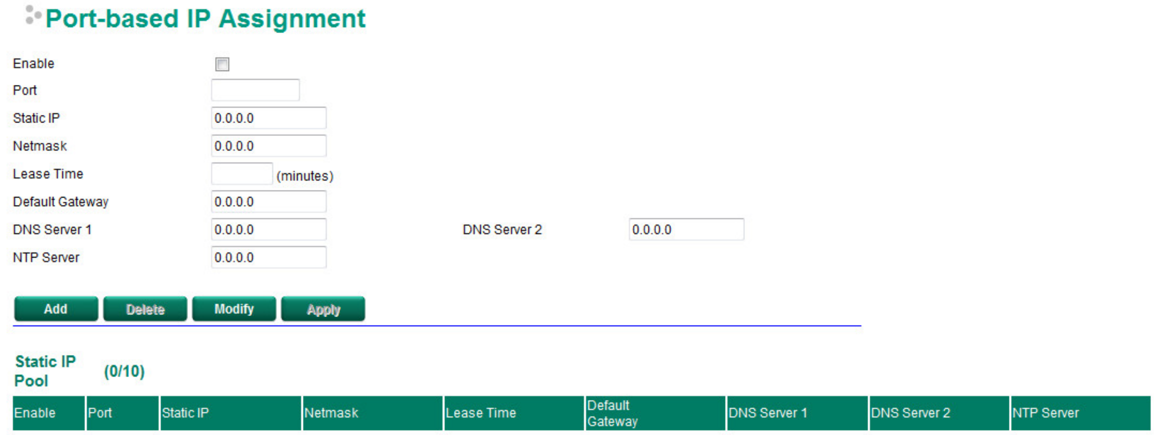
Delete

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

Modify

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

IP-Port Binding



Port-based IP Assignment

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

Static IP Pool (0/10)

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

IP-Port Binding Enable/Disable

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

Port

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

Static IP

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

Netmask

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

Lease Time

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

Default Gateway

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

DNS Server

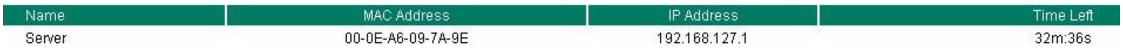
Setting	Description	Factory Default
IP Address	The DNS server for the connected device	0.0.0.0

NTP Server

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

Client List

Use the Client List to view the current DHCP clients.



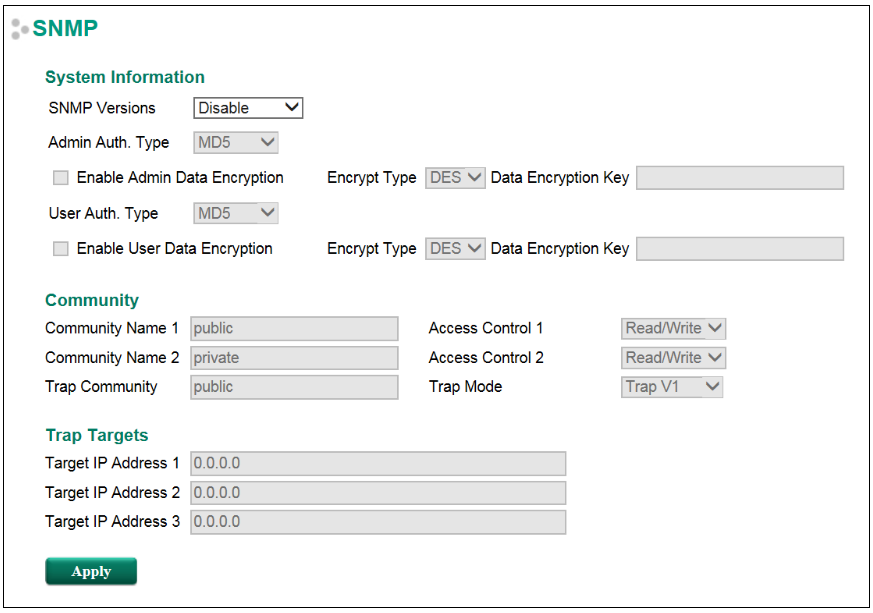
Name	MAC Address	IP Address	Time Left
Server	00-0E-A6-09-7A-9E	192.168.127.1	32m:36s

SNMP Settings

The 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

System Information

SNMP Versions: Disable

Admin Auth. Type: MD5

☐ Enable Admin Data Encryption Encrypt Type: DES Data Encryption Key:

User Auth. Type: MD5

☐ Enable User Data Encryption Encrypt Type: DES Data Encryption Key:

Community

Community Name 1: public Access Control 1: Read/Write

Community Name 2: private Access Control 2: Read/Write

Trap Community: public Trap Mode: Trap V1

Trap Targets

Target IP Address 1: 0.0.0.0

Target IP Address 2: 0.0.0.0

Target IP Address 3: 0.0.0.0

SNMP Versions

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

Auth. Type

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

Data Encryption Enable/Disable

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

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

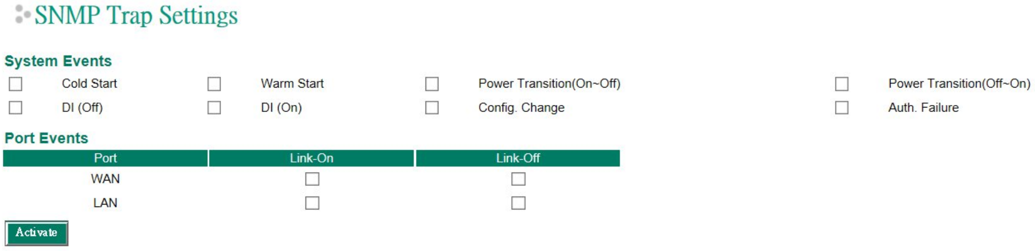
Setting	Description	Factory Default
Read/Write	Access control type after matching the community string	Read/Write
Read only (Public MIB only)		
No Access		

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.

SNMP Trap Setting

For EDR-G902/G903, when the events listed below occur, users can decide whether to send SNMP trap to notify the administrator.



SNMP Trap Settings

System Events

□ Cold Start	□ Warm Start	□ Power Transition(On~Off)	□ Power Transition(Off~On)
□ DI (Off)	□ DI (On)	□ Config. Change	□ Auth. Failure

Port Events

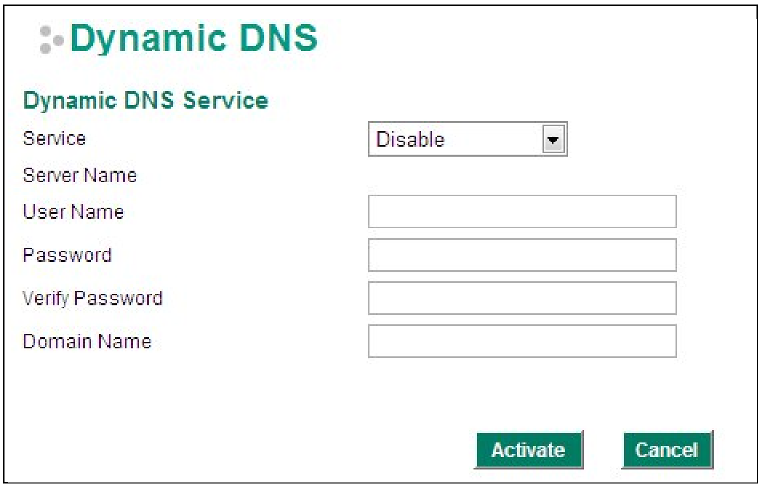
Port	Link-On	Link-Off
WAN	□	□
LAN	□	□

System Events	Description
Cold Start	Power is cut off and then reconnected.
Warm Start	Moxa's industrial secure router is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On->Off)	Moxa's industrial secure router is powered down.
Power Transition (Off->On)	Moxa's 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.

Port Events	Description
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).

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.



Dynamic DNS

Dynamic DNS Service

Service	Disable
Server Name	
User Name	
Password	
Verify Password	
Domain Name	

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

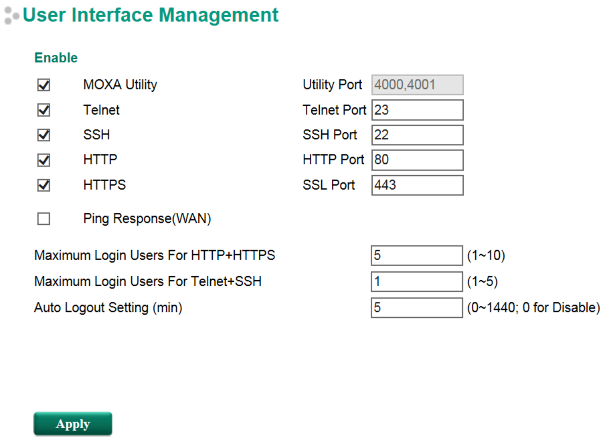
Setting	Description	Factory Default
Max. 30 characters	Verifies the DNS server password	None

Domain name

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

Security

User Interface Management



User Interface Management

Enable

☑	MOXA Utility	Utility Port	4000,4001
☑	Telnet	Telnet Port	23
☑	SSH	SSH Port	22
☑	HTTP	HTTP Port	80
☑	HTTPS	SSL Port	443
☐	Ping Response(WAN)		

Maximum Login Users For HTTP+HTTPS 5 (1~10)

Maximum Login Users For Telnet+SSH 1 (1~5)

Auto Logout Setting (min) 5 (0~1440; 0 for Disable)

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+HTTTPS	Set a limit for the amount of users who can be logged in to the EDR-810 using HTTP and HTTPS. The maximum number of users using HTTP and HTTPS is 10.	N/A

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 EDR-810 using HTTP and HTTPS. The maximum supported user numbers of Telnet+SSH is 5.	N/A

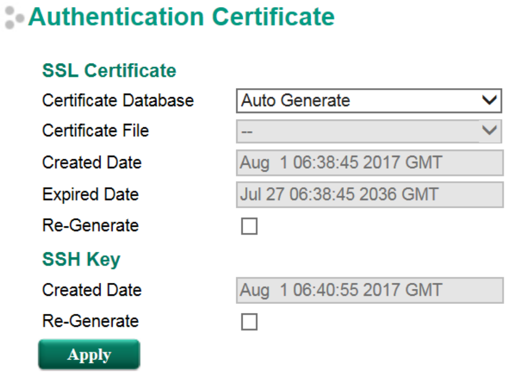
Auto Logout Setting (min)

Setting	Description	Factory Default
Auto Logout Setting (min)	When the user does not touch the EDR-810 management interface for a defined period of time, the management interface will logout automatically. The EDR-810 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 EDR-810 automatically or users can choose the certificate imported in Local certificate.



Authentication Certificate

SSL Certificate

Certificate Database	Auto Generate
Certificate File	--
Created Date	Aug 1 06:38:45 2017 GMT
Expired Date	Jul 27 06:38:45 2036 GMT
Re-Generate	□

SSH Key

Created Date	Aug 1 06:40:55 2017 GMT
Re-Generate	□

Certificate Database

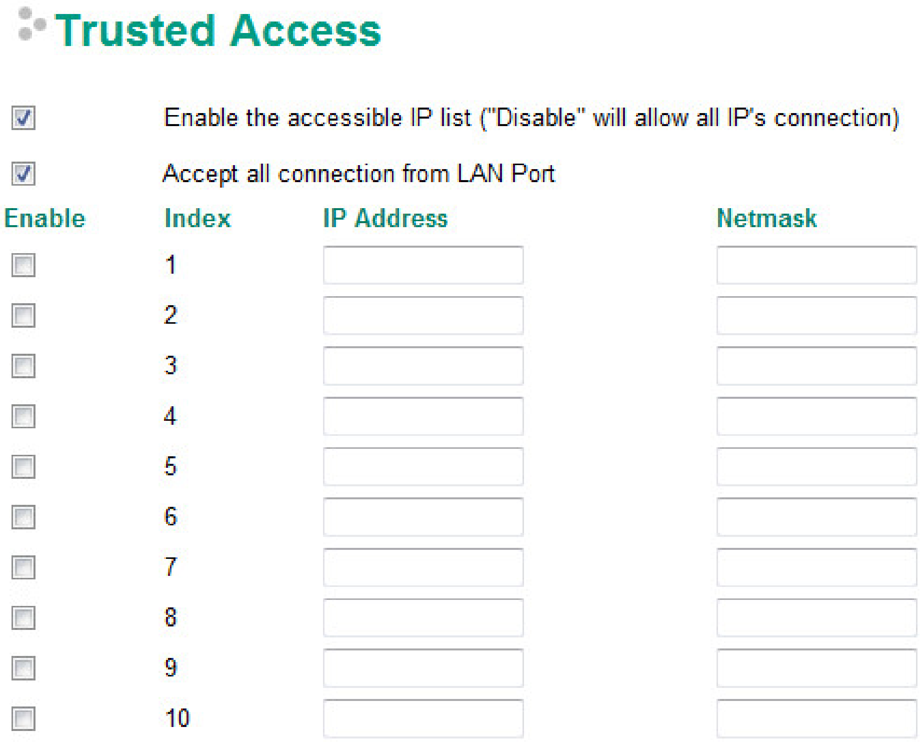
Setting	Description	Factory Default
Auto Generate	The EDR-810 will generate a certificate automatically. If not, please select "Re-Generate" to generate a certificate. Auto Generate is the default setting.	Auto Generate
Local Certificate Database	Select the certificate you import into Local Certificate. The certificate that is loaded here is limited to "Certificate from CSR" and "Certificate From PKCS#12".	

SSH Key Re-generate

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

Trusted Access

The EDR-810 uses an IP address-based filtering method to control access.



Trusted Access

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

☑ Accept all connection from LAN Port

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

You may add or remove IP addresses to limit access to the Moxa 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:

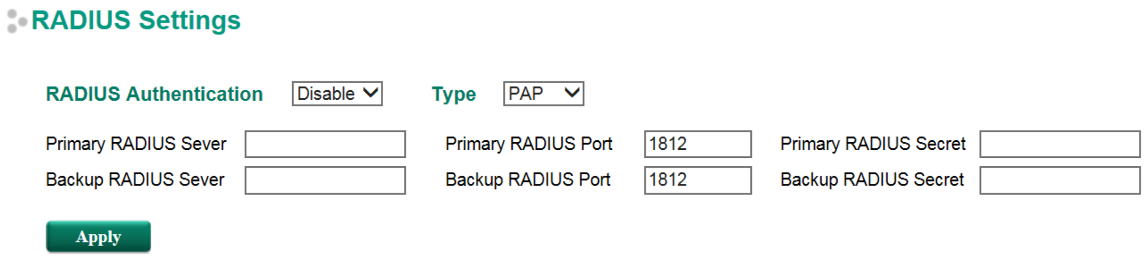
- **Grant access to one host with a specific IP address**
  For example, enter IP address 192.168.1.1 with netmask 255.255.255.255 to allow access to 192.168.1.1 only.
- **Grant access to any host on a specific subnetwork**
  For example, enter IP address 192.168.1.0 with netmask 255.255.255.0 to allow 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

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 EDR-810 will switch the connection to the backup RADIUS server.



RADIUS Settings

RADIUS Authentication: Disable
Type: PAP

Primary RADIUS Sever:
Primary RADIUS Port: 1812
Primary RADIUS Secret:

Backup RADIUS Sever:
Backup RADIUS Port: 1812
Backup RADIUS Secret:

Radius Status

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

Type

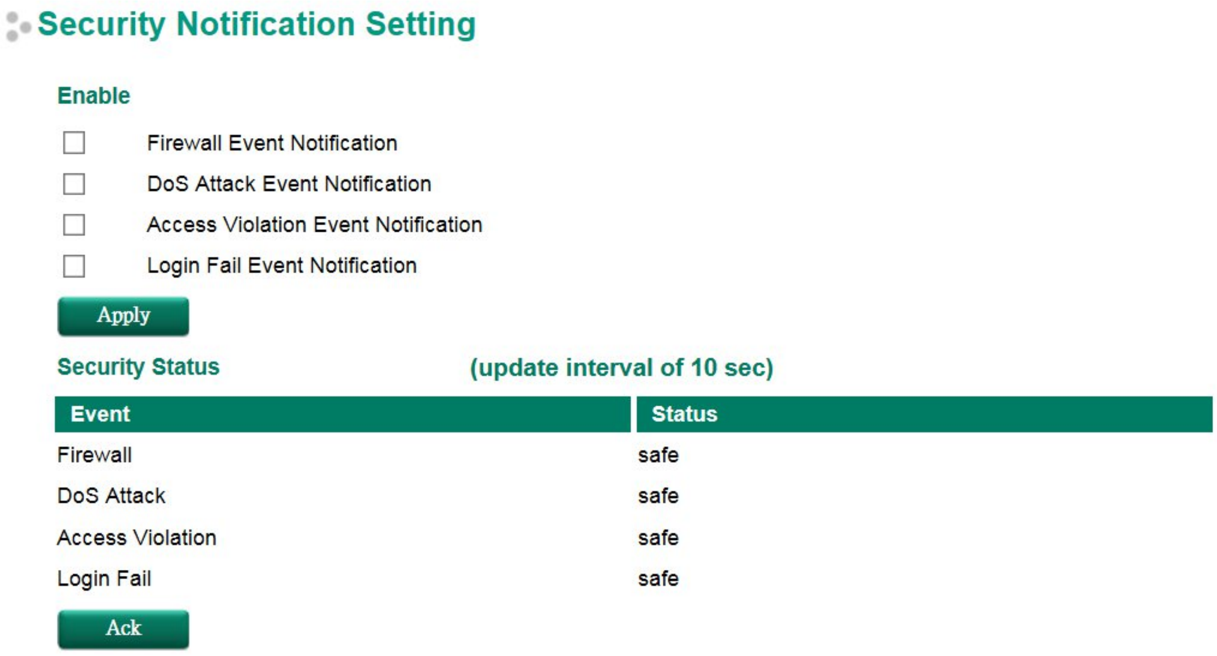
Setting	Description	Factory Default
PAP	Authentication type of Radius server	PAP
CHAP		

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

Security Notification Setting

When the events below are displayed, the EDR-810 will send an SNMP trap to notify the server.



Security Notification Setting

Enable

□ Firewall Event Notification

□ DoS Attack Event Notification

□ Access Violation Event Notification

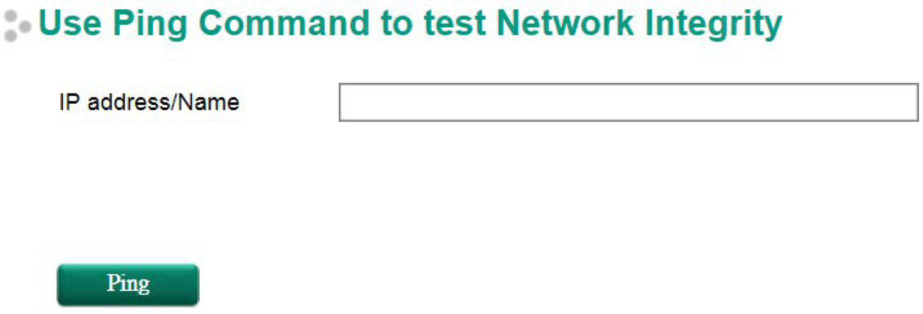
□ Login Fail Event Notification

Security Status (update interval of 10 sec)

Event	Status
Firewall	safe
DoS Attack	safe
Access Violation	safe
Login Fail	safe

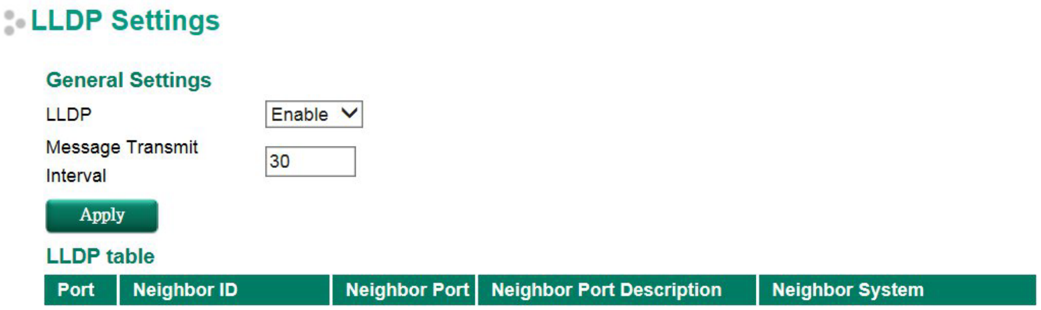
Diagnosis

When the system is setup, users can send an ICMP command-Ping to verify if the connection or firewall is functioning.



Use Ping Command to test Network Integrity

IP address/Name



LLDP Settings

General Settings

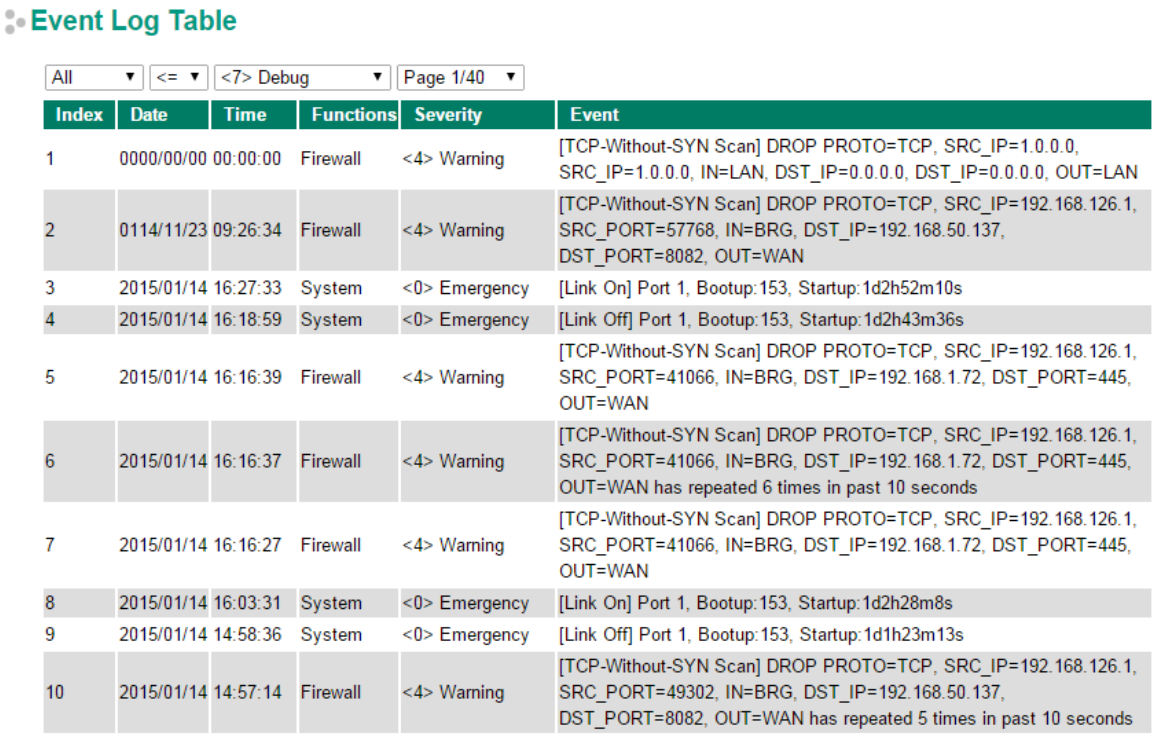
LLDP: Enable

Message Transmit Interval: 30

LLDP table

Port	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System

Event Log

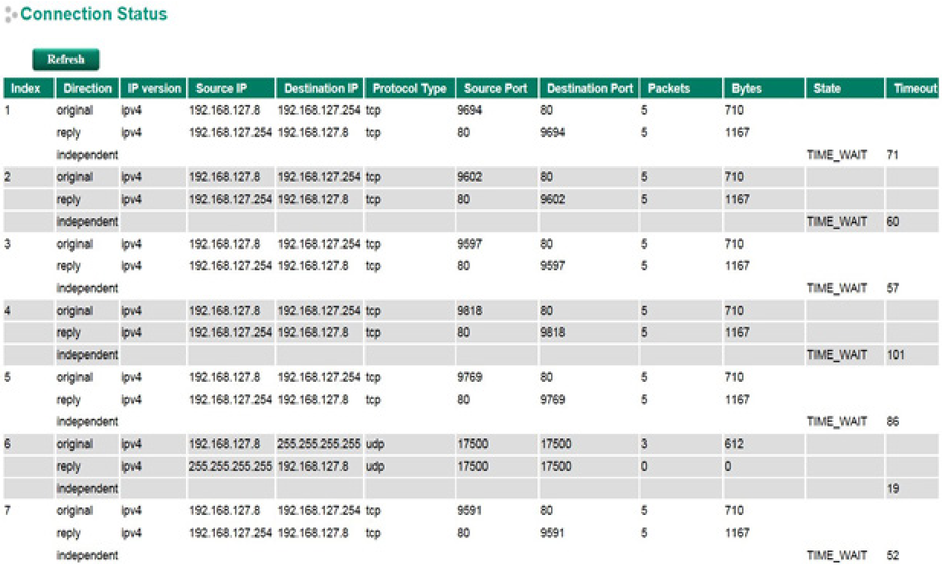


Index	Date	Time	Functions	Severity	Event
1	0000/00/00	00:00:00	Firewall	<4> Warning	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=1.0.0.0, SRC_IP=1.0.0.0, IN=LAN, DST_IP=0.0.0.0, DST_IP=0.0.0.0, OUT=LAN
2	0114/11/23	09:26:34	Firewall	<4> Warning	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.126.1, 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**.

Connection Status

For the connection status, the user can monitor most types of connection status including NAT, firewall, routing, and VPN. The data connection are will be shown in the list, e.g. source/ destination IP, protocol, and packet amount.



Index	Direction	IP version	Source IP	Destination IP	Protocol Type	Source Port	Destination Port	Packets	Bytes	State	Timeout
1	original	ipv4	192.168.127.8	192.168.127.254	tcp	9694	80	5	710		
	reply	ipv4	192.168.127.254	192.168.127.8	tcp	80	9694	5	1167		
	independent									TIME_WAIT	71
2	original	ipv4	192.168.127.8	192.168.127.254	tcp	9602	80	5	710		
	reply	ipv4	192.168.127.254	192.168.127.8	tcp	80	9602	5	1167		
	independent									TIME_WAIT	60
3	original	ipv4	192.168.127.8	192.168.127.254	tcp	9597	80	5	710		
	reply	ipv4	192.168.127.254	192.168.127.8	tcp	80	9597	5	1167		
	independent									TIME_WAIT	57
4	original	ipv4	192.168.127.8	192.168.127.254	tcp	9818	80	5	710		
	reply	ipv4	192.168.127.254	192.168.127.8	tcp	80	9818	5	1167		
	independent									TIME_WAIT	101
5	original	ipv4	192.168.127.8	192.168.127.254	tcp	9769	80	5	710		
	reply	ipv4	192.168.127.254	192.168.127.8	tcp	80	9769	5	1167		
	independent									TIME_WAIT	86
6	original	ipv4	192.168.127.8	255.255.255.255	udp	17500	17500	3	612		
	reply	ipv4	255.255.255.255	192.168.127.8	udp	17500	17500	0	0		
	independent										19
7	original	ipv4	192.168.127.8	192.168.127.254	tcp	9591	80	5	710		
	reply	ipv4	192.168.127.254	192.168.127.8	tcp	80	9591	5	1167		
	independent									TIME_WAIT	52

4

EDR-G902/G903 Series Features and Functions

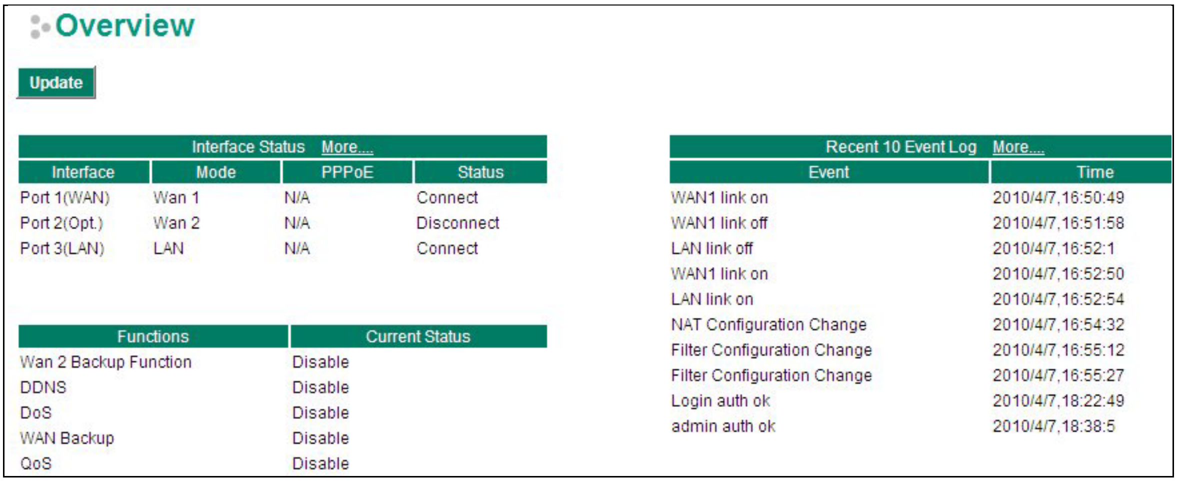
The following topics are covered in this chapter:

- **Overview**
- **Configuring Basic Settings**
  - System Identification
  - Hardware Acceleration
  - Accessible IP
  - Password
  - Time
  - SettingCheck
  - Relay Event Setup
- **Warning**
  - System Event Setting
  - System File Update—by Remote TFTP
  - System File Update—by Local Import/Export
  - Backup Media
  - Restart
  - Reset to Factory Default
- **Network Settings**
  - Mode Configuration
  - Link Fault Passthrough
  - MTU Configuration (for EDR-810/G902/G903)
  - Speed Configuration
  - WAN1 Configuration
  - WAN2 Configuration (includes DMZ Enable)
  - Using DMZ Mode
  - LAN Interface
  - 802.1Q VLAN Setting
- **Communication Redundancy**
  - WAN Backup (EDR-G903 only)
- **Security**
  - User Interface Management
  - Authentication Certificate
  - RADIUS Settings
  - Traffic Prioritization Setup
- **Monitor**
- **System Log**

- EventLog
- Syslog

Overview

The **Overview** page is divided into three major parts: Interface Status, Basic function status, and Recent 10 Event logs, and gives users a quick overview of the EtherDevice Router's current settings.



Overview

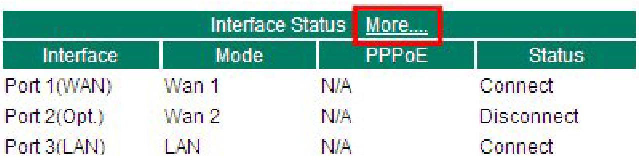
Update

Interface Status More....			
Interface	Mode	PPPoE	Status
Port 1(WAN)	Wan 1	N/A	Connect
Port 2(Opt.)	Wan 2	N/A	Disconnect
Port 3(LAN)	LAN	N/A	Connect

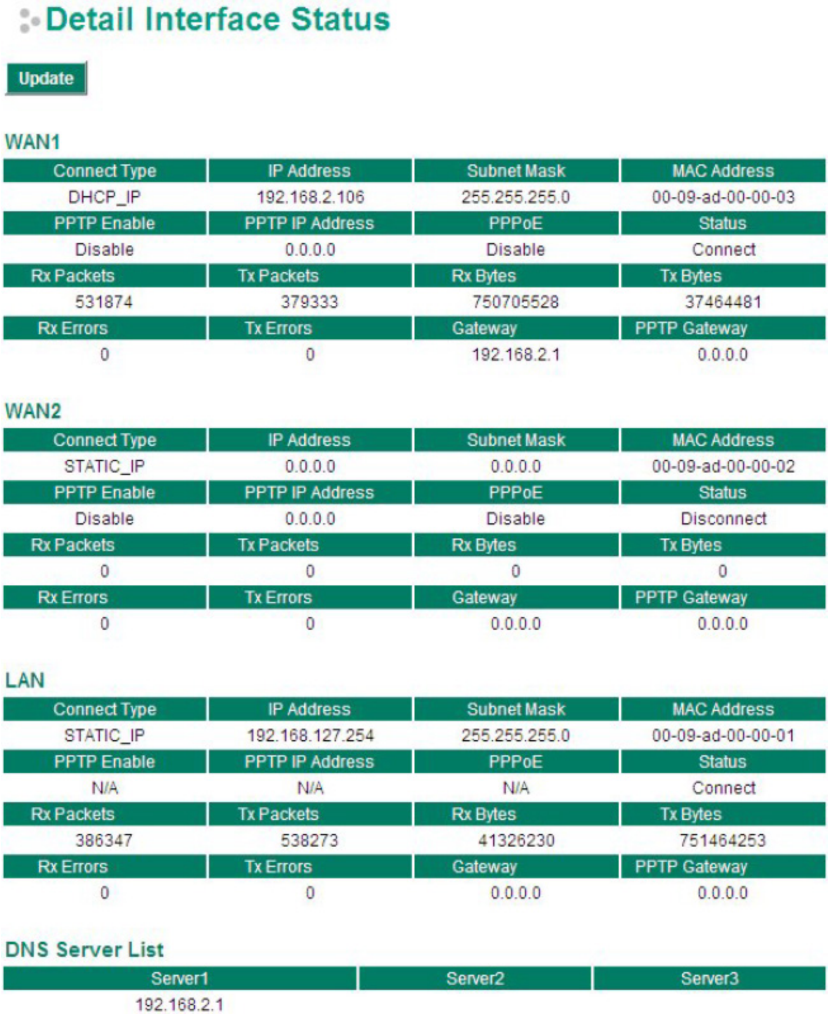
Functions	Current Status
Wan 2 Backup Function	Disable
DDNS	Disable
DoS	Disable
WAN Backup	Disable
QoS	Disable

Recent 10 Event Log More....	
Event	Time
WAN1 link on	2010/4/7,16:50:49
WAN1 link off	2010/4/7,16:51:58
LAN link off	2010/4/7,16:52:1
WAN1 link on	2010/4/7,16:52:50
LAN link on	2010/4/7,16:52:54
NAT Configuration Change	2010/4/7,16:54:32
Filter Configuration Change	2010/4/7,16:55:12
Filter Configuration Change	2010/4/7,16:55:27
Login auth ok	2010/4/7,18:22:49
admin auth ok	2010/4/7,18:38:5

Click **More...** at the top of the **Interface Status** table to see detailed information about all interfaces.



Interface Status More....			
Interface	Mode	PPPoE	Status
Port 1(WAN)	Wan 1	N/A	Connect
Port 2(Opt.)	Wan 2	N/A	Disconnect
Port 3(LAN)	LAN	N/A	Connect



Detail Interface Status

Update

WAN1

Connect Type	IP Address	Subnet Mask	MAC Address
DHCP_IP	192.168.2.106	255.255.255.0	00-09-ad-00-00-03
PPTP Enable	PPTP IP Address	PPPoE	Status
Disable	0.0.0.0	Disable	Connect
Rx Packets	Tx Packets	Rx Bytes	Tx Bytes
531874	379333	750705528	37464481
Rx Errors	Tx Errors	Gateway	PPTP Gateway
0	0	192.168.2.1	0.0.0.0

WAN2

Connect Type	IP Address	Subnet Mask	MAC Address
STATIC_IP	0.0.0.0	0.0.0.0	00-09-ad-00-00-02
PPTP Enable	PPTP IP Address	PPPoE	Status
Disable	0.0.0.0	Disable	Disconnect
Rx Packets	Tx Packets	Rx Bytes	Tx Bytes
0	0	0	0
Rx Errors	Tx Errors	Gateway	PPTP Gateway
0	0	0.0.0.0	0.0.0.0

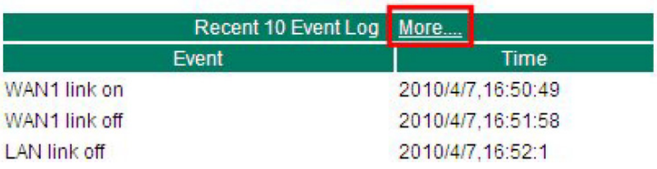
LAN

Connect Type	IP Address	Subnet Mask	MAC Address
STATIC_IP	192.168.127.254	255.255.255.0	00-09-ad-00-00-01
PPTP Enable	PPTP IP Address	PPPoE	Status
N/A	N/A	N/A	Connect
Rx Packets	Tx Packets	Rx Bytes	Tx Bytes
386347	538273	41326230	751464253
Rx Errors	Tx Errors	Gateway	PPTP Gateway
0	0	0.0.0.0	0.0.0.0

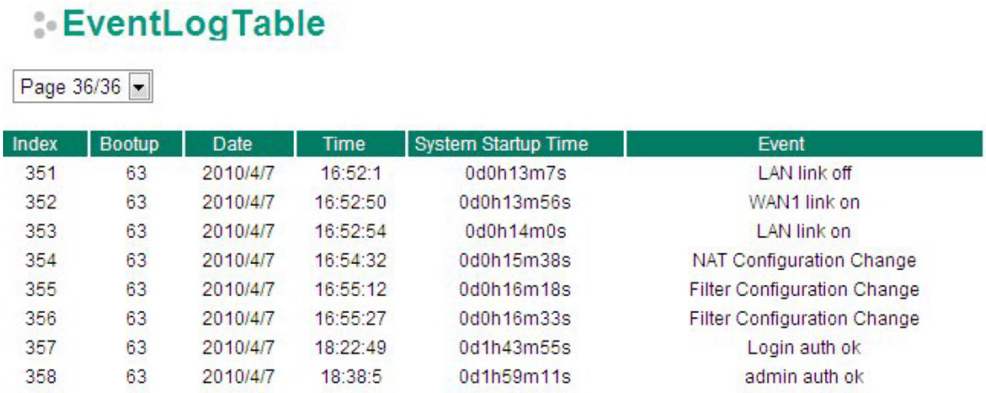
DNS Server List

Server1	Server2	Server3
192.168.2.1		

Click **More...** at the top of the **Recent 10 Event Log** table to open the **EventLogTable** page.



Recent 10 Event Log More....	
Event	Time
WAN1 link on	2010/4/7,16:50:49
WAN1 link off	2010/4/7,16:51:58
LAN link off	2010/4/7,16:52:1



EventLogTable

Page 36/36

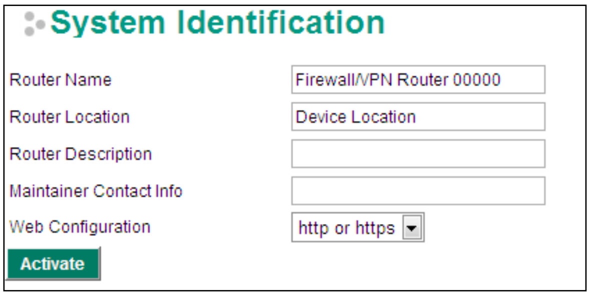
Index	Bootup	Date	Time	System Startup Time	Event
351	63	2010/4/7	16:52:1	0d0h13m7s	LAN link off
352	63	2010/4/7	16:52:50	0d0h13m56s	WAN1 link on
353	63	2010/4/7	16:52:54	0d0h14m0s	LAN link on
354	63	2010/4/7	16:54:32	0d0h15m38s	NAT Configuration Change
355	63	2010/4/7	16:55:12	0d0h16m18s	Filter Configuration Change
356	63	2010/4/7	16:55:27	0d0h16m33s	Filter Configuration Change
357	63	2010/4/7	18:22:49	0d1h43m55s	Login auth ok
358	63	2010/4/7	18:38:5	0d1h59m11s	admin auth ok

Configuring Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the EDR-G903.

System Identification

The system identification section gives you an easy way to identify the different switches connected to your network.



System Identification

Router Name	Firewall/VPN Router 00000
Router Location	Device Location
Router Description	
Maintainer Contact Info	
Web Configuration	http or https

Router name

Setting	Description	Factory Default
Max. 30 Characters	This option is useful for specifying the role or application of different EDR-G903 units. E.g., Factory Router 1.	Firewall/VPN router [Serial No. of this switch]

Router Location

Setting	Description	Factory Default
Max. 80 Characters	To specify the location of different EDR-G903 units. E.g., production line 1.	Device Location

Router Description

Setting	Description	Factory Default
Max. 30 Characters	Use this field to enter a more detailed description of the EDR-G903 unit.	None

Maintainer Contact Info

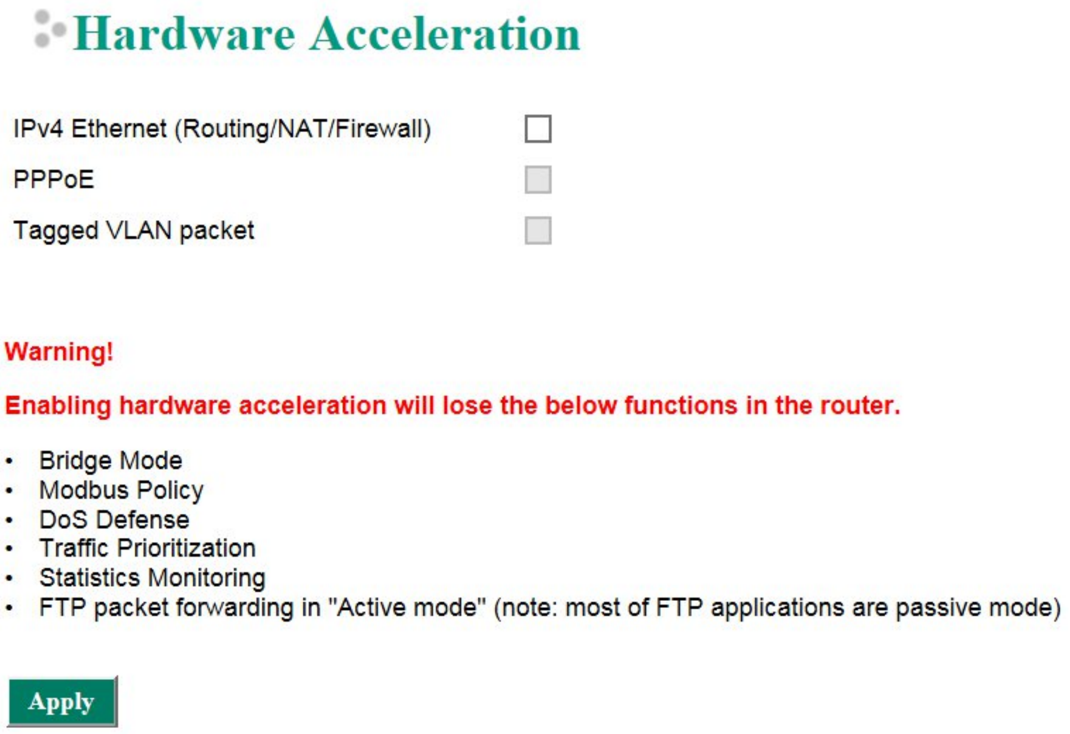
Setting	Description	Factory Default
Max. 30 Characters	Enter the contact information of the person responsible for maintaining this EDR-G903	None

Web Configuration

Setting	Description	Factory Default
http or https	Users can connect to the EDR-G903 router via http or https protocol.	http or https
https only	Users can connect to the EDR-G903 router via https protocol only.	

Hardware Acceleration

By optimizing the hardware and software, the throughput of the functions below will be improved, including IPv4 Ethernet (Routing/ NAT/ Firewall), PPPoE ad tagged VLAN packet. Please note that when Hardware Acceleration is enabled, some functions including bridge mode, Modbus policy, Dos defense, traffic prioritization, statics monitoring and FTP packet forwarding will be disabled.



Hardware Acceleration

IPv4 Ethernet (Routing/NAT/Firewall) □

PPPoE □

Tagged VLAN packet □

Warning!

Enabling hardware acceleration will lose the below functions in the router.

