

EDR-G903 User's Manual

First Edition, April 2010

www.moxa.com/product



© 2010 Moxa Inc. All rights reserved.
Reproduction without permission is prohibited.

EDR-G903 Series User's Manual

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

Copyright Notice

Copyright © 2010 Moxa Inc.

All rights reserved.

Reproduction without permission is prohibited.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.

All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

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

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

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

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

Technical Support Contact Information

www.moxa.com/support

Moxa Americas

Toll-free: 1-888-669-2872

Tel: +1-714-528-6777

Fax: +1-714-528-6778

Moxa Europe

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

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

Moxa China (Shanghai office)

Toll-free: 800-820-5036

Tel: +86-21-5258-9955

Fax: +86-10-6872-3958

Moxa Asia-Pacific

Tel: +886-2-8919-1230

Fax: +886-2-8919-1231

Table of Contents

1. Introduction.....	1-1
Overview	1-2
Package Checklist	1-2
Features	1-2
Industrial Networking Capability.....	1-2
Designed for Industrial Applications.....	1-2
Useful Utility and Remote Configuration	1-2
2. Getting Started	2-1
RS-232 Console Configuration (115200, None, 8, 1, VT100)	2-2
Using Telnet to Access the EDR-G903's Console	2-4
Using a Web Browser to Configure the EDR-G903	2-5
3. Features and Functions	3-1
Configuring Basic Settings	3-3
System Identification	3-3
Accessible IP.....	3-4
Password	3-5
Time.....	3-6
SettingCheck	3-8
System File Update—by Remote TFTP	3-9
System File Update—by Local Import/Export	3-10
Restart.....	3-11
Reset to Factory Default.....	3-11
Network Settings	3-11
WAN1 Configuration	3-11
WAN2 Configuration (includes DMZ Enable)	3-14
Using DMZ Mode	3-16
LAN Interface	3-17
DHCP Server.....	3-18
Static DHCP List	3-18
Dynamic DNS	3-19
Communication Redundancy	3-20
How Dual WAN Backup Works.....	3-20
WAN Backup Configuration	3-21
Static Routing	3-22
Network Address Translation (NAT).....	3-22
NAT Concept.....	3-22
N-to-1 NAT.....	3-23
Port Forwarding	3-24
1-to-1 NAT	3-25
Firewall Settings.....	3-27
Firewall Policy Concept.....	3-27
Firewall Policy Overview	3-27
Firewall Policy Configuration	3-28
Quick Automation Profile	3-29
PolicyCheck	3-31
Denial of Service (DoS) function.....	3-33
Traffic Prioritization.....	3-34
How Traffic Prioritization Works.....	3-34
Traffic Prioritization Configuration.....	3-35
Configuring SNMP.....	3-37
Using Auto Warning	3-39
Using Diagnosis	3-42
Using Monitor.....	3-43
Using System Log	3-44
Using HTTPs/SSL	3-45
A. MIB Groups	A-1

1

Introduction

Welcome to the Moxa EDR-G903 Series of Gigabit Firewall/VPN secure routers designed for connecting Ethernet-enabled devices in industrial field applications.

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

The EDR-G903 series is a Gigabit speed, all-in-one Firewall/VPN/Router for Ethernet security applications in sensitive remote control and monitoring networks. The EDR-G903 supports one WAN, one LAN, and a user-configurable WAN/DMZ interface that provides high flexibility for different applications, such as WAN redundancy or Data/FTP server security protection.

The Quick Automation Profile function of the EDR-G903'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 EDR-G903 is shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative for assistance.

- 1 Moxa EDR-G903 secure router
- RJ45 to DB9 console port cable
- Protective caps for unused ports
- DIN-Rail mounting kit (attached to the EDR-G903's rear panel by default)
- Hardware Installation Guide (printed)
- CD-ROM with User's Manual and Windows Utility
- Moxa Product Warranty statement

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

Getting Started

This chapter explains how to access the EDR-G903 for the first time. There are three ways to access the switch: (1) serial console, (2) Telnet console, or (3) web browser. The serial console connection method, which requires using a short serial cable to connect the EDR-G903 to a PC's COM port, can be used if you do not know the EDR-G903's IP address. The Telnet console and web browser connection methods can be used to access the EDR-G903 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 EDR-G903's Console**
- ❑ **Using a Web Browser to Configure the EDR-G903**

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

NOTE Connection Caution!

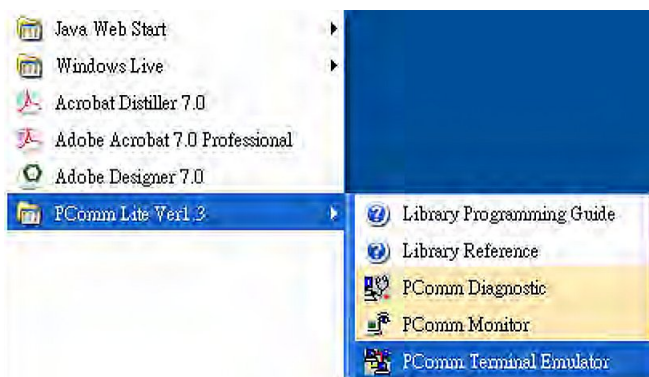
We strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your EDR-G903

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

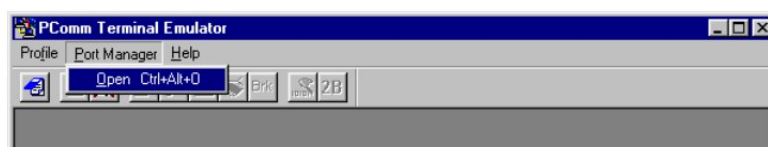
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the EDR-G903's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

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

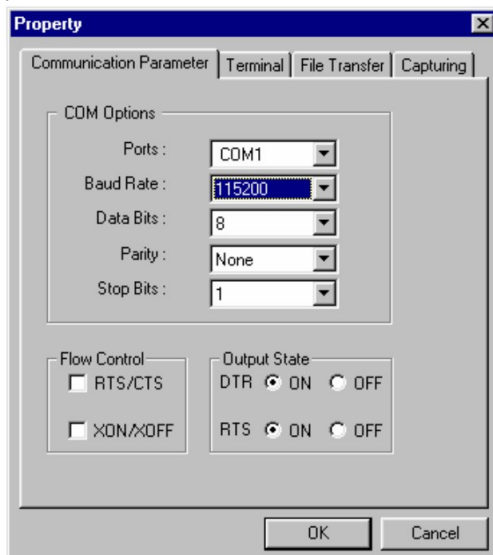
1. From the Windows desktop, click **Start → Programs → PCommLite1.3 → Terminal Emulator**.



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 for Console Connection, 115200 for Baud Rate, 8 for Data Bits, None for Parity, and 1 for Stop Bits



4. Click the **Terminal** tab, and select VT100 for Terminal Type. Click **OK** to continue.
5. Type **1** to select **ansi/VT100** terminal type, and then press **Enter**.
6. 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 (this is 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 EtherDevice Secure Router EDR-G903
Moxa Technologies Co., Ltd.

