

# VPort 704 User's Manual

---

First Edition, December 2010

[www.moxa.com/product](http://www.moxa.com/product)



© 2010 Moxa Inc. All rights reserved.

Reproduction without permission is prohibited.

# VPort 704 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](http://www.moxa.com/support)

### **Moxa Americas**

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

### **Moxa Europe**

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

### **Moxa China (Shanghai office)**

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

### **Moxa Asia-Pacific**

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

# Table of Contents

<b>1. Introduction</b>	<b>1</b>
Overview	2
Package Checklist	2
Features	2
Slot Modules	3
Recommended Accessories	3
<b>2. Getting Started</b>	<b>1</b>
RS-232 Console Configuration (115200, None, 8, 1, VT100)	2
Configuration using a Web Console	4
Network Environment with DHCP Server	4
Using the VPort 700 Utility (VPort700Utility.exe)	5
Network Environment without DHCP Server	6
<b>3. Featured Functions</b>	<b>1</b>
System Configuration by Web Console	2
Homepage	2
All Module List	2
Slot Module Information	3
System Information	3
System Time	4
Account	5
Accessible IP	6
SNMP	7
System IP	10
Device IP Settings	11
DHCP Relay Agent	12
Port Configuration	14
Port Monitor	15
Mirror Port	16
Rate Limiting	17
IEEE 802.1X	17
Port Lock	20
Port Access Table	20
Communication Redundancy	21
The STP/RSTP Concept	21
QoS	35
VLAN	37
IGMP	40
GMRP (GARP Multicast Registration Protocol)	44
Static Multicast MAC	45
Line Swap	46
Firmware Upgrade	47
Configuration Import/ Export	47
Factory Default	47
Reboot	48
Log History	48
Sys log	49
Email Alarm	49
Relay Alarm Event	52
Slot Configuration Maintenance	53
Slot Operation	54
Slot IP Settings	54
Slot Network Configure	55
Slot Monitor	55
Slot Test	55
Slot Event Log List	56
Slot Alarm Trigger	56
<b>4. VPort 700 Utility GUI</b>	<b>1</b>
Starting VPort 700 Utility	2
Broadcast Search	2
Search by IP address	3
Upgrade Firmware	3
Modify IP Address	4
Export Configuration	5
Import Configuration	6
Convert	7
<b>A. Modbus Address Table</b>	<b>1</b>

# Introduction

---

Welcome to the **Moxa VPort 704 Series industrial multi-service gateway**, an Ethernet gateway that provides a versatile communication interface and the convenience of a modular design.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Features**
  - Slot Modules
  - Recommended Accessories

## Overview

The VPort 704 series modular industrial multi-service gateways come with 3 built-in Gigabit ports, 3 10/100 Mbps fast Ethernet ports, and 4 slots with Ethernet, serial, or power interface. The 4 slots accept a versatile assortment of communications modules, including an IP video encoder (VPM-7304), serial-to-Ethernet module (VPM-7704), and other modules that adhere to the design rules for VPort 704 modules. The modular design turns the VPort 704 into an extremely versatile communications interface, and makes the VPort 704 particularly well suited for use at field sites. The VPort 704's -40 to 75°C wide operating temperature, metal housing, passive backplane, and fanless design make it particularly well suited for harsh industrial environments and mission-critical applications, including oil and gas, trackside, and city traffic monitoring systems.



## Package Checklist

The VPort 704 is shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative for assistance.