- Bridge Mode
- Modbus Policy
- DoS Defense
- Traffic Prioritization
- Statistics Monitoring
- FTP packet forwarding in "Active mode" (note: most of FTP applications are passive mode)

IPv4 Ethernet (Routing/NAT/Firewall)

Setting	Description	Factory Default
Check/Uncheck	Check it to improve throughput of IPv4 packet type except PPPoE and Tagged VLAN Packet.	Unchecked

PPPoE

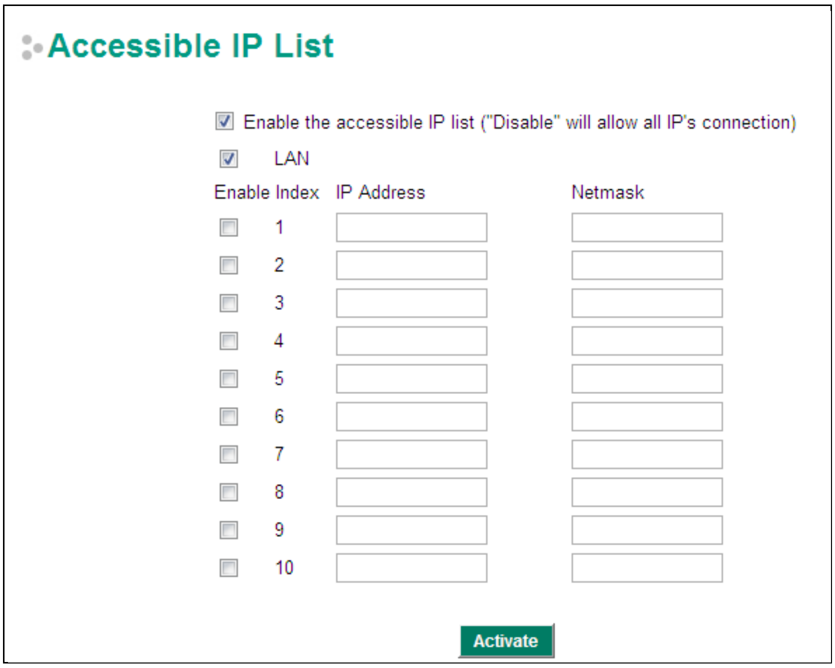
Setting	Description	Factory Default
Check/Uncheck	Check it to improve throughput of IPv4 packet and PPPoE packet.	Unchecked

Tagged VLAN Packet

Setting	**Description**	**Factory Default**
Check/Uncheck	Check it to improve throughput of IPv4 packet and tagged VLAN packet.	Uncheck

Accessible IP

The EtherDevice Router uses an IP address-based filtering method to control access to EtherDevice Router units.



Accessible IP List

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

☑ LAN

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

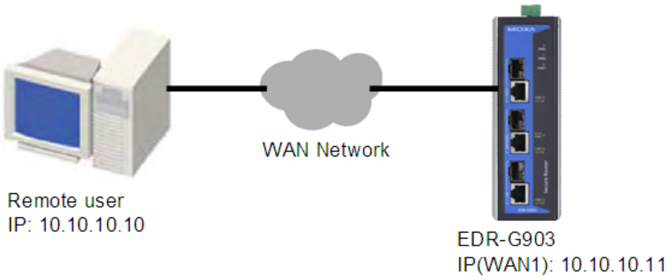
Accessible IP Settings allows you to add or remove "Legal" remote host IP addresses to prevent unauthorized access. Access to the EtherDevice Router is controlled by IP address. If a host's IP address is in the accessible IP table, then the host will have access to the EtherDevice Router. You can allow one of the following cases by setting this parameter:

- Only one host with the specified IP address can access this device.
  E.g., enter "192.168.1.1/255.255.255.255" to allow access to just the IP address 192.168.1.1.
- Any host on a specific subnetwork can access this device.
  E.g., enter "192.168.1.0/255.255.255.0" to allow access to all IPs on the subnet defined by this IP address/subnet mask combination.
- Any host can access the EtherDevice Router. (Disable this function by deselecting the Enable the accessible IP list option.)
- Any LAN can access the EtherDevice Router. (Disable this function by deselecting the LAN option to not allow any IP at the LAN site to access this device.)
  E.g., If the LAN IP Address is set to 192.168.127.254/255.255.255.0, then IP addresses 192.168.127.1 /24 to 192.168.127.253/24 can access the EtherDevice Router.

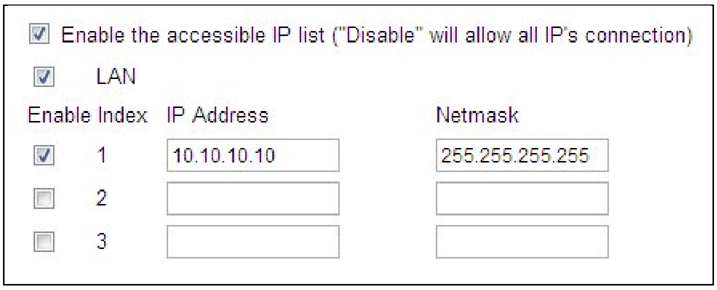
The following table shows additional configuration examples:

Allowable Hosts	**Input Format**
Ay 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

The Accessible IP list controls which devices can connect to the EtherDevice Router to change the configuration of the device. In the example shown below, the Accessible IP list in the EtherDevice Router contains 10.10.10.10, which is the IP address of the remote user's PC.



The remote user's IP address is shown below in the EtherDevice Router's Accessible IP list.



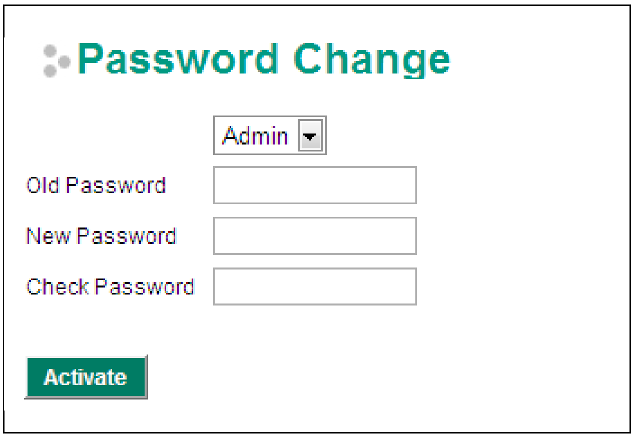
☑ Enable the accessible IP list ("Disable" will allow all IP's connection)

☑ LAN

Enable	Index	IP Address	Netmask
☑	1	10.10.10.10	255.255.255.255
□	2		
□	3		

Password

The EtherDevice Router provides two levels of access privilege: "admin privilege" gives read/write access to all EtherDevice Router configuration parameters, and "user privilege" provides read access only. You will be able to view the configuration, but will not be able to make modifications.



Password Change

Admin

Old Password

New Password

Check Password

ATTENTION

By default, the Password field is blank. If a Password is already set, then you will be required to type the Password when logging into the RS-232 console, Telnet console, or web browser interface.

Account

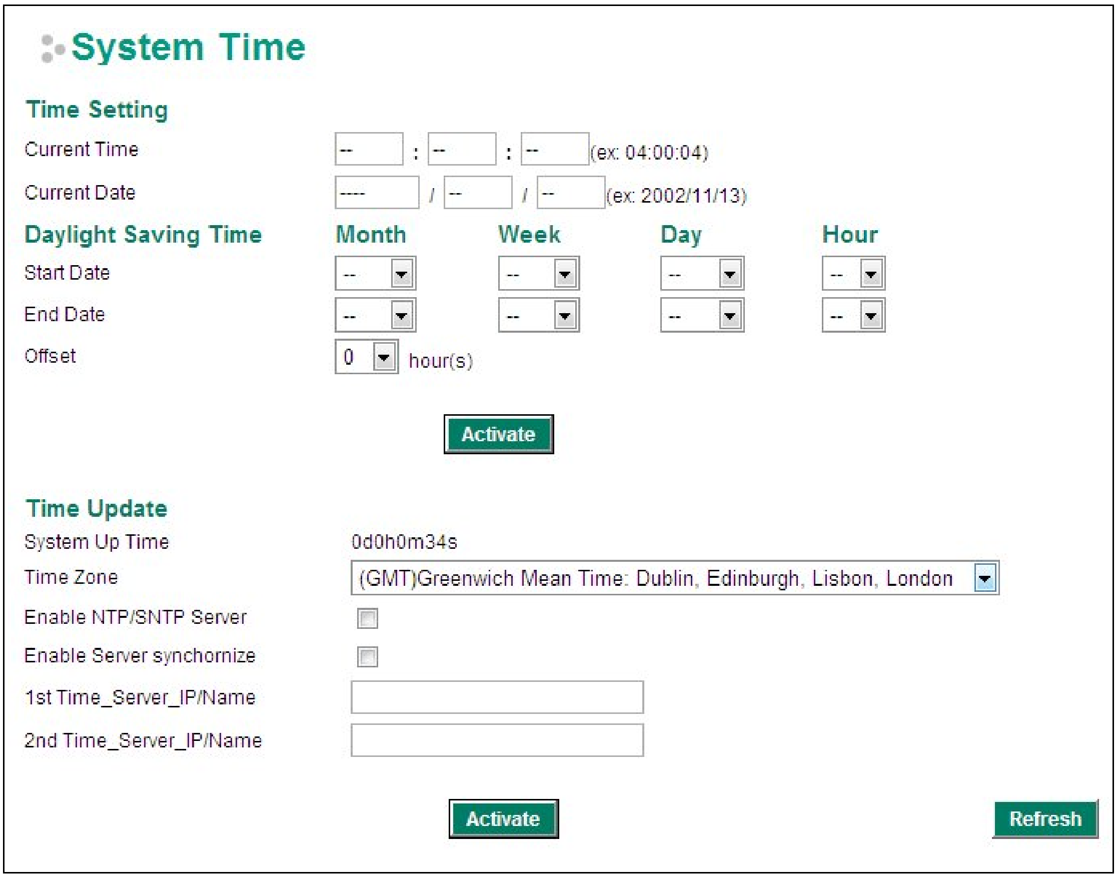
Setting	Description	Factory Default
Admin	"admin" privilege allows the user to modify all configurations.	Admin
User	"user" privilege only allows viewing device configurations.	

Password

Setting	Description	Factory Default
Old password (max. 16 Characters)	Type current password when changing the password	None
New password (max. 16 Characters)	Type new password when changing the password	None
Retype password (max. 16 Characters)	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	None

Time

The **Time** configuration page lets users set the time, date, and other settings. An explanation of each setting is given below.



System Time

Time Setting

Current Time -- : -- : -- (ex: 04:00:04)

Current Date ---- / -- / -- (ex: 2002/11/13)

Daylight Saving Time	Month	Week	Day	Hour
Start Date	--	--	--	--
End Date	--	--	--	--
Offset	0 hour(s)			

Time Update

System Up Time 0d0h0m34s

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

Enable NTP/SNTP Server □

Enable Server synchornize □

1st Time_Server_IP/Name

2nd Time_Server_IP/Name

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

NOTE The EtherDevice Router has a real time clock so the user does not need to update the Current Time and Current Date to set the initial time for the EtherDevice Router after each reboot. This is especially useful when the network does not have an Internet connection for an NTP server, or there is no NTP server on the network.

Current Time

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

Current Date

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

Daylight Saving Time

Daylight Saving Time (also known as DST or summer time) involves advancing clocks 1 hour during the summer to provide an extra hour of daylight in the evening.

Start Date

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

End Date

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

Offset

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

System Up Time

Indicates the ED-G903's up time from the last cold start. The unit is seconds.

Time Zone

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

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

Enable NTP/SNTP Server

Enable this function to configure the EtherDevice Router as a NTP/SNTP server on the network.

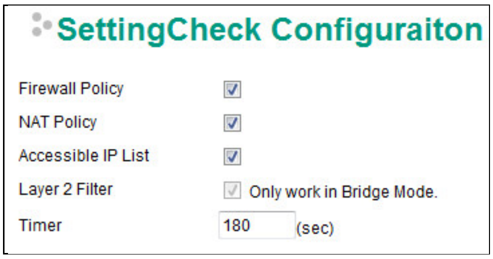
Enable Server synchronize

Enable this function to configure the EtherDevice Router as a NTP/SNTP client, It will synchronize the time information with another NTP/SNTP server.

Time Server IP/Name

Setting	Description	Factory Default
1st Time Server IP/Name	IP or Domain address (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	None
2nd Time Server IP/Name	The EtherDevice Router will try to locate the 2nd NTP Server if the 1st NTP Server fails to connect.	

SettingCheck


SettingCheck Configuraiton

Firewall Policy ☑

NAT Policy ☑

Accessible IP List ☑

Layer 2 Filter ☑ Only work in Bridge Mode.

Timer 180 (sec)

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 EtherDevice 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.

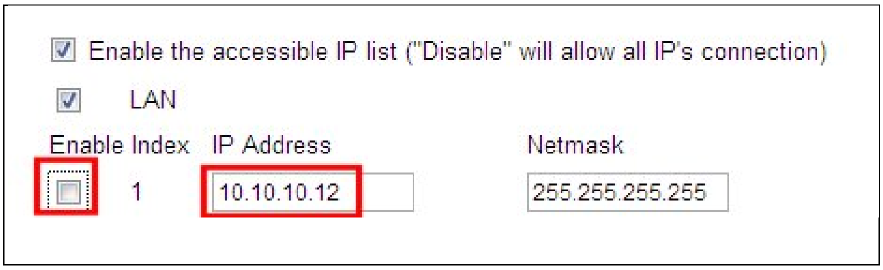
Layer 2 Filter

Enable or disable the SettingCheck function when the Layer 2 filter 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.)

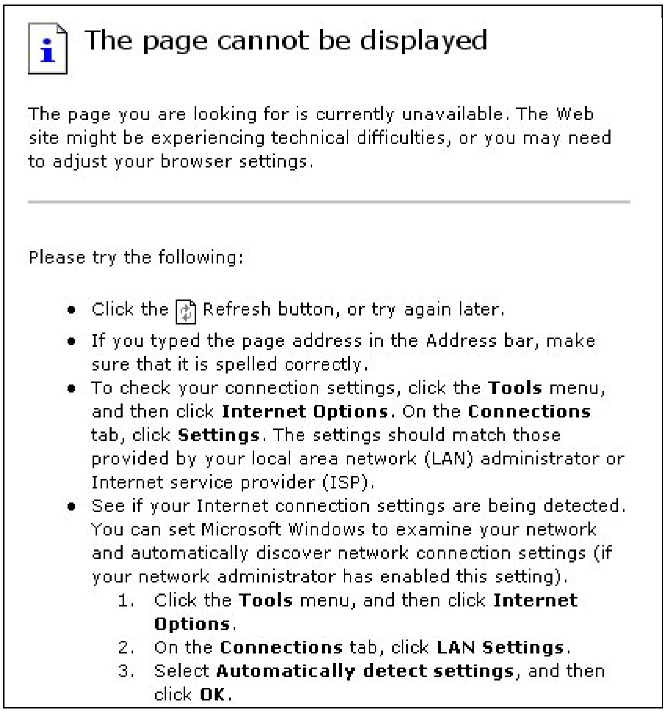
For example, if the remote user (IP: 10.10.10.10) connects to the EtherDevice Router and changes the accessible IP address to 10.10.10.12, or deselects the Enable checkbox accidently after the remote user clicks the Activate button, connection to the EtherDevice Router will be lost because the IP address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


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

☑ LAN

Enable	Index	IP Address	Netmask
□	1	10.10.10.12	255.255.255.255

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 EtherDevice 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 EtherDevice Router will roll back to the original Accessible IP List setting, allowing the remote user to reconnect to the EtherDevice Router and check what's wrong with the previous setting.



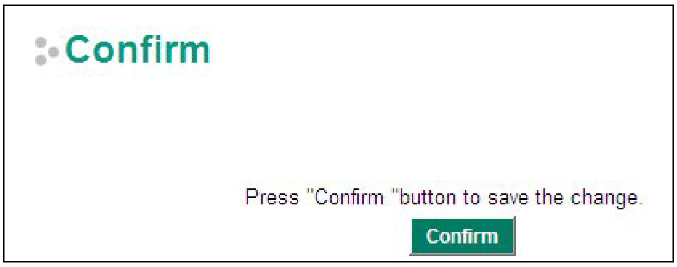
The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
  1. Click the **Tools** menu, and then click **Internet Options**.
  2. On the **Connections** tab, click **LAN Settings**.
  3. Select **Automatically detect settings**, and then click **OK**.

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

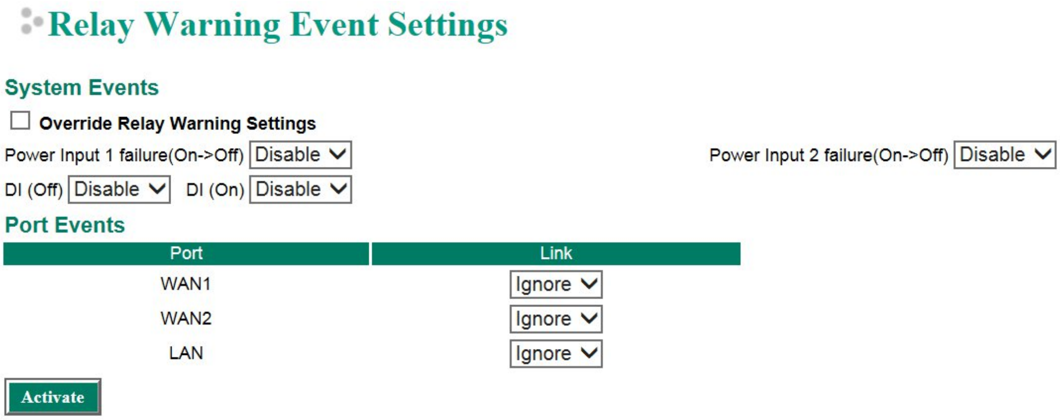


Confirm

Press "Confirm "button to save the change.

Relay Event Setup

The Industrial Secure Router supports digital input (DI) and digital output (Relay) in the top panel. In **Relay Event Setup**, users can configure which event will trigger the relay. The Industrial Secure Router supports three kinds of events which can trigger the relay, including Power 1/2 input failure, digital input, or at least one of the interfaces has a change of status.



Relay Warning Event Settings

System Events

□ Override Relay Warning Settings

Power Input 1 failure(On->Off) Disable   Power Input 2 failure(On->Off) Disable

DI (Off) Disable   DI (On) Disable

Port Events

Port	Link
WAN1	Ignore
WAN2	Ignore
LAN	Ignore

System Events

Override Relay Warning Settings

Setting	Description	Factory Default
Check/Uncheck	Check it to disable relay even when events occur. In this situation, events will still show in the Event Log	Unchecked

Power Input 1 failure (On->Off)

Setting	Description	Factory Default
Enable/Disable	Enable it to trigger relay if power input 1 status changes from on to off	Disabled

Power Input 2 failure (On->Off)

Setting	Description	Factory Default
Enable/Disable	Enable it to trigger relay if power input 2 status changes from on to off	Disabled

DI (Off)

Setting	Description	Factory Default
Enable/Disable	Enable it to trigger relay if there is no digital input	Disabled

DI (On)

Setting	Description	Factory Default
Enable/Disable	Enable it to trigger relay if there is digital input	Disabled

Port Events

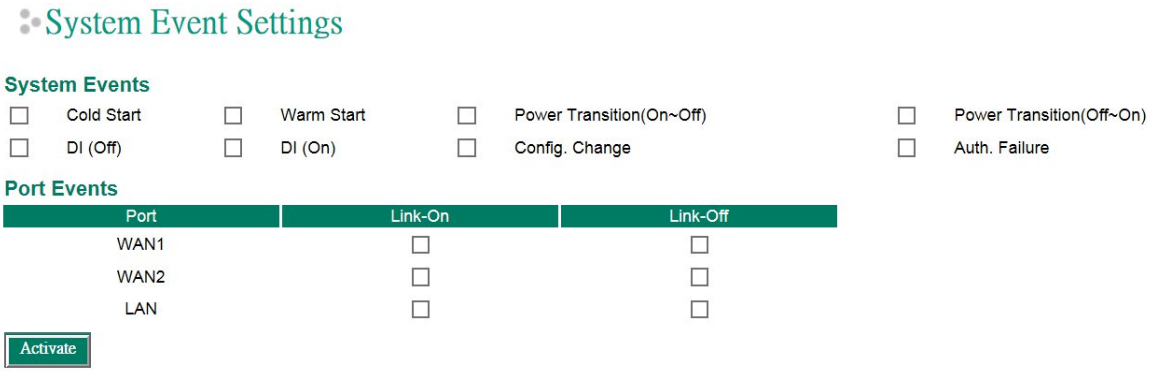
Link

Setting	Description	Factory Default
Ignore/On/Off	Choose which status will trigger relay, On or Off. Or just choose Ignore to stop interface events triggering relay	Ignore

Warning

System Event Setting

To monitor device events easily and in real time, users can receive event notifications through syslog and Email. If users do not enable sending the alerts through syslog/email, the default setting will be for these events to show in the Event Log Table. Users can decide which events they want to monitor. If users want to send an SNMP trap for these events, please refer to chapter SNMP.



System Event Settings

System Events

□ Cold Start	□ Warm Start	□ Power Transition(On~Off)	□ Power Transition(Off~On)
□ DI (Off)	□ DI (On)	□ Config. Change	□ Auth. Failure

Port Events

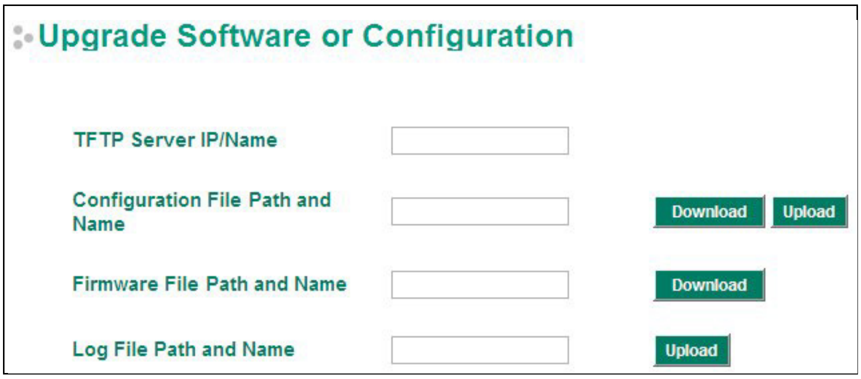
Port	Link-On	Link-Off
WAN1	□	□
WAN2	□	□
LAN	□	□

System Events	Description
Cold Start	Power is cut off and then reconnected.
Warm Start	Moxa's Industrial Secure Router has rebooted, e.g. when network parameters change (IP address, subnet mask, etc.).
Power Transition (On->Off)	Moxa's Industrial Secure Router is powered down.
Power Transition (Off->On)	Moxa's 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.

Port Events	Description
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).

System File Update—by Remote TFTP

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


Upgrade Software or Configuration
TFTP Server IP/Name
Configuration File Path and Name
Download
Upload
Firmware File Path and Name
Download
Log File Path and Name
Upload

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 EtherDevice Router's configuration file in the TFTP server.	None

Firmware File Path and Name

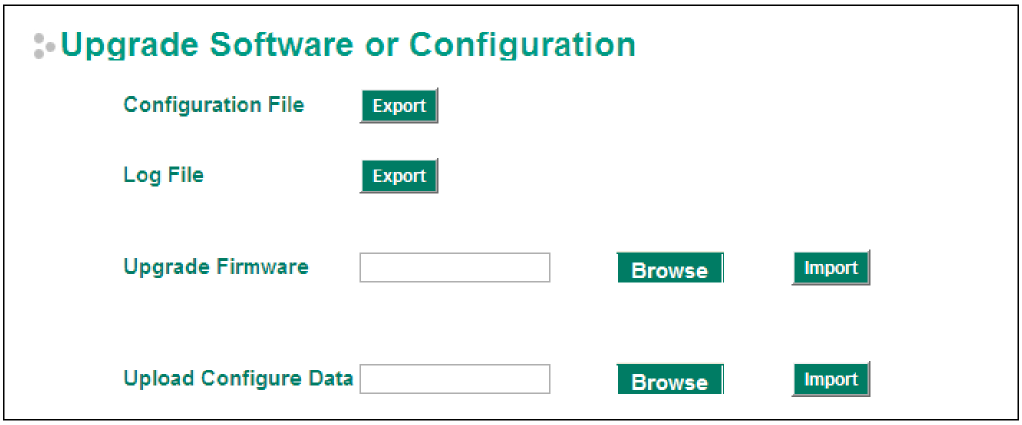
Setting	Description	Factory Default
Max. 40 Characters	The path and filename of the EtherDevice Router's firmware file	None

Log File Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and filename of the EtherDevice Router's log file	None

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

System File Update—by Local Import/Export



Upgrade Software or Configuration

Configuration File [Export]

Log File [Export]

Upgrade Firmware [ ] [Browse] [Import]

Upload Configure Data [ ] [Browse] [Import]

Configuration File

Click **Export** to export the configuration file of the EtherDevice Router to the local host.

Log File

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

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

Upgrade Firmware

To import a firmware file into the EtherDevice Router, click **Browse** to select a firmware file already saved on your computer. The upgrade procedure will proceed automatically after clicking Import. This upgrade procedure will take a couple of minutes to complete, including the boot-up time.

Upload Configuration Data

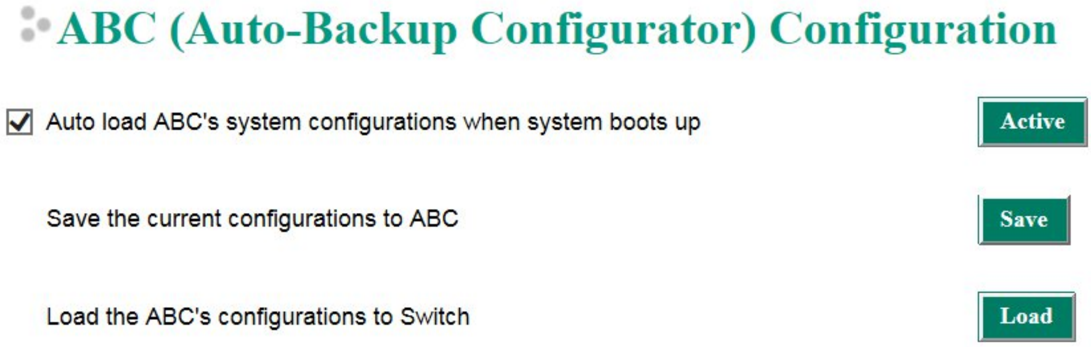
To import a configuration file to the EtherDevice Router, click **Browse** to select a configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking Import.

Backup Media

On large networks, administrators need to configure many network devices in order for the whole system to operate smoothly. This is a time-consuming process and errors frequently occur. By using Moxa's Automatic Backup Configurator (ABC-01), it is easy for administrators to duplicate system configuration across many systems in a short period of time.

Administrators only need to set-up the configurations in a system, e.g. firewall rule, certificate, and export configuration file in the ABC-01. And then the administrator can plug the ABC-01 into RS-232 console port of the remaining systems, and the remaining systems will sync with the same configuration file. For accessory ABC-01 details, please visit
https://www.moxa.com/product/Automatic_Backup_Configurator_ABC-01.htm

Moxa's Automatic Backup Configurator (ABC-01)



ABC (Auto-Backup Configurator) Configuration

☑ Auto load ABC's system configurations when system boots up

Save the current configurations to ABC

Load the ABC's configurations to Switch

Auto load ABC's system configurations when system boots up

Setting	Description	Factory Default
Checked	Allows system to load configuration file from ABC-01 automatically when booting up	Checked
Unchecked	System will not load configuration file from ABC-01 automatically when booting up	

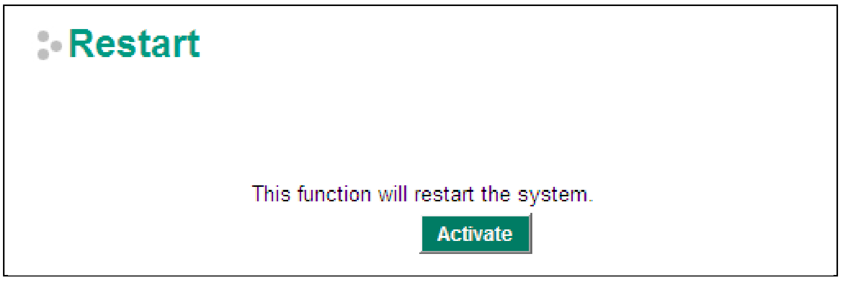
Save the current configurations to ABC-01

Setting	Description	Factory Default
Save	By pressing Save backups the system configuration files to the ABC-01	N/A

Load the ABC's configuration to Switch

Setting	Description	Factory Default
Load	Allows system to import configurations from ABC-01	N/A

Restart

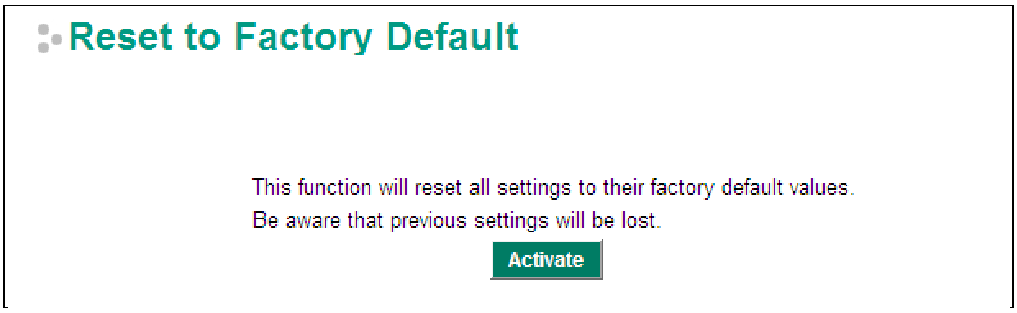


Restart

This function will restart the system.

This function is used to restart the EtherDevice Router.

Reset to Factory Default



Reset to Factory Default

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

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

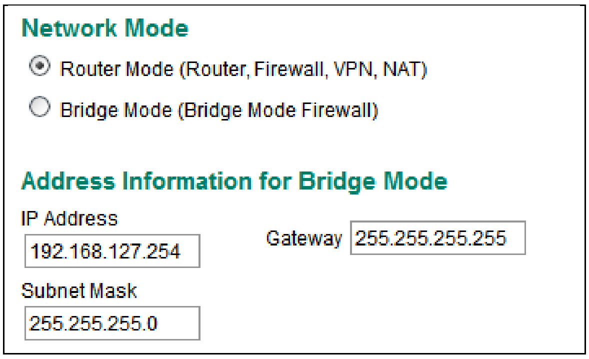
NOTE After activating the Factory Default function, you will need to use the default network settings to re-establish a web-browser or Telnet connection with your EtherDevice Router.

Network Settings

Mode Configuration

Network Mode

EtherDevice Router provides **Router Mode** and **Bridge Mode** operation for different applications:



Network Mode

● Router Mode (Router, Firewall, VPN, NAT)

○ Bridge Mode (Bridge Mode Firewall)

Address Information for Bridge Mode

IP Address: 192.168.127.254

Gateway: 255.255.255.255

Subnet Mask: 255.255.255.0

Router Mode

In this mode, EtherDevice Router operates as a gateway between different networks.

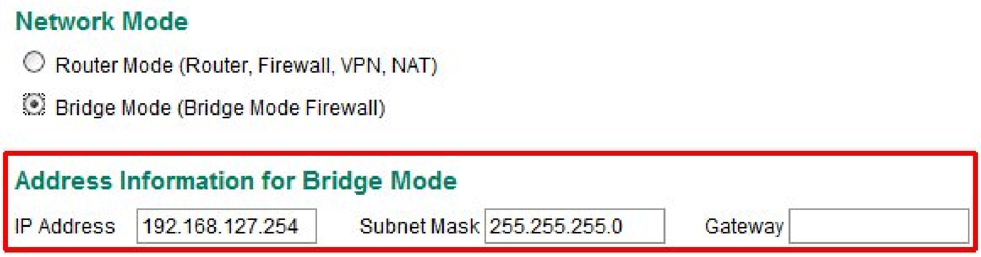
- Each interface (WAN1, WAN2 and LAN) has its own IP addresses & different subnet
- It provides Routing, Firewall, VPN and NAT functions
- Default setting of EtherDevice Router

Bridge Mode

In this mode, EtherDevice Router operates as a Bridge mode firewall (or call transparent firewall) in a single subnet. Users could simply insert EtherDevice Router into the existing single subnet without the need to reconfigure the original subnet into different subnets and without the need to reconfigure the IP address of existing devices.

- EtherDevice Router only has one IP address, Network mask and Gateway.

- VPN, NAT, WAN backup, VRRP, DHCP, Dynamic DNS are not supported in this mode



Network Mode

○ Router Mode (Router, Firewall, VPN, NAT)

● Bridge Mode (Bridge Mode Firewall)

Address Information for Bridge Mode

IP Address 192.168.127.254 Subnet Mask 255.255.255.0 Gateway

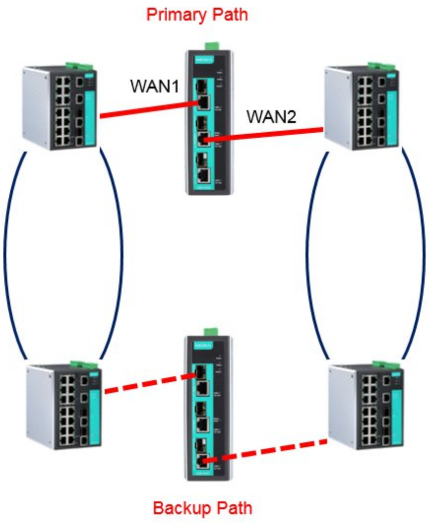
User could select the appropriate operation mode and press **Activate** to change the mode of EtherDevice Router. Change operation mode would take around 30-60 seconds to reboot system!!! If the webpage is no response after 30-60 seconds, please refresh webpage or press F5.

Link Fault Passthrough

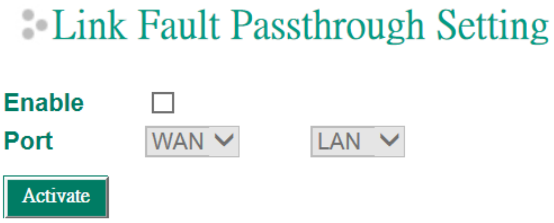
In a big network system, when a port link down or cable drops, this port cannot work normally. However, it takes time to update this information to other Ethernet devices and update the routing table. In this case, it will take a long time for the system to recover, which is unacceptable on industrial networks.

To improve the recovery time, the EDR-G902/ G903 supports a function called **Link Fault Passthrough**. By enabling this function, users can set up which two ports are linked together. When one port is link down, EDR-G902/ G903 will change the status of the other port as link down as well by software. And then the routing table can be updated quicker.

Using the network topology on the figure below as an example, these switches and the EDR-902 form a Turbo ring coupling. In normal situations, the packet goes through the primary path. But when WAN1 is link down, the WAN2 will be set as link fail as well by software. And then the routing table can be updated quicker.



For the EDR-G902 device the configuration setting is explained below:



Link Fault Passthrough Setting

Enable □

Port WAN LAN

Enable

Setting	Description	Factory Default
Check/ Uncheck	Check to enable Link Fault Passthrough function	Check

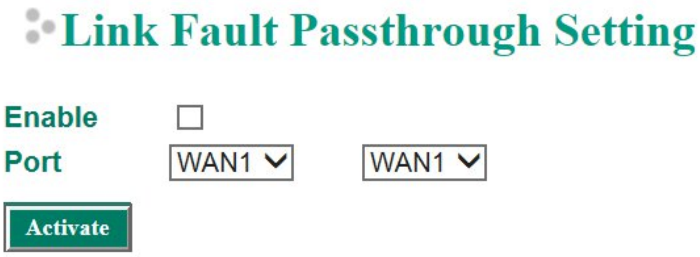
Port

Setting	Description	Factory Default
WAN	Select a port which user will monitor link status	WAN

Port

Setting	Description	Factory Default
LAN	Select a port which user will monitor link status	LAN

For the EDR-G903 device the configuration setting is explained as below:



Link Fault Passthrough Setting

Enable □

Port WAN1 WAN1

Link Fault Passthrough Setting

Setting	Description	Factory Default
Check/ Uncheck	Check to enable Link Fault Passthrough function	Uncheck

Port

Setting	Description	Factory Default
WAN1 WAN2 LAN	Select a port which user will monitor link status	WAN1

Port

Setting	Description	Factory Default
WAN1 WAN2 LAN	Select a port which user will monitor link status	WAN1

MTU Configuration (for EDR-810/G902/G903)

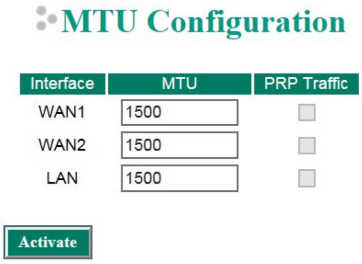
MTU stands for Maximum Transmission Unit, which is the maximum packet size (Byte) that packets can pass through Ethernet ports. Normally, the maximum packet size is 1500 bytes for Ethernet devices, e.g. router, or a switch. Default MTU in the Industrial Secure Router is 1500.

However, for some special industrial equipment, MTU 1500 byte is not acceptable. In this case, users can set a small MTU to fit this scenario. Users can configure MTU for each interface of the Industrial Secure Router. If MTU is set as 1430 bytes, when the inbound or outbound packet size over 1430, the Industrial Secure Router will drop this packet.

Users can set MTU for WAN1, WAN2, Bridge port, or LAN port in the Industrial Secure Router. For PRP packet (Parallel Redundancy Protocol), the Industrial Secure Router supports a function called **PRP Traffic**. PRP packet format is different with Ethernet packets. PRP packet contains a PRP trailer, which will be cut by kernel. Via enabling **PRP Traffic**, PRP packet will keep completed and be able to be routed by the Industrial Secure Router, and the MTU will be set as 1506 by default.

But for the **PRP Traffic** function, **PRP Traffic** function only works in G902/G903 in **Bridge Mode** and EDR-810 Bride port (**BRG_LAN).**

For the G902/903 devices, the configuration settings are explained below:



MTU Configuration

Interface	MTU	PRP Traffic
WAN1	1500	□
WAN2	1500	□
LAN	1500	□

WAN1

Setting	Description	Factory Default
MTU	Set Maximum Transmission Unit for WAN1 interface	1500

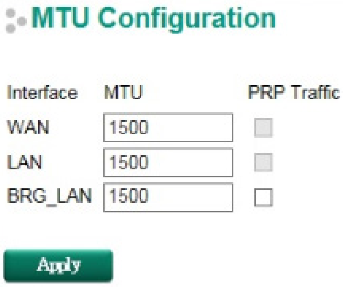
WAN2

Setting	Description	Factory Default
MTU	Set Maximum Transmission Unit for WAN2 interface	1500

LAN

Setting	Description	Factory Default
MTU	Set Maximum Transmission Unit for WAN3 interface	1500

For the EDR-810, the configuration setting are explained below:



MTU Configuration

Interface	MTU	PRP Traffic
WAN	1500	□
LAN	1500	□
BRG_LAN	1500	□

WAN

Setting	Description	Factory Default
MTU	Set Maximum Transmission Unit for WAN interface	1500

LAN

Setting	Description	Factory Default
MTU	Set Maximum Transmission Unit for LAN interface	1500

BRG_LAN

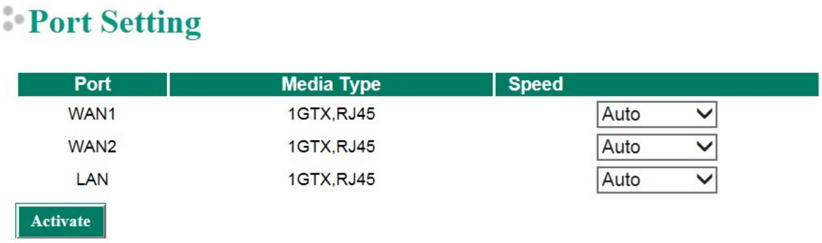
Setting	Description	Factory Default
MTU	Set Maximum Transmission Unit for BRG_LAN interface	1500

PRP Traffic

Setting	Description	Factory Default
Check/ Uncheck	Check to keep PRP Trail header	Uncheck

Speed Configuration

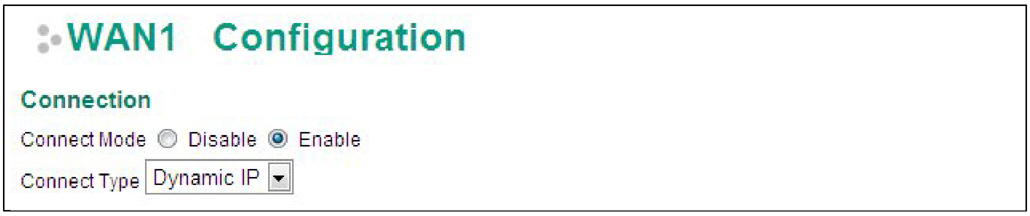
In the condition, some old generation devices do not support auto-negotiation, meaning users have to set the port speed manually. Users can set the same port speed on both the Industrial Secure Router and devices of the previous generation. Via this way, users can avoid packet loss or packet collision issues when the port speed is not the same.



Port Setting

Port	Media Type	Speed
WAN1	1GTX,RJ45	Auto
WAN2	1GTX,RJ45	Auto
LAN	1GTX,RJ45	Auto

WAN1 Configuration



WAN1 Configuration

Connection

Connect Mode ○ Disable ● Enable

Connect Type Dynamic IP

Connection

Note that there are three different connection types for the WAN1 interface: Dynamic IP, Static IP, and PPPoE. *A detailed explanation of the configuration settings for each type is given below.*

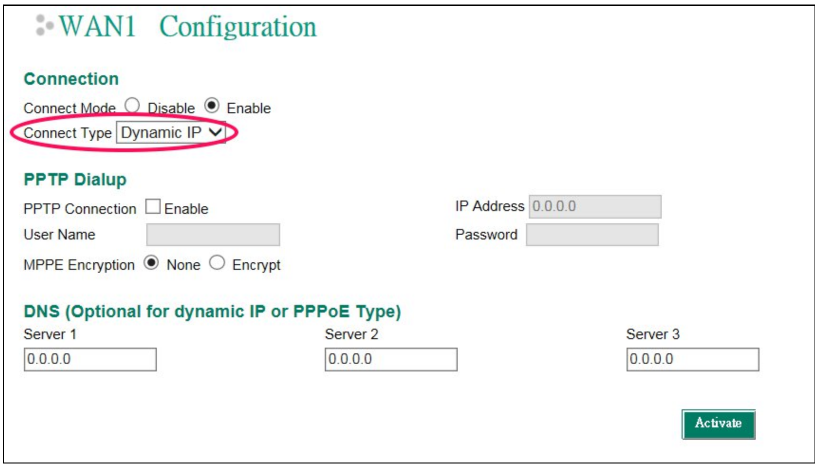
Connection Mode

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



WAN1 Configuration

Connection

Connect Mode ○ Disable ● Enable

Connect Type Dynamic IP

PPTP Dialup

PPTP Connection □ Enable

IP Address 0.0.0.0

User Name

Password

MPPE Encryption ● None ○ Encrypt

DNS (Optional for dynamic IP or PPPoE Type)

Server 1 0.0.0.0

Server 2 0.0.0.0

Server 3 0.0.0.0

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

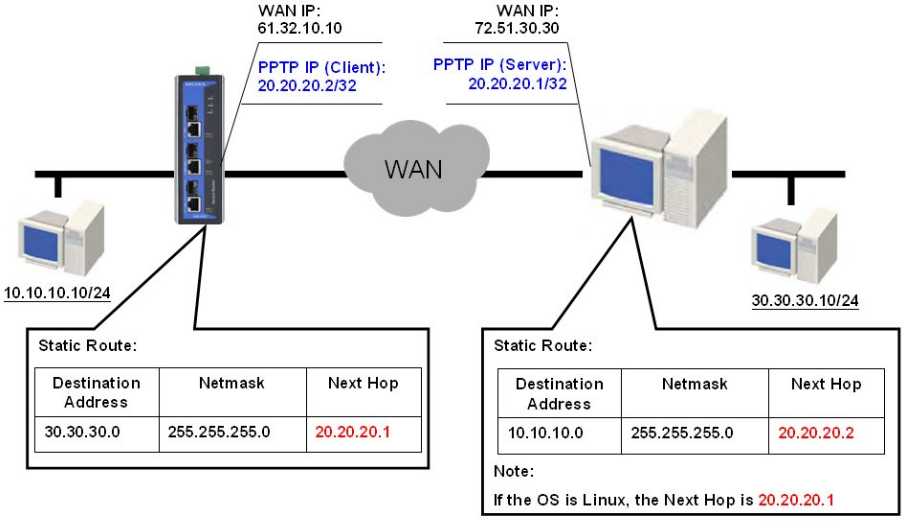
Password

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.