EDR-G903# _
```

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

```
EDR-G903#
disable      Switch the Admin mode to User mode
end          End current mode and change to enable mode
exit         Exit this consol mode connection
lan          Set the IP address of LAN interface
list         Print command list
no           Set the admin password to null
password     Set the admin password
ping         Send echo messages
quit         Exit this consol mode connection
reboot       Reboot this device
reload       Reload default configuration and reboot this device
show         Show running system information
ssh          Open a ssh connection
telnet       Open a telnet connection
EDR-G903# _
```

The following table shows a list of commands that can be used when the EDR-G903 is in console (serial or Telnet) mode:

Login by Admin account:

Command	Parameter/Example	Description
disable		Switch the Admin mode to User mode
exit/quit		Exit this consol mode connection
lan	lan ip address (A.B.C.D) netmask (A.B.C.D) Example: lan ip address 192.168.127.10 netmask 255.255.255.0	Set the IP address of LAN interface
list		Print command list
no	no password admin	Set the admin password to null
	no password user	Set the user password to null
password	password admin (password) Example: Password admin 1234	Set the admin password
	password user (password) Example: Password user 1234	Set the user password
ping	ping (IP address) Example: ping 192.168.127.10	Send echo message
reboot		Reboot this device
reload	default-config	Reload default configuration and Reboot this device
show	show lan	Show running system information

telnet	telnet (IP address) Example: telnet 192.168.127.10	Open a telnet connection
	telnet (IP address) (port number) Example: telnet 192.168.127.10 23	Open a telnet connection with port number
ssh	ssh (IP address) Example: ssh 192.168.127.10	Open a ssh connection

Login by User account:

Command	Parameter/Example	Description
exit/quit		Exit this consol mode connection
list		Print command list
ping	ping (IP address) Example: ping 192.168.127.10	Ping remote device via IP
show	show lan	Show running system information
ssh	ssh (IP address) Example: ssh 192.168.127.10	Open a ssh connection
telnet	telnet (IP address) Example: telnet 192.168.127.10	Open a telnet connection
	telnet (IP address) (port number) Example: telnet 192.168.127.10 23	Open a telnet connection with port number

Using Telnet to Access the EDR-G903's Console

You may use Telnet to access the EDR-G903'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 EDR-G903, you need to make sure that the PC host and the EDR-G903 are on the same logical subnet. To do this, check your PC host's IP address and subnet mask. By default, the EDR-G903's LAN IP address is 192.168.127.254 and the EDR-G903's 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.

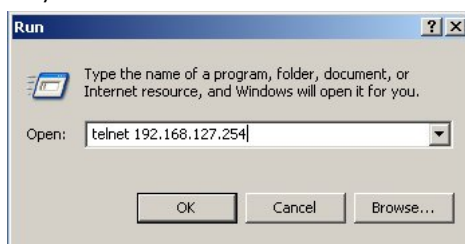
NOTE To use the EDR-G903's management and monitoring functions from a PC host connected to the same LAN as the EDR-G903, you must make sure that the PC host and the EDR-G903 are connected to the same logical subnet.

NOTE Before accessing the console utility via Telnet, first connect the EDR-G903'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 EDR-G903's default LAN IP address is 192.168.127.254.

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

1. Click Start (Run, and then telnet to the EDR-G903's IP address from the Windows Run window. (You may also issue the telnet command from the MS-DOS prompt.).



2. Refer to instructions 6 and 7 in the RS-232 Console Configuration (115200, None, 8, 1, VT100) section on page 2-3.

Using a Web Browser to Configure the EDR-G903

The EDR-G903's web browser interface provides a convenient way to modify the switch'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 EDR-G903's management and monitoring functions from a PC host connected to the same LAN as the EDR-G903, you must make sure that the PC host and the EDR-G903 are connected to the same logical subnet.

NOTE Before accessing the EDR-G903's web browser, first connect the EDR-G903'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.

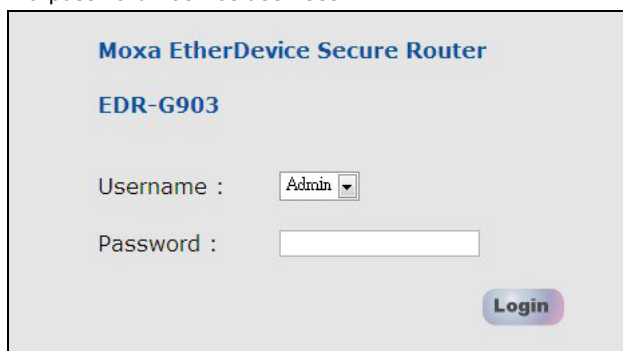
NOTE The EDR-G903's default LAN IP address is 192.168.127.254.

Perform the following steps to access the EDR-G903's web browser interface.

1. Start Internet Explorer and type the EDR-G903's LAN IP address in the Address field. Press Enter to establish the connection.



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



NOTE By default, the EDR-G903's password is not set (i.e., is blank).

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
www.moxa.com

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

Update

Interface Status				Recent 10 Event Log	
Interface	Mode	PPPoE	Status	Event	Time
Port 1(WAN)	Wan 1	N/A	Connect	LAN link off	2000/1/1,1:30:45
Port 2(Opt)	Wan 2	N/A	Disconnect	LAN link on	2000/1/1,2:18:14
Port 3(LAN)	LAN	N/A	Connect	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

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

Main Menu

Overview

- Basic Setting

- Network

- Communication Redundancy

- Routing

NAT

- Firewall Policy

- SNMP

- Traffic Prioritization

- Auto Warning

- Diagnosis

Monitor

- System Log



Best viewed with IE 5 above at resolution 1024 x 768

Features and Functions

In this chapter, we explain how to access the EDR-G903'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 EDR-G903, since you can both monitor the EDR-G903 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 EDR-G903's configuration and monitoring functions

The following topics are covered in this chapter:

- ❑ Configuring Basic Settings
 - System Identification
 - Accessible IP
 - Password
 - Time
 - SettingCheck
 - System File Update—by Remote TFTP
 - System File Update—by Local Import/Export
 - Restart
 - Reset to Factory Default
- ❑ Network Settings
 - WAN1 Configuration
 - WAN2 Configuration (includes DMZ Enable)
 - Using DMZ Mode
 - LAN Interface
 - DHCP Server
 - Static DHCP List