- 1 VPort 704
- Quick Installation Guide
- CD-ROM with User's Manual and Windows Utility
- Moxa Product Warranty Statement

## Features

### Rugged Hardware Design:

- Hot swappable for easy installation and maintenance
- Passive backplane and fanless design for high MTBF
- Capable of operating in a -40 to 75°C temperature (-T model)
- Aluminum housing with DIN-Rail or panel mounting
- 24 VDC redundant power input
- CE, FCC, UL508, NEMA TS2 compliance

### Function Features:

- 3 combo Gigabit Ethernet ports for backbone communication
- 3 10/100 Mbps fast Ethernet ports for connecting IP devices, such as an IP camera or IP phone
- Supports Turbo Ring V1/V2, RSTP
- Supports IGMP snooping/GMRP, VLAN, SNMP V1/V2c/V3
- Supports Rate Limiting

- Supports Line swap fast recovery
- 1 RS-232 console port for console management
- Single web console for module configurations
- Supports DHCP and Opt82 IP settings
- Supports traffic monitoring
- Supports firmware upgrading and configuration backup for all modules
- Supports system alarms for power failure and module failure
- Supports one relay output for system alarms
- Power your modules on and off the remotely
- LED indicator for power, system status, ring topology, and fault

## Slot Modules

### VPM-7304: 4-channel MPEG4/ MJPEG video encoder module



### VPM-7704: 4-port RS-232/422/485 device server module



## Recommended Accessories

- **SFP-1GSXLC**: Small form factor pluggable transceiver with 1000BaseSX, LC, 0.5 km, 0 to 60°C
- **SFP-1GSXLC-T**: Small form factor pluggable transceiver with 1000BaseSX, LC, 0.5 km, -20 to 75°C
- **SFP-1GLXLC**: Small form factor pluggable transceiver with 1000BaseLX, LC, 10 km, 0 to 60°C
- **SFP-1GLXLC-T**: Small form factor pluggable transceiver with 1000BaseLX, LC, 10 km, -40 to 75°C
- **SFP-1GLHXLC**: Small form factor pluggable transceiver with 1000BaseLHX, LC, 40 km, 0 to 60°C
- **SFP-1GLHXLC-T**: Small form factor pluggable transceiver with 1000BaseLHX, LC, 40 km, -40 to 75°C
- **SFP-1GZXLC**: Small form factor pluggable transceiver with 1000BaseZX, LC, 80 km, LC, 0 to 60°C
- **DR-4524**: 45W/2A DIN-Rail 24 VDC power supply with 85 to 264 VAC input
- **DR-75-24**: 75W/3.2A DIN-Rail 24 VDC power supply with 85 to 264 VAC input
- **DR-120-24**: 120W/5A DIN-Rail 24 VDC power supply with 88 to 132 VAC/176 to 264 VAC input by switch

# 2

## Getting Started

---

This chapter explains how to access the VPort 704 for the first time. There are two ways to access the switch: by serial console or web console. The serial console connection method, which requires using a short serial cable to connect the VPort 704 to a PC's COM port, can be used if you do not know the VPort 704's IP address. The web console can be used to access the VPort 704 over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

- ❑ **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- ❑ **Configuration using a Web Console**
- ❑ **Network Environment with DHCP Server**
- ❑ **Using the VPort 700 Utility (VPort700Utility.exe)**
- ❑ **Network Environment without DHCP Server**

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

**NOTE Connection Caution!**

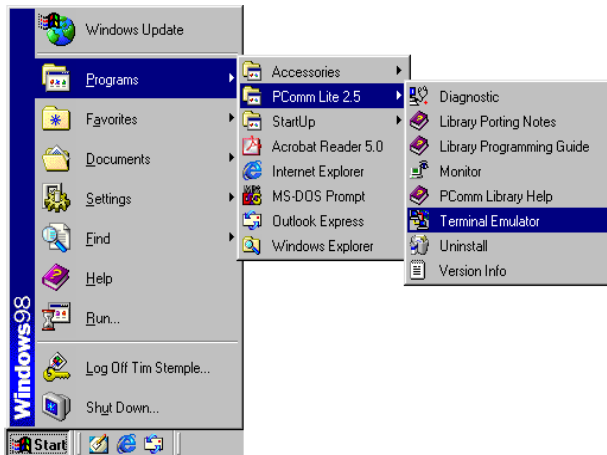
We strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your VPort 704.