Static Route:

Destination Address	Netmask	Next Hop
30.30.30.0	255.255.255.0	20.20.20.1

Static Route:

Destination Address	Netmask	Next Hop
10.10.10.0	255.255.255.0	20.20.20.2

Note:

If the OS is Linux, the Next Hop is 20.20.20.1

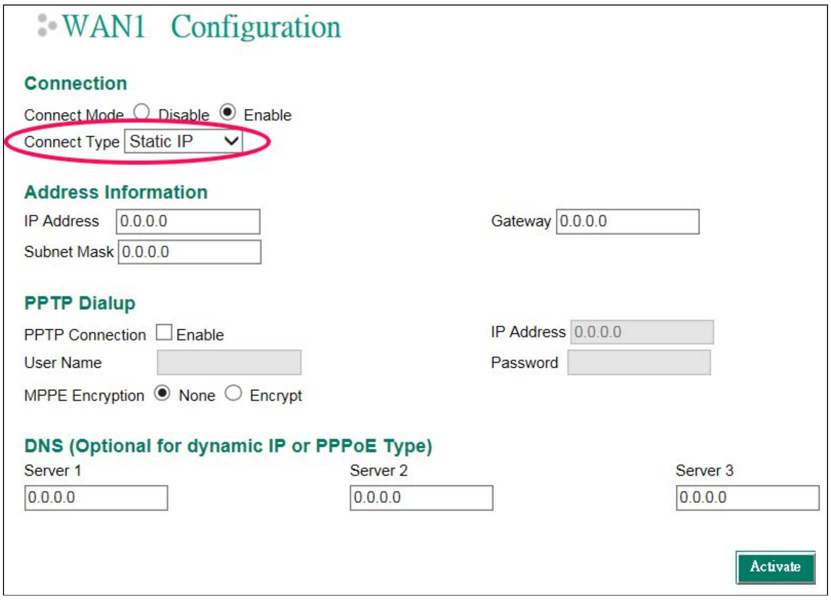
DNS (Doman Name Server; optional setting for Dynamic IP and PPPoE types)

Server 1/2/3

Setting	Description	Factory Default
IP Address	The DNS IP address	None

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

Detailed Explanation of Static IP Type



WAN1 Configuration

Connection

Connect Mode ○ Disable ● Enable

Connect Type Static IP

Address Information

IP Address 0.0.0.0

Gateway 0.0.0.0

Subnet Mask 0.0.0.0

PPTP Dialup

PPTP Connection □ Enable

IP Address 0.0.0.0

User Name

Password

MPPE Encryption ● None ○ Encrypt

DNS (Optional for dynamic IP or PPPoE Type)

Server 1 0.0.0.0

Server 2 0.0.0.0

Server 3 0.0.0.0

Address Information

IP Address

Setting	Description	Factory Default
IP Address	The interface IP address	None

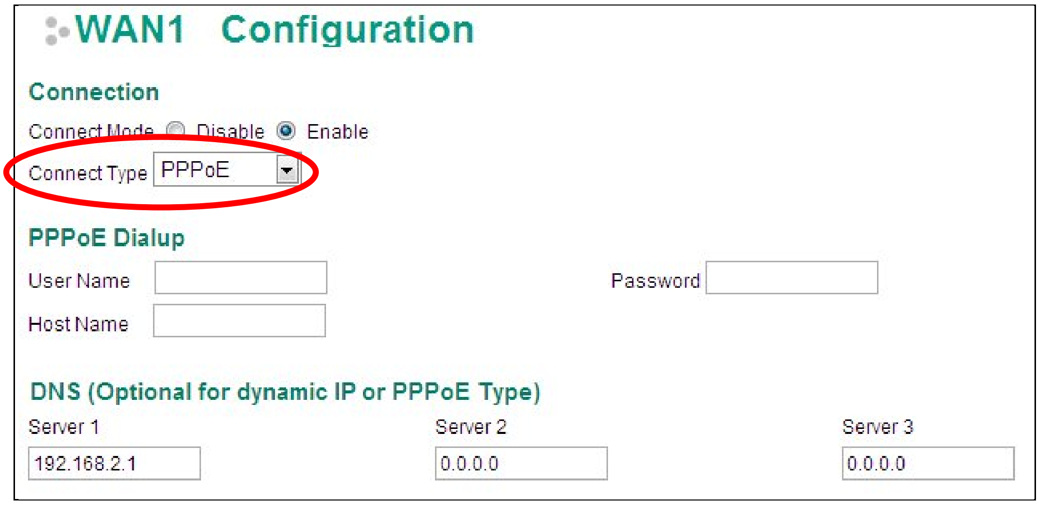
Subnet Mask

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



WAN1 Configuration

Connection

Connect Mode ○ Disable ● Enable

Connect Type PPPoE

PPPoE Dialup

User Name

Password

Host Name

DNS (Optional for dynamic IP or PPPoE Type)

Server 1 192.168.2.1

Server 2 0.0.0.0

Server 3 0.0.0.0

PPPoE Dialup

User Name

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

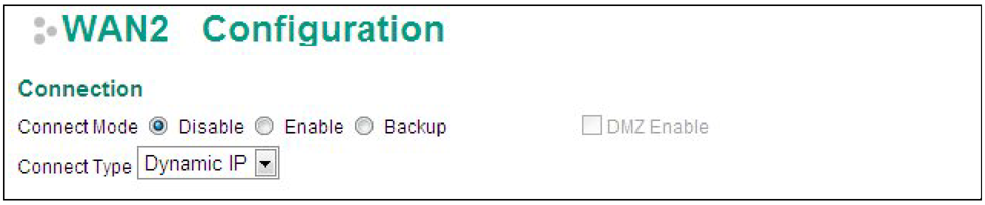
Host Name

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

WAN2 Configuration (includes DMZ Enable)


WAN2 Configuration

Connection

Connect Mode ● Disable ○ Enable ○ Backup □ DMZ Enable

Connect Type Dynamic IP

Connection

Note that there are there are three different connection types for the WAN2 interface: Dynamic IP, Static IP, and PPPoE. A detailed explanation of the configuration settings for each type is given below.

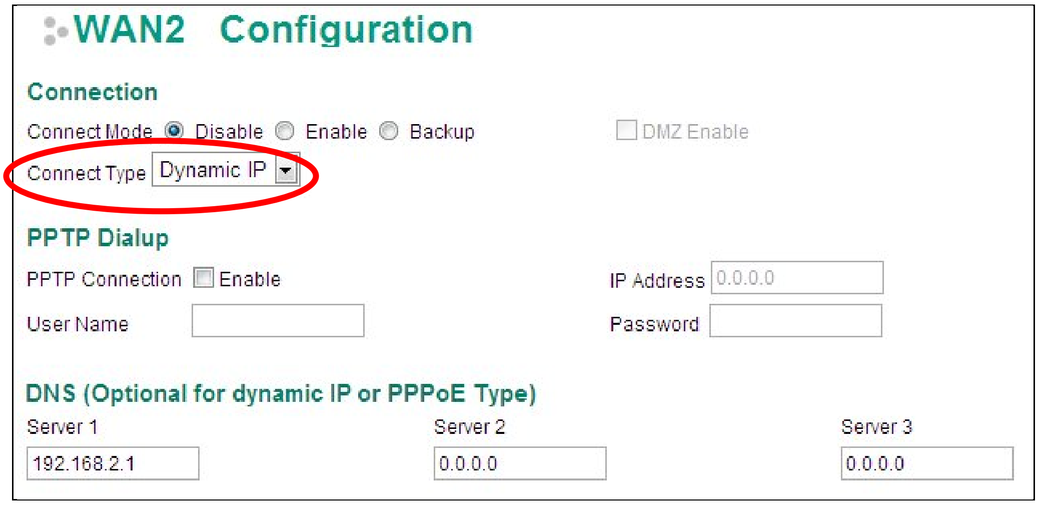
Connection Mode

Setting	Description	Factory Default
Enable or Disable	Enable or Disable the WAN interface.	None
Backup	Enable WAN Backup mode	
DMZ	Enable DMZ mode (can only be enabled when the connection type is set to Static IP)	

Connection Type

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

Detailed Explanation of Dynamic IP Type


WAN2 Configuration

Connection

Connect Mode ● Disable ○ Enable ○ Backup □ DMZ Enable

Connect Type Dynamic IP

PPTP Dialup

PPTP Connection □ Enable IP Address 0.0.0.0

User Name Password

DNS (Optional for dynamic IP or PPPoE Type)

Server 1 192.168.2.1

Server 2 0.0.0.0

Server 3 0.0.0.0

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

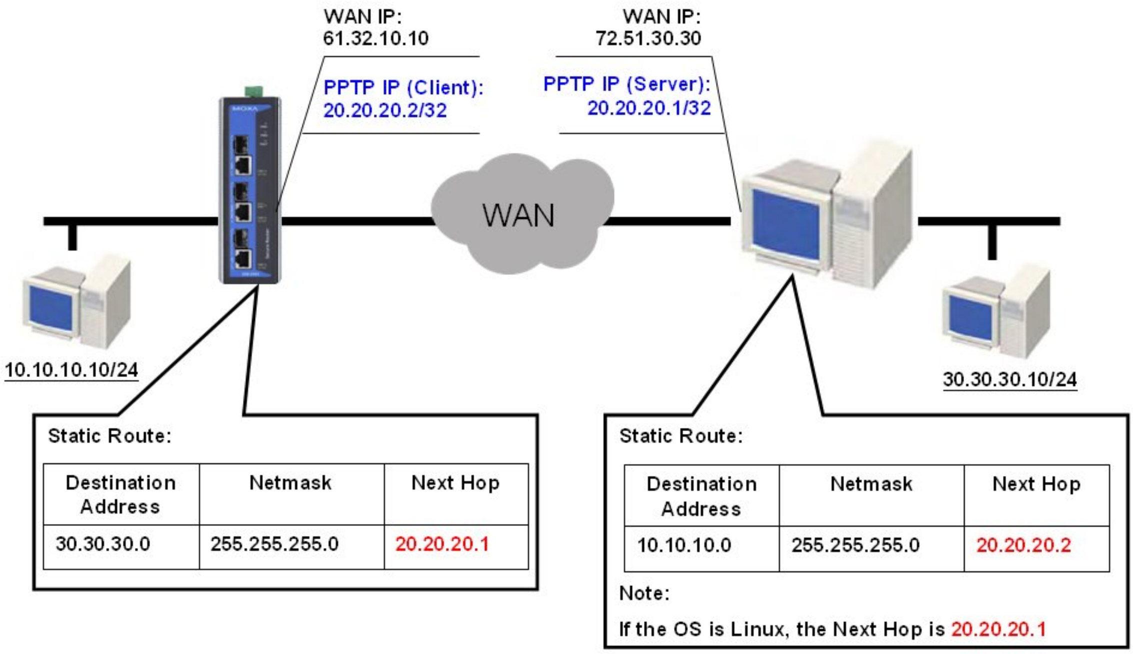
User name

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

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.



Static Route:

Destination Address	Netmask	Next Hop
30.30.30.0	255.255.255.0	20.20.20.1

Static Route:

Destination Address	Netmask	Next Hop
10.10.10.0	255.255.255.0	20.20.20.2

Note:

If the OS is Linux, the Next Hop is 20.20.20.1

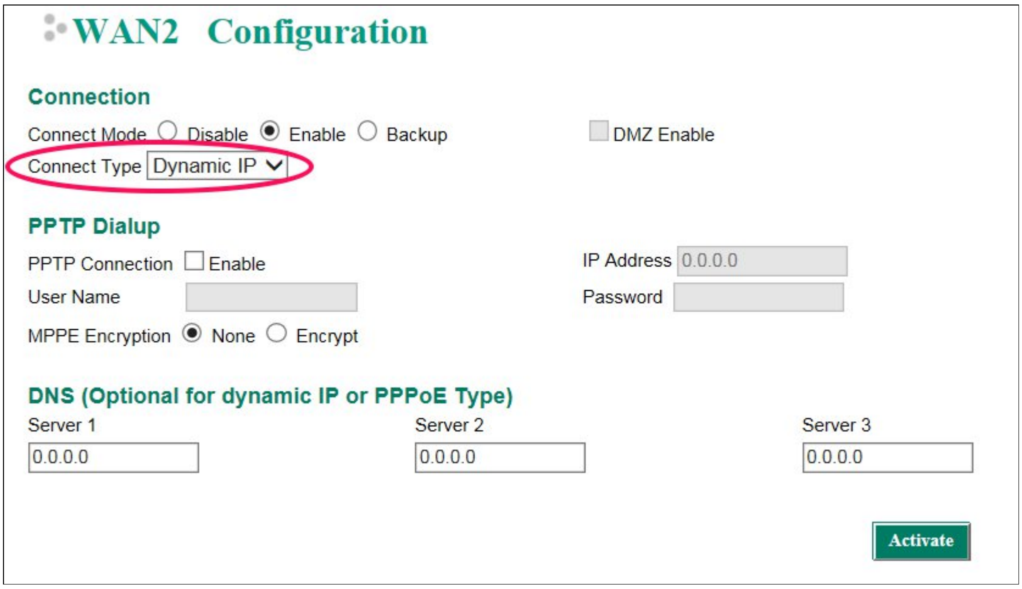
DNS (Doman Name Server; optional setting for Dynamic IP and PPPoE types)

Server 1/2/3

Setting	Description	Factory Default
IP Address	The DNS IP Address	None

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

Detailed Explanation of Static IP Type



WAN2 Configuration

Connection

Connect Mode ○ Disable ● Enable ○ Backup □ DMZ Enable

Connect Type Dynamic IP

PPTP Dialup

PPTP Connection □ Enable IP Address 0.0.0.0

User Name Password

MPPE Encryption ● None ○ Encrypt

DNS (Optional for dynamic IP or PPPoE Type)

Server 1 0.0.0.0 Server 2 0.0.0.0 Server 3 0.0.0.0

Address Information

IP Address

Setting	Description	Factory Default
IP Address	The interface IP address	None

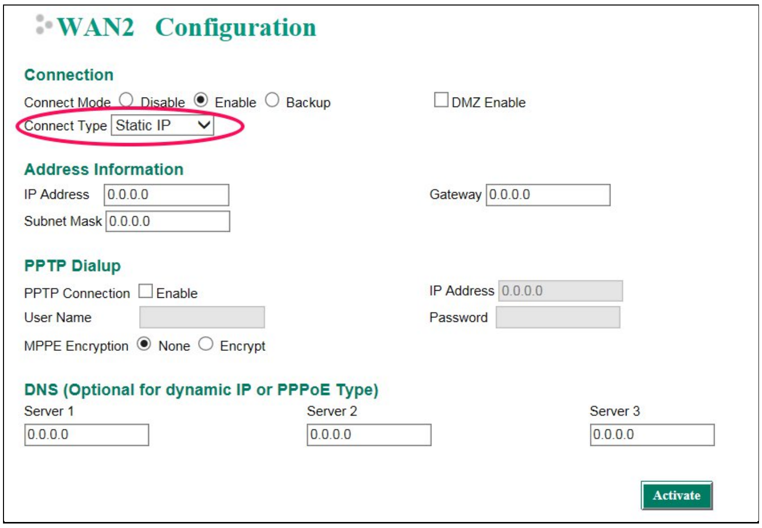
Subnet Mask

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



WAN2 Configuration

Connection

Connect Mode ○ Disable ● Enable ○ Backup □ DMZ Enable

Connect Type Static IP

Address Information

IP Address 0.0.0.0 Gateway 0.0.0.0

Subnet Mask 0.0.0.0

PPTP Dialup

PPTP Connection □ Enable IP Address 0.0.0.0

User Name Password

MPPE Encryption ● None ○ Encrypt

DNS (Optional for dynamic IP or PPPoE Type)

Server 1 0.0.0.0 Server 2 0.0.0.0 Server 3 0.0.0.0

PPPoE Dialup

User Name

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

Host Name

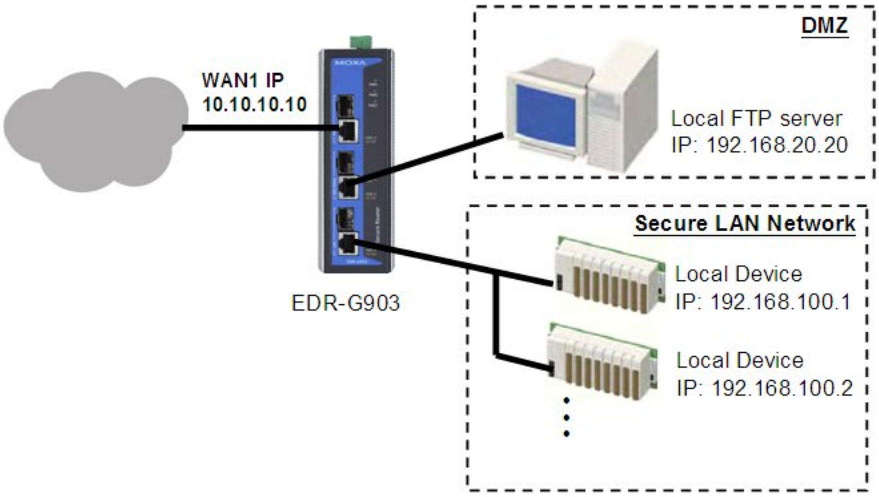
Setting	Description	Factory Default
Max. 30 characters	User-defined host name for this PPPoE server	None

Password

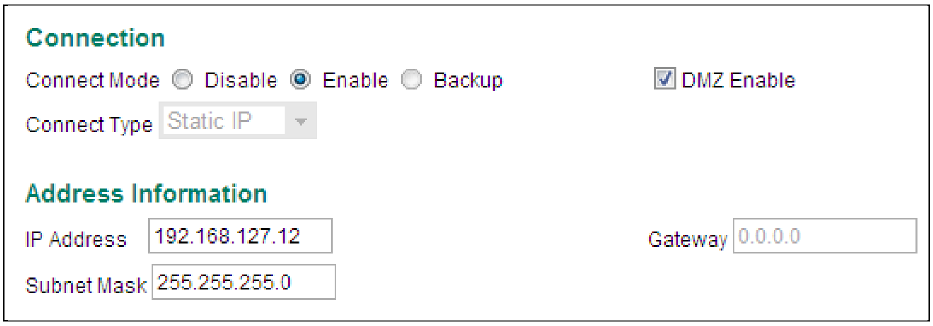
Setting	Description	Factory Default
Max. 30 characters	The login password for this PPPoE server	None

Using DMZ Mode

A DMZ (demilitarized zone) is an isolated network for devices—such as data, FTP, web, and mail servers connected to a LAN network—that need to frequently connect with external networks. The deployment of an FTP server in a DMZ is illustrated in the following figure.



DMZ mode is configured on the **WAN2 configuration** web page. Set Connect Mode to Enable, Connect Type to Static IP, and checkmark the DMZ Enable check box. You will also need to input the IP Address and Subnet Mask. Click the **Activate** button to save the settings.



Connection

Connect Mode ○ Disable ● Enable ○ Backup ☑ DMZ Enable

Connect Type: Static IP

Address Information

IP Address: 192.168.127.12

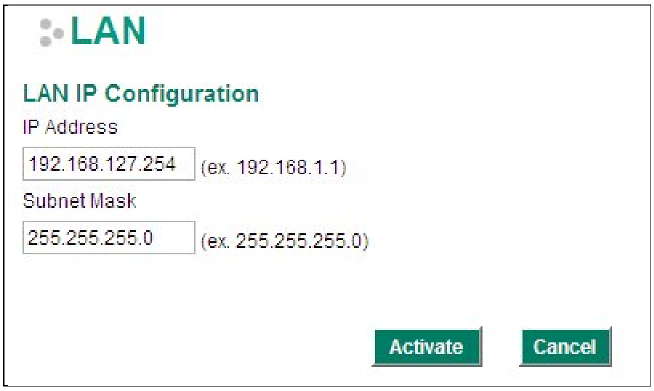
Gateway: 0.0.0.0

Subnet Mask: 255.255.255.0

NOTE WAN2 configuration and DMZ mode are only available on EDR-G903

LAN Interface

A basic application of an industrial Firewall/VPN device is to provide protection when the device is connected to a LAN. In this regard, the LAN port connects to a secure (or trusted) area of the network, whereas the WAN1 and WAN2/DMZ ports connect to an insecure (or untrusted) area.



LAN

LAN IP Configuration

IP Address: 192.168.127.254 (ex. 192.168.1.1)

Subnet Mask: 255.255.255.0 (ex. 255.255.255.0)

LAN IP Configuration

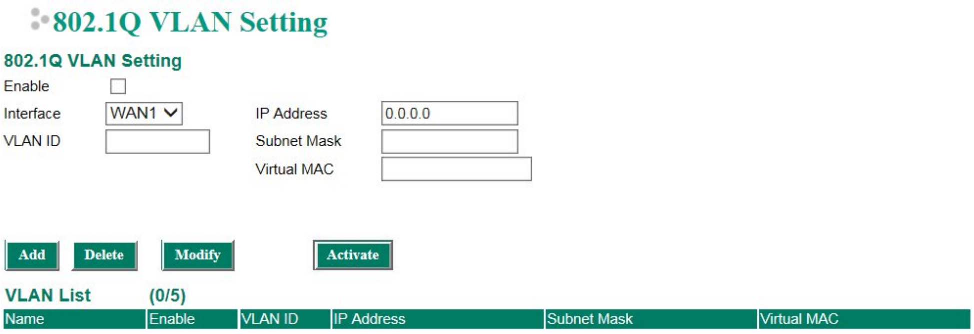
IP Address

Setting	Description	Factory Default
IP Address	The LAN interface IP address	192.168.127.254

Subnet Mask

Setting	Description	Factory Default
Subnet Mask	Network Mask of LAN IP	255.255.255.0

802.1Q VLAN Setting



802.1Q VLAN Setting

802.1Q VLAN Setting

Enable ☐

Interface: WAN1

VLAN ID:

IP Address: 0.0.0.0

Subnet Mask:

Virtual MAC:

VLAN List (0/5)

Name	Enable	VLAN ID	IP Address	Subnet Mask	Virtual MAC

Create a VLAN Interface

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

Delete a LAN Interface

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

Modify a LAN Interface

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

Activate the LAN Interface List

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

NOTE You can create up to 5 interfaces in WAN1/WAN2/WAN/LAN interface separately.

Communication Redundancy

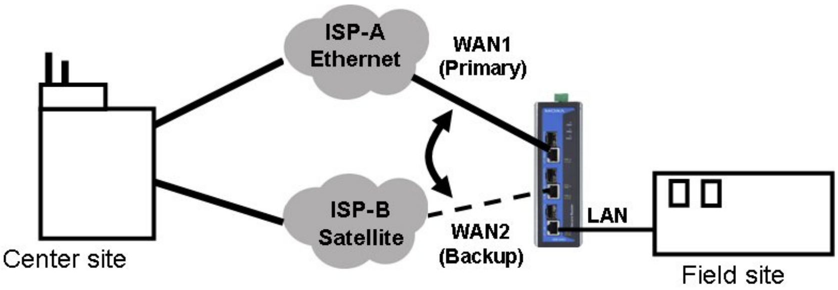
Moxa industrial secure router provides a communications redundancy function: WAN backup (EDR-G903 only). The industrial secure router has two WAN interfaces: WAN1 is the primary WAN interface and WAN2 is the backup interface. When the industrial secure router detects that connection WAN1 has failed (Link down or Ping fails), it will switch the communication path from WAN1 to WAN2 automatically. When WAN1 recovers, the major communication path will return to WAN1.

WAN Backup (EDR-G903 only)

How Dual WAN Backup Works

A power utility at a field site connects to a central office via two different ISPs (Internet Service Providers). ISP-A uses Ethernet and ISP-B uses satellite for data transmission, with Ethernet used as the major connection and the satellite as the backup connection. This makes sense since the cost of transmitting through the satellite is greater than the cost of transmitting over the Ethernet. Traditional solutions would use two routers to connect to the different ISPs. In this case, if the connection to the primary ISP fails, the connection must be switched to the backup ISP manually.

The EtherDevice Router's WAN backup function checks the link status and the connection integrity between the EtherDevice Router and the ISP or central office. When the primary WAN interface fails, it will switch to the backup WAN automatically to keep the connection alive.

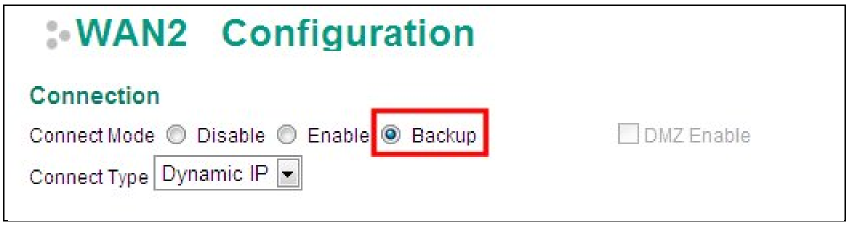


When configuring the EtherDevice Router, choose one of the two following conditions to activate the backup path:

- Link Check: WAN1 link down
- Ping Check: Sends ping commands to a specific IP address (e.g., the IP address of the ISP's server) from WAN1 based on user configurable Time Interval, Retry, and Timeout.

When the WAN backup function is enabled and the Link Check or Ping Check for the WAN1 interface fails, the backup interface (WAN2) will be enabled as the primary interface.

WAN Backup Configuration



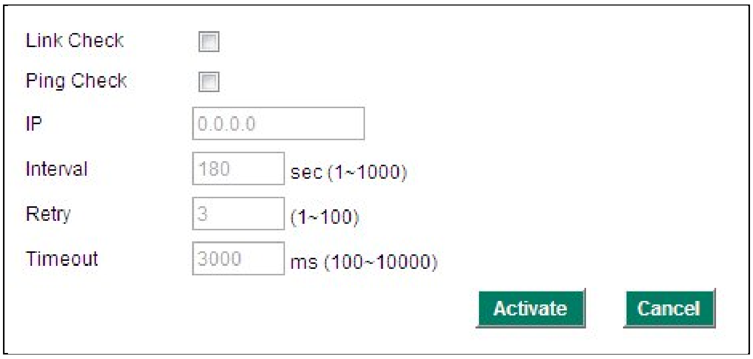
WAN2 Configuration

Connection

Connect Mode ○ Disable ○ Enable ● Backup □ DMZ Enable

Connect Type Dynamic IP

Select Backup for the WAN2/DMZ Connect Mode, and then go to the **Network Redundancy → WAN Backup** setting page for the WAN Backup configuration.



Link Check □

Ping Check □

IP 0.0.0.0

Interval 180 sec (1~1000)

Retry 3 (1~100)

Timeout 3000 ms (100~10000)

Link Check

Setting	Description	Factory Default
Enable or Disable	Activate Backup function by checking the link status of WAN1	Disabled

Ping Check

Setting	Description	Factory Default
Enable or Disable	Activates the Backup function if unable to ping from the EtherDevice Router to a specified IP address.	Disabled

IP

Setting	Description	Factory Default
IP address	The EtherDevice Router will check the ping integrity of this IP Address if the Ping Check function is Enabled	None

NOTE The IP address for Ping Check function should be on the network segment of WAN1.

Interval

Setting	Description	Factory Default
1 to 1000 sec	User can set up a different Ping Interval for a different network topology	180 sec.

Retry

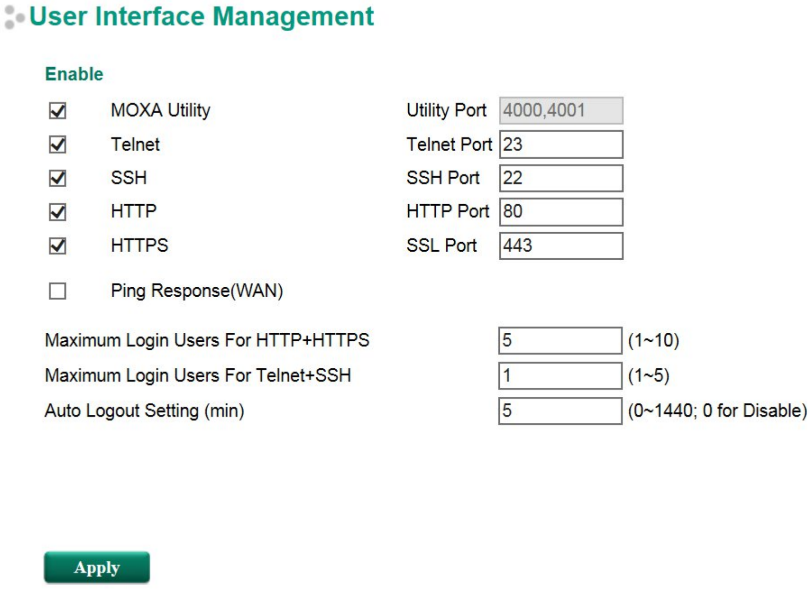
Setting	Description	Factory Default
1 to 100	User can configure the number of retries. If the number of continuous retries exceeds this number, the EtherDevice Router will activate the backup path.	3

Timeout

Setting	Description	Factory Default
100 to 10000 (ms)	The timeout criterion of Ping Check	3000 ms

Security

User Interface Management



User Interface Management

Enable

☑ MOXA Utility Utility Port 4000,4001

☑ Telnet Telnet Port 23

☑ SSH SSH Port 22

☑ HTTP HTTP Port 80

☑ HTTPS SSL Port 443

□ Ping Response(WAN)

Maximum Login Users For HTTP+HTTPS 5 (1~10)

Maximum Login Users For Telnet+SSH 1 (1~5)

Auto Logout Setting (min) 5 (0~1440; 0 for Disable)

Enable Ping Response (WAN)

Setting	Description	Factory Default
Select/Deselect	In the condition that the WAN connection is built, when the WAN port is pinged, WAN will send a response.	Deselect

Maximum Login Users For HTTP+HTTTPS

Limit the amount of users who can access the industrial secure router using HTTP and HTTPS. The maximum number of users currently supported is 10.

Maximum Login Users For Telnet+SSH

Limit the amount of users who can access the industrial secure router using Telnet or SSH. The maximum number of users currently supported is 5.

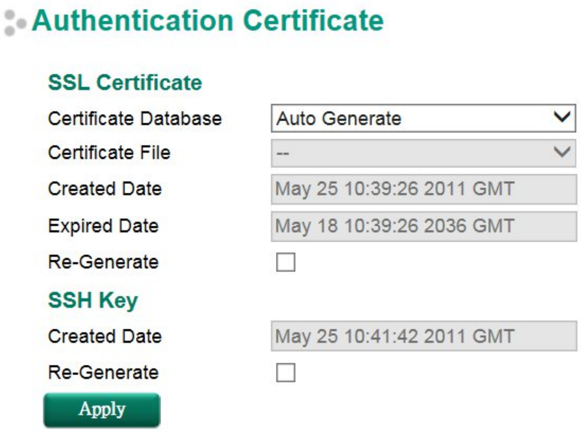
Auto Logout Setting (min)

When a user is not active on the industrial secure router management interface for some time, the management interface will automatically logout. The default setting for the industrial secure router is 5 minutes.

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

Authentication Certificate

Authentication certificate refers to certificates for HTTPS. The web console certificate can be generated by the EDR-810 automatically or users can choose to import the certificate in Local certificate.



Authentication Certificate

SSL Certificate

Certificate Database	Auto Generate
Certificate File	--
Created Date	May 25 10:39:26 2011 GMT
Expired Date	May 18 10:39:26 2036 GMT
Re-Generate	□

SSH Key

Created Date	May 25 10:41:42 2011 GMT
Re-Generate	□

Certificate Database

Auto Generate

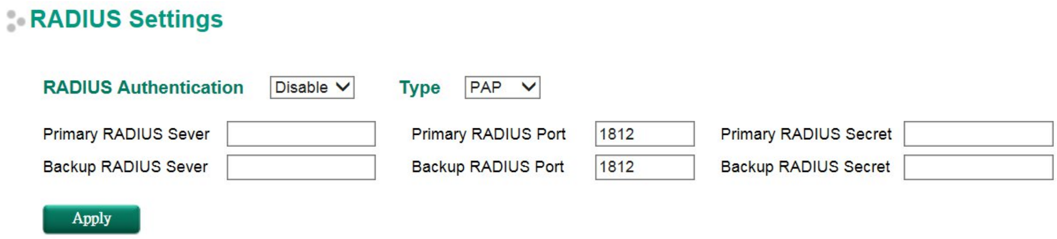
The industrial secure router generates certificates automatically. If this does not happen, please select "Re-Generate" to generate a new certificate. Auto Generate is the default setting.

Local Certificate Database

Select a certificate that has been imported into Local Certificate. Certificates that are loaded here are limited to "Certificate from CSR" and "Certificate from PKCS#12".

RADIUS Settings

Across the network, users can set up two RADIUS servers. One is the primary and the other one is the backup. When the primary RADIUS server fails, the industrial secure router will switch connections to the backup RADIUS server.



RADIUS Settings

RADIUS Authentication: Disable Type: PAP

Primary RADIUS Sever		Primary RADIUS Port	1812	Primary RADIUS Secret	
Backup RADIUS Sever		Backup RADIUS Port	1812	Backup RADIUS Secret	

Radius StaFunction Nametus

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

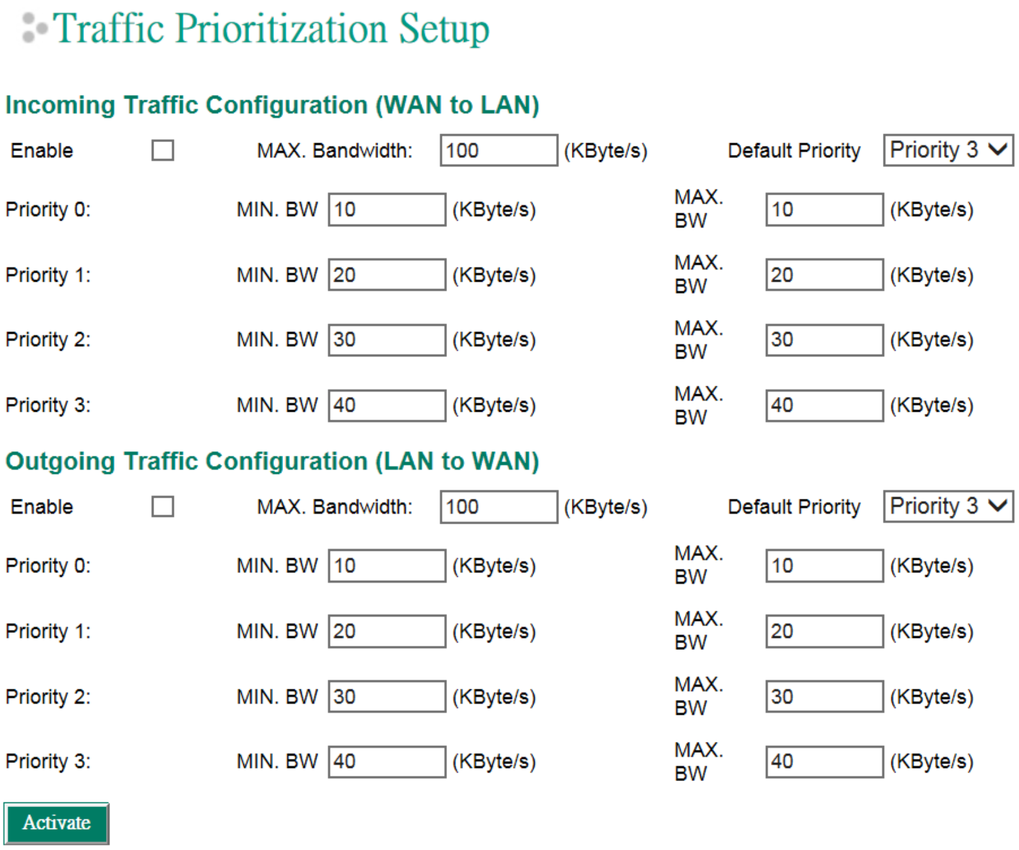
Setting	Description	Factory Default
RADIUS Server	Specifies the IP/name of the server	None
RADIUS Port	Specifies the port of the server	1812
RADIUS Secret	Specifies the shared key of the server	None

Traffic Prioritization Setup

With QoS technology, users can easily reserve bandwidth for traffic with high priority, to fulfill different applications, e.g. VOIP or MPEG. In the EDR-G902/ G903, there are four priorities, priority 0 to priority 4. Priority 0 to priority 4 are suitable for Unsolicited Granted service, real-time service, non-real time service, and best-effort service accordingly.

Priority 0 is the highest priority, which is used for Unsolicited Granted service, e.g. VOIP. Priority 4 is the lowest priority, which is used for best effort protocol, e.g. email, web access.

Users can set up minimum and maximum bandwidth for each priority. And when there is packet flow which does not meet any rules, the user can set up the default priority for this kind of packet flow.



Traffic Prioritization Setup

Incoming Traffic Configuration (WAN to LAN)

Enable	☐	MAX. Bandwidth:	100	(KByte/s)	Default Priority	Priority 3
Priority 0:	MIN. BW	10	(KByte/s)	MAX. BW	10	(KByte/s)
Priority 1:	MIN. BW	20	(KByte/s)	MAX. BW	20	(KByte/s)
Priority 2:	MIN. BW	30	(KByte/s)	MAX. BW	30	(KByte/s)
Priority 3:	MIN. BW	40	(KByte/s)	MAX. BW	40	(KByte/s)

Outgoing Traffic Configuration (LAN to WAN)

Enable	☐	MAX. Bandwidth:	100	(KByte/s)	Default Priority	Priority 3
Priority 0:	MIN. BW	10	(KByte/s)	MAX. BW	10	(KByte/s)
Priority 1:	MIN. BW	20	(KByte/s)	MAX. BW	20	(KByte/s)
Priority 2:	MIN. BW	30	(KByte/s)	MAX. BW	30	(KByte/s)
Priority 3:	MIN. BW	40	(KByte/s)	MAX. BW	40	(KByte/s)

Enable

Setting	Description	Factory Default
Check/ Uncheck	Enable QoS setting for traffic from WAN to LAN/ LAN to WAN	Unchecked

Max. Bandwidth

Setting	Description	Factory Default
Max. Bandwidth (Kbyte/s)	Maximum total bandwidth for priority 0 to 3 of traffic from WAN to LAN/ LAN to WAN	100

Default Priority

Setting	Description	Factory Default
Priority0/ Priority1/ Priority2/ Priority3/	Default priority for packet flow which does not meet any rules	Priority3

Priority0

Setting	Description	Factory Default
Min. bandwidth	Minimum bandwidth for each priority. User can set up sixty-four rules to classify packets. Take priority 0 as an example, packet flows classified as priority 3 will share this minimum bandwidth.	10
Max. bandwidth	Maximum bandwidth for each priority. Maximum bandwidth has to be greater than the minimum bandwidth.	10

Priority1

Setting	Description	Factory Default
Min. bandwidth	Minimum bandwidth for each priority. Users can set up sixty-four rules to classify packets. Take priority 1 as an example, packet flows classified as priority 3 will share this minimum bandwidth.	20
Max. bandwidth	Maximum bandwidth for each priority. Maximum bandwidth has to be greater than minimum bandwidth.	20

Priority2

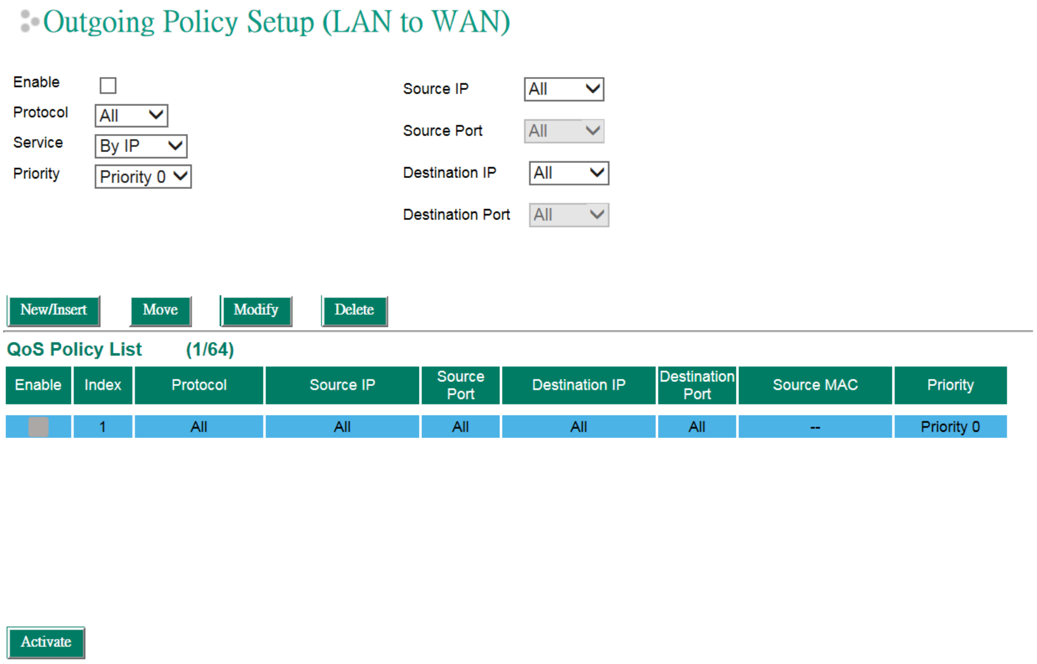
Setting	Description	Factory Default
Min. bandwidth	Minimum bandwidth for each priority. Users can set up sixty-four rules to classify packets. Take priority 2 as an example, packet flows classified as priority 3 will share this minimum bandwidth.	30
Max. bandwidth	Maximum bandwidth for each priority. Maximum bandwidth has to be greater than minimum bandwidth.	30

Priority3

Setting	Description	Factory Default
Min. bandwidth	Minimum bandwidth for each priority. Users can set up sixty-four rules to classify packets. Take priority 3 as an example, packet flows classified as priority 3 will share this minimum bandwidth.	40
Max. bandwidth	Maximum bandwidth for each priority. Maximum bandwidth has to be greater than minimum bandwidth.	40

Outgoing Policy Setup (LAN to WAN)

Users can set up rules to classify packet flow from LAN to WAN. Users can enter up to 64 rules. Users should click **New/Insert** to add a new rule, click **Move** to change the index of rule, click **Modify** to change rule setting, and click **Delete** to cancel rule.