 - Dynamic DNS
- ❑ Communication Redundancy
 - How Dual WAN Backup Works
 - WAN Backup Configuration
- ❑ Static Routing
- ❑ Network Address Translation (NAT)
 - NAT Concept
 - N-to-1 NAT
 - Port Forwarding
 - 1-to-1 NAT
- ❑ Firewall Settings
 - Firewall Policy Concept
 - Firewall Policy Overview
 - Firewall Policy Configuration
 - Quick Automation Profile
 - PolicyCheck
 - Denial of Service (DoS) function
- ❑ Traffic Prioritization
 - How Traffic Prioritization Works
 - Traffic Prioritization Configuration
- ❑ Configuring SNMP
- ❑ Using Auto Warning
- ❑ Using Diagnosis
- ❑ Using Monitor
- ❑ Using System Log
- ❑ Using HTTPs/SSL

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 EDR-G903'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

Router Location

Router Description

Maintainer Contact Info

Web Configuration

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.	

Accessible IP

The EDR-G903 uses an IP address-based filtering method to control access to EDR-G903 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		

Activate

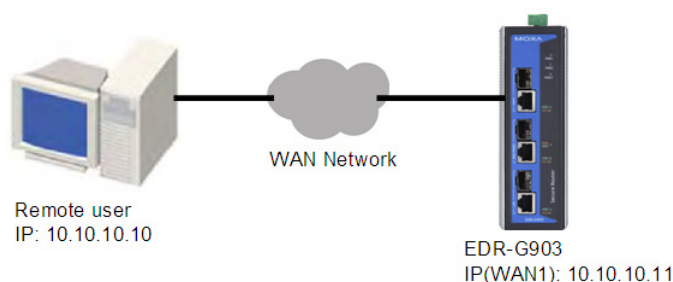
Accessible IP Settings allows you to add or remove "Legal" remote host IP addresses to prevent unauthorized access. Access to the EDR-G903 is controlled by IP address. If a host's IP address is in the accessible IP table, then the host will have access to the EDR-G903. You can allow one of the following 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 EDR-G903. (Disable this function by deselecting the Enable the accessible IP list option.)
- Any LAN can access the EDR-G903. (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 EDR-G903.

The following table shows additional configuration examples:

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

The Accessible IP list controls which devices can connect to the EDR-G903 to change the configuration of the device. In the example shown below, the Accessible IP list in the EDR-G903 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 EDR-G903'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 EDR-G903 provides two levels of access privilege: "admin privilege" gives read/write access to all EDR-G903 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

Activate



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.

The EDR-G903 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 EDR-G903 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 EDR-G903 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 know 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 EDR-G903 as a NTP/SNTP server on the network.

Enable Server synchronize

Enable this function to configure the EDR-G903 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 EDR-G903 will try to locate the 2nd NTP Server if the 1st NTP Server fails to connect.	

SettingCheck

Firewall Policy ☒

NAT Policy ☒

Accessible IP List ☒

Timer (sec)

Activate

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 policies, 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 EDR-G903 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 EDR-G903 and changes the accessible IP address to 10.10.10.12, or deselects the Enable checkbox accidentally after the remote user clicks the Activate button, connection to the EDR-G903 will be lost because the IP address is not in the EDR-G903'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 EDR-G903 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 EDR-G903 will roll back to the original Accessible IP List setting, allowing the remote user to reconnect to the EDR-G903 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 EDR-G903, 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.

Confirm

System File Update—by Remote TFTP

The EDR-G903 supports saving your configuration file to a remote TFTP server or local host to allow other EDR-G903 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 EDR-G903.

 **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 EDR-G903'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 EDR-G903's firmware file	None

Log File Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and filename of the EDR-G903'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 EDR-G903 to the local host.

Log File

Click **Export** to export the Log file of the EDR-G903 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.

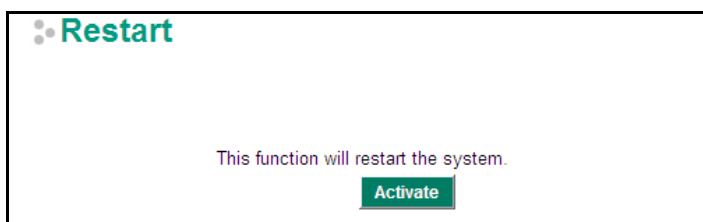
Upgrade Firmware

To import a firmware file into the EDR-G903, 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

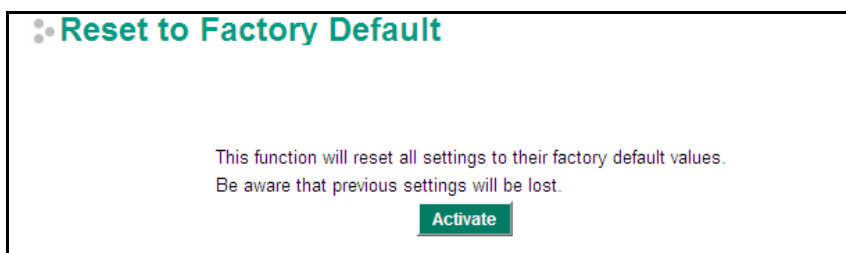
To import a configuration file to the EDR-G903, click **Browse** to select a configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking Import.

Restart



This function is used to restart the EDR-G903 router.

Reset to Factory Default



The **Reset to Factory Default** option gives users a quick way of restoring the EDR-G903'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 EDR-G903.

Network Settings

Network settings include the interface settings for WAN1, WAN2, DMZ, and LAN, and also include the DHCP Server, DHCP List, and Dynamic DNS settings.

WAN1 Configuration



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

User Name:

IP Address:

Password:

DNS (Optional for dynamic IP or PPPoE Type)

Server 1: Server 2: Server 3:

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

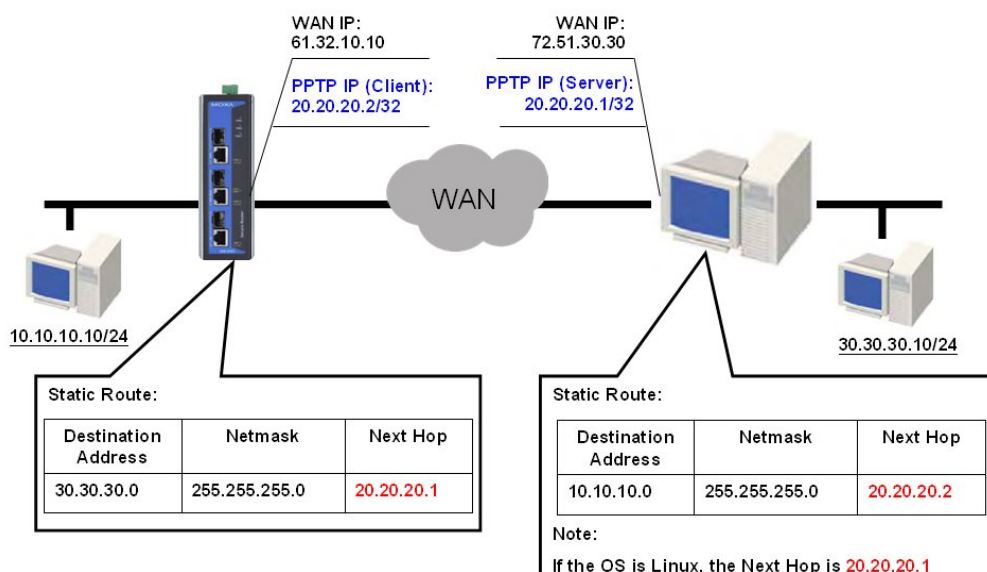
User Name

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.



DNS (Domain Name Server; optional setting for Dynamic IP and PPPoE types)***Server 1/2/3***

Setting	Description	Factory Default
IP Address	The DNS IP address	None

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

Detailed Explanation of Static IP Type