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

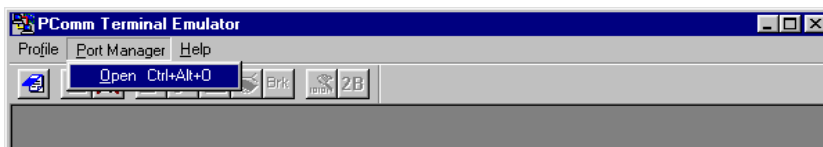
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the VPort 704's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

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

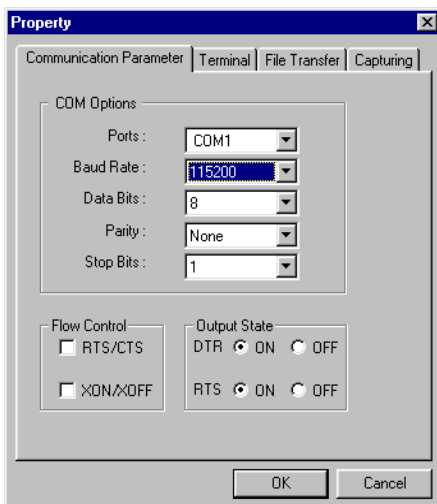
1. From the Windows desktop, click **Start → Programs → PCommLite2.5 → Terminal Emulator**.



2. Select **Open** under **Port Manager** to open a new connection.

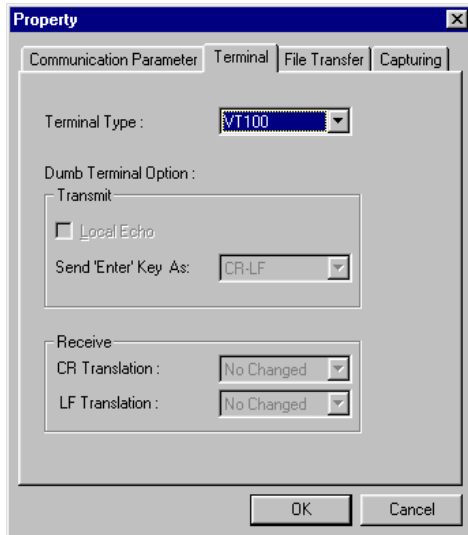


3. The **Communication Parameter** page of the **Property** window opens. Select the appropriate COM port for **Console Connection**, **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.