Outgoing Policy Setup (LAN to WAN)

Enable ☐

Protocol: All

Service: By IP

Priority: Priority 0

Source IP: All

Source Port: All

Destination IP: All

Destination Port: All

QoS Policy List (1/64)

Enable	Index	Protocol	Source IP	Source Port	Destination IP	Destination Port	Source MAC	Priority
☐	1	All	All	All	All	All	--	Priority 0

Enable

Setting	Description	Factory Default
Check/ Uncheck	Enable rules to classify packets flow.	Unchecked

Protocol

Setting	Description	Factory Default
All/ TCP/ UDP/ ICMP	Select which protocol is with high priority	All

Service

Setting	Description	Factory Default
By IP/ By MAC	Prioritize specific packet source/destination with IP or MAC	By IP

Priority

Setting	Description	Factory Default
Priority 0/1/2/3	Define priority of each rule. 0 is the highest priority	Priority 0

Source IP

Setting	Description	Factory Default
All/ Single/Range	Define packet from which source IP is with high priority	All

Source Port

Setting	Description	Factory Default
All/ Single/Range	Define TCP/UDP packet from which source port is with high priority	All

Destination IP

Setting	Description	Factory Default
All/ Single/Range	Define packet to which destination IP is with high priority	All

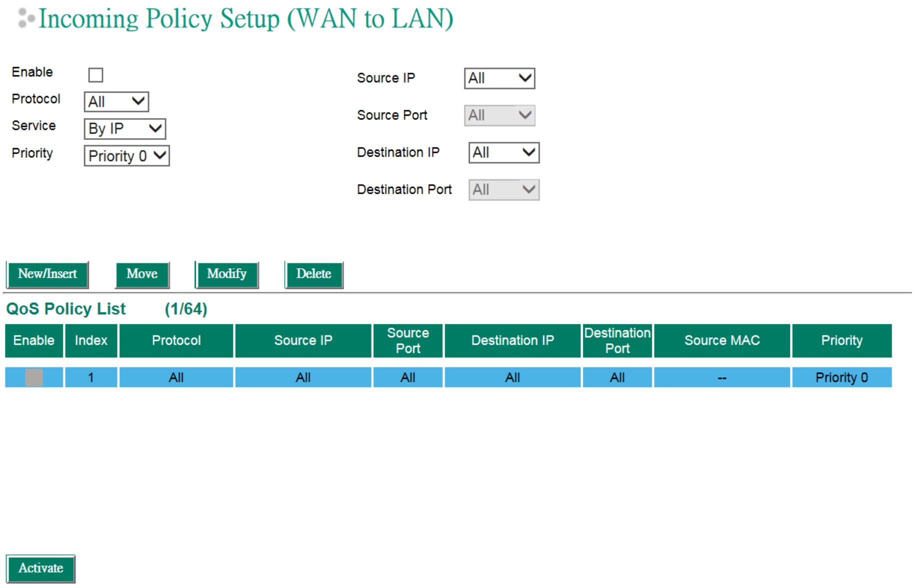
Destination Port

Setting	Description	Factory Default
All/ Single/Range	Define TCP/ UDP packet to which destination IP is with high priority	All

NOTE If rules are not enabled, the default packet flow will be ’All’.

Incoming Policy Setup (WAN to LAN)

Users can set up rules to classify packet flow from WAN to LAN. Users can enter up to 64 rules. User should click **New/Insert** to add new rule, click **Move** to changes index of rule, click **Modify** to change rule setting, and click **Delete** to cancel the rule.



Enable □

Protocol: All

Service: By IP

Priority: Priority 0

Source IP: All

Source Port: All

Destination IP: All

Destination Port: All

QoS Policy List (1/64)

Enable	Index	Protocol	Source IP	Source Port	Destination IP	Destination Port	Source MAC	Priority
□	1	All	All	All	All	All	--	Priority 0

Enable

Setting	Description	Factory Default
Check/Uncheck	Enable LAN to WAN traffic prioritize	Unchecked

Protocol

Setting	Description	Factory Default
All/ TCP/ UDP/ICMP	Select which protocol has the highest priority	All

Service

Setting	Description	Factory Default
By IP/By MAC	Prioritize specific packet source/destination with IP or MAC	By IP

Priority

Setting	Description	Factory Default
Priority 0/1/2/3	Define priority of each rule. 0 is the highest priority	Priority 0

Source IP

Setting	Description	Factory Default
All/ Single/Range	Define packet from which source IP has the highest priority	All

Source Port

Setting	Description	Factory Default
All/ Single/Range	Define TCP/UDP packet from which source port is with high priority	All

Destination IP

Setting	Description	Factory Default
All/ Single/Range	Define packet to which destination IP is with high priority	All

Destination Port

Setting	Description	Factory Default
All/ Single/Range	Define TCP/ UDP packet to which destination IP is with high priority	All

NOTE If rules are not enabled, the default packet flow will be 'All'.

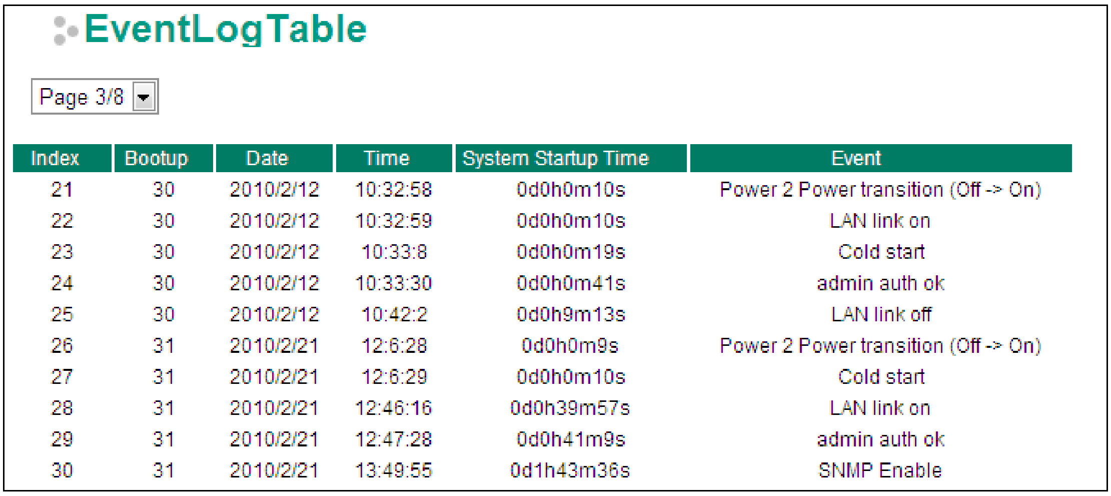
Monitor

You can monitor statistics in real time from the EtherDevice Router's web console.

System Log

The industrial secure router provides **EventLog** and **Syslog** functions to record important events.

EventLog



EventLogTable

Page 3/8

Index	Bootup	Date	Time	System Startup Time	Event
21	30	2010/2/12	10:32:58	0d0h0m10s	Power 2 Power transition (Off -> On)
22	30	2010/2/12	10:32:59	0d0h0m10s	LAN link on
23	30	2010/2/12	10:33:8	0d0h0m19s	Cold start
24	30	2010/2/12	10:33:30	0d0h0m41s	admin auth ok
25	30	2010/2/12	10:42:2	0d0h9m13s	LAN link off
26	31	2010/2/21	12:6:28	0d0h0m9s	Power 2 Power transition (Off -> On)
27	31	2010/2/21	12:6:29	0d0h0m10s	Cold start
28	31	2010/2/21	12:46:16	0d0h39m57s	LAN link on
29	31	2010/2/21	12:47:28	0d0h41m9s	admin auth ok
30	31	2010/2/21	13:49:55	0d1h43m36s	SNMP Enable

Field	Description
Bootup	This field shows how many times the device has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the "Basic Setting" page.
Time	The time is updated based on how the current time is set in the "Basic Setting" page.
System Startup Time	The system startup time related to this event.
Event	Events that have occurred.

The following events will be recorded in the EtherDevice Router EventLog Table:

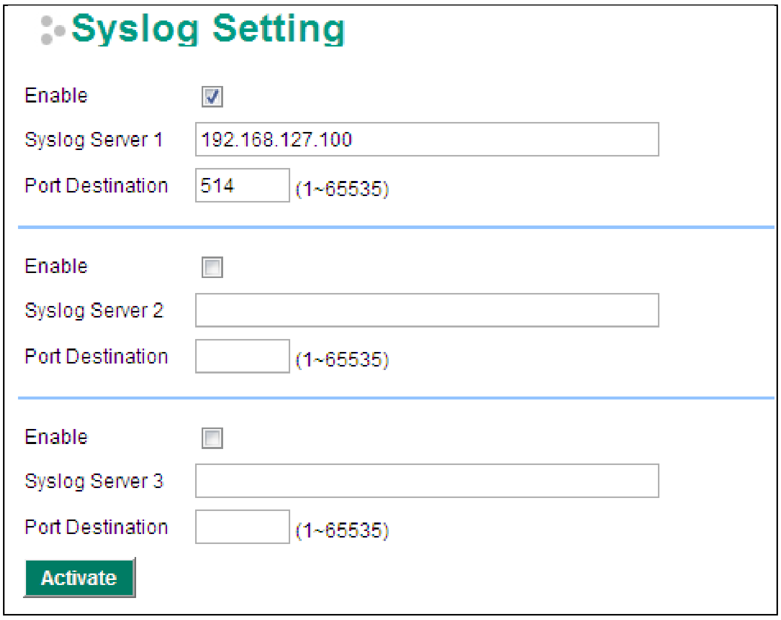
Event	Status
Syslog	Configuration change activated
DNS	Configuration change activated
Static Route	Configuration change activated
SYSTEMINFO	Configuration change activated
SNMPTRAP	Configuration change activated
Filter	Configuration change activated
NAT	Configuration change activated
DoS	Configuration change activated
QoS_Bandwith	Configuration change activated
QoS_DownStream	Configuration change activated
QoS_UpStream	Configuration change activated
DHCP	Configuration Change activated/ Enable / Disable

NTP	Configuration Change activated/ Enable / Disable
SNMP	Configuration Change activated/ Enable / Disable
DDNS	Configuration Change activated/ Enable / Disable
WAN Backup	Configuration change activated
LAN	Link on / Link off / IP change
WAN2	Link on / Link off / IP change
WAN1	Link on / Link off / IP change
Password	Configuration change activated
Login	Authentication Fail / Authentication Pass
Accessible IP function	Enable / Disable
Power transition (On -> Off)	
Power transition (Off -> On)	
DI transition (Off -> On)	
DI transition (On -> Off)	
Cold start	
Factory default	Warm start
System restart	Warm start
Firmware Upgrade	Warm start
Configuration Upgrade	Warm start

NOTE The maximum number of event entries is 1000.

Syslog

This 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.



Syslog Setting

Enable ☑
Syslog Server 1 192.168.127.100
Port Destination 514 (1~65535)

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

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

Syslog Server 1/2/3

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

5

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)
- **Broadcast Forwarding (EDR-810 only)**
- **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.

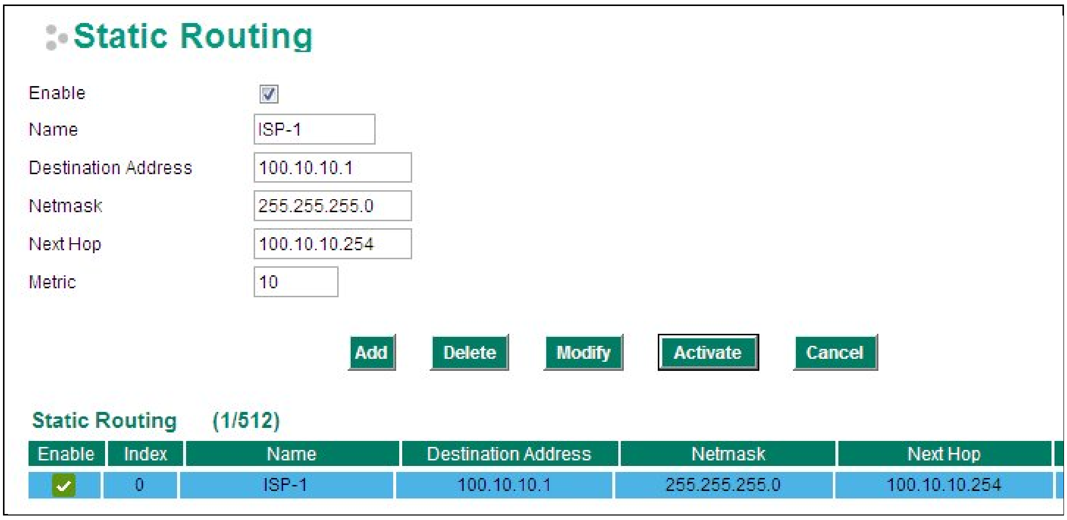
RIP (Routing Information Protocol)

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.



Static Routing

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

Static Routing (1/512)

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

Enable

Click the checkbox to enable Static Routing.

Name

The name of this Static Router list

Destination Address

You can specify the destination IP address.

Netmask

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

Next Hop

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

Metric

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

Clickable Buttons

Add

For adding an entry to the Static Routing Table.

Delete

For removing selected entries from the Static Routing Table.

Modify

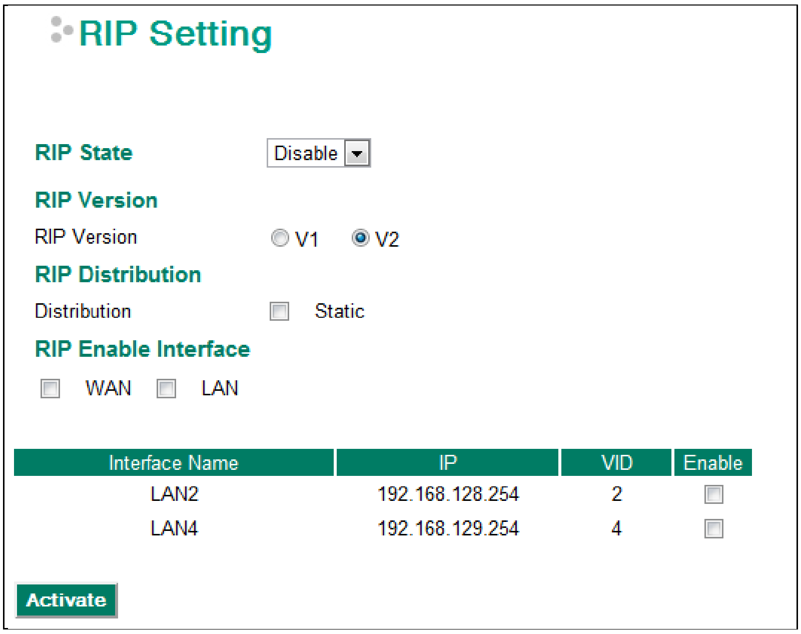
For modifying the content of a selected entry in the Static Routing Table.

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

RIP (Routing Information Protocol)

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

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



RIP Setting

RIP State: Disable

RIP Version

RIP Version ○ V1 ● V2

RIP Distribution

Distribution □ Static

RIP Enable Interface

□ WAN □ LAN

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

RIP State

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

RIP Version

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

RIP Distribution

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

RIP Enable Interface

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

RIP Interface Table (EDR-810 series only)

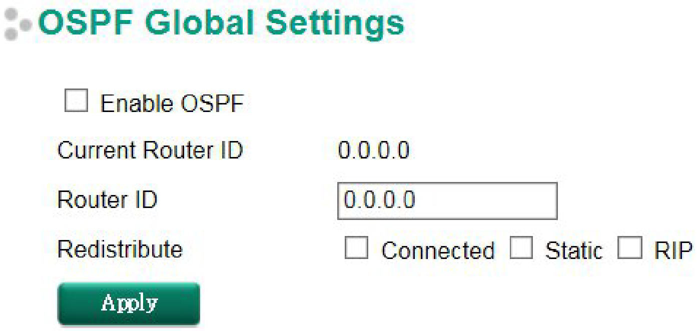
Setting	Description	Factory Default
Enable/Disable	Check the checkbox to enable RIP for each interface.	Unchecked

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



OSPF Global Settings

☐ Enable OSPF

Current Router ID 0.0.0.0

Router ID 0.0.0.0

Redistribute ☐ Connected ☐ Static ☐ RIP

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

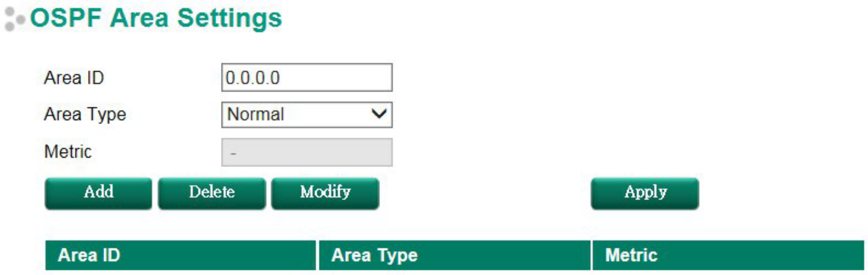
Setting	Description	Factory Default
Connected	Entries learned from the directly connected interfaces will be re-distributed if this option is enabled.	Checked (Enable)
Static	Entries set in a static route will be re-distributed if this option is enabled.	Unchecked (disable)
RIP	Entries learned from the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


OSPF Area Settings

Area ID: 0.0.0.0

Area Type: Normal

Metric: -

Area ID	Area Type	Metric

Area ID

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

Area Type

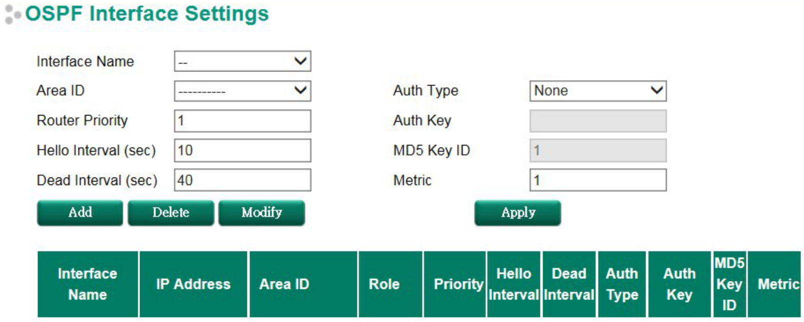
Setting	Description	Factory Default
Normal/Stub/NSSA	Defines the area type.	Normal

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.



OSPF Interface Settings

Interface Name	--		
Area ID	----------	Auth Type	None
Router Priority	1	Auth Key	
Hello Interval (sec)	10	MD5 Key ID	1
Dead Interval (sec)	40	Metric	1

Interface Name	IP Address	Area ID	Role	Priority	Hello Interval	Dead Interval	Auth Type	Auth Key	MD5 Key ID	Metric

Interface Name

Setting	Description	Factory Default
Interface Name	Defines the interface name.	N/A

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	1

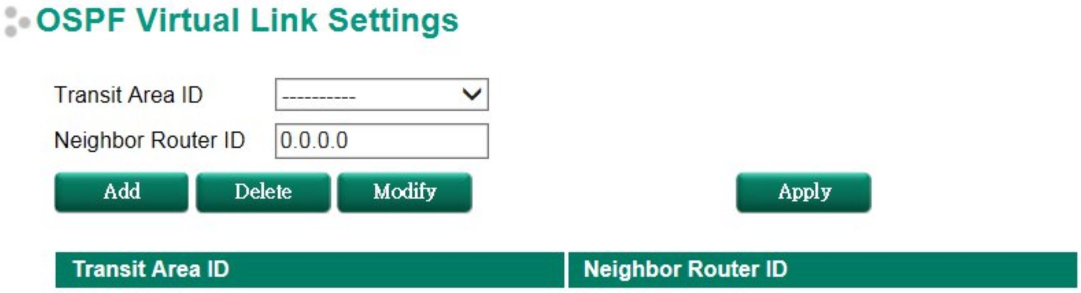
	authentication key. This hash value is transmitted in the packet, along with a key ID.	

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.


OSPF Virtual Link Settings

Transit Area ID: ----------

Neighbor Router ID: 0.0.0.0

Transit Area ID	Neighbor Router ID

Transit Area ID

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

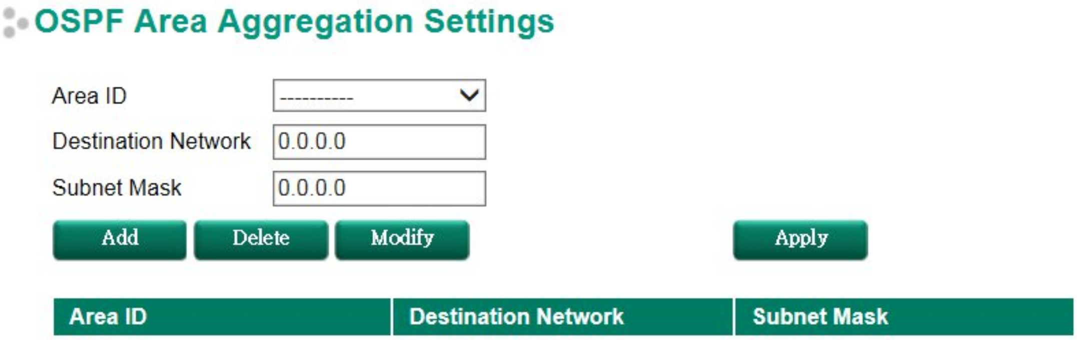
Neighbor Router ID

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.


OSPF Area Aggregation Settings

Area ID: ----------

Destination Network: 0.0.0.0

Subnet Mask: 0.0.0.0

Area ID	Destination Network	Subnet Mask

Area ID

Setting	Description	Factory Default
Area ID	Select the Area ID that you want to configure.	0.0.0.0

Destination Network

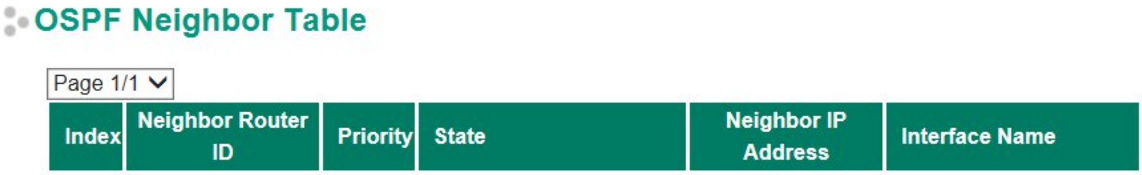
Setting	Description	Factory Default
Destination Network	Fill in the network address in the area.	0.0.0.0

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.



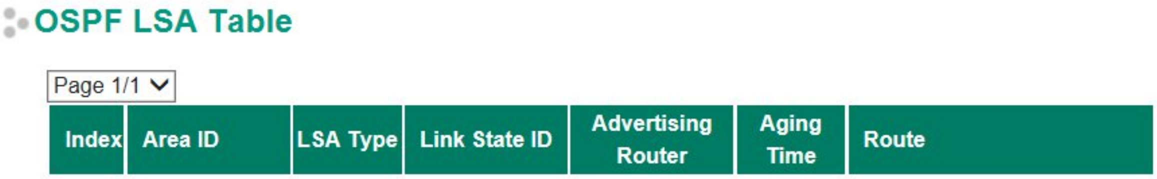
OSPF Neighbor Table

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.



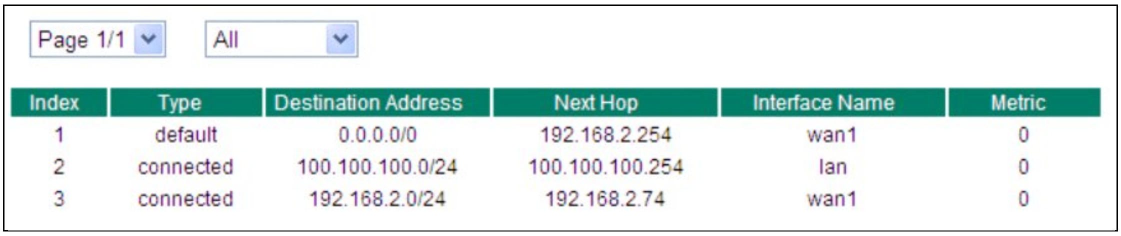
OSPF LSA Table

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

All Routing Entry List

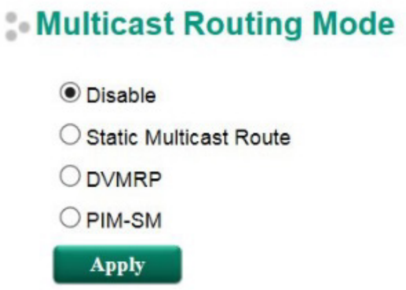
Setting	Description	Factory Default
All	Show all routing entries	N/A
Connected	Show connected routing entries	N/A
Static	Show Static routing entries	N/A
RIP	Show RIP routing entries	N/A
Others	Show others routing entries	N/A

Multicast Route

The industrial secure router supports three multicast routing protocols: Static Multicast Route, Distance Vector Multicast Routing Protocol (DVMRP), and Protocol Independent Multicast Sparse Mode (PIM-SM).

Global setting

Only one multicast routing protocol can be enabled in one industrial secure router. Static Multicast Route, DVMRP and PIM-SM cannot be enabled simultaneously. Please select the multicast protocol that suits your application best.

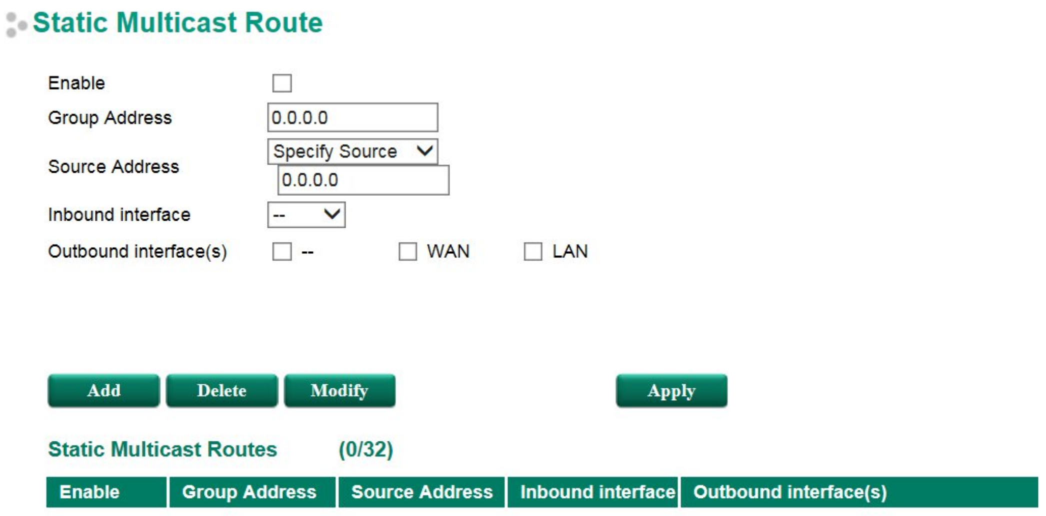


Multicast Routing Mode

● Disable
○ Static Multicast Route
○ DVMRP
○ PIM-SM

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

Static Multicast



Static Multicast Route

Enable	□
Group Address	0.0.0.0
Source Address	Specify Source 0.0.0.0
Inbound interface	--
Outbound interface(s)	□ -- □ WAN □ LAN

Static Multicast Routes (0/32)

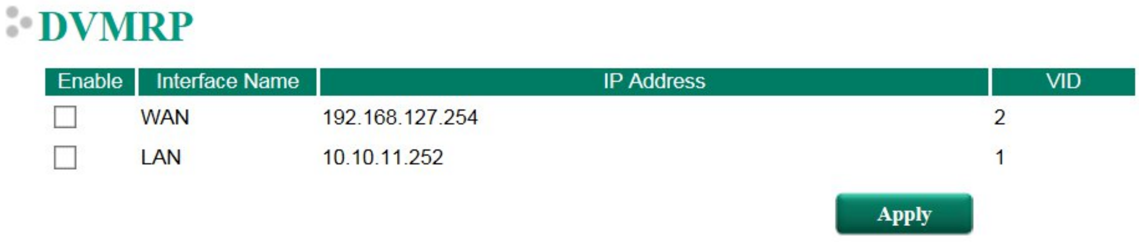
Enable	Group Address	Source Address	Inbound interface	Outbound interface(s)

Distance Vector Multicast Routing Protocol (DVMRP)

Distance Vector Multicast Routing Protocol (DVMRP) is used to build multicast delivery trees on a network. When a Layer 3 switch receives a multicast packet, DVMRP provides a routing table for the relevant multicast group, and includes distance information on the number of devices between the router and the packet destination. The multicast packet will then be forwarded through the Layer 3 switch interface specified in the multicast routing table.

Setting

Users can select which interface or VLAN can transmit multicast data stream.



DVMRP

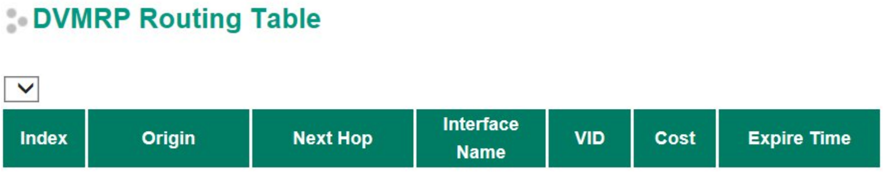
Enable	Interface Name	IP Address	VID
□	WAN	192.168.127.254	2
□	LAN	10.10.11.252	1

Enable (individual)

Setting	Description	Factory Default
Enable/Disable	Enable or disable corresponding VLAN to transmit multicast data stream	Uncheck

DVMRP Routing Table

The DVMRP Routing table page shows all routing entries. The "Expire Time" column specifies the routing information regarding the expiration period. If the industrial secure router does not receive this routing information update before the expiration period, the routing information will be canceled.

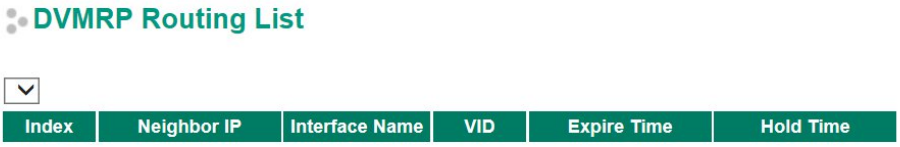


DVMRP Routing Table

Index	Origin	Next Hop	Interface Name	VID	Cost	Expire Time

DVMRP Neighbors Table

This table shows the current DVMRP Neighbor table. The "Hold Time" column specifies the time period for which a neighbor considers the sending router to be operating.



DVMRP Routing List

Index	Neighbor IP	Interface Name	VID	Expire Time	Hold Time

Protocol Independent Multicast Sparse Mode (PIM-SM)

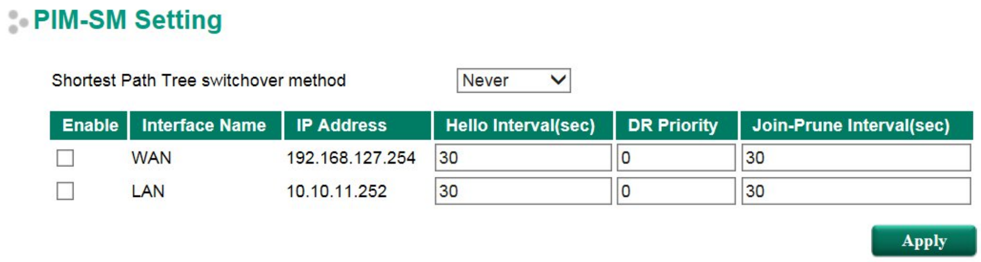
Protocol Independent Multicast (PIM) is a method of forwarding traffic to multicast groups over the network using any pre-existing unicast routing protocol, such as RIP or OSPF, set on routers within a multicast network.

In protocol Independent Multicast Sparse Mode (PIM-SM), the multicast source will not flood multicast packets to all routers. The source will send multicast packets when the source receives a joint message.

Receivers send a joint message to the Rendezvous Point (RP) and select which group to join. The source subscribes information in the RP. And then the RP can forward a joint message to the source or forward multicast information to receivers.

PIM-SM builds a shared tree to distribute multicast packets. There will be one RP for each group. By following the Shortest Path Tree (SPT), the source sends multicast packets to the RP and then the RP sends multicast packets to receivers.

Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) builds trees that are rooted in just one source, which offers a more secure and scalable model for a limited number of applications.



PIM-SM Setting

Shortest Path Tree switchover method: Never

Enable	Interface Name	IP Address	Hello Interval(sec)	DR Priority	Join-Prune Interval(sec)
□	WAN	192.168.127.254	30	0	30
□	LAN	10.10.11.252	30	0	30

Shortest Path Tree Switchover Method

Setting	Description	Factory Default
Never/Immediate	Define how Shortest Path Tree switches over	Never

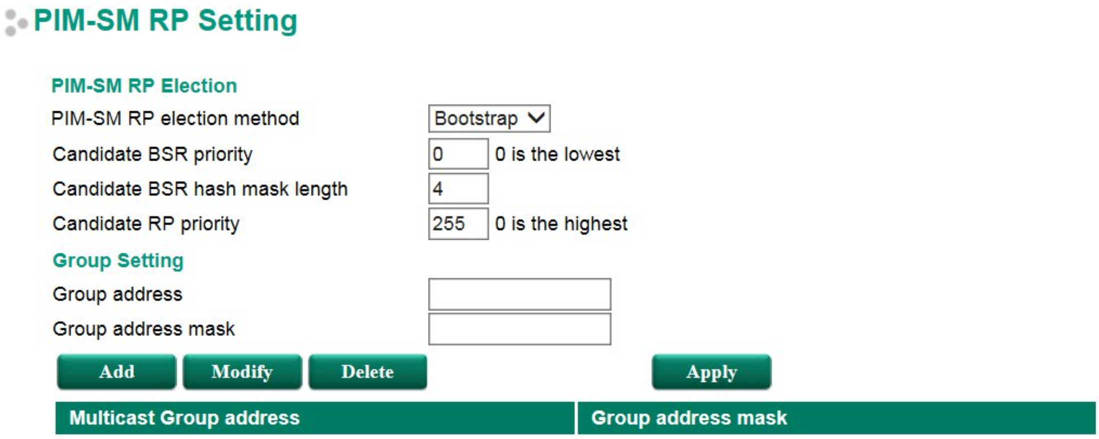
Enable (individual)

Setting	Description	Factory Default
Enable/Disable	Enable or disable PIM-SM by the selected interface	Disable

NOTE Only one multicast routing protocol can be enabled on one Moxa Layer 3 switch. DVMRP, PIM-DM, and PIM-SM can NOT be enabled simultaneously.

This page is used to set up the PIM-SM RP settings for Moxa Layer 3 switches. There are two RP Election Methods: Bootstrap and Static.

Bootstrap



PIM-SM RP Setting

PIM-SM RP Election

PIM-SM RP election method: Bootstrap

Candidate BSR priority: 0 — 0 is the lowest

Candidate BSR hash mask length: 4

Candidate RP priority: 255 — 0 is the highest

Group Setting

Group address:

Group address mask:

Multicast Group address	Group address mask

Candidate BSR Priority

Setting	Description	Factory Default
0 to 255	Define the priority of BSR election	0

Candidate BSR Hash Mask Length

Setting	Description	Factory Default
4 to 32	Define the Hash mask length of BSR election	4

Candidate RP Priority

Setting	Description	Factory Default
0 to 255	Define the priority of RP election	255

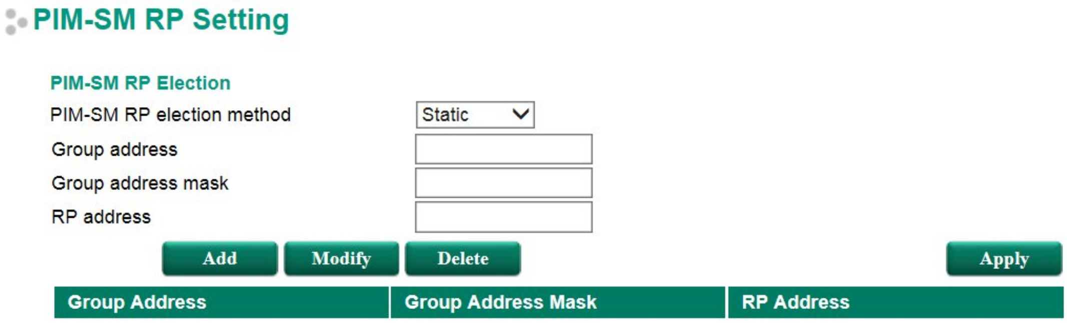
Group Address

Setting	Description	Factory Default
Group Address	Define the group address	N/A

Group Address Mask

Setting	Description	Factory Default
4(240.0.0.0) to 32(255.255.255.255)	Select the group address mask.	N/A

Static


PIM-SM RP Setting

PIM-SM RP Election

PIM-SM RP election method: Static

Group address

Group address mask

RP address

Group Address	Group Address Mask	RP Address

Group Address

Setting	Description	Factory Default
Group Address	Define the group address	N/A

Group Address Mask

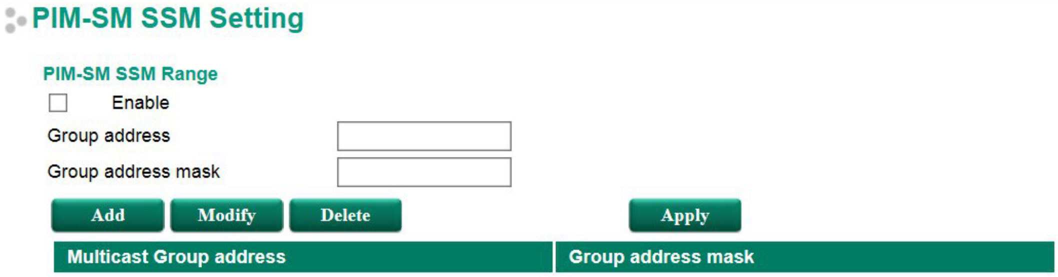
Setting	Description	Factory Default
4(240.0.0.0) to 32(255.255.255.255)	Select the group address mask.	N/A

RP Address

Setting	Description	Factory Default
RP Address	Define the RP address	N/A

PIM-SM SSM Setting

This page is used to set up the PIM-SM SSM settings for Moxa Layer 3 switches.


PIM-SM SSM Setting

PIM-SM SSM Range

□ Enable

Group address

Group address mask

Multicast Group address	Group address mask

Enable PIM-SSM

Setting	Description	Factory Default
Enable/Disable	Enable or disable PIM-SSM	Disable

Group Address

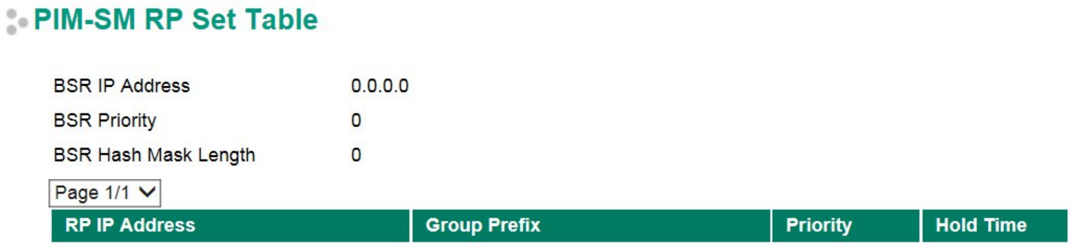
Setting	Description	Factory Default
Group Address	Define the group address	N/A

Group Address Mask

Setting	Description	Factory Default
4(240.0.0.0) to 32(255.255.255.255)	Select the group address mask.	N/A

PIM-SM RP Set Table

This is a table showing the current PIM-SM RP-Set table.



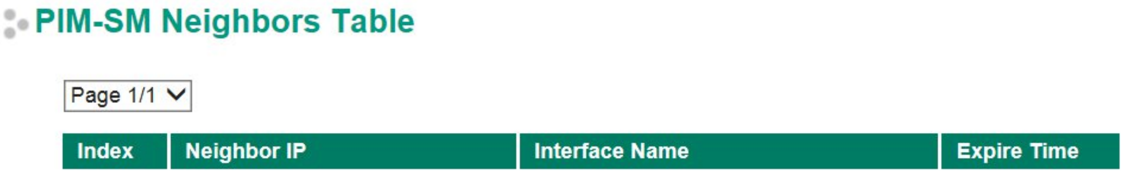
PIM-SM RP Set Table

BSR IP Address	0.0.0.0
BSR Priority	0
BSR Hash Mask Length	0

Page 1/1

RP IP Address	Group Prefix	Priority	Hold Time

This is a table showing the current PIM-SM Neighbor table.

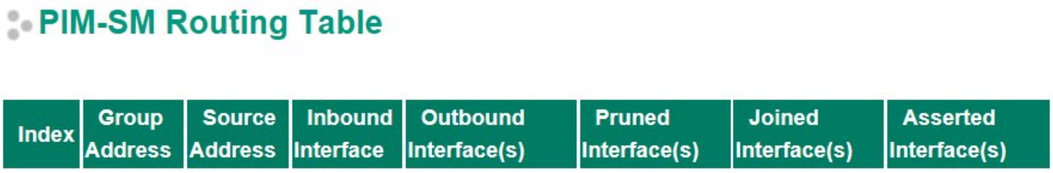


PIM-SM Neighbors Table

Page 1/1

Index	Neighbor IP	Interface Name	Expire Time

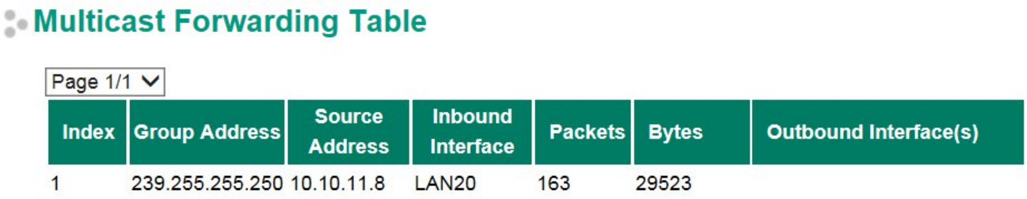
This is a table showing the current PIM-SM multicast routing table.



PIM-SM Routing Table

Index	Group Address	Source Address	Inbound Interface	Outbound Interface(s)	Pruned Interface(s)	Joined Interface(s)	Asserted Interface(s)

This is a table showing the current Multicast Forwarding table.



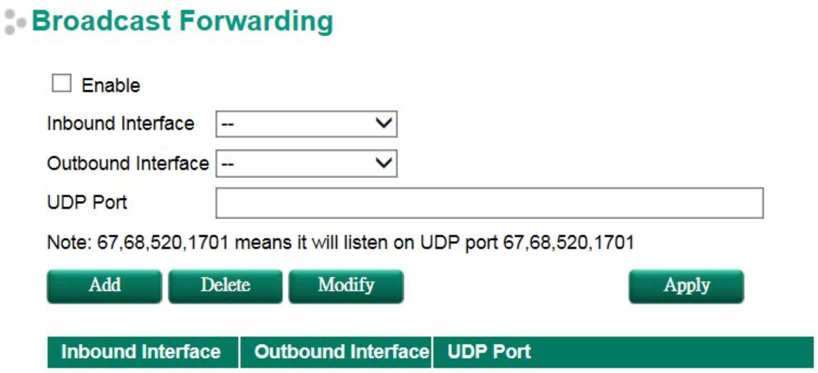
Multicast Forwarding Table

Page 1/1

Index	Group Address	Source Address	Inbound Interface	Packets	Bytes	Outbound Interface(s)
1	239.255.255.250	10.10.11.8	LAN20	163	29523	

Broadcast Forwarding (EDR-810 only)

In some scenarios, users have to issue broadcast packets to query all the devices in the network for data collecting, such as Modbus devices. However, normally, broadcast packets cannot pass through the router. With the EDR-810, users can configure which interface and UDP port numbers that broadcast packet will pass through. Users can set up multiple rules by click Add. When configuration is done, click Apply.