The screenshot shows the WAN1 Configuration page. Under the 'Connection' section, 'Connect Mode' is set to 'Enable' and 'Connect Type' is set to 'Static IP' (highlighted with a red circle). The 'Address Information' section shows fields for IP Address (0.0.0.0), Subnet Mask (0.0.0.0), and Gateway (0.0.0.0). The 'PPTP Dialup' section has 'PPTP Connection' set to 'Enable' and fields for IP Address (0.0.0.0), User Name, and Password. The 'DNS (Optional for dynamic IP or PPPoE Type)' section has three servers: Server 1 (192.168.2.1), Server 2 (0.0.0.0), and 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

The screenshot shows the WAN1 Configuration page. Under the 'Connection' section, 'Connect Mode' is set to 'Enable' and 'Connect Type' is set to 'PPPoE' (highlighted with a red circle). The 'PPPoE Dialup' section has fields for User Name, Password, and Host Name. The 'DNS (Optional for dynamic IP or PPPoE Type)' section has three servers: Server 1 (192.168.2.1), Server 2 (0.0.0.0), and 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:

Connection

Note that 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:

PPTP Dialup

PPTP Connection: ☐ Enable IP Address:

User Name: Password:

DNS (Optional for dynamic IP or PPPoE Type)

Server 1: Server 2: Server 3:

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

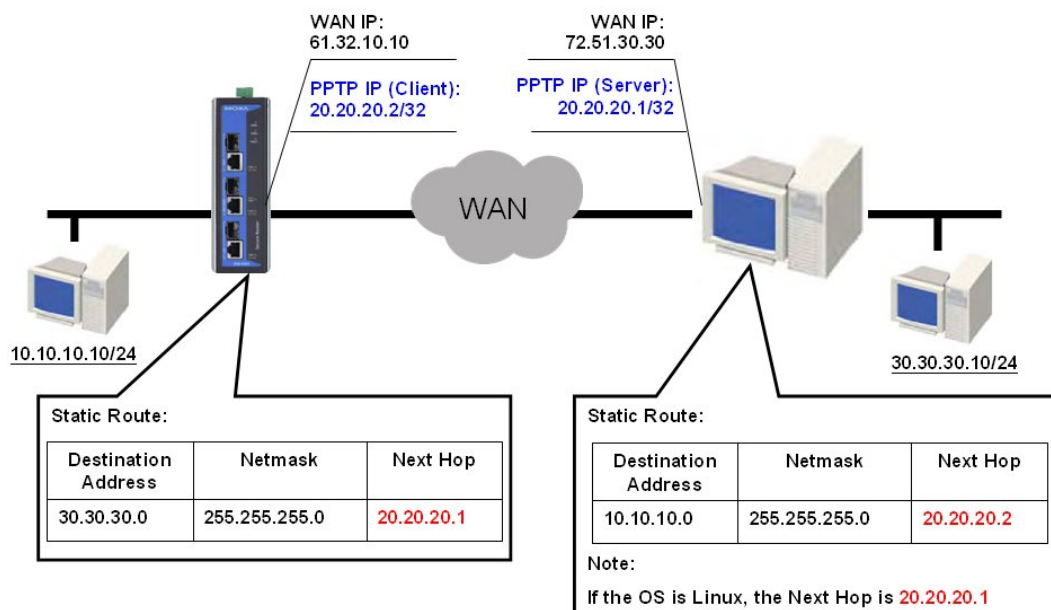
User name

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.

**DNS (Domain Name Server; optional setting for Dynamic IP and PPPoE types)****Server 1/2/3**

Setting	Description	Factory Default
IP Address	The DNS IP Address	None

NOTE The priority of a manually configured DNS will 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: **Static IP**

Address Information

IP Address: 192.168.1.1 Gateway: 0.0.0.0

Subnet Mask: 255.255.255.0

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

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:

PPPoE Dialup
 User Name:
 Host Name:
 Password:

DNS (Optional for dynamic IP and PPPoE Type)
 Server 1: Server 2: Server 3:

PPPoE Dialup**User Name**

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

Host Name

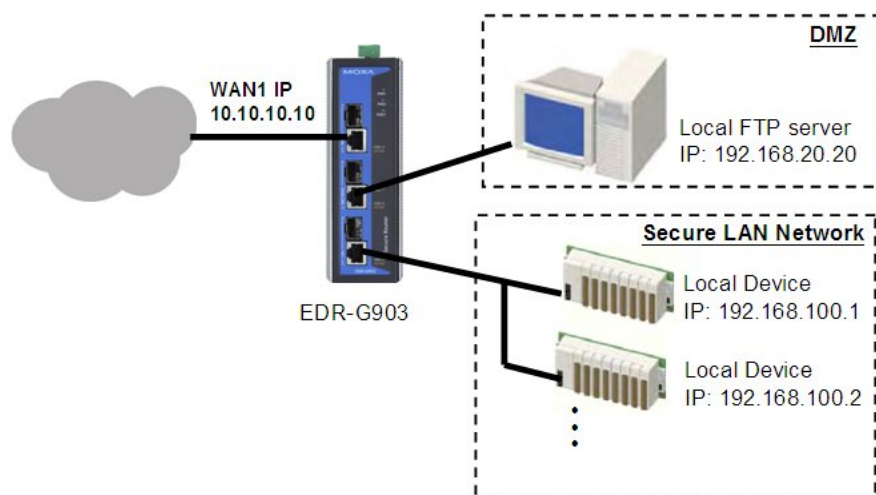
Setting	Description	Factory Default
Max. 30 characters	User-defined host name for this PPPoE server	None

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

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)

Activate
Cancel

LAN IP Configuration

IP Address

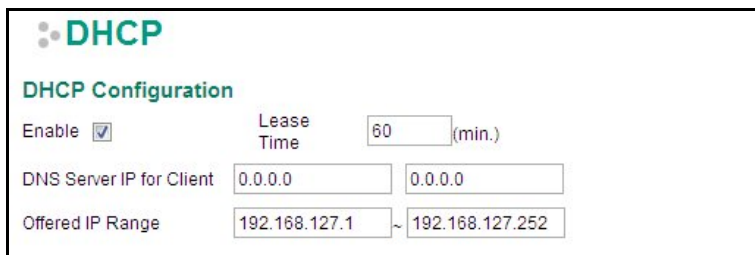
Setting	Description	Factory Default
IP Address	The LAN interface IP address	192.168.127.254

Subnet Mask

Setting	Description	Factory Default
IP Address	The subnet mask	255.255.255.0

DHCP Server

The EDR-G903 provides a DHCP (Dynamic Host Configuration Protocol) server function for LAN interfaces. When configured, the EDR-G903 will automatically assign an IP address to a Ethernet device from a defined IP range.



DHCP Configuration

Enable ☒ Lease Time (min.)

DNS Server IP for Client

Offered IP Range ~

DHCP configuration

DHCP Server Enable/Disable

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

Lease Time

Setting	Description	Factory Default
≥ 5 min.	The lease time of the DHCP server	60 (min.)

DNS Server IP for Client

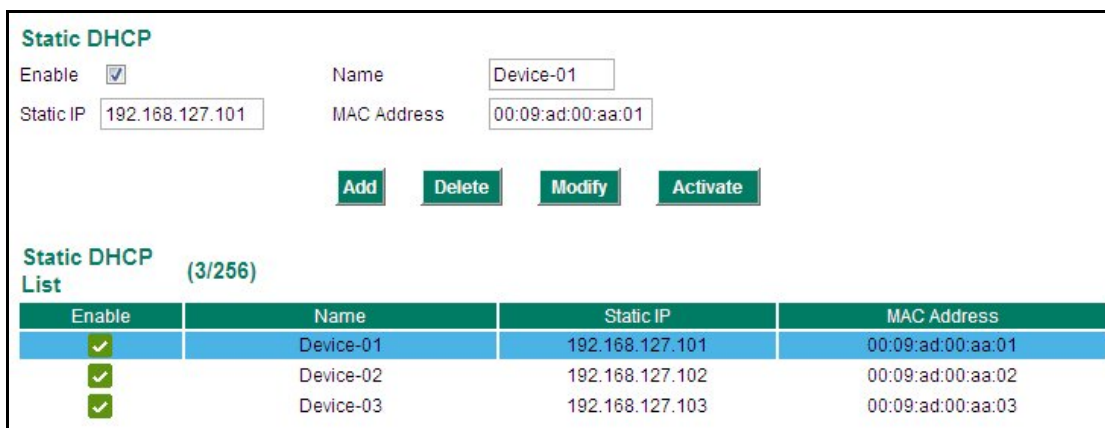
Setting	Description	Factory Default
IP Address	The DHCP server's IP address	None

Offered IP Range

Setting	Description	Factory Default
IP address	The offered IP address range for the DHCP server	192.168.127.1 to 192.168.127.252

Static DHCP List

Use the Static DHCP list to ensure that devices connected to the EDR-G903 always use the same IP address. The static DHCP list matches IP addresses to MAC addresses.



Static DHCP

Enable ☒ Name Static IP MAC Address

Static DHCP List (3/256)

Enable	Name	Static IP	MAC Address
☒	Device-01	192.168.127.101	00:09:ad:00:aa:01
☒	Device-02	192.168.127.102	00:09:ad:00:aa:02
☒	Device-03	192.168.127.103	00:09:ad:00:aa:03

In the above example, a device named "Device-01" was added to the Static DHCP list, with static IP address set to 192.168.127.101 and MAC address set to 00:09:ad:00:aa:01. When a device with MAC address of 00:09:ad:00:aa:01 is connected to the EDR-G903, the EDR-G903 will offer the IP address 192.168.127.101 to this device.

Enable or Disable

Setting	Description	Factory Default
Enable or Disable	Enable or Disable the selected device in the Static DHCP List	Disabled

Name

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

Static IP Address

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

MAC Address

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

Clickable Buttons

Add: Use the Add button to input a new DHCP list. The Name, Static IP, and MAC address must be different than for the existing list.

Delete: Use the Delete button to delete the 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.

Dynamic DNS

Dynamic DNS (Domain Name Server) allows you to use a domain name (e.g., moxa.edr-g903) to connect to the EDR-G903. The EDR-G903 can connect to 4 free DNS servers and register the user configurable Domain name in these servers.

Service

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

User Name

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

Password

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

Verify Password

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

Domain name

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

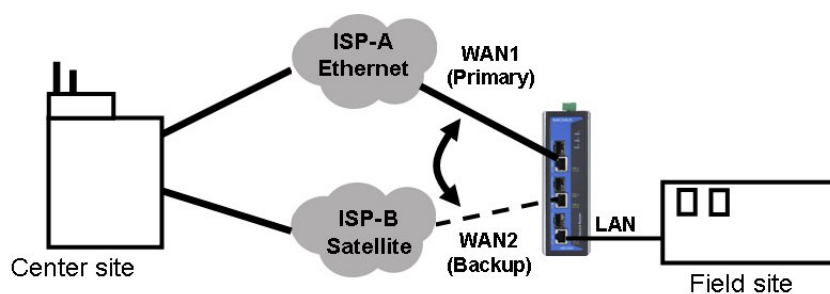
Communication Redundancy

Use the EDR-G903's WAN backup function for dual WAN redundancy applications. The EDR-G903 has two WAN interfaces: WAN1 is the primary WAN interface and WAN2 is the backup interface. When the EDR-G903 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.

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 EDR-G903's WAN backup function checks the link status and the connection integrity between the EDR-G903 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 EDR-G903, 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

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

Link Check ☐

Ping Check ☐

IP

Interval sec (1~1000)

Retry (1~100)

Timeout 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 EDR-G903 to a specified IP address.	Disabled

IP

Setting	Description	Factory Default