Broadcast Forwarding

□ Enable

Inbound Interface: --

Outbound Interface: --

UDP Port:

Note: 67,68,520,1701 means it will listen on UDP port 67,68,520,1701

Inbound Interface	Outbound Interface	UDP Port

Enable

Setting	Description	Factory Default
Check/Uncheck	Permit broadcast packet to pass through the ERD-810	Unchecked

Inbound Interface

Setting	Description	Factory Default
WAN/LAN	Which interface broadcast packet will come from	N/A

Outbound Interface

Setting	Description	Factory Default
WAN/LAN	Which interface broadcast packet will pass through	N/A

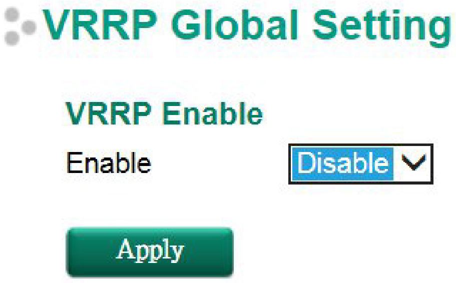
UDP Port

Setting	Description	Factory Default
UDP Port Number	Service port number. User can enter multiple port numbers.	N/A

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


VRRP Global Setting

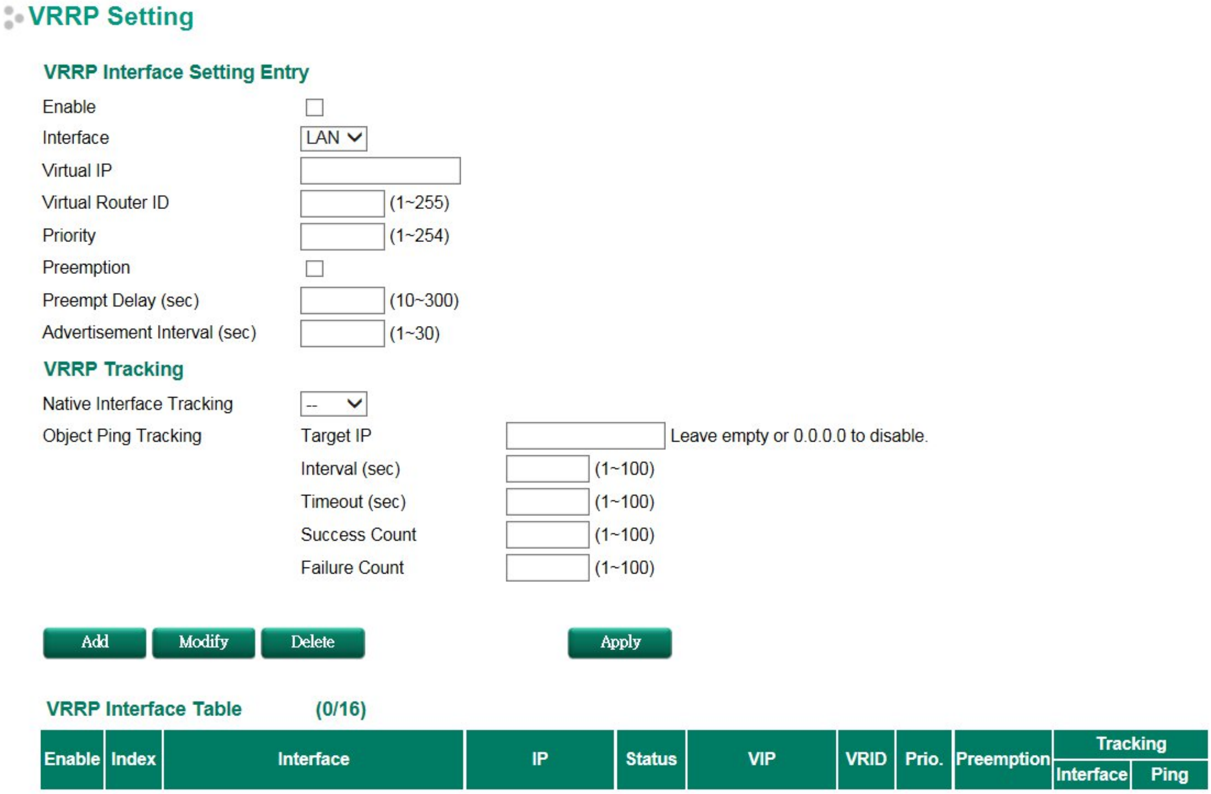
VRRP Enable

Enable Disable

Enable

Setting	Description	Factory Default
Enable	Enables all VRRP interface	Disable

VRRP Setting


VRRP Setting

VRRP Interface Setting Entry

Enable	□		
Interface	LAN		
Virtual IP			
Virtual Router ID	(1~255)		
Priority	(1~254)		
Preemption	□		
Preempt Delay (sec)	(10~300)		
Advertisement Interval (sec)	(1~30)		

VRRP Tracking

Native Interface Tracking	--		
Object Ping Tracking	Target IP		Leave empty or 0.0.0.0 to disable.
	Interval (sec)		(1~100)
	Timeout (sec)		(1~100)
	Success Count		(1~100)
	Failure Count		(1~100)

VRRP Interface Table (0/16)

Enable	Index	Interface	IP	Status	VIP	VRID	Prio.	Preemption	Tracking	
									Interface	Ping

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.	N/A
Virtual Router ID (VRID)	Virtual Router ID is used to assign a VRRP group. The Industrial secure routers, which operate as master / backup, should	N/A

	have the same ID. Industrial secure routers support 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".	N/A
Preemption	When the master is back alive, it determines whether the master will take the authority back or not.	Unchecked
Preemption Delay (sec)	When preemption 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.	N/A
Advertisement Interval (sec)	For every defined period of time, the master will send packets to all slave devices to inform who the master is.	N/A

VRRP Tracking Enable

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

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.	N/A
Interval (sec)	How many seconds to ping destination to verify connection.	N/A
TimeOut (sec)	See how many seconds it takes for the ping response before timeout	N/A
Success Count	Know how many times the ping responds in order to know the connection is working.	N/A
Failure Count	Know how long until the ping does not respond in order to know the connection is not working.	N/A

6

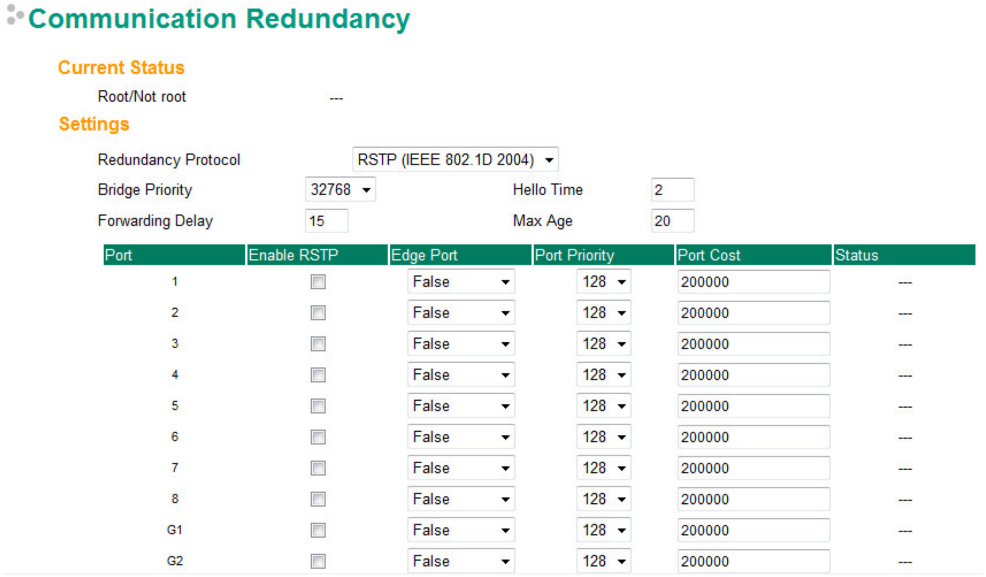
Network Redundancy

The following topics are covered in this chapter:

Layer 2 Redundant Protocols (EDR-810 series only)

Configuring STP/RSTP

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



Communication Redundancy

Current Status

Root/Not root ---

Settings

Redundancy Protocol: RSTP (IEEE 802.1D 2004)

Bridge Priority: 32768 Hello Time: 2

Forwarding Delay: 15 Max Age: 20

Port	Enable RSTP	Edge Port	Port Priority	Port Cost	Status
1	□	False	128	200000	---
2	□	False	128	200000	---
3	□	False	128	200000	---
4	□	False	128	200000	---
5	□	False	128	200000	---
6	□	False	128	200000	---
7	□	False	128	200000	---
8	□	False	128	200000	---
G1	□	False	128	200000	---
G2	□	False	128	200000	---

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

Now Active:

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

Root/Not Root

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

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

Redundancy Protocol

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

Bridge priority

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

Forwarding Delay (sec.)

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

Hello time (sec.)

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

Max. Age (sec.)

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

Enable STP 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.

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

Port Priority

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

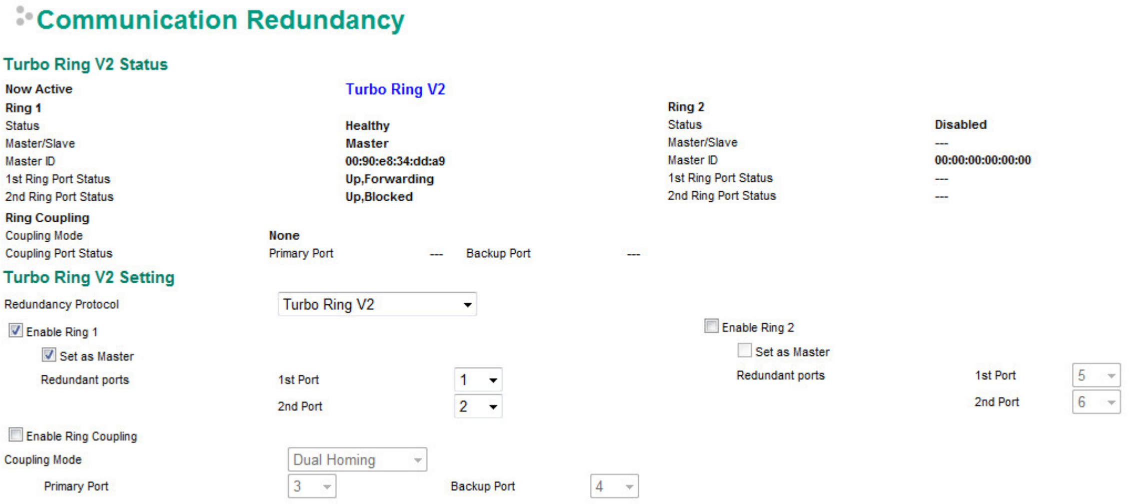
Port Cost

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

Port Status

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

Configuring Turbo Ring V2



Communication Redundancy

Turbo Ring V2 Status

Now Active: Turbo Ring V2

Ring 1		Ring 2	
Status	Healthy	Status	Disabled
Master/Slave	Master	Master/Slave	---
Master ID	00:90:e8:34:dd:a9	Master ID	00:00:00:00:00:00
1st Ring Port Status	Up,Forwarding	1st Ring Port Status	---
2nd Ring Port Status	Up,Blocked	2nd Ring Port Status	---

Ring Coupling

Coupling Mode: None

Coupling Port Status: Primary Port --- Backup Port ---

Turbo Ring V2 Setting

Redundancy Protocol: Turbo Ring V2

☑ Enable Ring 1

☑ Set as Master

Redundant ports: 1st Port 1; 2nd Port 2

☐ Enable Ring 2

☐ Set as Master

Redundant ports: 1st Port 5; 2nd Port 6

☐ Enable Ring Coupling

Coupling Mode: Dual Homing

Primary Port 3 Backup Port 4

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 EDS is the Master of the Turbo Ring. (This field appears only when Turbo Ring or Turbo Ring V2 modes are selected.)

NOTE The user does not need to set the master to use Turbo Ring. If master is not set, the Turbo Ring protocol will assign master status to one of the EDS 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.

Coupling—Mode

It indicates either **None**, **Dual Homing**, or **Ring Coupling**.

Coupling—Coupling Port status

It indicates either **Primary**, or **Backup**.

Explanation of "Settings" Items

Redundancy Protocol

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

Enable Ring 1

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

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.	See the following table

Enable Ring Coupling

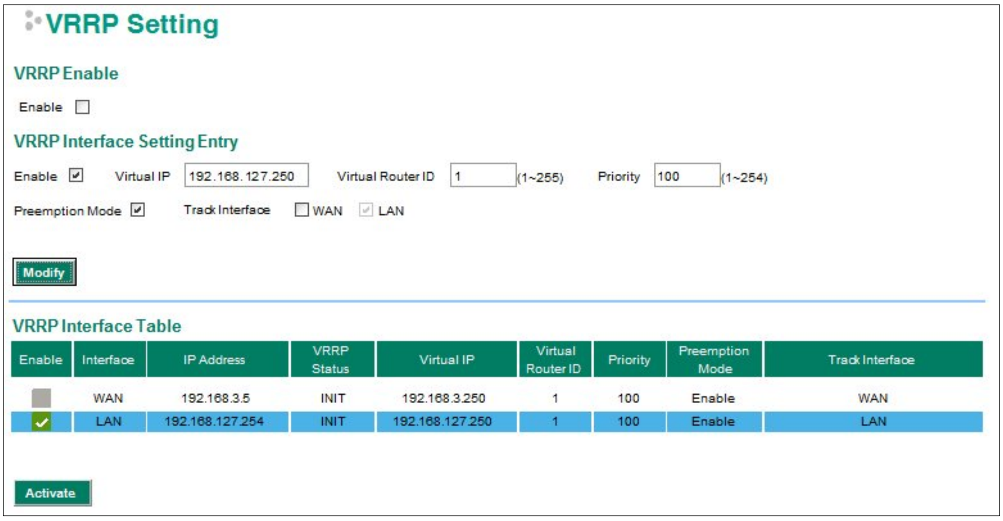
Setting	Description	Factory Default
Enable	Select this EDS as Coupler	Not checked
Disable	Do not select this EDS as Coupler	

Coupling Mode

Setting	Description	Factory Default
Dual Homing	Select this item to change to the Dual Homing configuration page	See the following table
Ring Coupling (backup)	Select this item to change to the Ring Coupling (backup) configuration page	See the following table
Ring Coupling (primary)	Select this item to change to the Ring Coupling (primary) configuration page	See the following table

Layer 3 Redundant Protocols

VRRP Settings



VRRP Setting

VRRP Enable

Enable ☐

VRRP Interface Setting Entry

Enable ☑ Virtual IP 192.168.127.250 Virtual Router ID 1 (1~255) Priority 100 (1~254)

Preemption Mode ☑ Track Interface ☐ WAN ☑ LAN

VRRP Interface Table

Enable	Interface	IP Address	VRRP Status	Virtual IP	Virtual Router ID	Priority	Preemption Mode	Track Interface
☐	WAN	192.168.3.5	INIT	192.168.3.250	1	100	Enable	WAN
✓	LAN	192.168.127.254	INIT	192.168.127.250	1	100	Enable	LAN

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

Enable

Setting	Description	Factory Default
Enable	Enables VRRP	Disable

VRRP Interface Setting Entry

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

7

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:

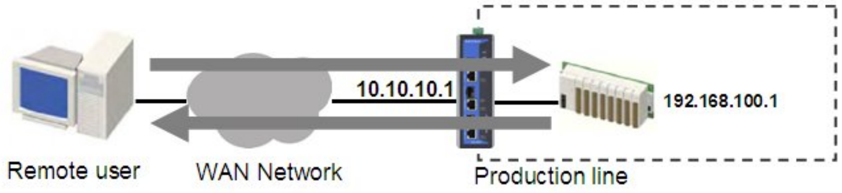
- Uses the N-1 or Port forwarding Nat function to hide the Internal IP address of a critical network or device to increase the level of security of industrial network applications.
- Uses the same private IP address for different, but identical, groups of Ethernet devices. For example, 1-to-1 NAT makes 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 128.

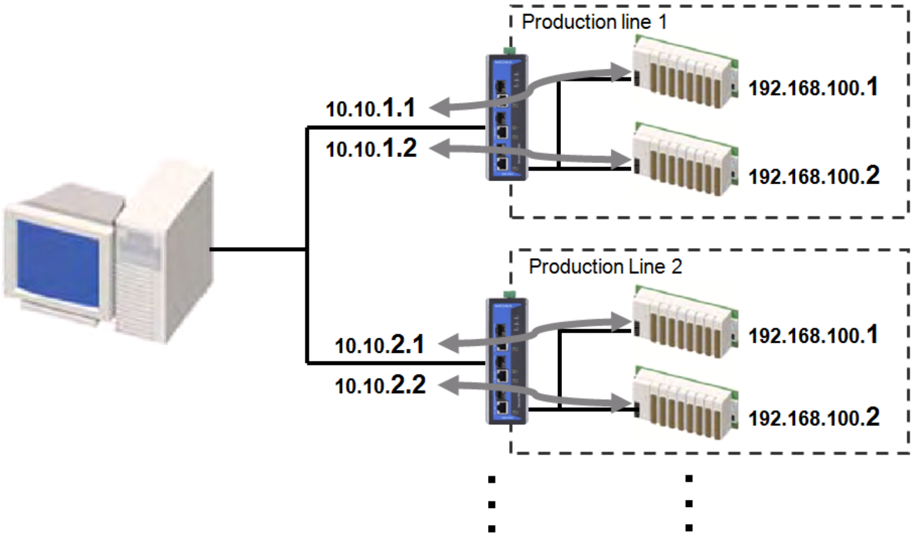
1-to-1 NAT Overview

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).

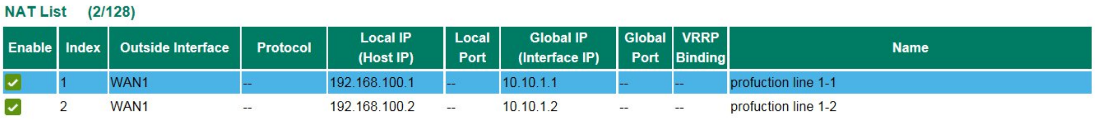


1-to-1 NAT is usually used when you have a group of internal servers with private IP addresses that must connect to the external network. You can use 1-to-1 NAT to map the internal servers to public IP addresses. The IP address of the internal device will not change.

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.



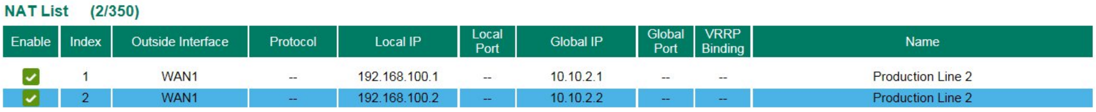
1-to-1 NAT Setting for EDR-G903 in Production Line 1



NAT List (2/128)

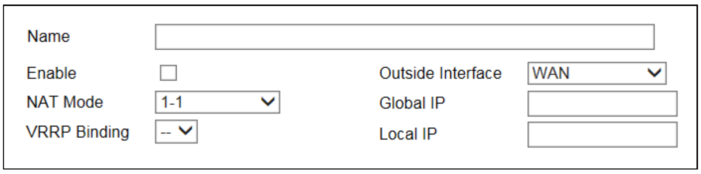
Enable	Index	Outside Interface	Protocol	Local IP (Host IP)	Local Port	Global IP (Interface IP)	Global Port	VRRP Binding	Name
☑	1	WAN1	--	192.168.100.1	--	10.10.1.1	--	--	profuction line 1-1
☑	2	WAN1	--	192.168.100.2	--	10.10.1.2	--	--	profuction line 1-2

1-to-1 NAT Setting for EDR-G903 in Production Line 2



NAT List (2/350)

Enable	Index	Outside Interface	Protocol	Local IP	Local Port	Global IP	Global Port	VRRP Binding	Name
☑	1	WAN1	--	192.168.100.1	--	10.10.2.1	--	--	Production Line 2
☑	2	WAN1	--	192.168.100.2	--	10.10.2.2	--	--	Production Line 2



Name

Enable □ Outside Interface WAN

NAT Mode 1-1 Global IP

VRRP Binding -- Local IP

1-to-1 NAT

Name

Setting	Description	Factory Default
Name	Naming NAT rule	None

Enable

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

NAT Mode

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

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.

Outside Interface

Setting	Description	Factory Default
Auto, WAN, WAN1, WAN2, BRG_LAN, LAN	In the EDR-810, select WAN/LAN/BRG_LAN interface for NAT rule. In the EDR-G903, select WAN/WAN2/LAN interface for NAT rule. In the EDR-G902, select Auto/WAN/LAN interface for NAT rule. When Auto is selected, the G902 will check if WAN interface can route the packet with NAT.	WAN1 (for EDR-G903), WAN (for EDR-810), Auto (for EDR-G902)

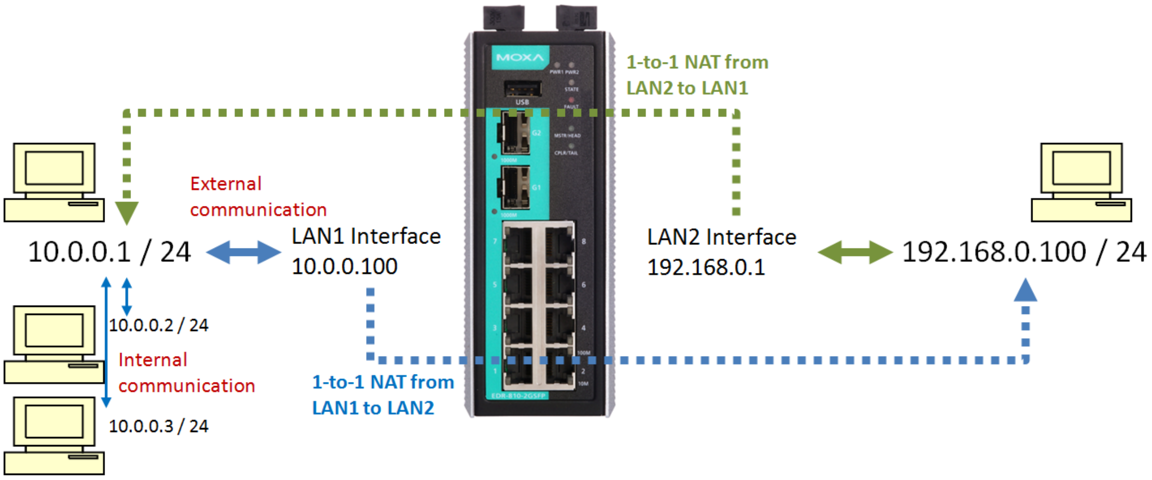
Global IP

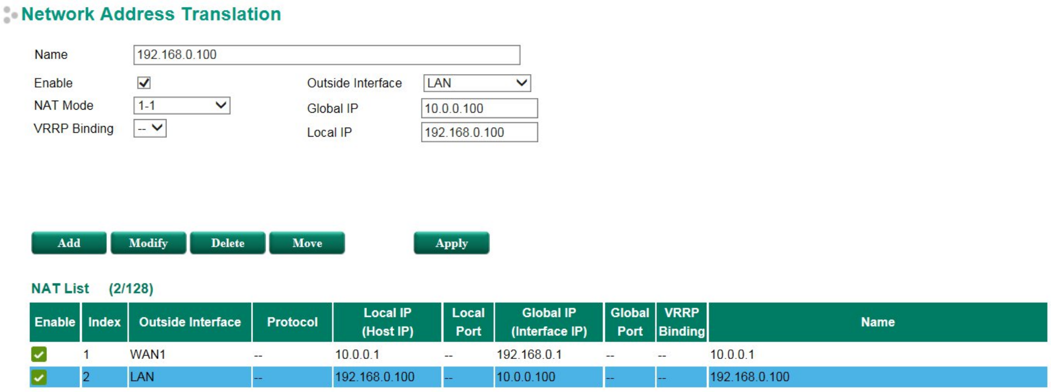
Setting	Description	Factory Default
IP Address	Set the public IP address which the internal IP will be translated into.	None

Local IP

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

Bidirectional 1-to-1 NAT





Network Address Translation

Name	192.168.0.100		
Enable	☑	Outside Interface	LAN
NAT Mode	1-1	Global IP	10.0.0.100
VRRP Binding	--	Local IP	192.168.0.100

NAT List (2/128)

Enable	Index	Outside Interface	Protocol	Local IP (Host IP)	Local Port	Global IP (Interface IP)	Global Port	VRRP Binding	Name
☑	1	WAN1	--	10.0.0.1	--	192.168.0.1	--	--	10.0.0.1
☑	2	LAN	--	192.168.0.100	--	10.0.0.100	--	--	192.168.0.100

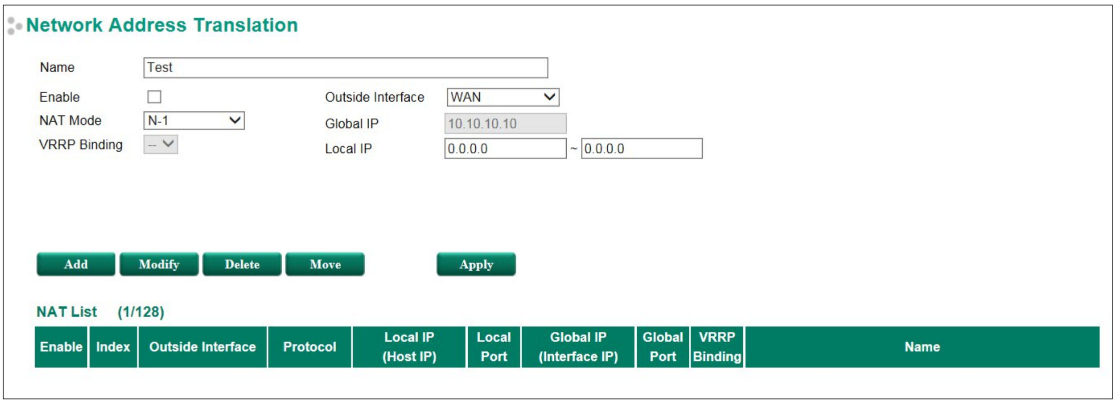
For some applications, devices need to talk to both internal devices and external devices without using a gateway. Bidirectional 1-to-1 NAT can do Network Address Translation in both directions without a gateway.

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.



Network Address Translation

Name	Test		
Enable	□	Outside Interface	WAN
NAT Mode	N-1	Global IP	10.10.10.10
VRRP Binding	--	Local IP	0.0.0.0 ~ 0.0.0.0

NAT List (1/128)

Enable	Index	Outside Interface	Protocol	Local IP (Host IP)	Local Port	Global IP (Interface IP)	Global Port	VRRP Binding	Name

Enable/Disable NAT Policy

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

NAT Mode

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

Interface (N-1 mode)

Setting	Description	Factory Default
WAN, LAN, BRG_LAN, Auto, WAN1, WAN2, LAN	In the EDR-810, select WAN/LAN/BRG_LAN interface for NAT rule. In the EDR-G903, select Auto/WAN1/WAN2/LAN interface for NAT rule. In the EDR-G902, select Auto/WAN/LAN interface for NAT rule. When Auto is selected, the G902 will check if the WAN interface can route the packet with NAT.	Auto(for, EDR-902 & EDR-G903), WAN (for EDR-810)

The Industrial Secure Router provides a Dual WAN backup function for network redundancy. If the interface is set to Auto, the NAT Mode is set to N-1, and the WAN backup function is enabled, the primary WAN interface is WAN1. If the WAN1 connection fails, the WAN interface of this N-1 policy will apply to WAN2 and switch to WAN2 for N-1 outgoing traffic until the WAN1 interface recovers.

IP Range

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

WAN IP (N-1 mode)

Setting	Description	Factory Default
IP address	The IP address of the user selected interface (WAN1, WAN2, and Auto) in this N-to-1 policy.	None

Add a NAT Rule

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

Delete a NAT Rule

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

Modify a NAT Rule

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

Activate NAT List Table

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

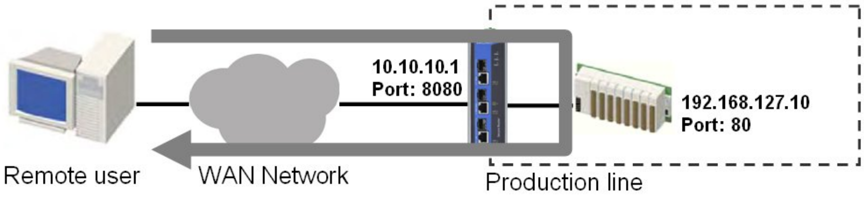
NOTE The Industrial Secure Router will add an N-1 policy from the source IP, 192.168.127.1 to 192.168.127.252 to the WAN1 interface after activating the Factory Default.

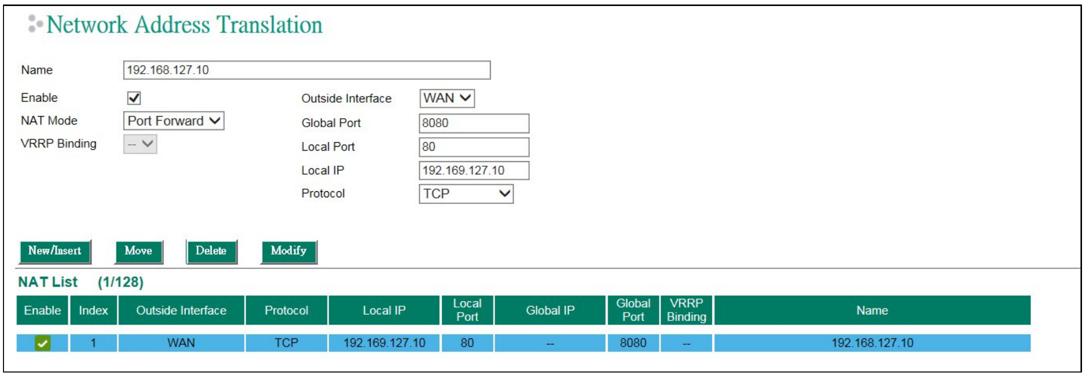
Port Forward

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.




Network Address Translation

Name	192.168.127.10		
Enable	☑	Outside Interface	WAN
NAT Mode	Port Forward	Global Port	8080
VRRP Binding	--	Local Port	80
		Local IP	192.169.127.10
		Protocol	TCP

NAT List (1/128)

Enable	Index	Outside Interface	Protocol	Local IP	Local Port	Global IP	Global Port	VRRP Binding	Name
✓	1	WAN	TCP	192.169.127.10	80	--	8080	--	192.168.127.10

Enable/Disable NAT policy

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

NAT Mode

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

Interface (Port Forward mode)

Setting	Description	Factory Default
WAN, LAN, BRG_LAN, Auto, WAN1, WAN2, LAN	Select the Interface for this NAT Policy	WAN (for EDR-902), WAN1 (for EDR-G903), WAN (for EDR-810)

Protocol (Port Forward mode)

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

WAN Port (Port Forward mode)

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

LAN/DMZ IP (Port Forward mode)

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

LAN/DMZ Port (Port Forward mode)

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

8

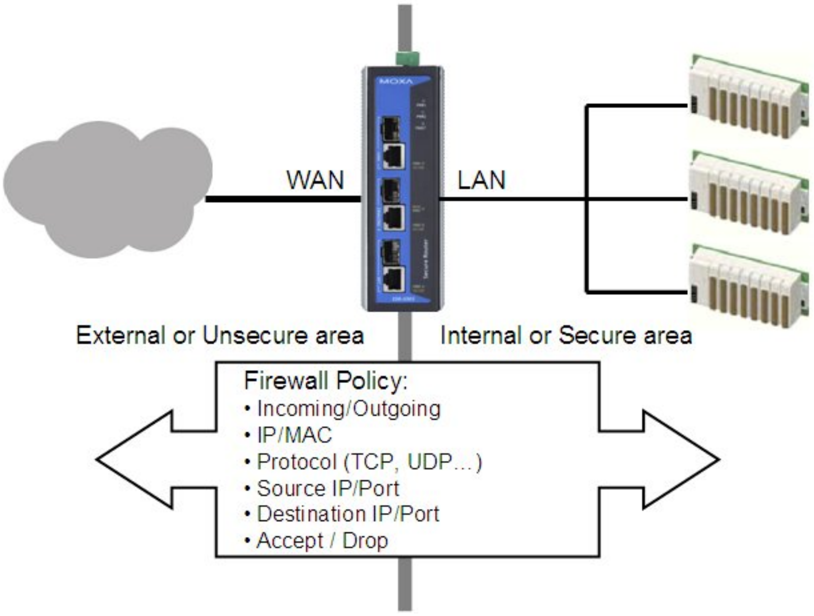
Firewall

The following topics are covered in this chapter:

- ❒ **Policy Concept**
- ❒ **Policy Overview**
- ❒ **Firewall**
  - ➢ Layer 2 policy
  - ➢ Layer 2 Policy Setup (Only in Bridge Mode for EDR-G902/G903)
  - ➢ Layer 3 policy
  - ➢ Quick Automation Profile
  - ➢ Policy Check
- ❒ **Modbus TCP Policy**
- ❒ **Denial of Service (DoS) Defense**
- ❒ **Firewall Event Log**

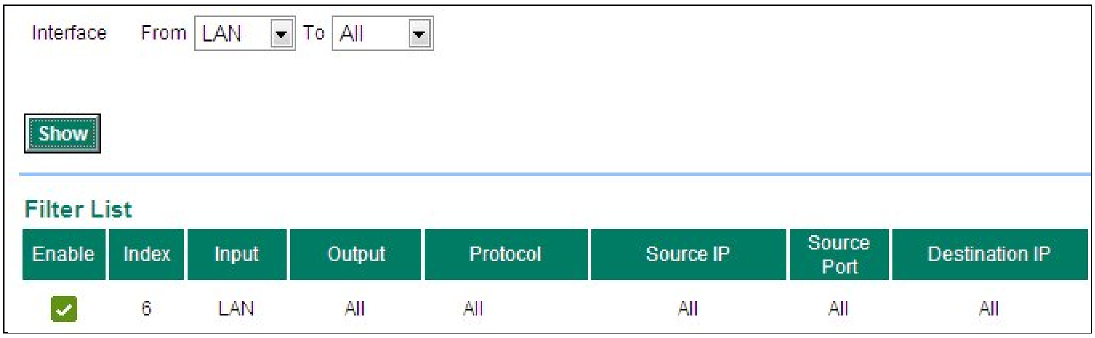
Policy Concept

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.



Interface From LAN To All

Filter List

Enable	Index	Input	Output	Protocol	Source IP	Source Port	Destination IP
✓	6	LAN	All	All	All	All	All

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.

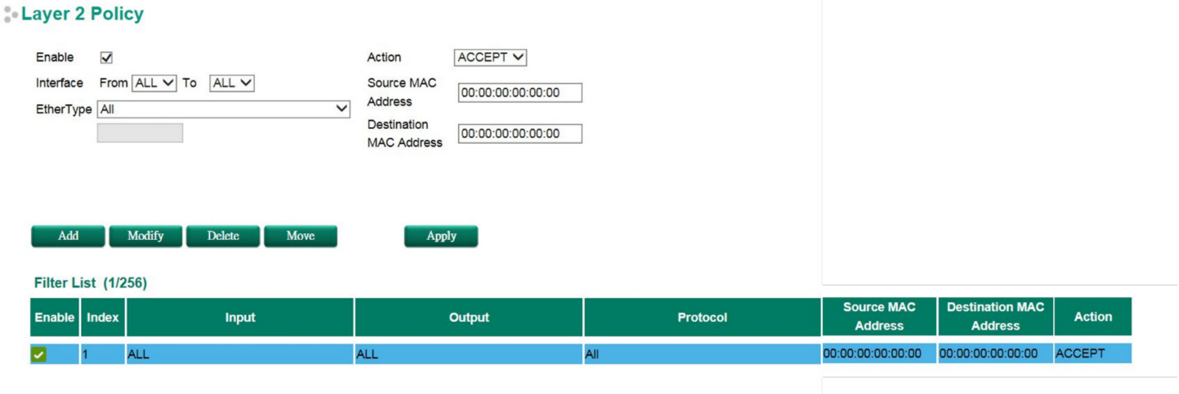
Interface From/To

Setting	Description	Factory Default
All (WAN1/WAN2/LAN)	Select the From Interface and To interface	From All to All
WAN1		
WAN2		
LAN		

Firewall

Layer 2 policy

EDR-810 and EDR-G902/903 (in Bridge Mode (referring to section of Mode Configuration in Network) provide 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.



Layer 2 Policy

Enable ☑

Interface From ALL To ALL

EtherType All

Action ACCEPT

Source MAC Address 00:00:00:00:00:00

Destination MAC Address 00:00:00:00:00:00

Filter List (1/256)

Enable	Index	Input	Output	Protocol	Source MAC Address	Destination MAC Address	Action
✓	1	ALL	ALL	All	00:00:00:00:00:00	00:00:00:00:00:00	ACCEPT

Interface From/To

Setting	Description	Factory Default
All (WAN1/WAN2/LAN)	Select the From Interface and To interface	None
WAN1		None
WAN2		None
LAN		None

Protocol

Setting	Description	Factory Default
Refer to table "EtherType for Layer 2 Protocol" for a more detailed description	Select the Layer 2 Protocol in this Firewall Policy	None

EtherType

Setting	Description	Factory Default
0x0600 to 0xFFFF	When Protocol is set to "Manual" you can set up EtherType manually	None

Target

Setting	Description	Factory Default
Accept	The packet will pass the Firewall when it matches the policy	None
Drop	The packet will not pass the Firewall when it matches this Firewall policy	None

Source MAC Address

Setting	Description	Factory Default
Mac Address	This Firewall Policy will check all Source MAC addresses of the packet	00:00:00:00:00:00

Destination MAC Address

Setting	Description	Factory Default
Mac Address	This Firewall Policy will check all 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 2 Policy Setup (Only in Bridge Mode for EDR-G902/G903)

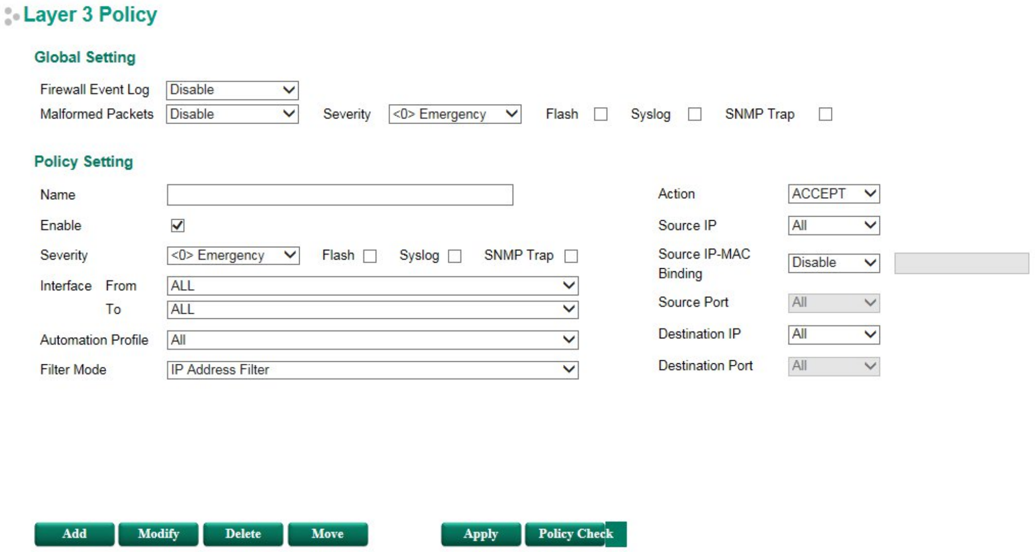
When the Industrial Secure Router is in Bridge Mode (referring to section of Mode Configuration in Network Settings), it provides an advanced Layer 2 firewall policy for secure traffic control, which depends on the following parameters:

EtherType

Setting	Description	Factory Default
0x0600 to 0xFFFF	When Protocol is set to “Manual” you can set up EtherType manually	None

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.



Layer 3 Policy

Global Setting

Firewall Event Log: Disable

Malformed Packets: Disable Severity: <0> Emergency Flash □ Syslog □ SNMP Trap □

Policy Setting

Name:

Enable: ☑

Severity: <0> Emergency Flash □ Syslog □ SNMP Trap □

Interface From: ALL

To: ALL

Automation Profile: All

Filter Mode: IP Address Filter

Action: ACCEPT

Source IP: All

Source IP-MAC Binding: Disable

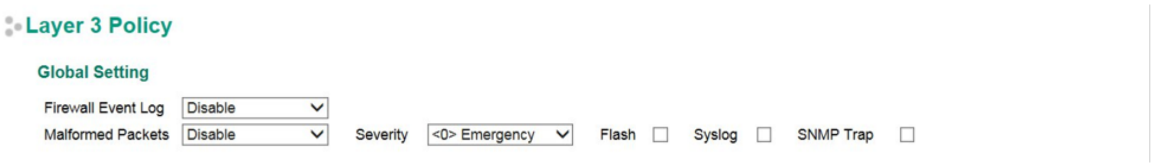
Source Port: All

Destination IP: All

Destination Port: All

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.



Layer 3 Policy

Global Setting

Firewall Event Log: Disable

Malformed Packets: Disable Severity: <0> Emergency Flash □ Syslog □ SNMP Trap □

Enable Logging Firewall Events

To enable the function logging events including malformed packet drop and firewall white/black rules, select the Enable option in Firewall Event Log. For firewall white/black rules event logs, users can select where to store this log in "Policy Setting".

Enable Malformed Packets

To enable the function logging dropping malformed packet and storing it in flash or send out syslog/ SNMP trap. User can set severity of the event.

Policy Setting

Name

Give a name for each firewall rule

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	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 (WAN1/WAN2/LAN)	Select the From Interface and To interface	From All to All
WAN1		
WAN2		
LAN		

Automation Profile

Setting	Description	Factory Default
Refer to the "Quick Automation Profile" section.	Select the Protocol parameters in this Firewall Policy	None

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	Accept
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 MAC

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

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	

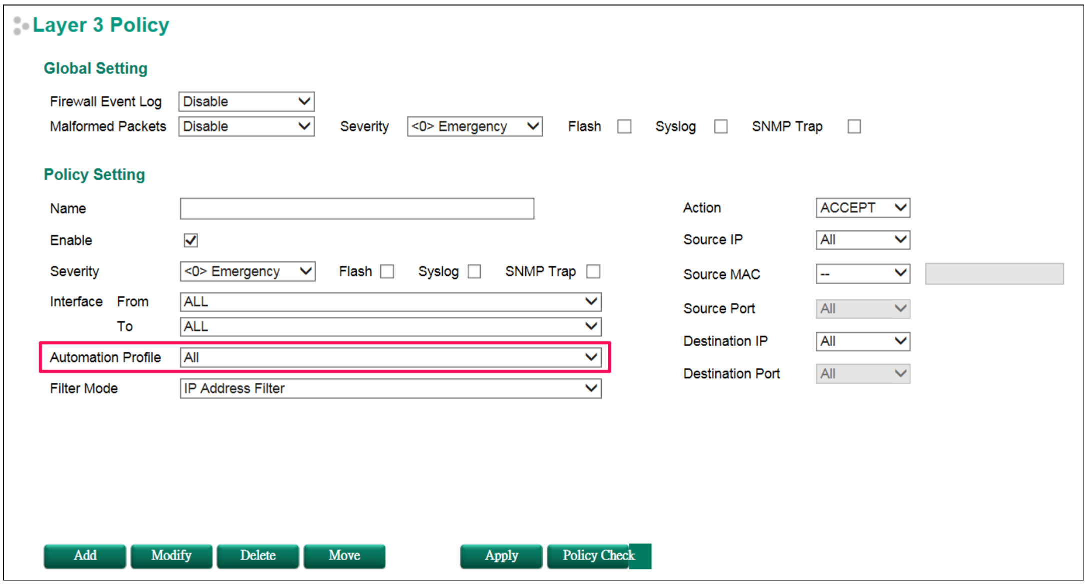
NOTE The Industrial Secure Router’s firewall function will check if incoming or outgoing packets match the firewall policy. It starts by checking the packet with the first policy (Index=1); if the packet matches this policy, it will accept the packet immediately and then check the next packet. If the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

NOTE The maximum number of Firewall policies for the EDR-810 and EDR-G902 is 256, and for EDR-G903 is 512.

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.



Layer 3 Policy

Global Setting

Firewall Event Log: Disable

Malformed Packets: Disable   Severity: <0> Emergency   Flash □   Syslog □   SNMP Trap □

Policy Setting

Name:

Enable ☑

Severity: <0> Emergency   Flash □   Syslog □   SNMP Trap □

Interface From: ALL

To: ALL

Automation Profile: All

Filter Mode: IP Address Filter

Action: ACCEPT

Source IP: All

Source MAC: --

Source Port: All

Destination IP: All

Destination Port: All

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

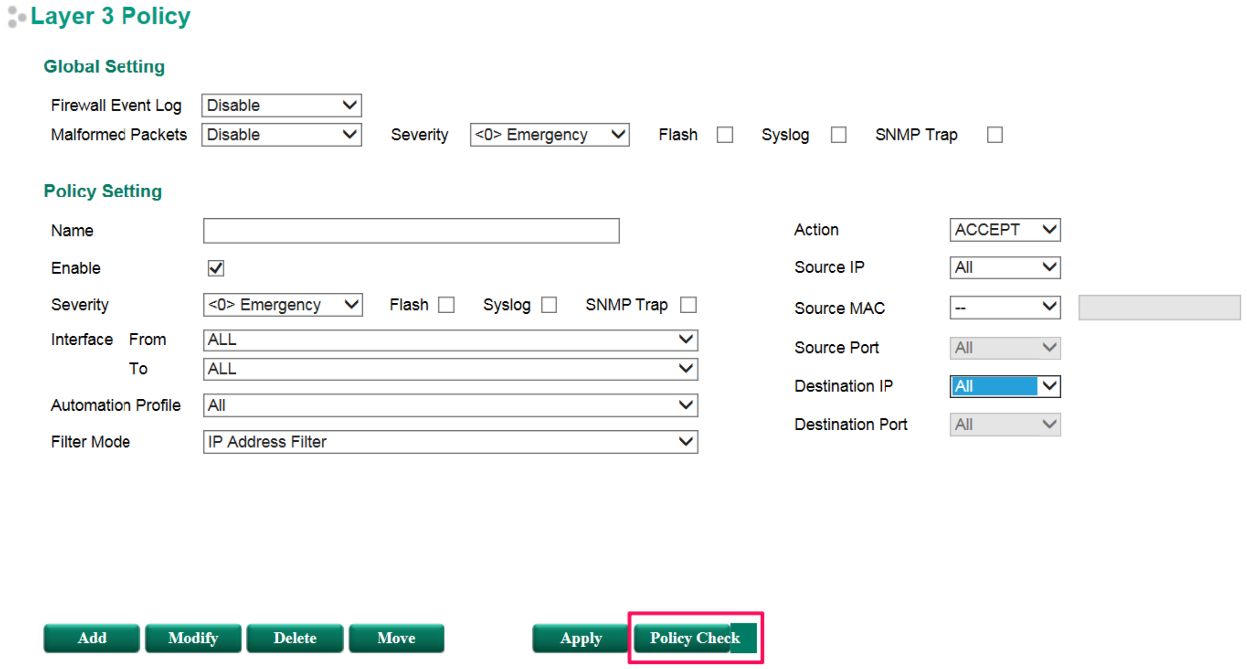
Ethernet Fieldbus Protocol	Port Number
EtherCat port (TCP)	34980
EtherCat port (UDP)	34980
EtherNet/IP I/O (TCP)	2222
EtherNet/IP I/O (UDP)	2222
EtherNet/IP Messaging (TCP)	44818
EtherNet/IP Messaging (UDP)	44818
FF Annunciation (TCP)	1089
FF Annunciation (UDP)	1089
FF Fieldbus Message (TCP)	1090
FF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



Layer 3 Policy

Global Setting

Firewall Event Log: Disable

Malformed Packets: Disable   Severity: <0> Emergency   Flash □   Syslog □   SNMP Trap □

Policy Setting

Name:

Enable: ☑

Severity: <0> Emergency   Flash □   Syslog □   SNMP Trap □

Interface From: ALL

To: ALL

Automation Profile: All

Filter Mode: IP Address Filter

Action: ACCEPT

Source IP: All

Source MAC: --

Source Port: All

Destination IP: All

Destination Port: All

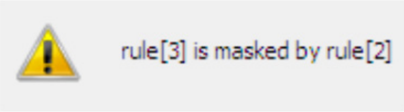
The Industrial Secure Router supports a **PolicyCheck** function for maintaining the firewall policy list. The **PolicyCheck** function detects firewall policies that may be configured incorrectly. **PolicyCheck** provides an auto detection function for detecting common configuration errors in the Firewall 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.



rule[3] is masked by rule[2]

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

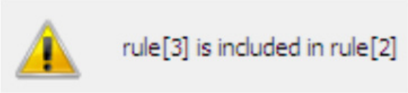
The Source/Destination IP range or Source/Destination port number of policy [X] is less than or equal to policy [Y], and the action target (Accept/Drop) is the same. In this case policy [X] will increase the loading of the Industrial Secure Router and lower its performance. For example, two firewall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


rule[3] is included in rule[2]

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

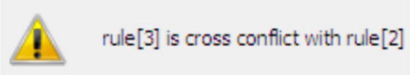
Two firewall policy configurations, such as Source IP, Destination IP, Source port, and Destination port, in policy [X] and policy [Y] are masked, and the action target (Accept/Drop) is different. For example, two firewall policies are shown in the following table:

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].


rule[3] is cross conflict with rule[2]

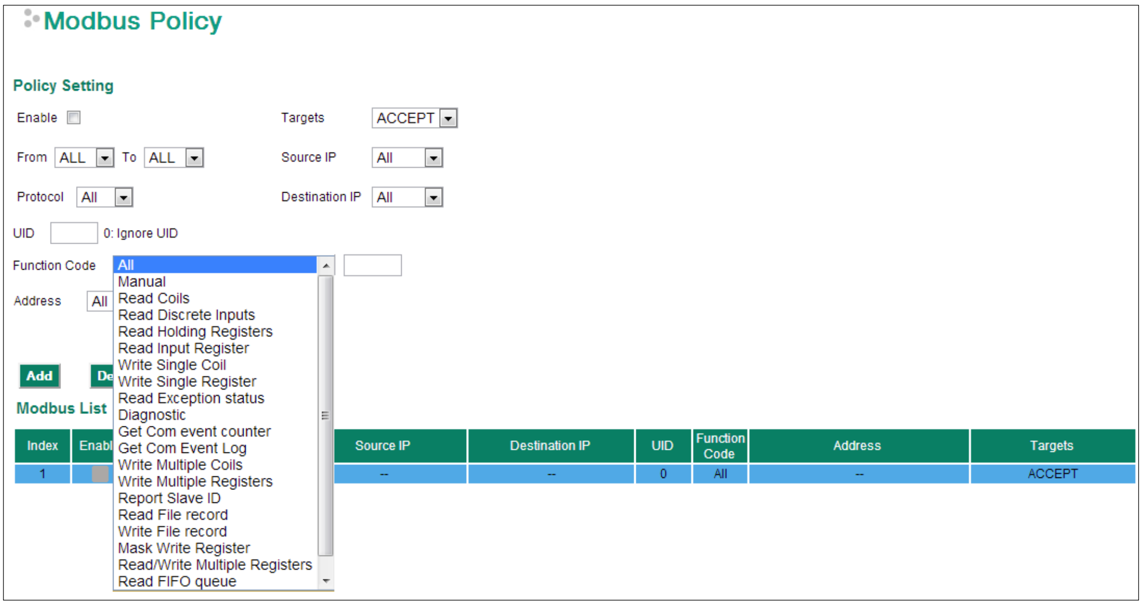
Modbus TCP Policy

Modbus TCP is a Modbus protocol used for communications over TCP/IP networks, connecting over port 502 by default. Some have experimented with using Modbus over UDP on IP networks, which removes the overheads required for TCP. The following table shows the Modbus TCP frame format:

Modbus TCP Frame Format		
Description	**Length**	**Function**
Transaction Identifier	2 bytes	Synchronization between messages of server & client
Protocol Identifier	2 bytes	The value is 0 for Modbus TCP protocol
Length Field	2 bytes	Number of remaining following bytes in this frame
Unit Identifier	1 byte	Slave Address (255 is used for device broadcast information)
Function code	1 byte	Define message type
Data bytes	n bytes	Data block with additional information

Modbus Policy Setup

The Industrial Secure Router provides Modbus policy inspection of Modbus TCP packets, which allows users to control Modbus TCP traffic based on the following parameters:



Modbus Policy

Policy Setting

Enable □

Targets ACCEPT

From ALL To ALL

Source IP All

Protocol All

Destination IP All

UID 0: Ignore UID

Function Code All

Address All

Modbus List

Index	Enabl	Source IP	Destination IP	UID	Function Code	Address	Targets
1		--	--	0	All	--	ACCEPT

Add a Modbus TCP Filtering Rule

Check the "Enable" checkbox and input the correspondent Modbus TCP parameters in the page, and then click "Add" to add it into the Modbus Filtering Table. Finally, click "Activate" to activate the configuration.

Delete a Modbus TCP Filtering Rule

Select the item in the Modbus Filtering Table, then, click "Delete" to delete the item.

Modify a Modbus TCP Filtering Rule

Select the item in the Modbus Filtering Table. Modify the attributes and click "Modify" to change the configuration.

Activate Modbus TCP Filtering Table

After adding/deleting/modifying any Modbus TCP Filtering Rules, make sure to click "Activate" to activate the item.

Enable/Disable Modbus Policy

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

Interface From/To

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

Protocol

Setting	**Description**	**Factory Default**
All (TCP/UDP)	This Modbus Policy will check the UDP packet, TCP packet or both.	All
TCP		
UDP		

UID

Setting	**Description**	**Factory Default**
1 to 255	Unit Identifier, 0 indicate this Modbus policy will check all UIDs in the packet.	0

Function Code

Setting	**Description**	**Factory Default**
Refer to the “Common function codes” section on page 3-52.	Select the function code parameters in this Modbus policy. When the function code is set to “Manual” you can set up the function code manually.	All

Address

Setting	**Description**	**Factory Default**
All (Address Index)	This Modbus policy will check all Data Address Index in the packet.	All
Single (Address Index)	This Modbus policy will check single Data Address Index in the packet.	
Range (Address Index)	This Modbus policy will check multiple Data Address Indexes in the packet.	

Target

Setting	**Description**	**Factory Default**
Accept	The packet will penetrate the firewall when it matches this Modbus policy.	Accept
Drop	The packet will not penetrate the firewall when it matches this Modbus policy.	

Source IP

Setting	**Description**	**Factory Default**
All (IP Address)	This Modbus policy will check all Source IP addresses in the packet.	All
Single (IP Address)	This Modbus policy will check single Source IP addresses in the packet.	
Range (IP Address)	This Modbus policy will check multiple Source IP addresses in the packet.	

Destination IP

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

Unit identifier (UID) is used with Modbus/TCP devices that are composites of several Modbus devices. It may be used to communicate via devices such as bridges and gateways which use a single IP address to support multiple independent end units.

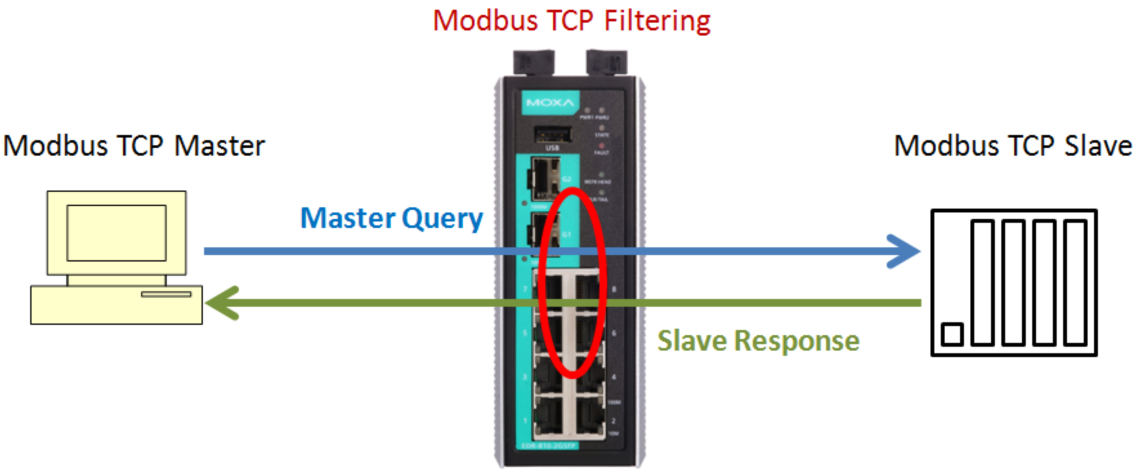
Function code defines the message type and the type of action required by the slave. The parameter contains one byte of information. Valid function codes are in the range 1 to 255. Not all Modbus devices recognize the same set of function codes. The most common codes are supported for quick settings, and user-defined function codes are also supported.

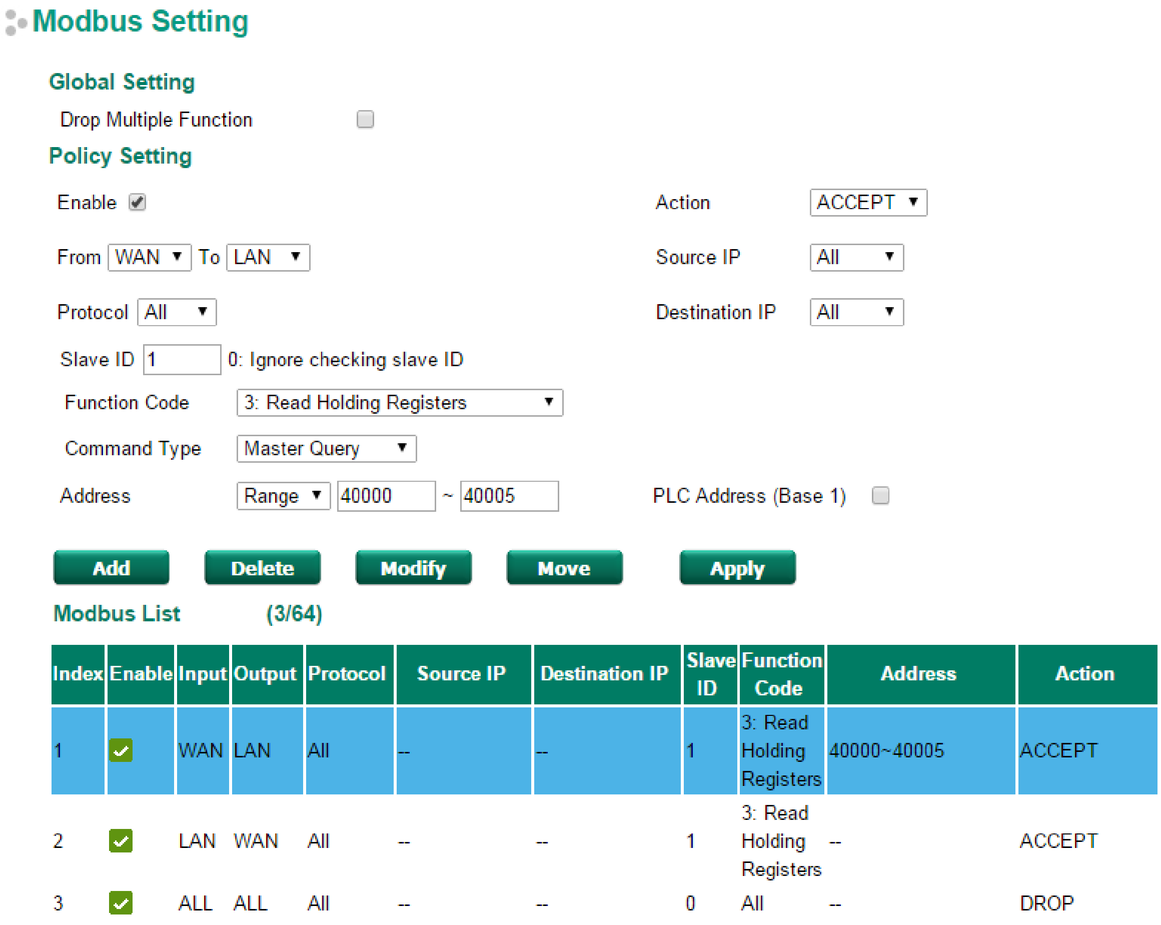
Most function code addresses a single address or a range of addresses. The Industrial Secure Router provides code for deep data inspection.

Common function codes

The following table shows the various reading, writing, and other operations.

			Function Name	Function Code
Data Access	Bit Access	Physical Discrete Inputs	Read Discrete Inputs	2
		Internal Bits or Physical Coils	Read Coils	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bit Access	Physical Input Registers	Read Input Register	4
		Internal Registers or Physical Output Registers	Read Holding Registers	3
			Write Single Register	6
			Write Multiple Registers	16
			Read/Write Multiple Registers	23
			Mask Write Register	22
			Read FIFO Queue	24
	File Record Access		Read File Record	20
			Write File Record	21
Diagnostics			Read Exception Status	7
			Diagnostic	8
			Get Com Event Counter	11
			Get Com Event Log	12
			Report Slave ID	17
			Read Device Identification	43





Modbus Setting

Global Setting

Drop Multiple Function □

Policy Setting

Enable	☑	Action	ACCEPT
From	WAN To LAN	Source IP	All
Protocol	All	Destination IP	All
Slave ID	1 0: Ignore checking slave ID		
Function Code	3: Read Holding Registers		
Command Type	Master Query		
Address	Range 40000 ~ 40005	PLC Address (Base 1)	□

Modbus List (3/64)

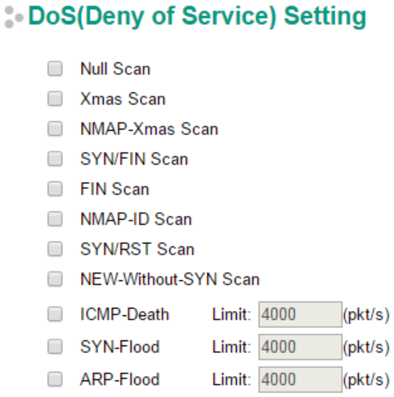
Index	Enable	Input	Output	Protocol	Source IP	Destination IP	Slave ID	Function Code	Address	Action
1	✓	WAN	LAN	All	--	--	1	3: Read Holding Registers	40000~40005	ACCEPT
2	✓	LAN	WAN	All	--	--	1	3: Read Holding Registers	--	ACCEPT
3	✓	ALL	ALL	All	--	--	0	All	--	DROP

Modbus TCP Filtering controls both directions of communication between Modbus Master and Modbus Slave. Users need to set up two rules for the data transaction between Master and Slave. One rule is to accept the Master commands and another rule is to accept the Slave response.

NOTE The main Firewall Policy rules are the first tier of filtering in the Network Layer, and the Modbus Filtering rules are the second tier of filtering in both the Network Layer and Application Layer.

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.



DoS(Deny of Service) Setting

□ Null Scan
□ Xmas Scan
□ NMAP-Xmas Scan
□ SYN/FIN Scan
□ FIN Scan
□ NMAP-ID Scan
□ SYN/RST Scan
□ NEW-Without-SYN Scan
□ ICMP-Death Limit: 4000 (pkt/s)
□ SYN-Flood Limit: 4000 (pkt/s)
□ ARP-Flood Limit: 4000 (pkt/s)

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

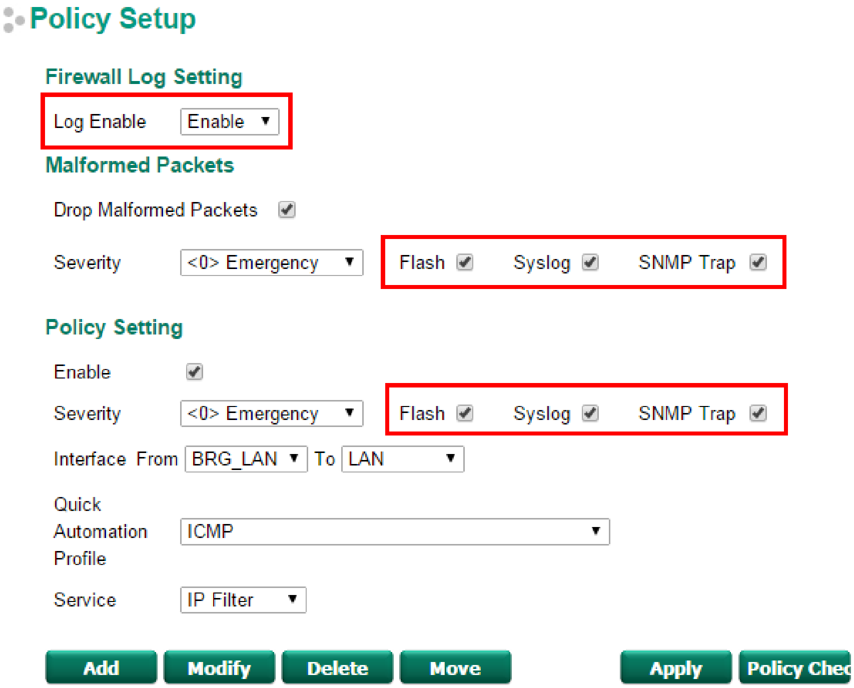
Setting	Description	Factory Default
Enable or Disable	Enable or disable the Null Scan function	None
Limit (Packets/Second)	The limit value to activate SYN-Flood defense	None

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	

Firewall Event Log

The 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.



Policy Setup

Firewall Log Setting

Log Enable: Enable

Malformed Packets

Drop Malformed Packets ☑

Severity: <0> Emergency Flash ☑ Syslog ☑ SNMP Trap ☑

Policy Setting

Enable ☑

Severity: <0> Emergency Flash ☑ Syslog ☑ SNMP Trap ☑

Interface From: BRG_LAN To: LAN

Quick Automation Profile: ICMP

Service: IP Filter

Action: DROP

Source IP: All

Source Port: All

Destination IP: All

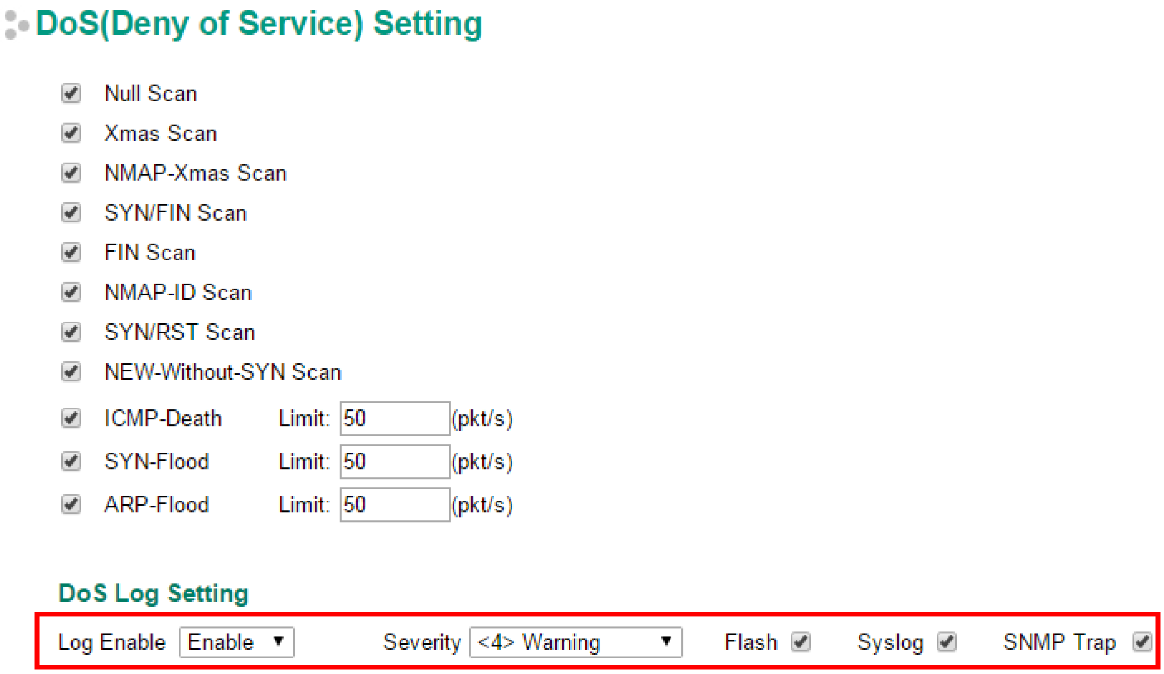
Destination Port: All

Enable Logging Firewall Events

To enable the overall event log function, select the **Enable** option in **Log Enable**.

Enable Firewall Rule Event log

To enable the specific firewall event log, click **Flash**, **Syslog**, or **SNMP Trap**. You may also define the severity of the firewall rule and record it in the event.



DoS(Deny of Service) Setting

☑ Null Scan

☑ Xmas Scan

☑ NMAP-Xmas Scan

☑ SYN/FIN Scan

☑ FIN Scan

☑ NMAP-ID Scan

☑ SYN/RST Scan

☑ NEW-Without-SYN Scan

☑ ICMP-Death Limit: 50 (pkt/s)

☑ SYN-Flood Limit: 50 (pkt/s)

☑ ARP-Flood Limit: 50 (pkt/s)

DoS Log Setting

Log Enable: Enable ▼ Severity: <4> Warning ▼ Flash ☑ Syslog ☑ SNMP Trap ☑

Enable Logging DoS Events

To enable the DoS 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 DoS types and record it in the event.

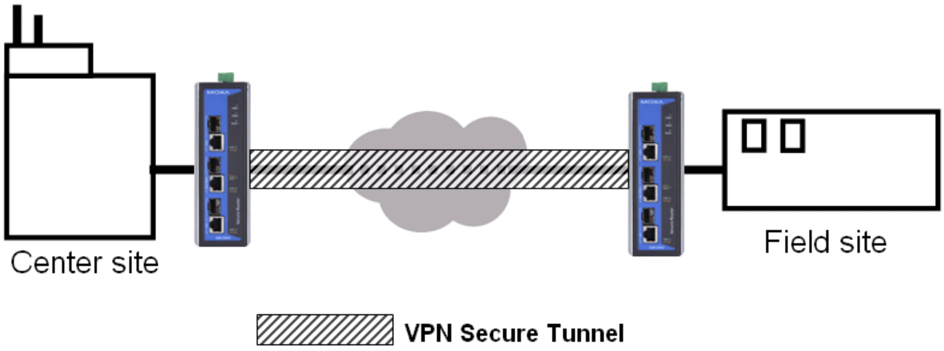
9

Virtual Private Network (VPN)

The following topics are covered in this chapter:

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 three 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.

OpenVPN (Open Source VPN) for Mobile Device User: Using OpenSSL encryption, OpenVPN can provide secure data communication. Download the free OpenVPN app on a mobile device and this app allows the user to create a VPN connection between the server and a mobile device.

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.

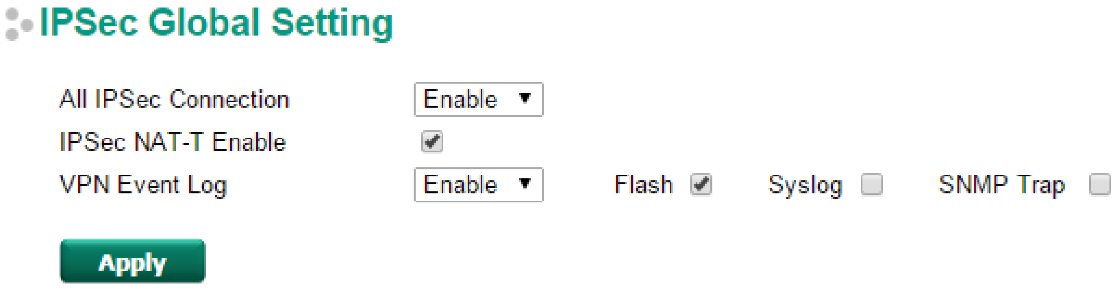
Data Exchange (IPsec Phase 2): In Phase 2, the VPN gateways negotiate to determine additional IPsec connection details, which include the data encryption algorithm.

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



IPSec Global Setting

All IPSec Connection: Enable ▼

IPSec NAT-T Enable: ☑

VPN Event Log: Enable ▼ Flash ☑ Syslog □ SNMP Trap □

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.

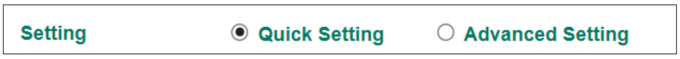
VPN Event Log

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.



Setting ● Quick Setting ○ Advanced Setting

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

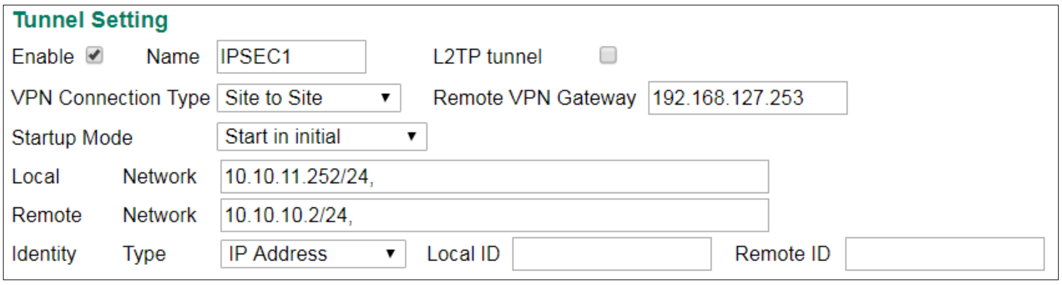
NOTE The Encryption strength and Pre-Shared key should be configured identically for both Industrial Secure Router units.

IPsec Advanced Setting

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

Setting ● Advanced Setting

Tunnel Setting



Tunnel Setting

Enable ☑ Name IPSEC1 L2TP tunnel □

VPN Connection Type Site to Site ▼ Remote VPN Gateway 192.168.127.253

Startup Mode Start in initial ▼

Local Network 10.10.11.252/24,

Remote Network 10.10.10.2/24,

Identity Type IP Address ▼ Local ID Remote ID

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	None

Connection Interface

Setting	Description	Factory Default
WAN1 WAN2 Default Route	The interface of the VPN Tunnel If the user enables the WAN backup function, WAN1 would be the primary default route and WAN2 would be the backup route.	WAN1

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.	192.168.127.254/24

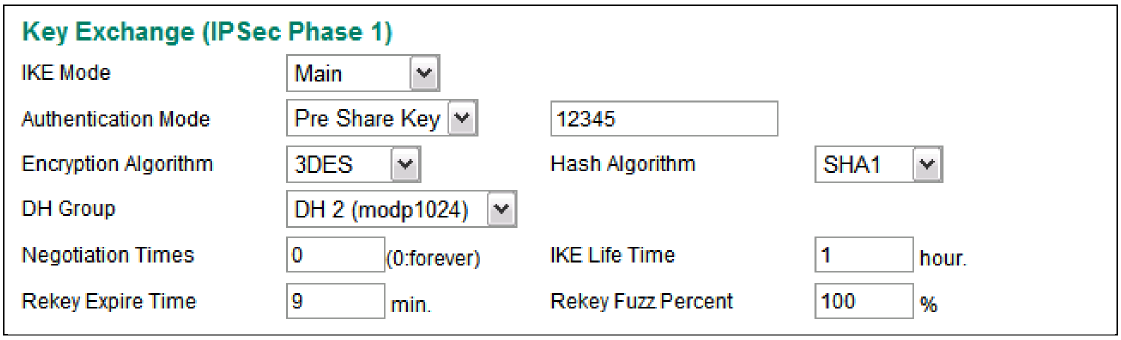
Remote Network

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.	N/A

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.	IP address
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)



Key Exchange (IPSec Phase 1)

IKE Mode	Main		
Authentication Mode	Pre Share Key	12345	
Encryption Algorithm	3DES	Hash Algorithm	SHA1
DH Group	DH 2 (modp1024)		
Negotiation Times	0 (0:forever)	IKE Life Time	1 hour.
Rekey Expire Time	9 min.	Rekey Fuzz Percent	100 %

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.	

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

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	3DES

Hash Algorithm

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

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 1024)

Negotiation Time

Setting	Description	Factory Default
Negotiation time	The number of allowed reconnect times when startup mode is initiated. If the number is 0, this tunnel will always try connecting to the remote gateway when the VPN tunnel is not created successfully.	0

IKE Lifetime

Setting	Description	Factory Default
IKE lifetime (hours)	Lifetime for IKE SA	1 (hr)

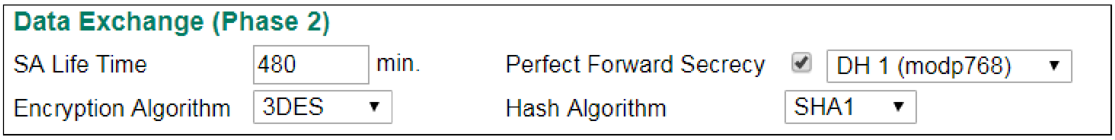
Rekey Expire Time

Setting	Description	Factory Default
Rekey expire time (minutes)	Start to Rekey before the IKE lifetime has expired	9 (min)

Rekey Fuzz Percent

Setting	Description	Factory Default
0-100 (%)	The key exchange interval will change randomly to enhance security. "Rekey Expire Time" is the baseline interval to exchange keys. Rekey fuzz percent represents the percentage of how much "Rekey Expire Time" will change. For example, the "Rekey Expire Time" is set as 9 mins, and "Rekey Fuzz Percent" is set as 50%. The key exchange interval will be 4.5 mins.	100%

Data Exchange (IPsec phase II)



Data Exchange (Phase 2)

SA Life Time 480 min.

Perfect Forward Secrecy ☑ DH 1 (modp768)

Encryption Algorithm 3DES

Hash Algorithm SHA1

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 (modp768)

SA Lifetime

Setting	Description	Factory Default
SA lifetime (minutes)	Lifetime for SA in Phase 2	480 (min)

Encryption Algorithm

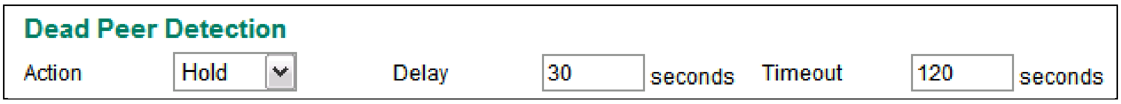
Setting	Description	Factory Default
DES 3DES AES-128 AES-192 AES-256	Encryption Algorithm in data exchange	3DES

Hash Algorithm

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

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.



Dead Peer Detection

Action: Hold

Delay: 30 seconds

Timeout: 120 seconds

Action

Action when a dead peer is detected.

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

Delay

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

Timeout

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

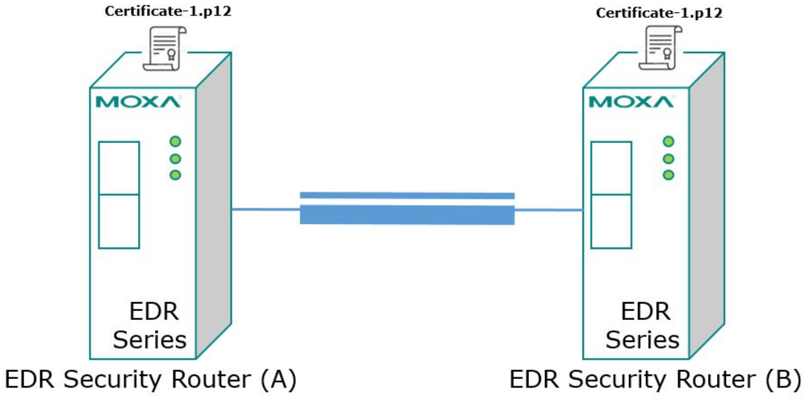
IPsec Use Case Demonstration

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.



EDR Security Router (A)

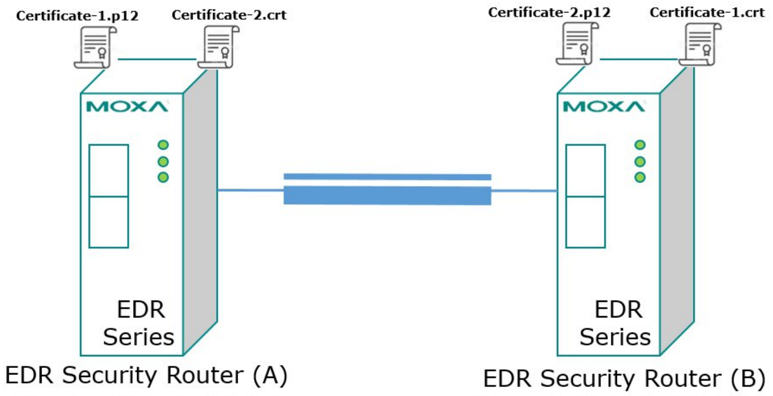
1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Enter "IPSec setting", and in "Advanced Setting", select X.509 authentication mode.
3. In "Local", select No.1
4. In "Remote", select No.1

EDR Security Router (B)

1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Enter "IPSec setting", and in "Advanced Setting", select X.509 authentication mode.
3. In "Local", select No.1
4. In "Remote", select No.1

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.



EDR Security Router (A)

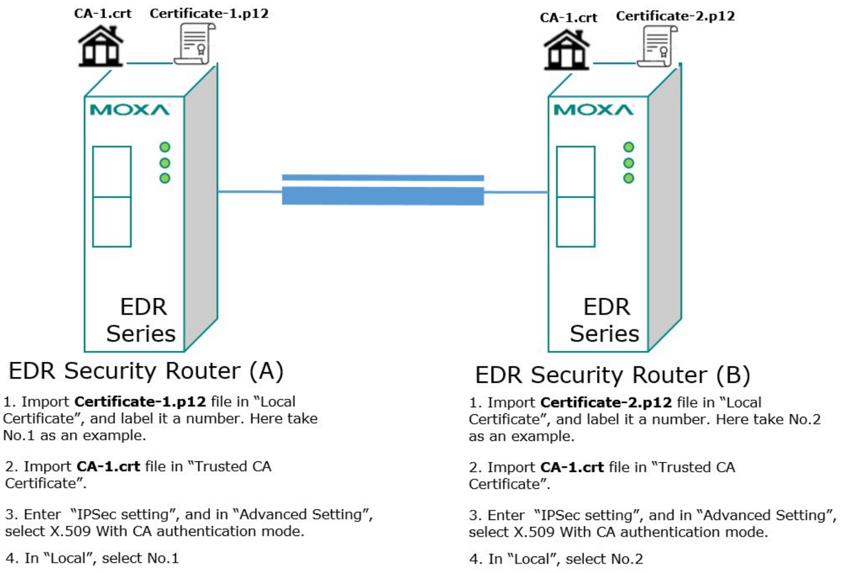
1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Import **Certificate-2.crt** file or **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.
3. Enter "IPSec setting", and in "Advanced Setting", select X.509 authentication mode.
4. In "Local", select No.1
5. In "Remote", select No.2

EDR Security Router (B)

1. Import **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Import **Certificate-1.crt** file or **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.
3. Enter "IPSec setting", and in "Advanced Setting", select X.509 authentication mode.
4. In "Local", select No.2
5. In "Remote", select No.1

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.



EDR Security Router (A)

1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.

2. Import **CA-1.crt** file in "Trusted CA Certificate".

3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

4. In "Local", select No.1

EDR Security Router (B)

1. Import **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.

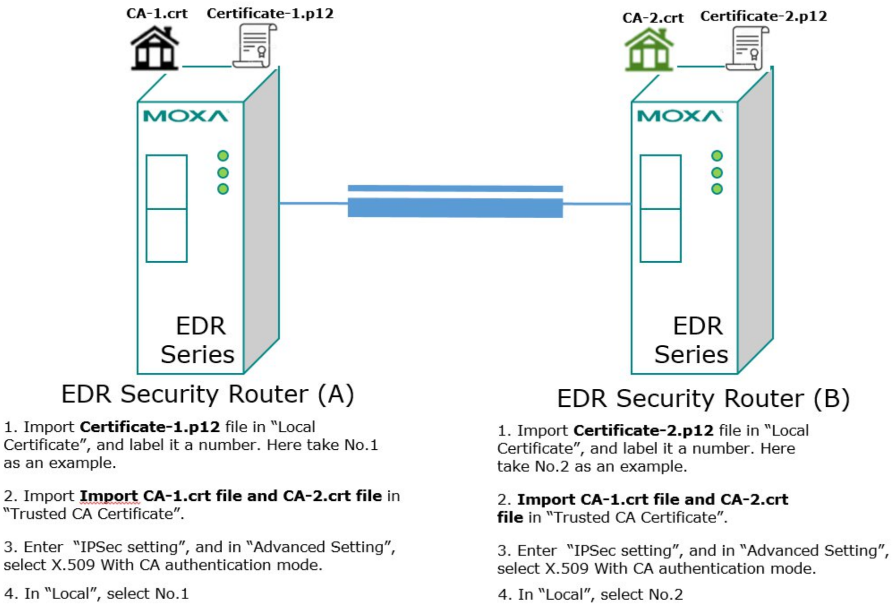
2. Import **CA-1.crt** file in "Trusted CA Certificate".

3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

4. In "Local", select No.2

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.



EDR Security Router (A)

1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.

2. Import **Import CA-1.crt file and CA-2.crt file** in "Trusted CA Certificate".

3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

4. In "Local", select No.1

EDR Security Router (B)

1. Import **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.

2. **Import CA-1.crt file and CA-2.crt file** in "Trusted CA Certificate".

3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

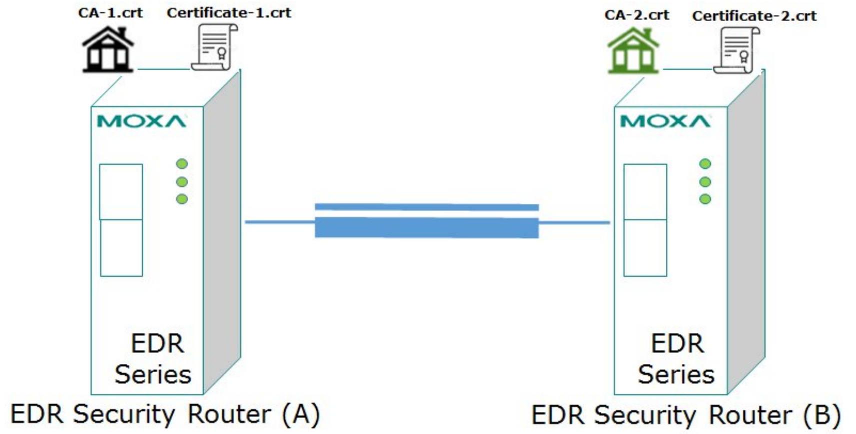
4. In "Local", select No.2

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.



EDR Security Router (A)

1. Generate Key in "Key Pair Generate", and give it a name. Here take One as an example.

2. Generate CSR in "CSR Generate". Select One in "Private Key". Name this CSR in "Common Name". Here name this CSR as Certificate-1 as an example.

3. Export **Certificate-1.csr** file and send it to CA-1.

4. Download **Certificate-1.crt** and **CA-1.crt** from CA-1.

5. Import **Certificate-1.crt** file in "Local Certificate. In "Import Identity Certificate" select "Certificate From CSR". In "CSR Common Name" select **Certificate-1.csr**.

6. Import **CA-2.crt** file in "Trusted CA Certificate.

7. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

8. In "Local", select No.1

EDR Security Router (B)

1. Generate Key in "Key Pair Generate", and give it a name. Here take Two as an example.

2. Generate CSR in "CSR Generate". Select Two in "Private Key". Name this CSR in "Common Name". Here name this CSR as Certificate-2 as an example.

3. Export **Certificate-2.csr** file and send it to CA-2.

4. Download **Certificate-2.crt** and **CA-2.crt** from CA-1.

5. Import **Certificate-2.crt** file in "Local Certificate. In "Import Identity Certificate" select "Certificate From CSR". In "CSR Common Name" select **Certificate-2.csr**.

6. Import **CA-1.crt** file in "Trusted CA Certificate.

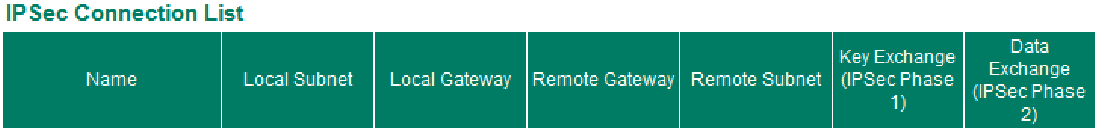
7. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

8. In "Local", select No.2

IPsec Status

The user can check the VPN tunnel status in the **IPsec Connection List**.