IP address	The EDR-G903 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 EDR-G903 will activate the backup path.	3

Timeout

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

Static Routing

The Static Routing page is used to configure the EDR-G903's static routing table.

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 EDR-G903's routing table until you click the Activate button.

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 EDR-G903 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 EDR-G903 is 128.

N-to-1 NAT

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

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

Enable	☒	LAN IP Range	192.168.127.1 ~ 192.168.127.252
NAT Mode	N-1	WAN IP	0.0.0.0
Interface	Auto		

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	Select the NAT types	N-1
1-1		
Port Forwarding		

Interface (N-1 mode)

Setting	Description	Factory Default
Auto	Select the Interface for this NAT Policy	Auto
WAN1		
WAN2		

The EDR-G903 provides a Dual WAN backup function for communication 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

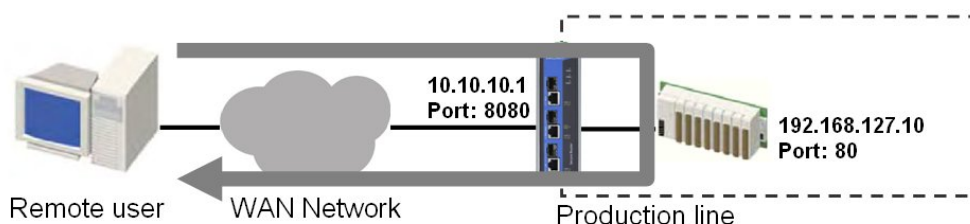
NOTE The EDR-G903 will add an N-1 policy from the source IP, 192.168.127.1 to 192.168.127.252 to the WAN1 interface after activating the Factory Default.

Port Forwarding

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 EDR-G903 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 be able to initiate a connection from the internal network to the external network.



Enable	☒	Protocol	TCP
NAT Mode	Port Forward	WAN Port	
Interface	WAN1	LAN/DMZ IP	
		LAN/DMZ Port	

Enable/Disable NAT policy

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

NAT Mode

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

Interface (Port Forward mode)

Setting	Description	Factory Default
WAN1	Select the Interface for this NAT Policy	WAN1
WAN2		

Protocol (Port Forward mode)

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

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)

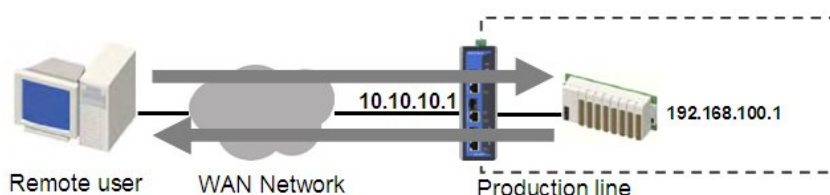
Setting	Description	Factory Default
IP Address	The translated IP address in the internal network	None

LAN/DMZ Port (Port Forward mode)

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

1-to-1 NAT

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

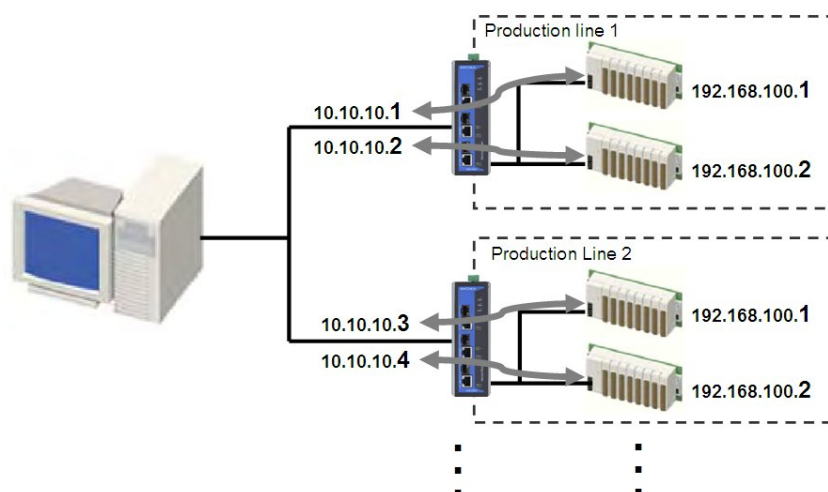


1-to-1 NAT is usually used when you have a group of internal servers with private IP addresses that must connect to the external network. You can use 1-to-1 NAT to map the internal servers to public IP addresses. The IP address of the internal device will not change.

The figure below illustrates how a user could extend production lines and the private IP addresses of internal devices. 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.

NAT List

Enable	Index	IF	Protocol	Source IP	Source Port	Destination IP
✓	1	WAN1	--	192.168.100.1	--	10.10.10.1
✓	2	WAN1	--	192.168.100.2	--	10.10.10.2
✓	3	WAN1	--	192.168.100.3	--	10.10.10.3
✓	4	WAN1	--	192.168.100.4	--	10.10.10.4



Enable	☒	LAN/DMZ IP	
NAT Mode	1-1	WAN IP	
Interface	WAN1		

Enable/Disable NAT policy

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

NAT Mode

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

Interface (1-1 NAT type)

Setting	Description	Factory Default
WAN1	Select the Interface for this NAT Policy	WAN1
WAN2		

LAN/DMZ IP (1-1 NAT type)

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

WAN IP (1-1 NAT type)

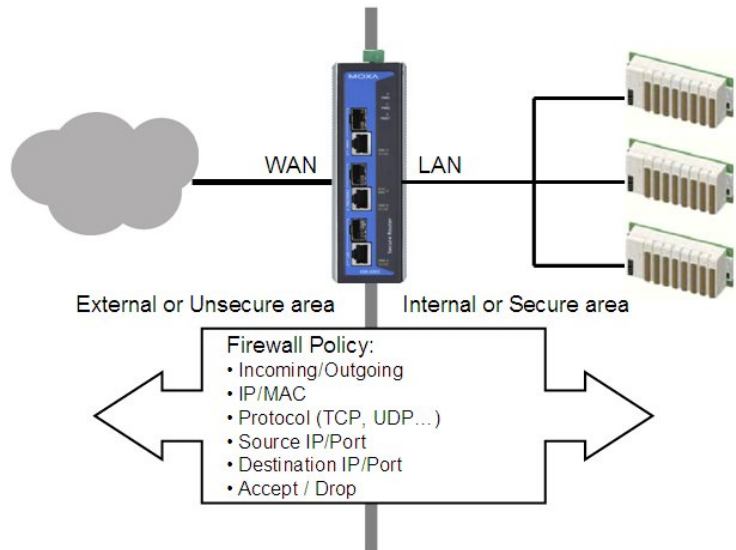
Setting	Description	Factory Default
IP Address	Select the external IP address in WAN network area	None

NOTE The EDR-G903 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.

Firewall Settings

Firewall 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).



Firewall Policy Overview

The EDR-G903 provides a Firewall Policy Overview that lists firewall policies by interface direction.

Interface

From

LAN

To

All

Show

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 Policy Configuration

The EDR-G903's Firewall policy provides secure traffic control, allowing users to control network traffic based on the following parameters.

Enable ☒	Targets ACCEPT
Interface From All To All	Source IP All
Protocol All	Source Port All
Service IP Filter	Destination IP All
	Destination Port All

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		

Quick Automation Profile

Setting	Description	Factory Default
Refer to the "Quick Automation Profile" section on page 3-29.	Select the Protocol parameters in this Firewall Policy	None

Service

Setting	Description	Factory Default
IP Filter	This Firewall policy will filter by IP address	IP Filter
MAC Filter	This Firewall policy will filter by MAC address	

Target

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 matches 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 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	

Source 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 EDR-G903'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 or drop 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-G903 is 256.

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 EDR-G903 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.

Enable ☒

Interface From To

Protocol

Service

Targets

Source IP

Source Port

Destination IP

Destination Port

Filter List									
Enable	Index	Input	Output	Protocol	Source IP	Source Port	Destination IP	Destination Port	
☒	1	All	All	Modbus tcp/ip (TCP)	All	All	All	502	

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

PolicyCheck

The EDR-G903 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 EDR-G903 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**.

Mask: Policy [X] is masked by Policy [Y]

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.

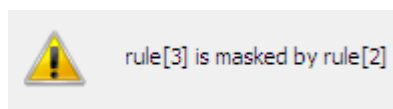
For example, two firewall policies are shown below:

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 EDR-G903 will issue a message informing the user that policy [3] is **masked** by policy [2] because the IP range of policy [3] is smaller than the IP range of policy [2], and the Target action is different.



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

The Source/Destination IP range or Source/Destination port number of policy [X] is less than or equal to policy [Y], and the action target (Accept/Drop) is the same. In this case policy [X] will increase the loading of the EDR-G903 and lower its performance.

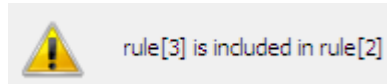
For example, two firewall policies are shown in the following table:

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 EDR-G903 will issue a message informing the user that policy [3] is **included** in policy [2] because the IP range of policy [3] is smaller than the IP range of policy [2], and the Target action is the same.



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

Two firewall policy configurations, such as Source IP, Destination IP, Source port, and Destination port, in policy [X] and policy [Y] are masked, and the action target (Accept/Drop) is different.

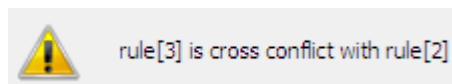
For example, two firewall policies are shown in the following table:

Index	Input	Output	Protocol	Source IP	Destination IP	Target
1	WAN1	LAN	All	10.10.10.10	192.168.127.10	ACCEPT
2	WAN2	LAN	All	20.20.20.20 to 20.20.20.30	192.168.127.25	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 EDR-G903 will issue a message informing the user that policy [3] is in **Cross Conflict** with policy [2].



Denial of Service (DoS) function

The EDR-G903 provides 9 different DoS functions for detecting or defining abnormal packet format or traffic flow. The EDR-G903 will drop the packets when it detects an abnormal packet format. The EDR-G903 will also monitor some traffic flow parameters and activate the defense process when abnormal traffic conditions are detected.

☐ Null Scan	
☐ Xmas Scan	
☐ NMAP-Xmas Scan	
☐ SYN/FIN Scan	
☐ FIN Scan	
☐ NMAP-ID Scan	
☐ SYN/RST Scan	
☐ ICMP-Death	Limit: 4000 (pkt/s)
☐ SYN-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

ICMP-Death

Setting	Description	Factory Default
Enable or Disable	Enable or disable the ICMP-Death defense	None
Packet/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
Packet/Second	The limit value to activate SYN-Flood defense	None

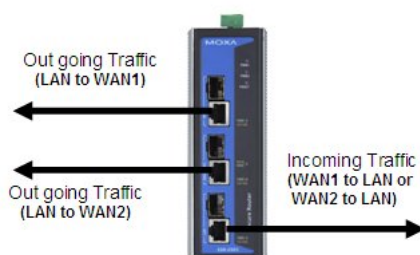
Traffic Prioritization

The EDR-G903's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network.

NOTE The maximum number of Firewall policies for the EDR-G903 is 256.

How Traffic Prioritization Works

The EDR-G903 provides four different priorities levels (0-3, high to low) for incoming and outgoing traffic. The following figure illustrates incoming traffic, which refers to the traffic transmitted from WAN1 to LAN or WAN2 to LAN interface. Outgoing traffic refers to the traffic transmitted from LAN to WAN1 or from LAN to WAN2.



The following figures show the configuration for incoming and outgoing traffic. Users can manage the priority of incoming traffic (WAN1 to LAN and WAN2 to LAN) and outgoing traffic (LAN to WAN1 and LAN to WAN2).

Incoming Traffic Configuration (WAN1/2 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 WAN1)			
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 WAN2)			
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)	

Traffic Prioritization Configuration

Enable or Disable

Setting	Description	Factory Default
Enable or Disable	Enable or disable the Traffic Prioritization function	Disabled

Max. Bandwidth

Setting	Description	Factory Default
1 to 1,000,000 KBytes/s	The maximum bandwidth for total incoming or outgoing traffic	100 KBytes/s

Default Priority

Setting	Description	Factory Default
Priority 0/1/2/3	A packet without matching any incoming/outgoing policy will adhere to the default priority	Priority 3

Minimum Bandwidth of Priority 0/1/2/3

Setting	Description	Factory Default
1 to 1,000,000 KBytes/s	The minimum bandwidth for Priority 0/1/2/3	Priority 0: 10 KBytes/s Priority 1: 20 KBytes/s Priority 2: 30 KBytes/s Priority 3: 40 KBytes/s

Maximum Bandwidth of Priority 0/1/2/3

Setting	Description	Factory Default
1 to 1,000,000 KBytes/s	The maximum bandwidth for Priority 0/1/2/3	Priority 0: 10 KBytes/s Priority 1: 20 KBytes/s Priority 2: 30 KBytes/s Priority 3: 40 KBytes/s

Outgoing/Incoming Policy Setup

After configuring the minimum/maximum bandwidth for each priority, users can set up the incoming or outgoing policies for Ethernet traffic, providing the setup meets all of the following conditions:

Enable	☒	Targets	Priority 3
To	All	Source IP	Single 192.168.127.13
Protocol	All	Source Port	All
Service	By IP	Destination IP	All
		Destination Port	All

Enable or Disable

Setting	Description	Factory Default
Enable or Disable	Enable or disable this Incoming or Outgoing Policy	Disabled

Packet To / From

Setting	Description	Factory Default
All (WAN1 or WAN2)	Select the direction of Ethernet traffic for this policy	All
WAN1	To: For outgoing policy	
WAN2	From: For incoming policy	

Protocol

Setting	Description	Factory Default
All (TCP/UDP/ICMP)	Select the Protocol for in this Policy	All
TCP		
UDP		
ICMP		

Service

Setting	Description	Factory Default
By IP	Select the service type (IP address or MAC address) for this policy	By IP
By MAC		

Target

Setting	Description	Factory Default
Priority 0/1/2/3	Select the priority for this policy	Priority 0

Source IP

Setting	Description	Factory Default
All (IP Address)	Select the Source IP address for this policy	All
Single (IP Address)		
Range (IP Address)		

Source Port

Setting	Description	Factory Default
All (Port number)	Select the Source port number for this policy	All
Single (Port number)		
Range (Port number)		

Destination IP

Setting	Description	Factory Default
All (IP Address)	Select the Destination IP address for this policy	All
Single (IP Address)		
Range (IP Address)		

Destination Port

Setting	Description	Factory Default
All (Port number)	Select the Destination port number for this policy	All
Single (Port number)		
Range (Port number)		

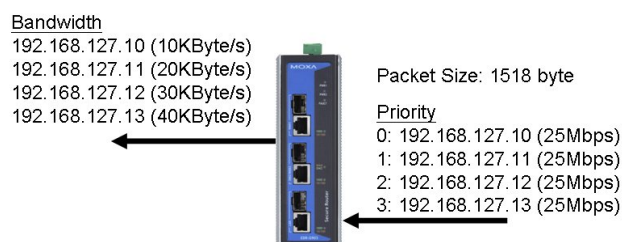
The following table shows the management of outgoing traffic. The maximum bandwidth from LAN to WAN is 100 Kbytes. 10 Kbyte is reserved for traffic that matches the parameters of Priority 0. 20 Kbytes is reserved for traffic that matches the parameters of priority 2 and so forth.

Outgoing Traffic Configuration (LAN to WAN1)			
Enable	☒		
MAX. Bandwidth:	100	(KByte/s)	
Default Priority	Priority 3		
Priority 0:	MIN. BW 10	MAX. BW 100	(KByte/s)
Priority 1:	MIN. BW 20	MAX. BW 100	(KByte/s)
Priority 2:	MIN. BW 30	MAX. BW 100	(KByte/s)
Priority 3:	MIN. BW 40	MAX. BW 100	(KByte/s)

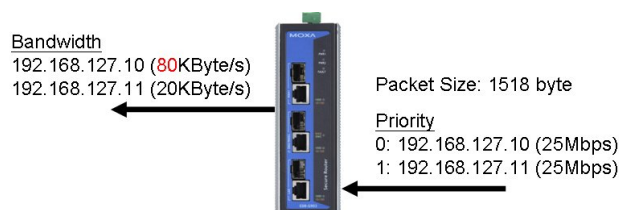
Set up the outgoing policies as below:

Index	Output	Protocol	Source IP	Source Port	Destination IP	Destination Port	MAC Address	Targets
1	WAN1	All	192.168.127.10	All	All	All	--	Priority 0
2	WAN1	All	192.168.127.11	All	All	All	--	Priority 1
3	WAN1	All	192.168.127.12	All	All	All	--	Priority 2
4	WAN1	All	192.168.127.13	All	All	All	--	Priority 3

The EDR-G903 will manage the bandwidth for outgoing packets. Based on the four outgoing policies below, when the source IP of the Ethernet traffic matches the outgoing policies, the maximum bandwidth for a packet sent from these source IP addresses will be reserved by its target priority.



If there are only two kinds of traffic packets, priority 0 and priority 1, then transmission will proceed from LAN to WAN1, and the EDR-G903 will reserve the minimum bandwidth (10 KBytes/s and 20 Kbyte/s) based on these two different IP addresses. In this case, there are still 100 KBytes/s - 10 KBytes/s - 20 KBytes/s = 70 KBytes/s that do not belong to any priority. So, the EDR-G903 will increase the bandwidth from highest priority (0) to lowest priority (3). The EDR-G903 will add this 70 KBytes/s bandwidth to priority 0 because the maximum bandwidth of priority 0 is 100 KBytes/s. The following figure shows the bandwidth arrangement of the EDR-G903 based on this configuration.



Configuring SNMP

The EDR-G903 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 EDR-G903 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 on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

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

SNMP Read Settings

System Information

SNMP Versions

Contact Person

Auth. Type

Data Encryption Key

Community

Community Name 1

Access Control 1

Community Name 2

Access Control 2

Trap Targets

Target IP Address 1 (ex. xxx.xxx.xxx.xxx)

Target IP Address 2

Target IP Address 3

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

Contact Person

Setting	Description	Factory Default
Admin or user	Admin privilege allows access and authorization to read and write the MIB file. User privilege only allows reading the MIB file, but does give authorization to write.	Admin

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.	

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 1/2

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

Access Control

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

Target IP Address

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

SNMP Trap Type

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
WAN1	☐	☐
WAN2	☐	☐
LAN	☐	☐

SNMP Trap Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the router, whereas Port Events are related to the activity of a specific port.

System Events	SNMP Trap is sent when...
Cold Start	Power is cut off and then reconnected.
Warm Start	The EDR-G903 is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On-Off)	The EDR-G903 is powered down.
Power Transition (Off-On)	The EDR-G903 is powered up.
DI (Off)	Digital Input is triggered by an on to off transition
DI (On)	Digital Input is triggered by an off to on transition
Config. Change	A configuration item has been changed.
Auth. Failure	An incorrect password is entered.

Port Events	SNMP Trap 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).

Using Auto Warning

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet 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 EDR-G903 supports different approaches to warn engineers automatically, such as by using email and relay output. It also supports one digital input to integrate sensors with your system and automate alarms using email and relay output.

Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place. Three basic steps are required to set up the Auto Warning function:

1. Configure Email Event Types

Select the desired Event types from the Web Browser **Event type** page (a description of each event type is given later in the Email Alarm Events setting subsection).

2. Configure Email Settings

To configure the EDR-G903's email setup from a browser interface, enter your Mail Server's IP/Name (IP address or name), Account Name, Account Password, the sender's email address, and the email address to which warning messages will be sent.

3. Activate your settings and if necessary, test the email

After configuring and activating your EDR-G903's Event Types and Email Setup, you can use the Test Email function to see if your e-mail addresses and mail server address have been properly configured.

Event Type

Email Warning 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	☐	☐

Email Warning Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the router, whereas Port Events are related to the activity of a specific port.

System Events	Warning email is sent when...
Cold Start	Power is cut off and then reconnected.
Warm Start	The EDR-G903 is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On-Off)	The EDR-G903 is powered down.
Power Transition (Off-On)	The EDR-G903 is powered up.
DI (Off)	Digital Input is triggered by on to off transition
DI (On)	Digital Input is triggered by off to on transition
Config. Change	A configuration item has been changed.
Auth. Failure	An incorrect password is entered.

Port Events	Warning email 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).

E-mail Setup