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



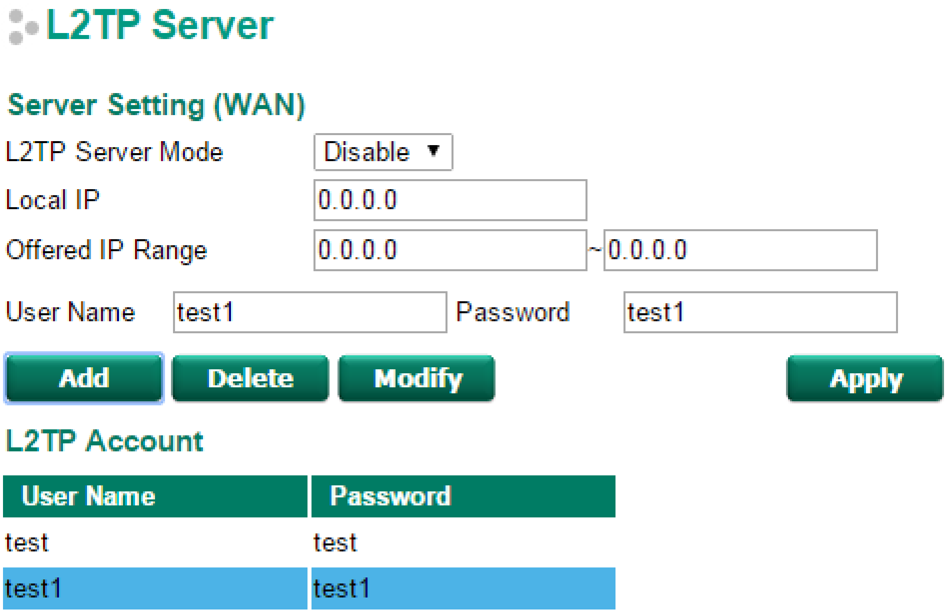
IPSec Connection List

Name	Local Subnet	Local Gateway	Remote Gateway	Remote Subnet	Key Exchange (IPSec Phase 1)	Data Exchange (IPSec Phase 2)

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



L2TP Server

Server Setting (WAN)

L2TP Server Mode: Disable
Local IP: 0.0.0.0
Offered IP Range: 0.0.0.0 ~ 0.0.0.0
User Name: test1 Password: test1

L2TP Account

User Name	Password
test	test
test1	test1

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	NULL

Login Password

Setting	Description	Factory Default
Max. 32 characters.	Password for L2TP connection	NULL

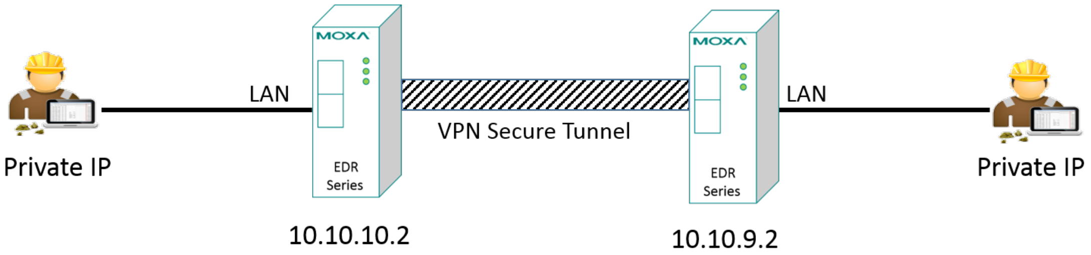
OpenVPN Configuration

Open VPN configuration contains two parts

- OpenVPN Server: Set up the VPN connection, VPN network plan, and user management
- OpenVPN Client: Set up the VPN connection and VPN network, e.g. server IP, and port number.

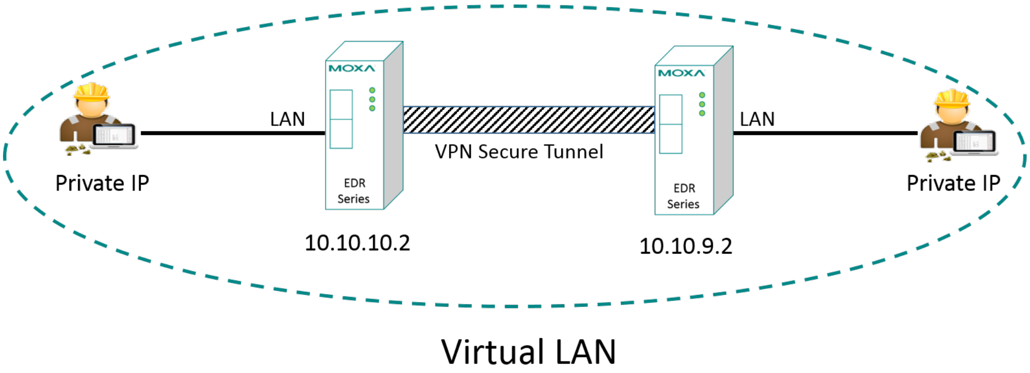
OpenVPN—Router Mode

Use the OpenVPN router mode to connect two sites that are under different subnets (Layer 3) and encrypt the TCP/UDP package data transmission. The OpenVPN router mode cannot process broadcast or multicast frames.



OpenVPN—Bridge Mode

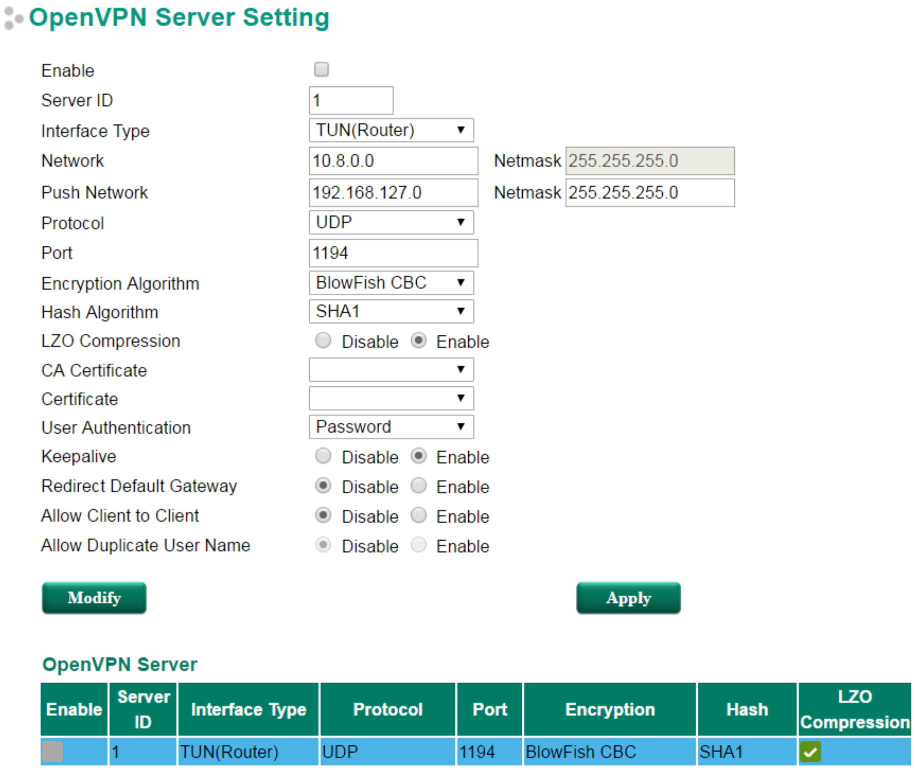
Use the OpenVPN bridge mode to have two locations using different subnets, but there appears to be only one subnet for encrypting IP packages during data transmission. In this mode, layer 2 broadcast packets can transmit between different subnets.



Server Settings

When the Industrial Secure Router is functioning as the OpenVPN Server, it can build connections with up to five different clients in either TUN mode or TAP mode.

Server Settings–TUN (Router Mode)



OpenVPN Server Setting

Enable	□		
Server ID	1		
Interface Type	TUN(Router)		
Network	10.8.0.0	Netmask	255.255.255.0
Push Network	192.168.127.0	Netmask	255.255.255.0
Protocol	UDP		
Port	1194		
Encryption Algorithm	BlowFish CBC		
Hash Algorithm	SHA1		
LZO Compression	○ Disable ● Enable		
CA Certificate			
Certificate			
User Authentication	Password		
Keepalive	○ Disable ● Enable		
Redirect Default Gateway	● Disable ○ Enable		
Allow Client to Client	● Disable ○ Enable		
Allow Duplicate User Name	● Disable ○ Enable		

OpenVPN Server

Enable	Server ID	Interface Type	Protocol	Port	Encryption	Hash	LZO Compression
□	1	TUN(Router)	UDP	1194	BlowFish CBC	SHA1	✓

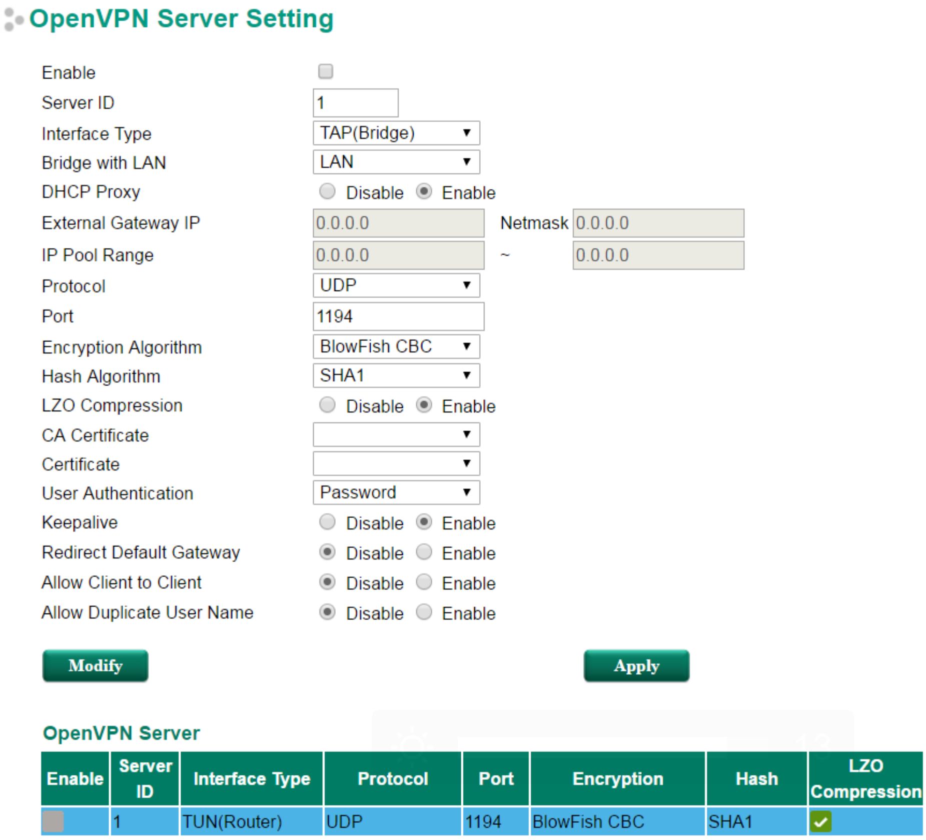
OpenVPN Server Setting-TUN

Setting	Description	Factory Default
Enable	Enable or disable the VPN tunnel.	Disable
Server ID	Indicate the server user set. The Industrial Secure Router only supports one server at a time.	1
Interface Type	Select the OpenVPN tunnel connection by using either router mode or bridge mode.	TUN (Router)
Network	This interface is a virtual interface for server internal usage. Via this interface, server can identify OpenVPN packet and process it. The default value is 10.8.0.0. Please make sure the system IP assignment does not conflict with this network interface.	10.8.0.0
Netmask	The subnet netmask of virtual network is set to 255.255.255.0	255.255.255.0
Push network IP	The client will send traffic to the Industrial Secure Router which will forward it to the Push network IP address. The destination of traffic from client is often the server's LAN network, so the default value is the server's LAN network.	192.168.127.0
Push netmask	Enter the netmask of the network behind the VPN server.	255.255.255.0
Protocol	Select the protocol to be used for the VPN.	UDP
Port	Enter the port number for the TCP/UDP connection.	1194

Encryption algorithm	Select the authentication mode for key exchange. The configuration fields vary depending on the authentication mode you select.	BlowFish CBC
Hash algorithm	Select the MD5, SHA-1, or SHA-256 VPN key exchange phase 1 hash mode.	SHA1
LZO compression	Compress tunnel packets using the LZO algorithm.	Enable
CA Certificate	Select the Certificate Authority (.crt) uploaded in 'Trusted CA Certificate'	N/A
Certificate	Select the certificate (.crt) uploaded in 'Local Certificate'	N/A
User authentication	Only password authentication is supported in server mode	Password
Keepalive	Check if the client connection is alive	Enable
Redirect to default gateway	Select Enable to force all clients' generated traffic to pass through the tunnel	Disable
Allow Client-to-client	Select Enable to allow communication between clients connected to the server. If this function is disabled, the clients will only be able to communicate with the server. For more details, please see the section 'Examples for Typical VAPN Applications'.	Disable

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.

Server Setting–TAP (Bridge Mode)



OpenVPN Server Setting

Enable	□
Server ID	1
Interface Type	TAP(Bridge)
Bridge with LAN	LAN
DHCP Proxy	○ Disable ● Enable
External Gateway IP	0.0.0.0 Netmask 0.0.0.0
IP Pool Range	0.0.0.0 ~ 0.0.0.0
Protocol	UDP
Port	1194
Encryption Algorithm	BlowFish CBC
Hash Algorithm	SHA1
LZO Compression	○ Disable ● Enable
CA Certificate	
Certificate	
User Authentication	Password
Keepalive	○ Disable ● Enable
Redirect Default Gateway	● Disable ○ Enable
Allow Client to Client	● Disable ○ Enable
Allow Duplicate User Name	● Disable ○ Enable

OpenVPN Server

Enable	Server ID	Interface Type	Protocol	Port	Encryption	Hash	LZO Compression
□	1	TUN(Router)	UDP	1194	BlowFish CBC	SHA1	✓

OpenVPN Server Settings-TAP

Setting	Description	Factory Default
Enable	Enable or disable the VPN tunnel.	Disable
Server ID	Indicates the server the user set. The industrial secure router only supports one server at a time	1
Interface Type	Select OpenVPN tunnel connection by router mode or bridge mode	TUN (Router)
Bridge with LAN	In TAP mode, select the LAN interface of the server that will connect with the client. Please refer to the Interface section for how to create different LAN interfaces	LAN
DHCP Proxy	Please refer to DHCP Proxy demonstration.	Enable
External Gateway IP	Enter in the LAN interface IP which is selected in Bridge with LAN. When OpenVPN server plays as DHCP server, the LAN interface of the server will be the default gateway of the client. And client's traffic will be route this LAN.	0.0.0.0
External Gateway Netmask	Enter in the LAN interface netmask which is selected in Bridge with LAN.	0.0.0.0
IP Pool Range	This is the network that will access the remote VPN server and the IP range that can be assigned (clients number) in this local network. The IP address entered here will be the start IP for the local network (client).	0.0.0.0
Protocol	Select the protocol to be used for VPN.	UDP
Port	Enter the port number for the TCP/UDP connection	1194
Encryption algorithm	Select authentication mode for the key exchange. The configuration fields vary depending on the authentication mode you select.	BlowFish CBC
Hash algorithm	Select the MD5, SHA-1 or SHA-256 VPN key exchange phase 1 hash mode.	SHA1
LZO compression	Compress tunnel packets using the LZO algorithm	Enable
CA Certificate	Select the Certificate Authority (.crt) uploaded in 'Trusted CA Certificate'	N/A
Certificate	Select the certificate (.crt) uploaded in 'Local Certificate'	
User authentication	Only password authentication is supported in server mode.	Password
Keepalive	Select Enable to check if the client connection is alive	Enable
Redirect to default gateway	Select Enable to force all clients' generated traffic to pass through the tunnel. For more details, please check the section Example for Typical VPN Applications.	Disable
Allow Client-to-client	Select Enable to allow communication between clients connected to the server. If this function is disabled, the clients will only be able to communicate with the server. For more details please check the section Example for Typical VPN Applications.	Disable

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.

DHCP Proxy demonstration

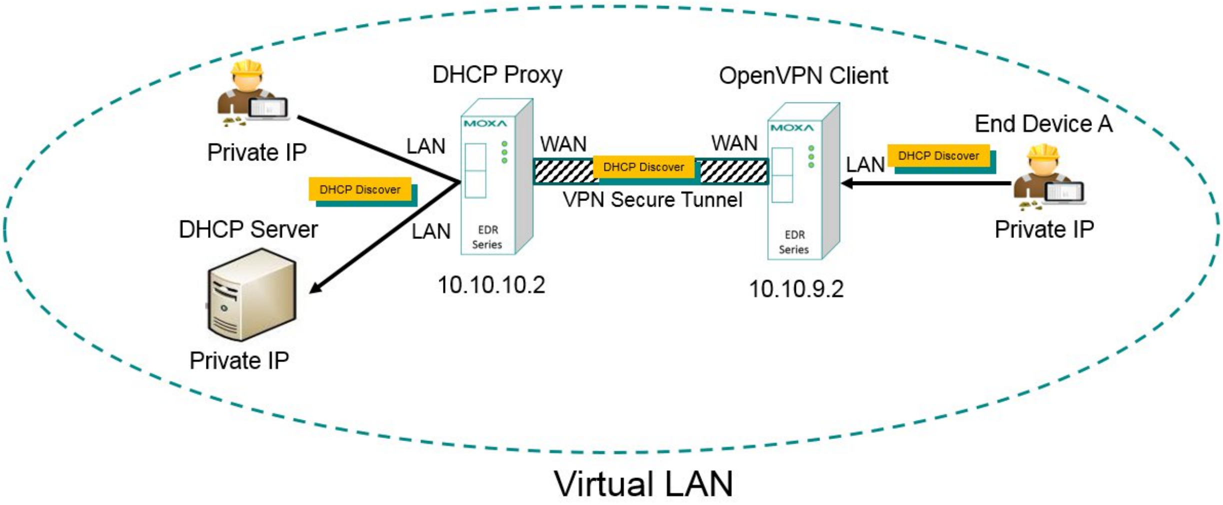
In OpenVPN Bridge mode (TAP interface type), the client and server are configured as one local area network. In this case, all of the devices will be set as in one subnet. Therefore broadcast packets can be received by all the devices. To achieve this, the OpenVPN server will assign IP to clients to make sure clients' IP are in the same subnet with server's IP.

If there is a DHCP server behind OpenVPN server, OpenVPN server can play as DHCP proxy to relay DHCPDISCOVER to DHCP server, and DHCP server will send IP setting (DHCPOFFER, DHCPACK) to clients. If there is no DHCP server behind OpenVPN server, OpenVPN server will play as DHCP sever to send IP setting to clients.

According to this user scenario, users can set OpenVPN server as DHCP server or DHCP proxy in **DHCP Proxy.**

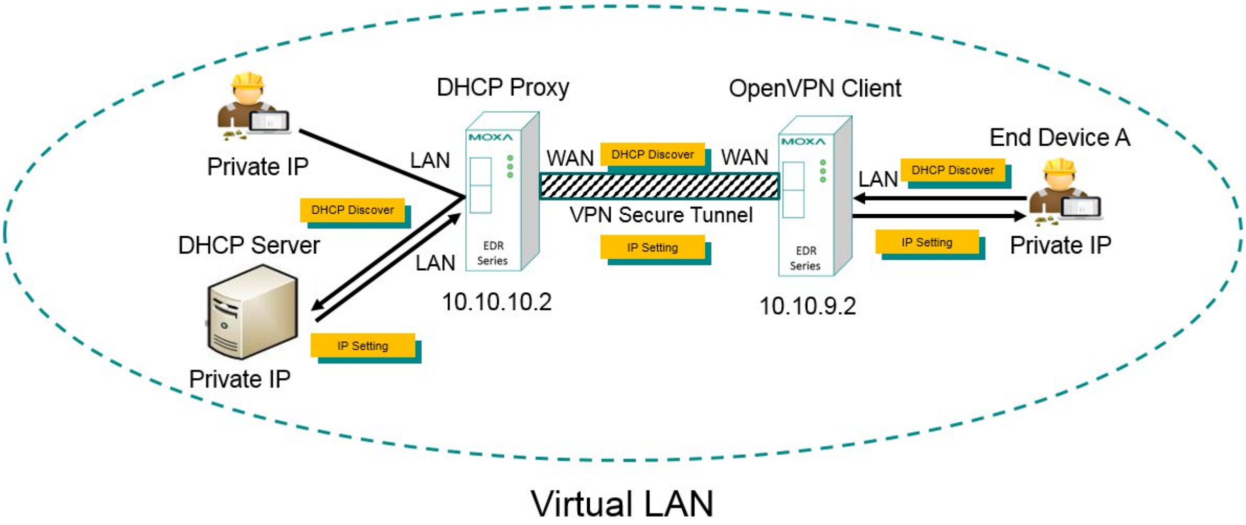
DHCP proxy Enable

When **DHCP Proxy** is enabled, OpenVPN server will play as DHCP proxy to relay DHCPDISCOVER from clients to DHCP server. Packet flow is as below figure.



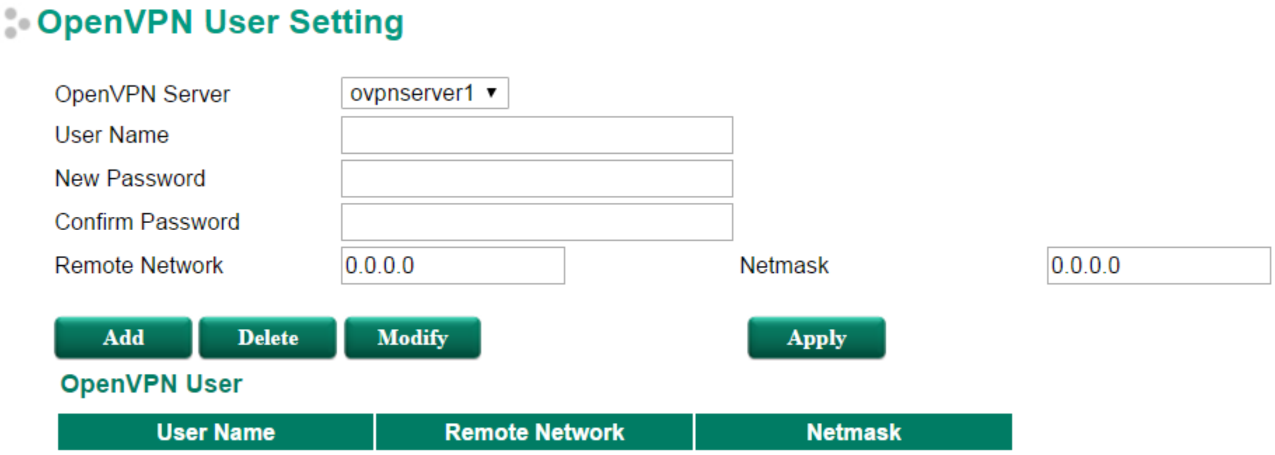
DHCP Proxy Disable

When **DHCP Proxy** is disabled, OpenVPN server will play as DHCP server and will manage DHCPDISCOVER from clients. OpenVPN server will send IP setting to clients. After TCP/IP is set up, OpenVPN server will be clients' default gateway. Packet flow is as below figure.



User Management

Enables management and export of user configurations.



OpenVPN User Setting

OpenVPN Server	ovpnserver1 ▾		
User Name			
New Password			
Confirm Password			
Remote Network	0.0.0.0	Netmask	0.0.0.0

OpenVPN User

User Name	Remote Network	Netmask

OpenVPN User Setting

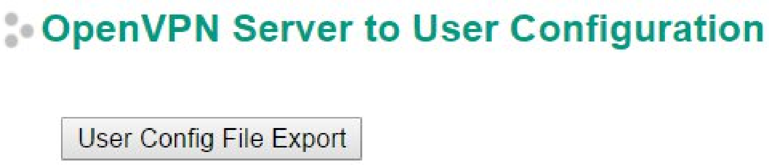
Setting	Description	Factory Default
OpenVPN Server	Indicate the server that the client will connect with.	ovpnserver1
User Name	Enter the User Name. The Industrial Secure Router supports five clients to connect with a server, which allows the user to set up the user name and password for five clients.	NULL
New Password	Enter the new password.	NULL
Confirm Password	Enter the password again.	NULL
Remote Network	Enter the subnet of each user. The Industrial Secure Router is set up to support 5 different subnets.	0.0.0.0
Netmask	Enter the remote network subnet mask of each user.	0.0.0.0

Server to User Config

After finishing the server settings, the user has to create a profile (.ovpn file) as well. However, in order to achieve this you need basic network knowledge. In order to simplify this process, the Industrial Secure Router can generate .ovpn file, named ovpnclient, for user to import into the client device.

In Server to User Config, the user can export the ovpnclient.ovpn file and import it into the client device to build the VPN connection. Below we use a simple case to demonstrate the setup process.

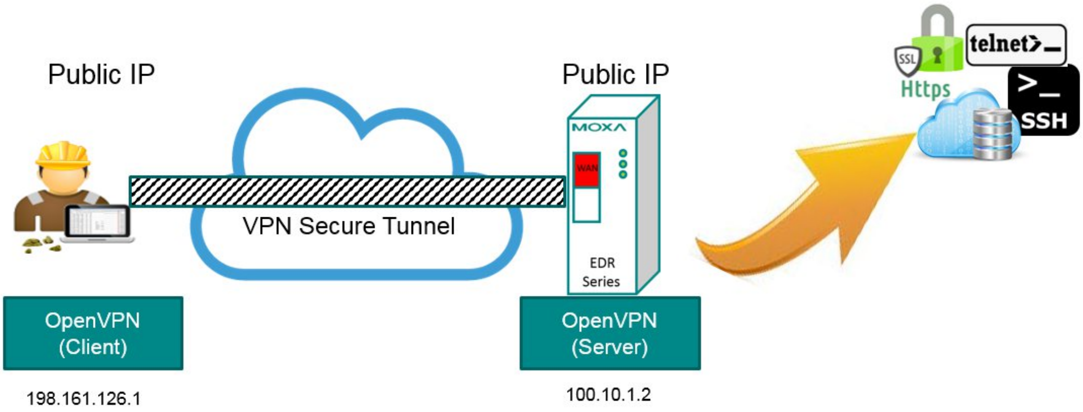
In the following, we will demonstrate how to import this ovpnclient.ovpn file and create OpenVPN connection.



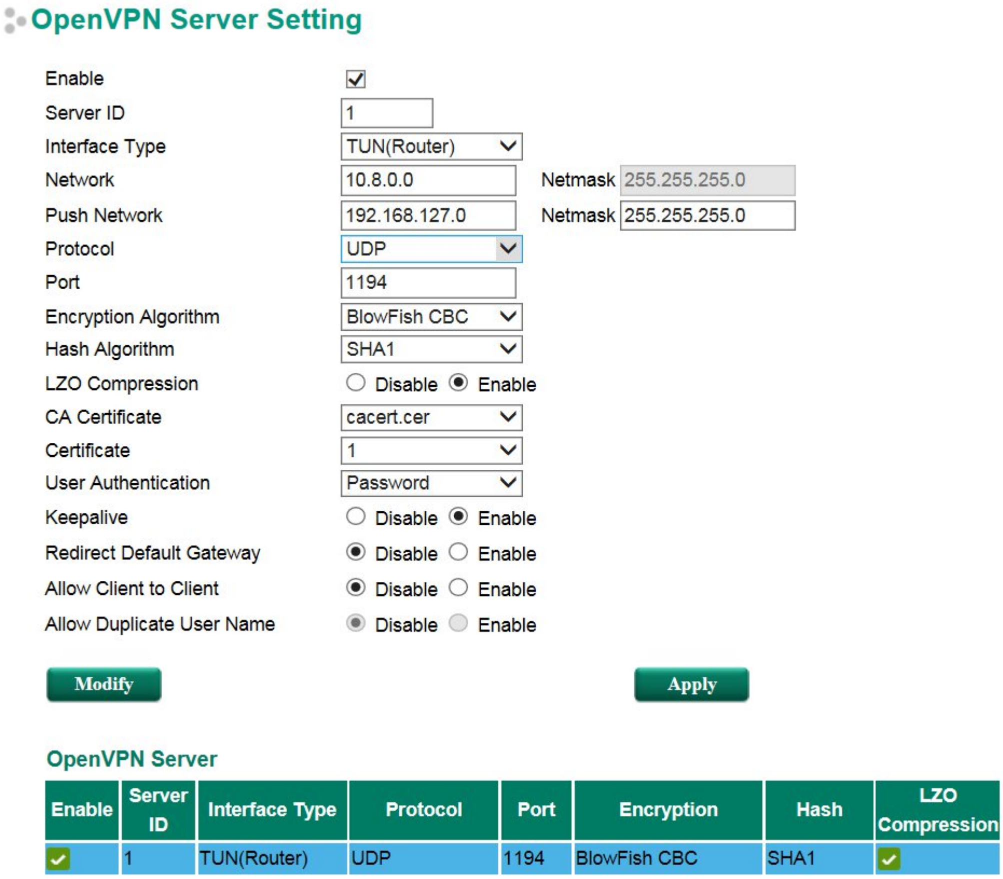
OpenVPN Server to User Configuration

Server to User Config demonstration

In the topology below, the client wants to build a VPN connection with OpenVPN server.



Step 1: Setup OpenVPN server



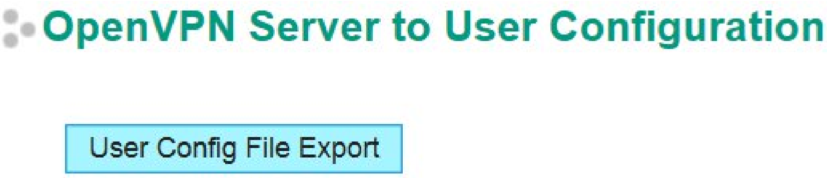
OpenVPN Server Setting

Enable	☑		
Server ID	1		
Interface Type	TUN(Router)		
Network	10.8.0.0	Netmask	255.255.255.0
Push Network	192.168.127.0	Netmask	255.255.255.0
Protocol	UDP		
Port	1194		
Encryption Algorithm	BlowFish CBC		
Hash Algorithm	SHA1		
LZO Compression	○ Disable ● Enable		
CA Certificate	cacert.cer		
Certificate	1		
User Authentication	Password		
Keepalive	○ Disable ● Enable		
Redirect Default Gateway	● Disable ○ Enable		
Allow Client to Client	● Disable ○ Enable		
Allow Duplicate User Name	● Disable ○ Enable		

OpenVPN Server

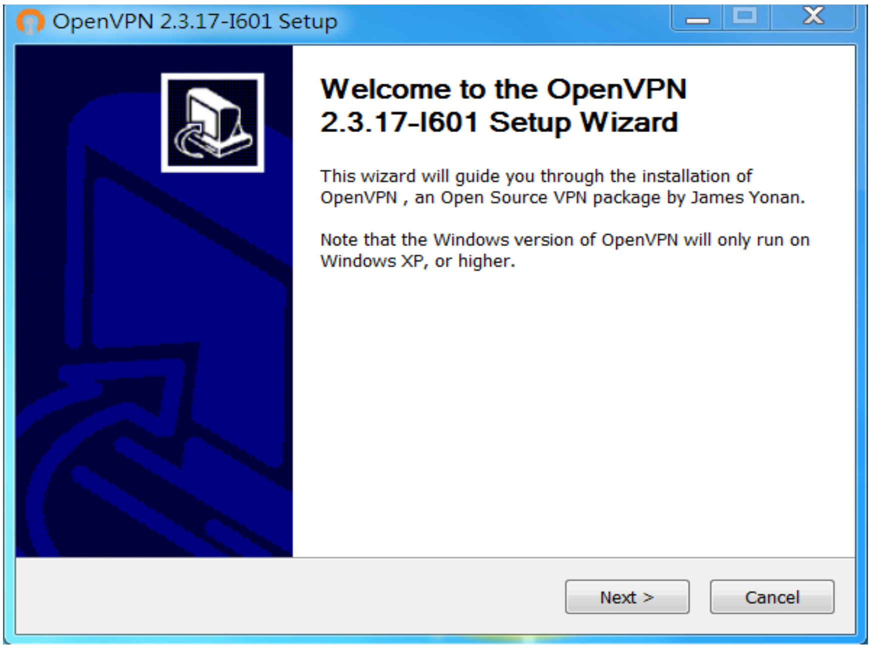
Enable	Server ID	Interface Type	Protocol	Port	Encryption	Hash	LZO Compression
✓	1	TUN(Router)	UDP	1194	BlowFish CBC	SHA1	✓

Step 2: Export ovpnclient.ovpn file from the server



OpenVPN Server to User Configuration

Step 3: Download OpenVPN installer and install it in to the client device. Keep the default settings until the setup is complete.



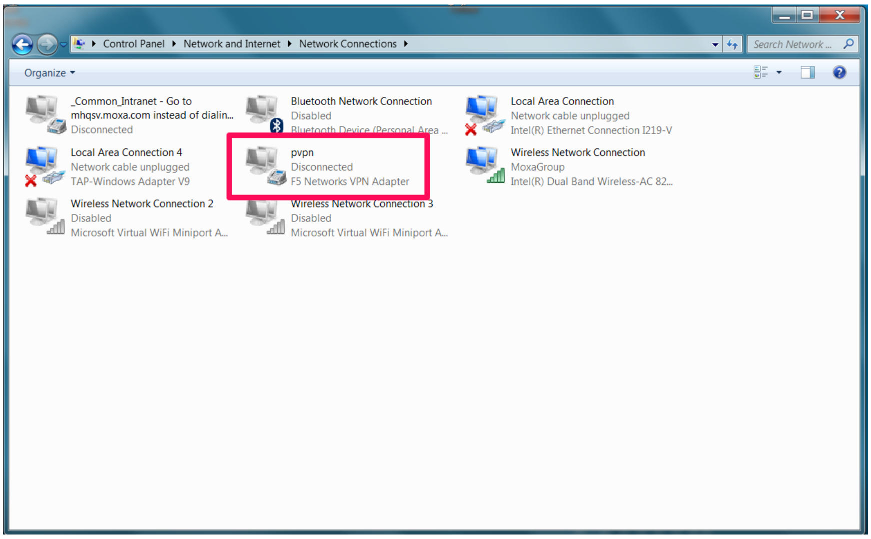
OpenVPN 2.3.17-I601 Setup

Welcome to the OpenVPN 2.3.17-I601 Setup Wizard

This wizard will guide you through the installation of OpenVPN , an Open Source VPN package by James Yonan.

Note that the Windows version of OpenVPN will only run on Windows XP, or higher.

Rename virtual interface to pvpn.



Control Panel ▸ Network and Internet ▸ Network Connections ▸

Organize ▾

_Common_Intranet - Go to mhqsv.moxa.com instead of dialin... Disconnected

Bluetooth Network Connection Disabled Bluetooth Device (Personal Area ...

Local Area Connection Network cable unplugged Intel(R) Ethernet Connection I219-V

Local Area Connection 4 Network cable unplugged TAP-Windows Adapter V9

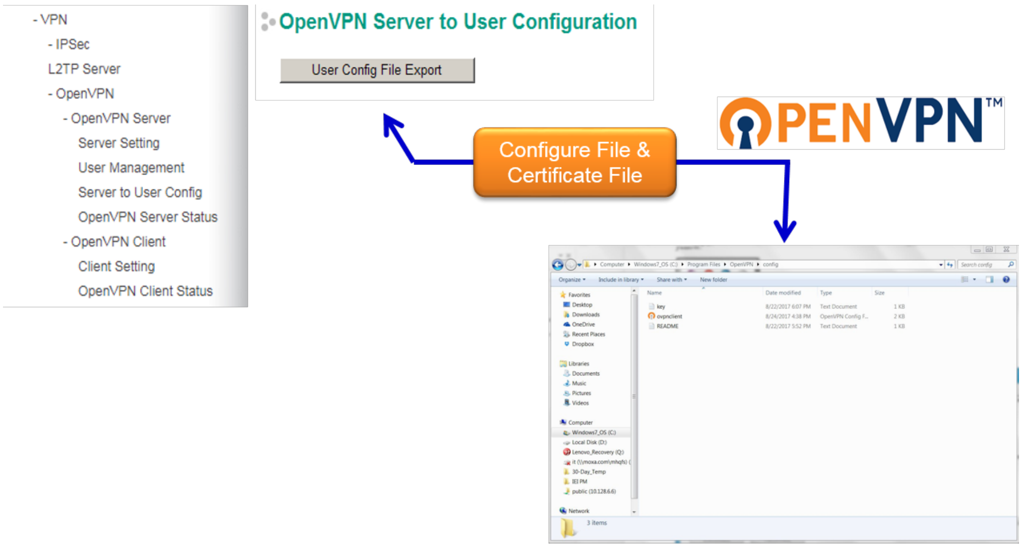
pvpn Disconnected F5 Networks VPN Adapter

Wireless Network Connection MoxaGroup Intel(R) Dual Band Wireless-AC 82...

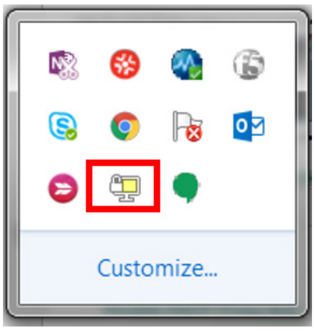
Wireless Network Connection 2 Disabled Microsoft Virtual WiFi Miniport A...

Wireless Network Connection 3 Disabled Microsoft Virtual WiFi Miniport A...

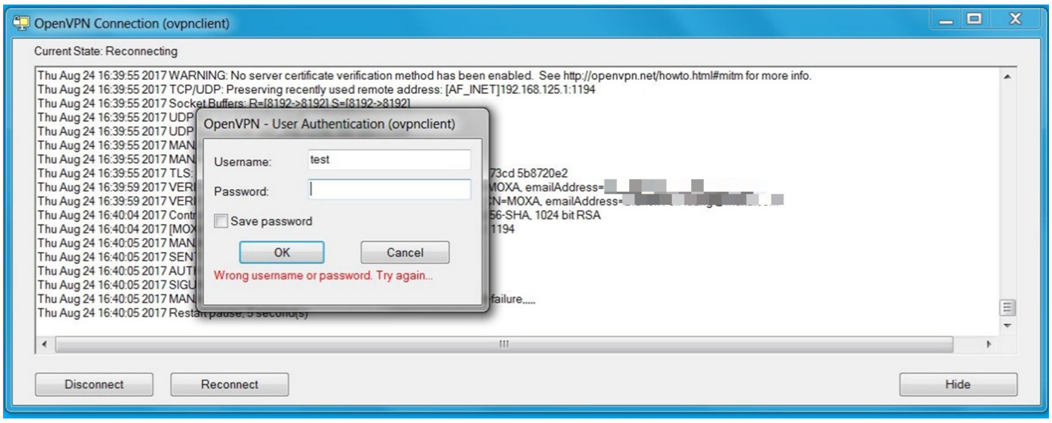
Step 4. Import ovpnclient.ovpn file in OpenVPN cofig file.



Step 5: Connect client to the server. Click the OpenVPN GUI icon. When OpenVPN connection is not built up, the icon will show in yellow.



Type in the user account and password which can be set in “User Management”.



Current State: Reconnecting

```
Thu Aug 24 16:39:55 2017 WARNING: No server certificate verification method has been enabled.  See http://openvpn.net/howto.html#mitm for more info.
Thu Aug 24 16:39:55 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.125.1:1194
Thu Aug 24 16:39:55 2017 Socket Buffers: R=[8192->8192] S=[8192->8192]
Thu Aug 24 16:39:55 2017 UDP
Thu Aug 24 16:39:55 2017 UDP
Thu Aug 24 16:39:55 2017 MAN
Thu Aug 24 16:39:55 2017 MAN
Thu Aug 24 16:39:55 2017 TLS:                                73cd 5b8720e2
Thu Aug 24 16:39:59 2017 VERI                                MOXA, emailAddress=[redacted]
Thu Aug 24 16:39:59 2017 VERI                                N=MOXA, emailAddress=[redacted]
Thu Aug 24 16:40:04 2017 Contr                               56-SHA, 1024 bit RSA
Thu Aug 24 16:40:04 2017 [MOX                                1194
Thu Aug 24 16:40:05 2017 MAN
Thu Aug 24 16:40:05 2017 SEN
Thu Aug 24 16:40:05 2017 AUT
Thu Aug 24 16:40:05 2017 SIGU
Thu Aug 24 16:40:05 2017 MAN                                 failure.....
Thu Aug 24 16:40:05 2017 Restart pause, 5 second(s)
```

OpenVPN - User Authentication (ovpnclient)

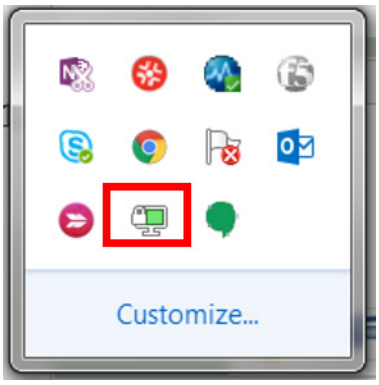
Username: test

Password:

☐ Save password

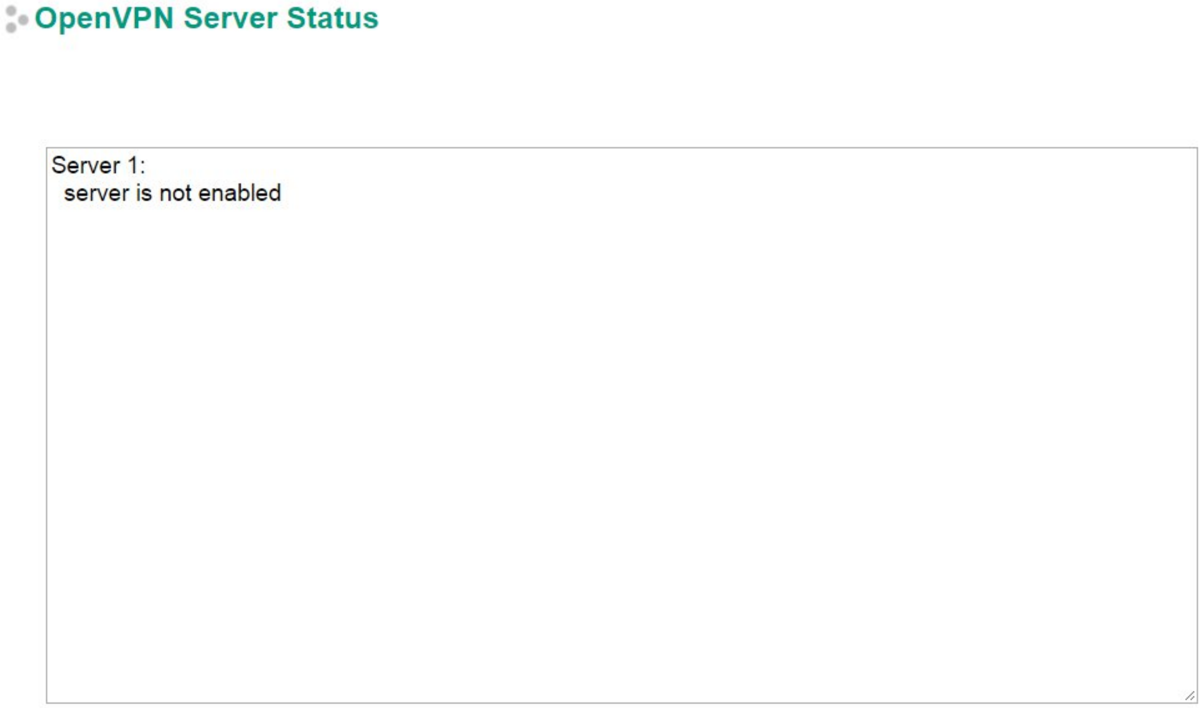
Wrong username or password. Try again...

Step 6: When OpenVPN is built up, the OpenVPN GUI icon will turn green.



OpenVPN Server Status

Here will show the OpenVPN server connection information, including client name, real IP address and start time.

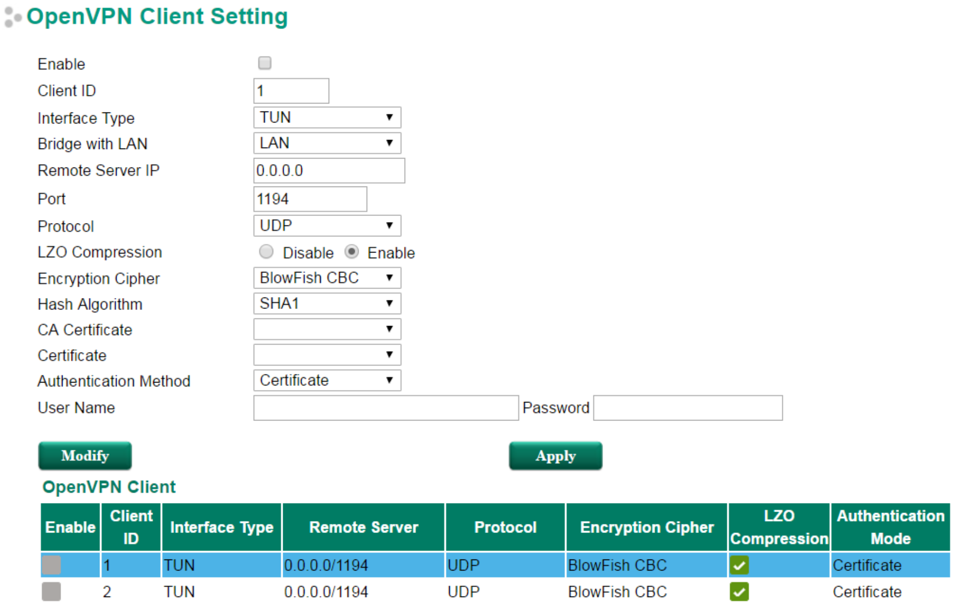


OpenVPN Server Status

```
Server 1:
  server is not enabled
```

Client Settings

When the Industrial Secure Router is functioning as the OpenVPN Client, it can build connections with up to two different servers in either TUN mode or TAP mode.



OpenVPN Client Setting

Enable	□
Client ID	1
Interface Type	TUN ▾
Bridge with LAN	LAN ▾
Remote Server IP	0.0.0.0
Port	1194
Protocol	UDP ▾
LZO Compression	○ Disable ● Enable
Encryption Cipher	BlowFish CBC ▾
Hash Algorithm	SHA1 ▾
CA Certificate	▾
Certificate	▾
Authentication Method	Certificate ▾
User Name	Password

OpenVPN Client

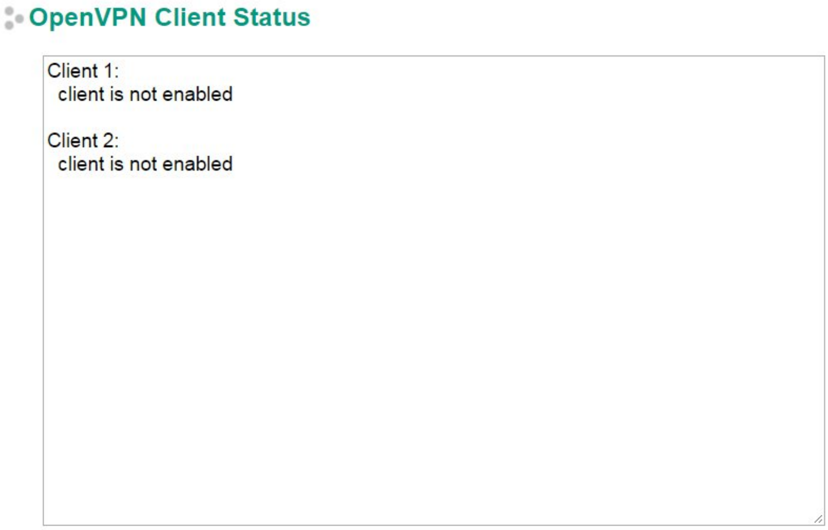
Enable	Client ID	Interface Type	Remote Server	Protocol	Encryption Cipher	LZO Compression	Authentication Mode
□	1	TUN	0.0.0.0/1194	UDP	BlowFish CBC	✓	Certificate
□	2	TUN	0.0.0.0/1194	UDP	BlowFish CBC	✓	Certificate

Client Setting

Setting	Description	Factory Default
Enable	Select Enable to activate the OpenVPN Client.	Disable
Client ID	The Industrial Secure Router can build connections with a maximum of two different servers.	1
Interface type	Select OpenVPN tunnel connection by router or bridge mode.	TUN
Bridge with LAN	In TAP mode, select the LAN interface of the client that will connect with the server. Please refer to the Interface section for how to create different LAN interfaces.	LAN
Remote server IP	Enter the IP address of the VPN server that the client wants to connect with.	0.0.0.0
Port	Enter the remote server port number for TCP or UDP connection.	1194
Protocol	Select the protocol to be used for the VPN.	UDP
LZO compression	Compress tunnel packets using the LZO algorithm.	Enable
Encryption cipher	Select authentication mode for key exchange. The configuration fields vary depending on the authentication mode the user selects.	BlowFish CBC
Hash algorithm	Select the MD5 or SHA-1 VPN key exchange phase 1 hash mode.	SHA1
CA Certificate	Select the Certificate Authority (.crt) uploaded in 'Trusted CA Certificate'	NULL
Certificate	Select the certificate (.crt) uploaded in 'Local Certificate'.	NULL
Authentication method	Users can select either password or certification to protect the authentication.	Certificate
User name	Enter the user name for the client that you set on the server.	NULL
Password	Enter the client password that you set on the server (up to 15 characters.)	NULL

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.

OpenVPN Client Status



OpenVPN Client Status

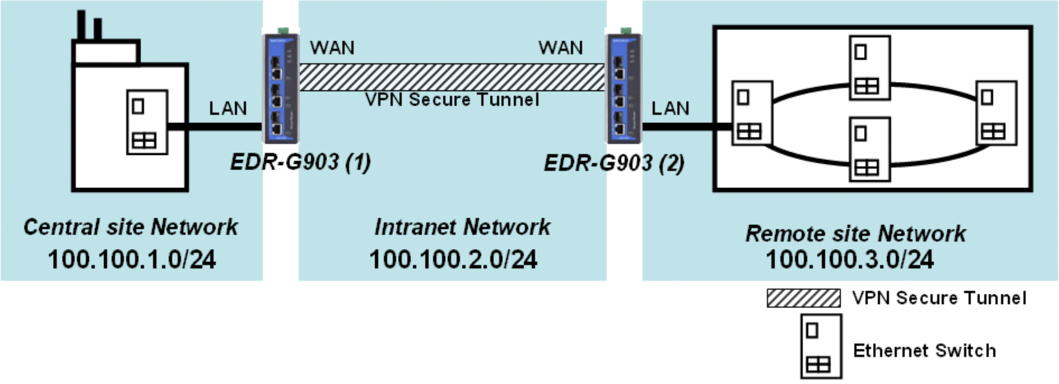
Client 1:
client is not enabled

Client 2:
client is not enabled

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.

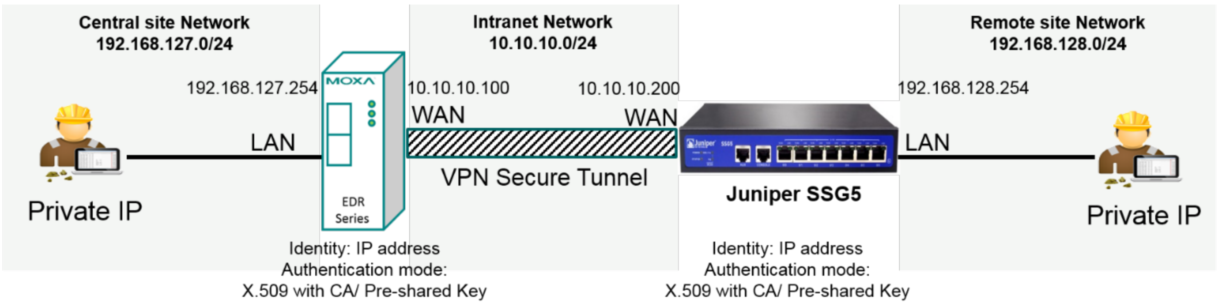
	Configuration	Industrial Secure Router (1)	Industrial Secure Router (2)
EDR-G903 Interface Setting	WAN IP	100.100.2.1	100.100.2.2
	LAN IP	100.100.1.1	100.100.3.1

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, 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	**EDR 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:

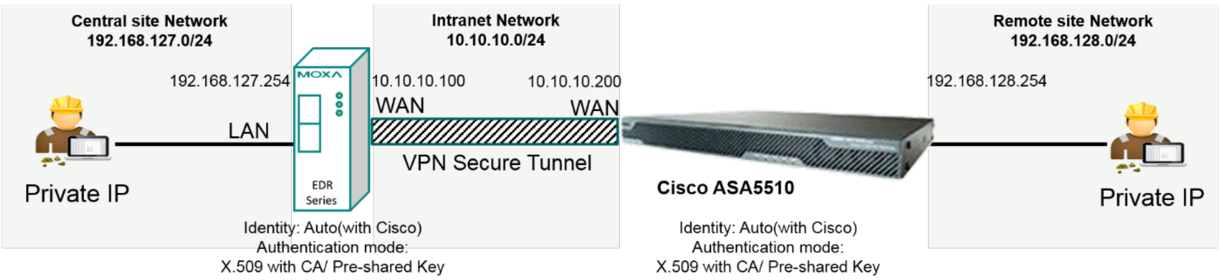
	Configuration	**EDR Series**	**Juniper SSG5**
Tunnel Setting	Connection Type	Site to Site	Site to Site
	Remote VPN gateway	10.10.10.200	10.10.10.100
	Startup mode	Wait for Connection	Start in Initial
	Local Network / Netmask	192.168.127.0 / 255.255.255.0	192.168.128.0 / 25.255.255.0
	Remote Network / 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 EDR 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:

EDR 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	**EDR 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	**EDR 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.

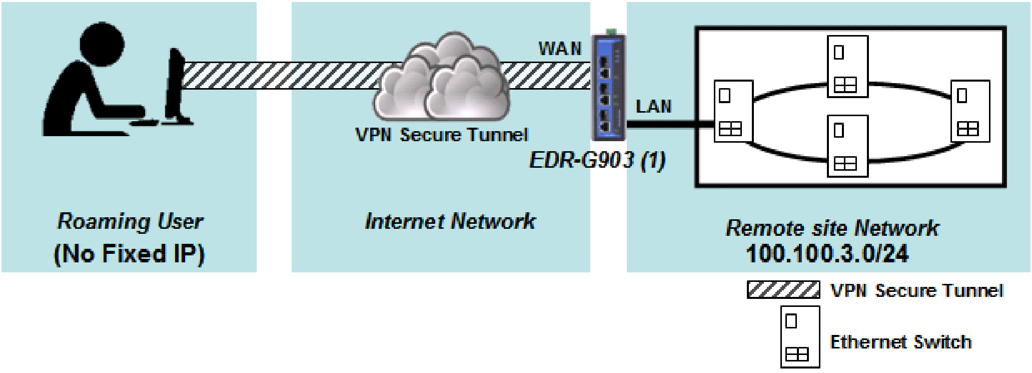
If you prefer Pre-shared Key, the identity can be set as "**IP Address**", "**FQDN**", "**Key ID**", or "**Auto (with Cisco)**". If you X.509 with CA, the identity should be set as "**Auto (with Cisco)**". The Industrial Secure Router with Cisco compliance matrix is shown below:

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.

EDR 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.

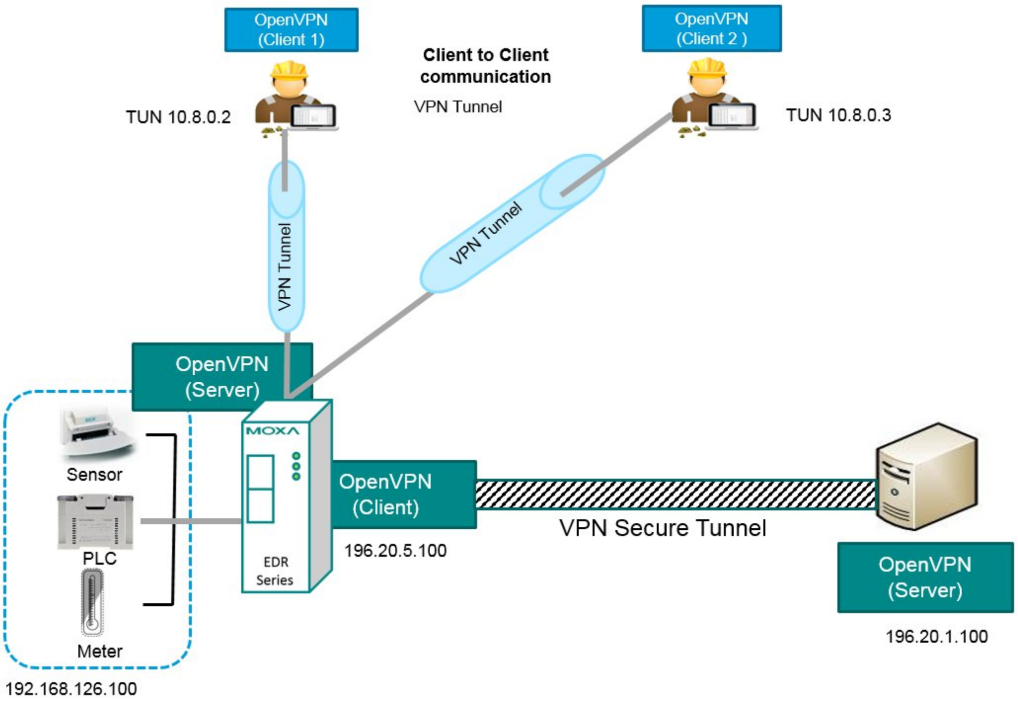
	Configuration	**Industrial Secure Router (1)**
EDR-G903 Interface Setting	WAN IP	100.100.2.1
	LAN IP	100.100.3.1

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

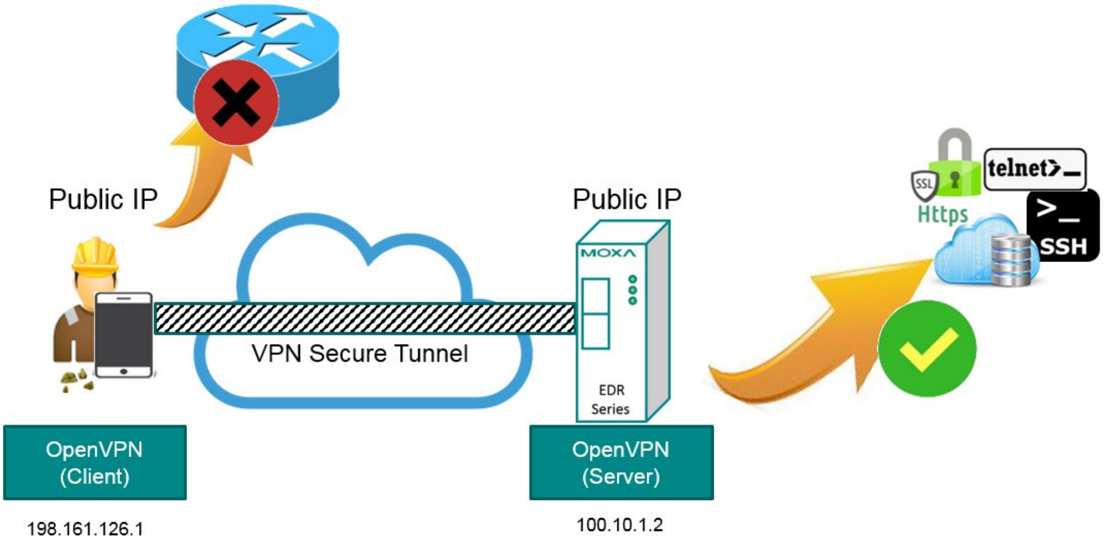
Client-to-Client communication via OpenVPN

Industrial Secure Router supports Client-to Client communication via OpenVPN. In this setting, clients can have secure communications with each other. At the field site, system security can be significantly strengthened using this method.



Redirect default gateway via OpenVPN

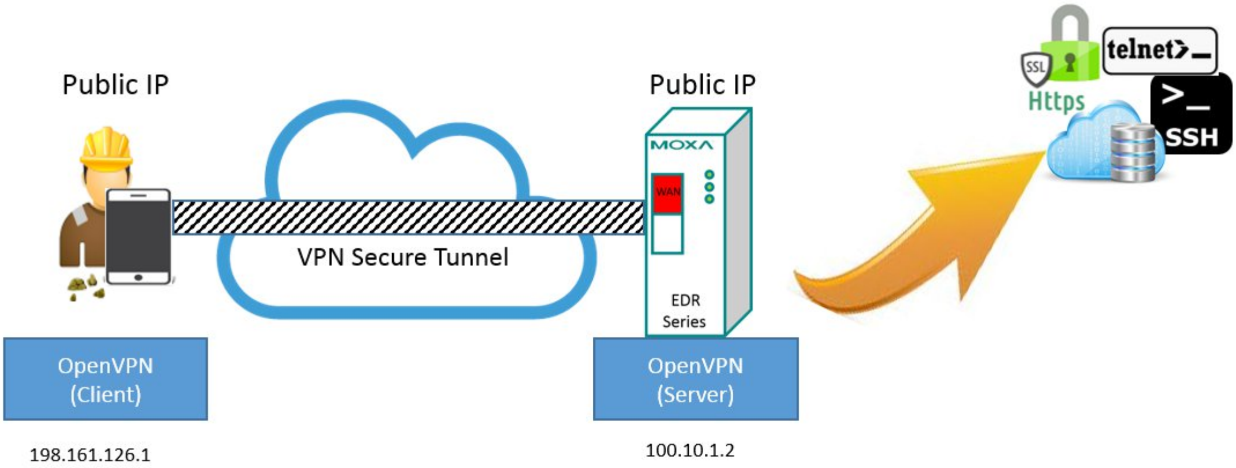
For some scenarios, user has high security requirements for end devices that are connected to the Internet. Any traffic destined for the Internet should be examined by OpenVPN server before connecting to the Internet. First, the traffic will go through the Industrial Secure Router, and then it will pass to the Internet. Under this setting, traffic from client devices will all be transferred to OpenVPN server first, and then pass to Internet.



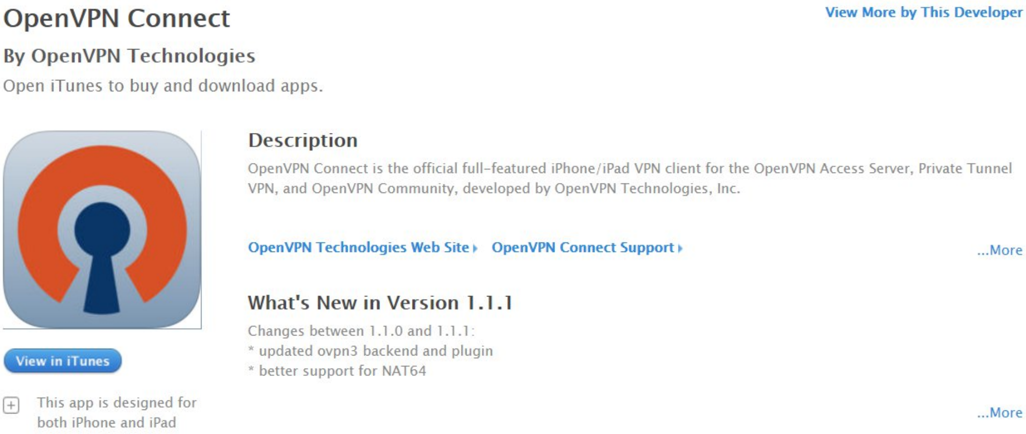
Create OpenVPN connection on a mobile device

User can use a mobile device to create OpenVPN connection with OpenVPN server.

Please follow the steps below:



Step 1: Download the OpenVPN Connect App into your mobile device. (The OpenVPN Connect App is compatible with iOS and Android platforms.)



OpenVPN Connect

By OpenVPN Technologies

Open iTunes to buy and download apps.

View More by This Developer

Description

OpenVPN Connect is the official full-featured iPhone/iPad VPN client for the OpenVPN Access Server, Private Tunnel VPN, and OpenVPN Community, developed by OpenVPN Technologies, Inc.

OpenVPN Technologies Web Site ▸ OpenVPN Connect Support ▸ ...More

What's New in Version 1.1.1

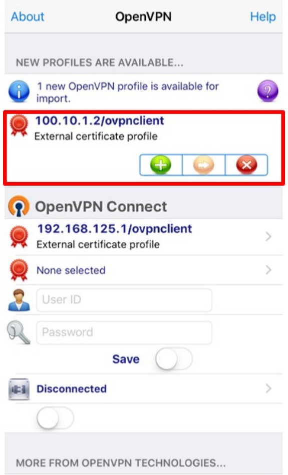
Changes between 1.1.0 and 1.1.1:
* updated ovpn3 backend and plugin
* better support for NAT64

...More

View in iTunes

This app is designed for both iPhone and iPad

Step2: Download the ovpnclient.ovpn file from the Industrial Secure Router into the mobile device. And then open it with the OPenVPN. Connect App. Then the user will see the server IP, which is marked in red below. Then press "+"icon to add this VPN connection.



About OpenVPN Help

NEW PROFILES ARE AVAILABLE...

1 new OpenVPN profile is available for import.

100.10.1.2/ovpnclient
External certificate profile

OpenVPN Connect

192.168.125.1/ovpnclient
External certificate profile

None selected

User ID

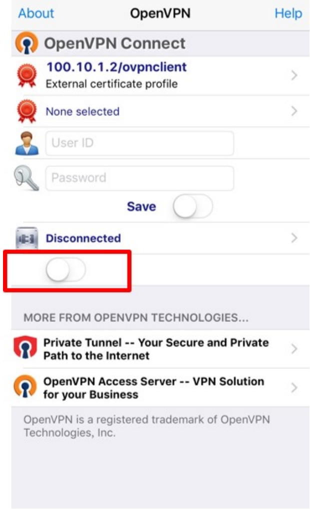
Password

Save

Disconnected

MORE FROM OPENVPN TECHNOLOGIES...

Step 3: Type in User ID and password. Then slide the button from disconnected to connected, which is highlighted in red below.



About OpenVPN Help

OpenVPN Connect

100.10.1.2/ovpnclient
External certificate profile

None selected

User ID

Password

Save

Disconnected

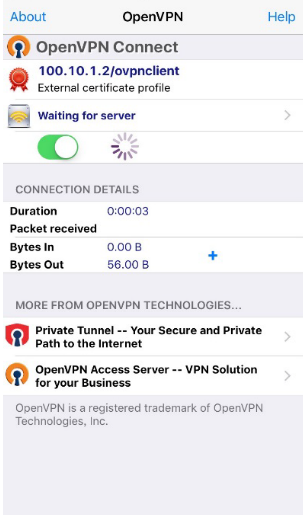
MORE FROM OPENVPN TECHNOLOGIES...

Private Tunnel -- Your Secure and Private Path to the Internet

OpenVPN Access Server -- VPN Solution for your Business

OpenVPN is a registered trademark of OpenVPN Technologies, Inc.

Step 4: Waiting for server verification.



About OpenVPN Help

OpenVPN Connect

100.10.1.2/ovpnclient
External certificate profile

Waiting for server

CONNECTION DETAILS

Duration	0:00:03
Packet received	
Bytes In	0.00 B
Bytes Out	56.00 B

MORE FROM OPENVPN TECHNOLOGIES...

Private Tunnel -- Your Secure and Private Path to the Internet

OpenVPN Access Server -- VPN Solution for your Business

OpenVPN is a registered trademark of OpenVPN Technologies, Inc.

10

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.

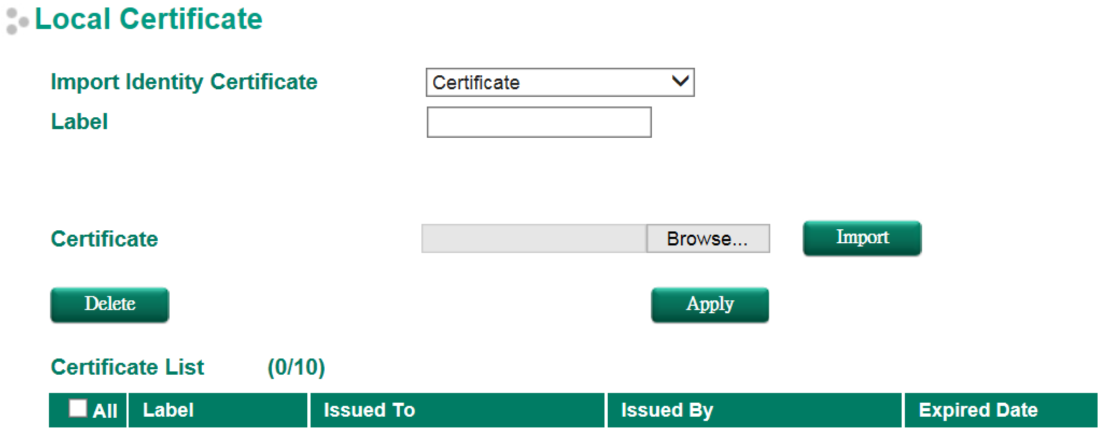
Certificates are a time related authentication mechanism. Before processing certificate management, please make ensure the industrial secure router is synced with the local device. For more details regarding time sync, please refer to section Date and Time

The following topics are covered in this chapter:

❒ **Local Certificate**
❒ **Trusted CA Certificates**
❒ **Certificate Signing Request**
❒ **CA Server**

Local Certificate

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



Local Certificate

Import Identity Certificate: Certificate

Label

Certificate

Certificate List (0/10)

☐ All	Label	Issued To	Issued By	Expired Date

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

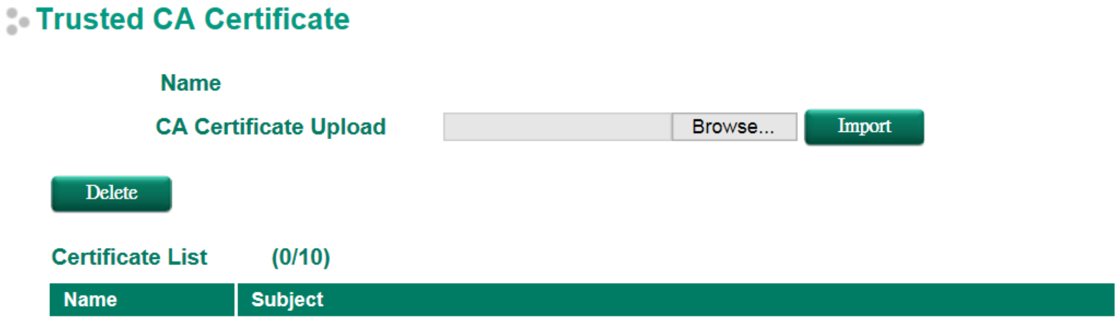
Label

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.



Trusted CA Certificate

Name

CA Certificate Upload

Certificate List (0/10)

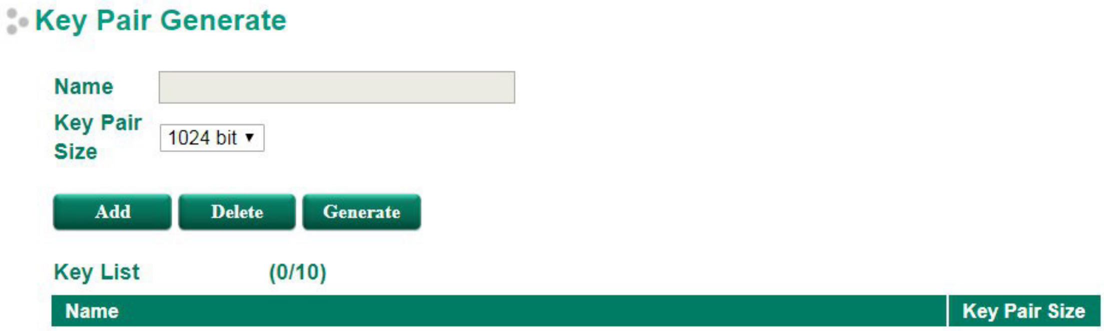
Name	Subject

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 Size: 1024 bit

Key Pair Generate

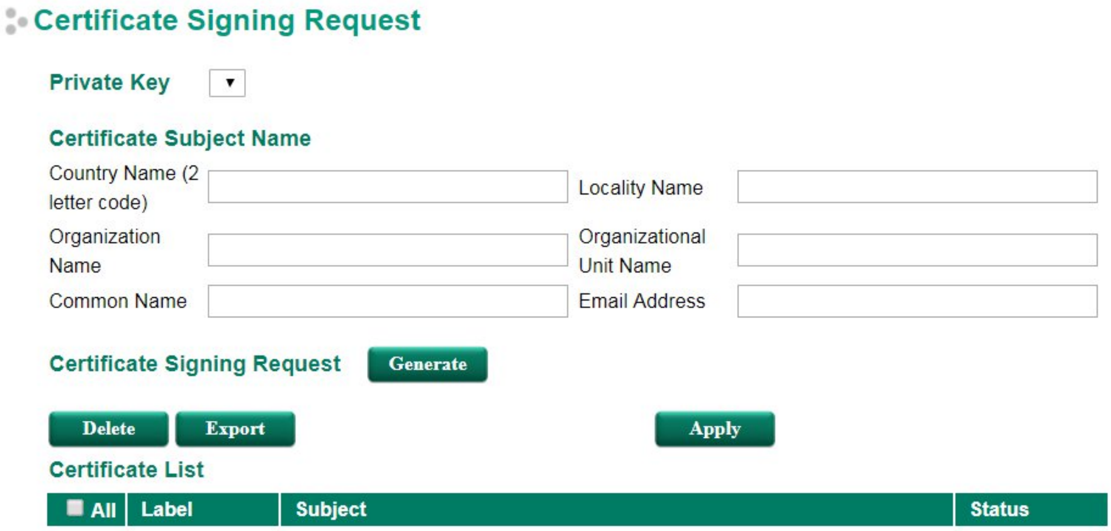
Name

Setting	Description	Factory Default
Name	Naming each private key	N/A

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	N/A

CA Server

Aside from getting the certificate from other CAs, the Industrial Secure Router can act as a RootCA to issue a certificate for each connection. After the RootCA has been set up, the Industrial Secure Router can send requests to ask for a certificate from the RootCA.

Certificate Request

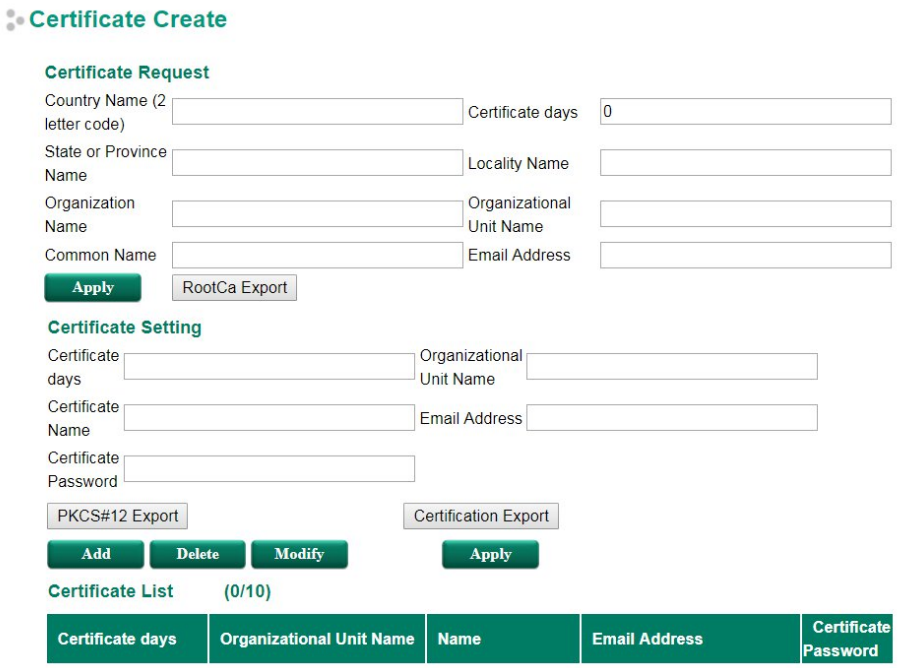
If a system only has their own certificate on hand, and do not have other systems' certificates, how can the system recognize other systems? The answer to this problem is Trust CA. As mentioned in the section Trust CA certificate, users can import a CA (.cer) that they trust into the Industrial Secure Router. When the user does this, the system will accept the certificate that was issued by a trusted CA.

If users want to use a certificate issued by the Industrial Secure Router functioning as a RootCA, the receiver must import this RootCA settings (.cer) as a trusted CA and recognize then it will recognize the RootCA certificate during connection. Otherwise, this connection will be rejected by the receiver. Users can create RootCA via Certificate Request and export the RootCA settings by clicking RootCA Export.

The user has to fill in all the RootCA information in the Certificate Request in order to create the RootCA.

Certificate Setting

After creating the RootCA successfully, users can issue a request for a certificate from the RootCA in the Certificate Setting. After filling in the information, users can generate two kinds of certificate: PKCS#12 (.p12) and certificate (.crt). A PKCS#12 request includes a private key but a certificate does not. To export a PKCS#12 certificate, please click PKCS#12 Export. To export a certificate request, please click Certification Export.



Certificate days	Organizational Unit Name	Name	Email Address	Certificate Password

11

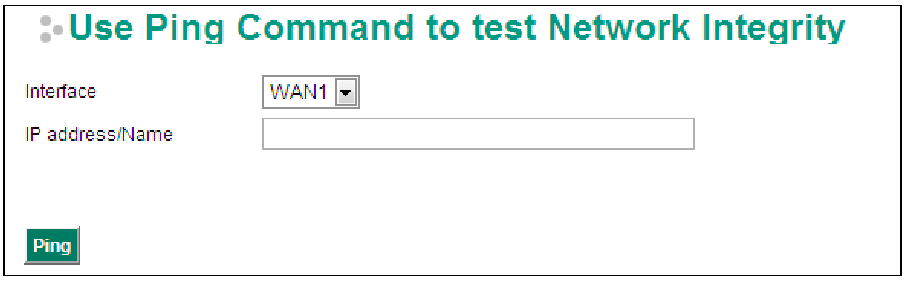
Diagnosis

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

The following topics are covered in this chapter:

- **Ping**
- **LLDP**
- **Monitor**
  - Statistics
  - Bandwidth Utilization
  - Display Setting
  - Display Setting

Ping



Use Ping Command to test Network Integrity

Interface: WAN1

IP address/Name:

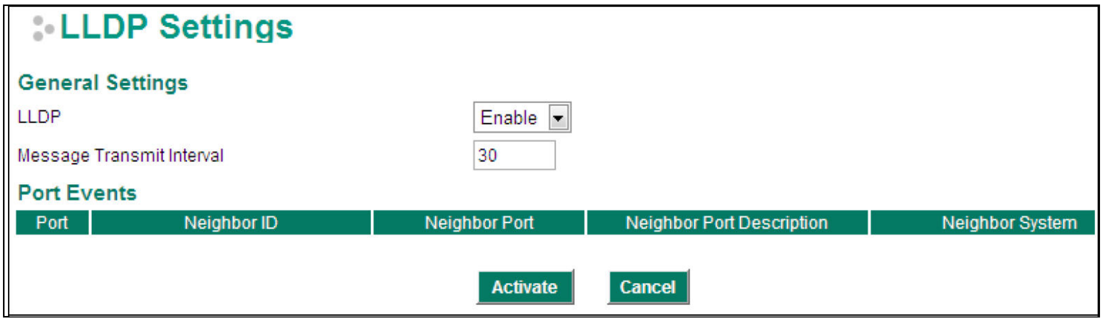
The Ping function uses the ping command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the Industrial Secure Router itself.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

1. Select which interface will be used to send the ping commands. You may choose from WAN1, WAN2, and LAN.
2. 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.



LLDP Settings

General Settings

LLDP: Enable

Message Transmit Interval: 30

Port Events

Port	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System

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

LLDP Setting

Enable LLDP

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

Message Transmit Interval

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

LLDT Table

Port: The port number that connects to the neighbor device.
Neighbor ID: A unique entity that identifies a neighbor device; this is typically the MAC address.
Neighbor Port: The port number of the neighbor device.
Neighbor Port Description: A textual description of the neighbor device’s interface.
Neighbor System: Hostname of the neighbor device.

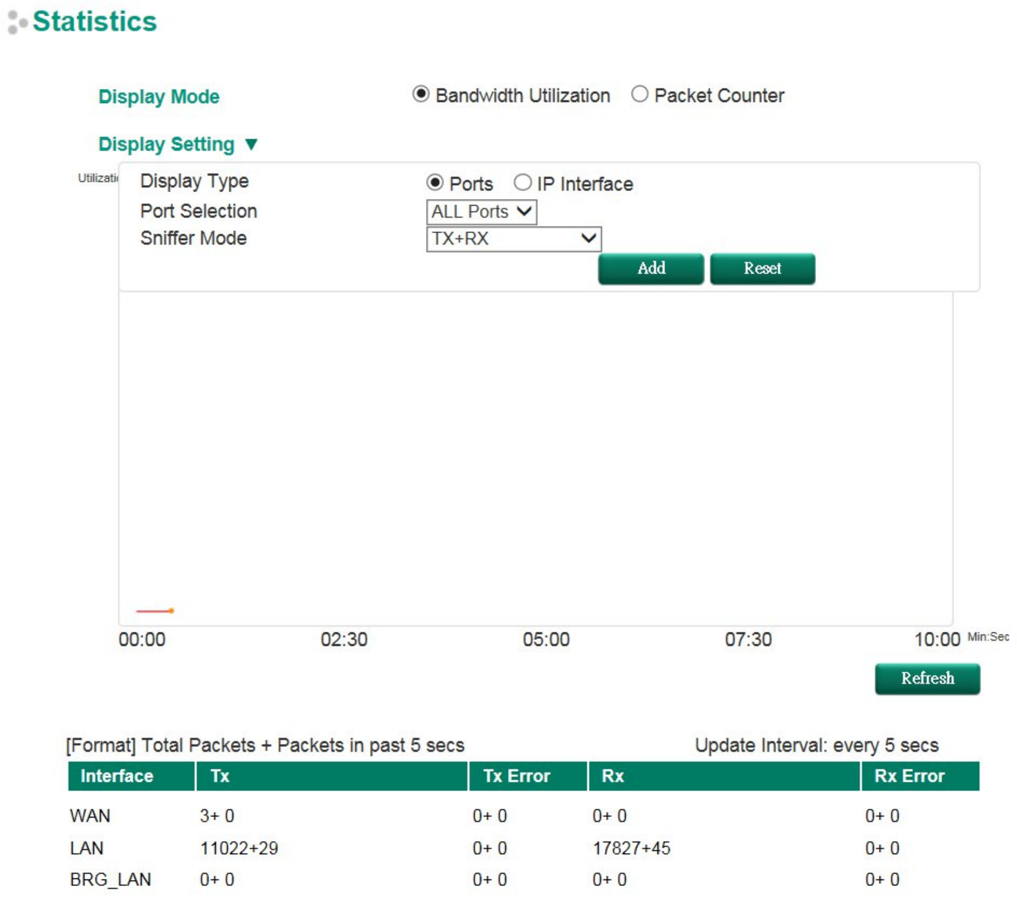
Monitor

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.


Statistics

Display Mode ● Bandwidth Utilization ○ Packet Counter

Display Setting ▼

Display Type ● Ports ○ IP Interface
Port Selection: ALL Ports
Sniffer Mode: TX+RX

[Format] Total Packets + Packets in past 5 secs   Update Interval: every 5 secs

Interface	Tx	Tx Error	Rx	Rx Error
WAN	3+ 0	0+ 0	0+ 0	0+ 0
LAN	11022+29	0+ 0	17827+45	0+ 0
BRG_LAN	0+ 0	0+ 0	0+ 0	0+ 0

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 (only supported in EDR-810)	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/ PortG1/ PortG2	Users can select which port or port group they want to monitor traffic from	ALL Ports

Interface Selection

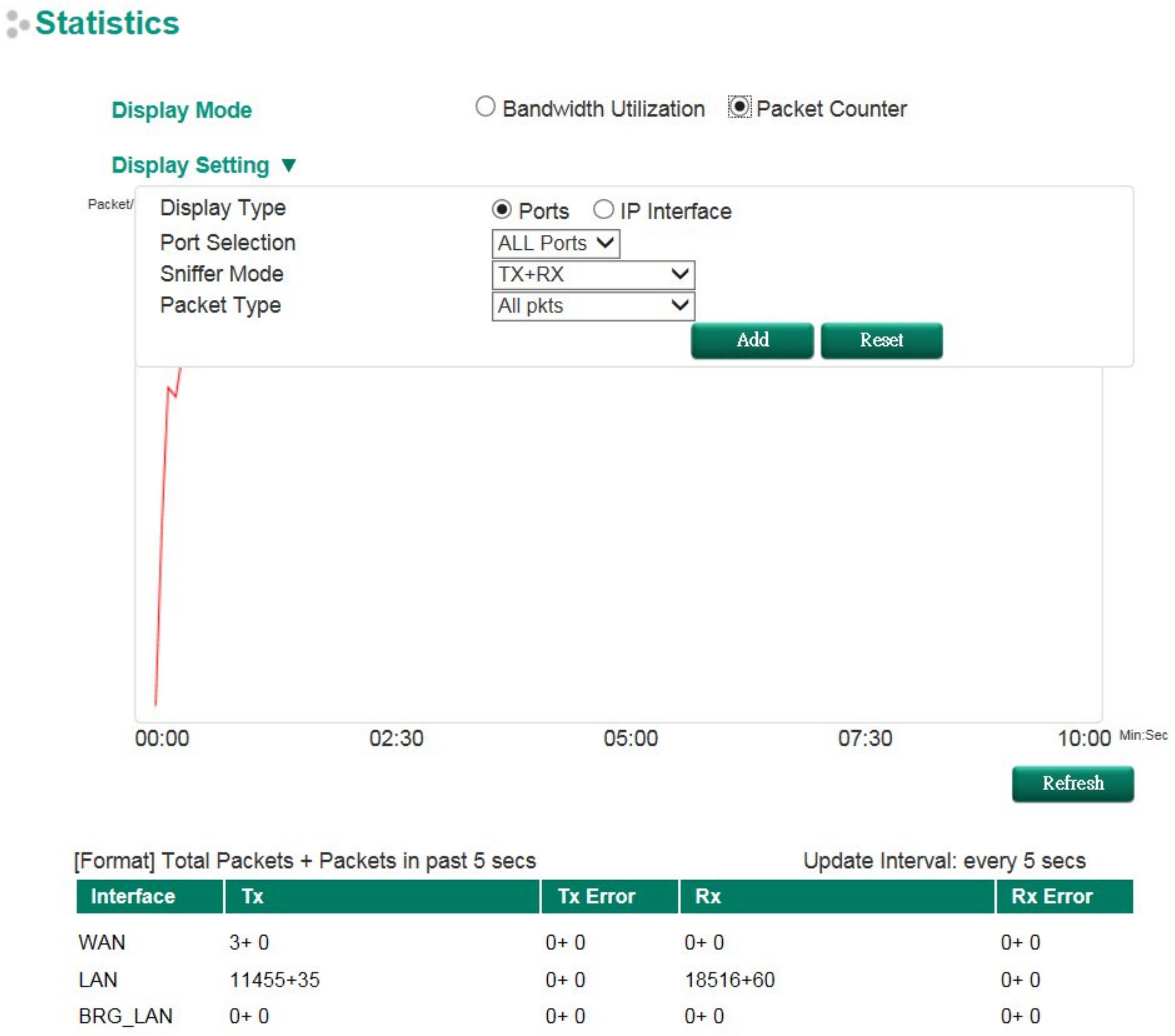
Setting	Description	Factory Default
All/LAN/WAN/Bridge_LAN	Select which interface user want to monitor traffic	All

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.



Statistics

Display Mode ○ Bandwidth Utilization ● Packet Counter

Display Setting ▼

Display Type	● Ports ○ IP Interface
Port Selection	ALL Ports
Sniffer Mode	TX+RX
Packet Type	All pkts

[Format] Total Packets + Packets in past 5 secs Update Interval: every 5 secs

Interface	Tx	Tx Error	Rx	Rx Error
WAN	3+ 0	0+ 0	0+ 0	0+ 0
LAN	11455+35	0+ 0	18516+60	0+ 0
BRG_LAN	0+ 0	0+ 0	0+ 0	0+ 0

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/ PortG1/ PortG2	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/ Unicast/ Broadcast/ Multicast/ Error	Select which packet type is monitored	All

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
4. DI Trap

The Industrial Secure Router also provides a MIB file, located in the file “Moxa-EDRG903-MIB.my” on the Industrial Secure Router Series utility CD-ROM for SNMP trap message interpretation