Email Warning Events Settings

Email Alert Configuration

Email (SMTP) Server Address:

PORT:

User Name:

Password:

Sender Address:

1st Recipient Address:

2nd Recipient Address:

3rd Recipient Address:

4th Recipient Address:

Main Server IP/Name

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

Port

Setting	Description	Factory Default
Port number	The port number of your email server.	None

Account Name

Setting	Description	Factory Default
Max. 30 Characters	Your email account name (typically your user name)	None

Email Password

Setting	Description	Factory Default
Max. 30 characters	The Password of your email account	None

Sender Email Address

Setting	Description	Factory Default
IP address	The IP Address of the email sender	None

Recipient Email Address

Setting	Description	Factory Default
Max. 50 characters	You can set up to 4 email addresses to receive alarm emails from the EDR-G903.	None

Send Test Email

After configuring the email settings, you should first click **Activate** to activate those settings, and then click **Send Test Email** to verify that the settings are correct.

NOTE Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PLAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism. We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.

Configuring Relay Warning

The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

1. Configuring Relay Event Types

Select the desired **Event types** from the Web Browser Event type page (a description of each event type is given later in the Relay Alarm Events setting subsection).

2. Activate your settings

After completing the configuration procedure, you will need to activate your EDR-G903's Relay Event Types.

Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the router, whereas Port Events are related to the activity of a specific port.

System Events	Warning Relay output is triggered when...
Power Input 1 failure (On→Off)	Power input 1 is down.
Power Input 2 failure (On→Off)	Power input 2 is down.
DI (Off)	Digital Input is triggered by on to off transition
DI (On)	Digital Input is triggered by off to on transition

Port Events	Warning Relay output is triggered when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out or the opposing device shuts down).
Ignore	Ignore the status of the port

Override relay alarm settings

Select this option to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition.

Warning List

Use this table to see if any relay alarms have been issued.

Current Warning List	
Index	Event
1	WAN2 Link Off !
2	WAN1 Link Off !

Using Diagnosis

The EDR-G903 provides **Ping** tools and **LLDP** for administrators to diagnose network systems.

Ping

Interface

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 EDR-G903 itself. In this way, the user can essentially control the EDR-G903 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 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.

General Settings

LLDP

Message Transmit Interval

Port Events

Port	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System
Activate Cancel				

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.

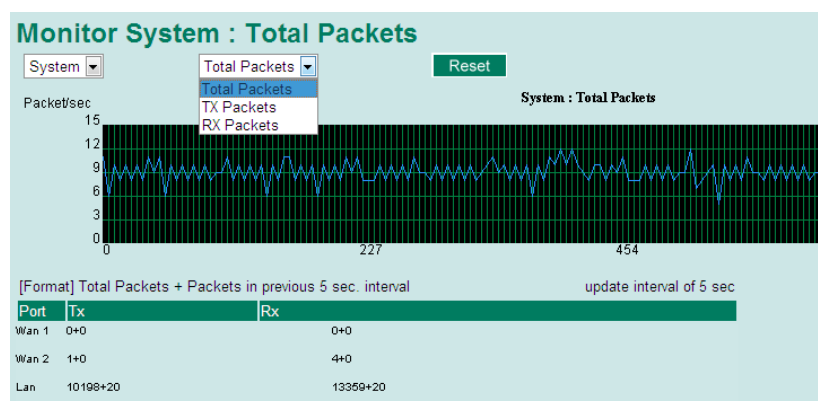
Neighbor System: Hostname of the neighbor device.

Using Monitor

You can monitor statistics in real time from the EDR-G903's web console.

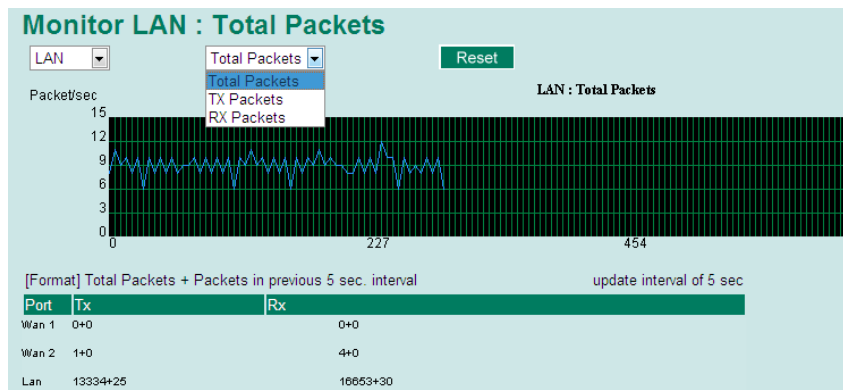
Monitor by System

Access the Monitor by selecting "System" from the left selection bar. Monitor by System allows the user to view a graph that shows the combined data transmission activity of all the EDR-G903's 3 ports. Click one of the three options—Total Packets, TX Packets or RX Packets—to view transmission activity of specific types of packets. Recall that TX Packets are packets sent out from the EDR-G903, and RX Packets are packets received from connected devices. The Total Packets option displays a graph that combines TX and RX activity. The graph displays data transmission activity by showing **Packets/s** (i.e., packets per second, or pps) versus **sec.** (seconds). The graph is updated every few seconds, allowing you to analyze data transmission activity in real time.



Monitor by Port

Access the Monitor by Port function by selecting the WAN1, WAN2, or LAN interface from the left drop-down list. You can view graphs that show All Packets, TX Packets, or RX Packets, but in this case, only for an individual port. The graph displays data transmission activity by showing **Packets/s** (i.e., packets per second, or pps) versus **sec.** (seconds). The graph is updated every few seconds, allowing you to analyze data transmission activity in real time.



Using System Log

The EDR-G903 provides **EventLog** and **Syslog** functions to record important events.

Using 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 EDR-G509 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 EDR-G903 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_Bandwidth	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.

Using 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 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

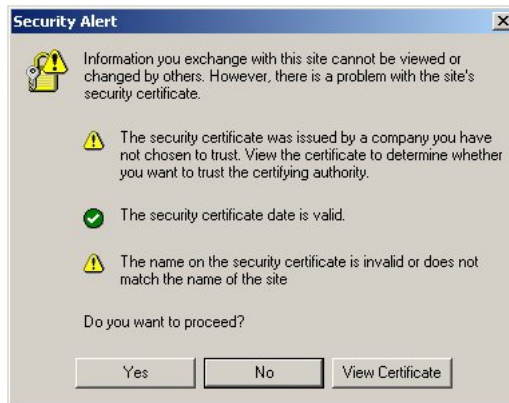
Using HTTPs/SSL

To secure your HTTP access, the EDR-G903 supports HTTPS/SSL to encrypt all HTTP traffic. Perform the following steps to access the EDR-G903's web browser interface via HTTPS/SSL.

1. Open Internet Explorer and type `https://<EDR-G903's IP address>` in the address field. Press Enter to establish the connection.



2. A warning message will appear to warn the user that the security certificate was issued by a company they have not chosen to trust.



3. Select **Yes** to enter the EDR-G903's web browser interface and access the web browser interface secured via HTTPS/SSL.

MIB Groups

The EDR-G903 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 EDR-G903 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 EDR-G903 also provides a MIB file, located in the file "Moxa-EDRG903-MIB.my" on the EDR-G903 Series utility CD-ROM for SNMP trap message interpretation