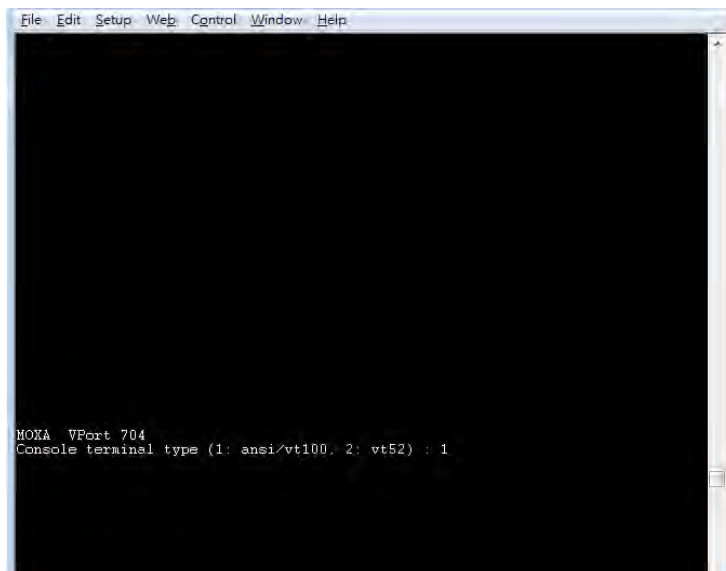




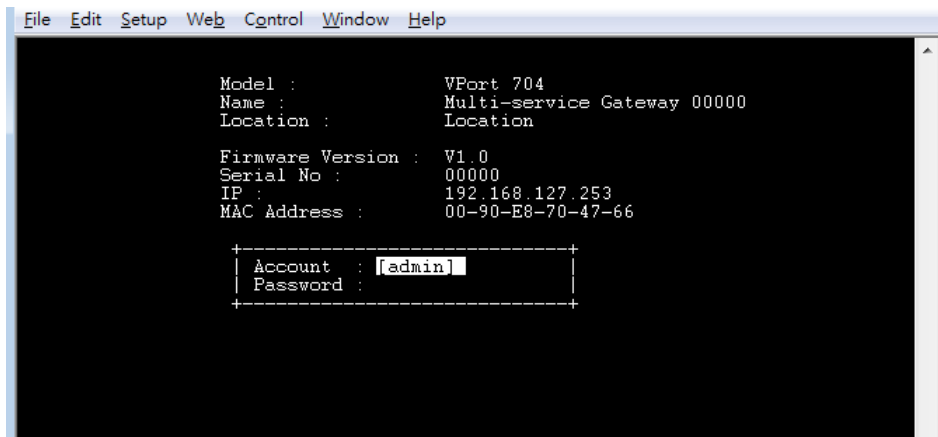
4. Click the **Terminal** tab, and select **VT100** for **Terminal Type**. Click **OK** to continue.



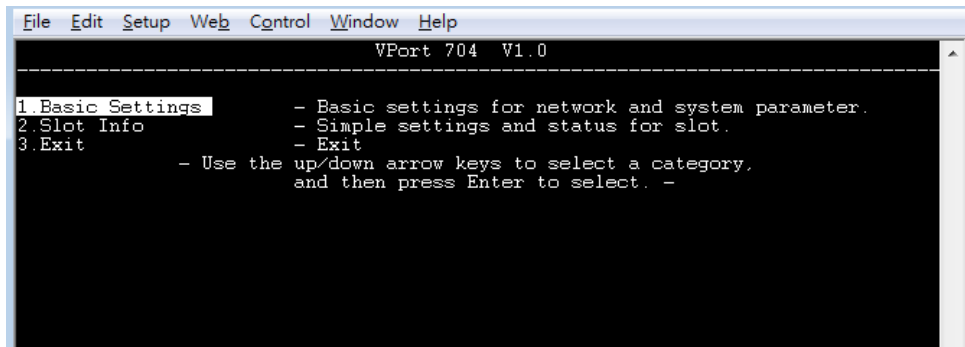
5. Type **1** to select **ansi/VT100** terminal type, and then press **Enter**.



6. The Console login screen will appear. Press **Enter** to open the Account pop-up selector and then select either **admin** or **user**. Use the keyboard's down arrow to move the cursor 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**.



7. The VPort 704's **Main Menu** will be displayed. (NOTE: To modify the appearance of the PComm Terminal Emulator window, select **Font...** under the **Edit** menu, and then choose the desired formatting options.)



8. After entering the **Main Menu**, use the following keys to move the cursor, and to select options.

Key	Function
Up/Down/Left/Right arrows, or Tab	Move the onscreen cursor
Enter	Display & select options
Space	Toggle options
Esc	Previous Menu

## Configuration using a Web Console

The VPort 704'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 VPort 704's management and monitoring functions from a PC host connected to the same LAN as the VPort 704, you must make sure that the PC host and the VPort 704 are on the same logical subnet.

**NOTE** If the VPort 704 is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

**NOTE** Before accessing the VPort 704's web browser interface, first connect one of the switch's RJ45 Ethernet ports to your Ethernet LAN, or connect directly to your PC's Ethernet card (NIC). You can establish a connection using either a straight-through or cross-over Ethernet cable.

**NOTE** The VPort 704's default IP is 192.168.127.253.

## Network Environment with DHCP Server

In this case, the IP address of the VPort 704 is assigned by a DHCP Server. Use the DHCP Server's IP address table, or use the VPort 704 to determine the IP address that was assigned by the DHCP Server.

**NOTE** After powering on the VPort 704, wait a few seconds for the POST (Power On Self Test) to run. The IP address will be assigned when the 10/100/1000 Mbps NETWORK LED blinks.

# Using the VPort 700 Utility (VPort700Utility.exe)


1. Install the **VPort700Utility.exe** program

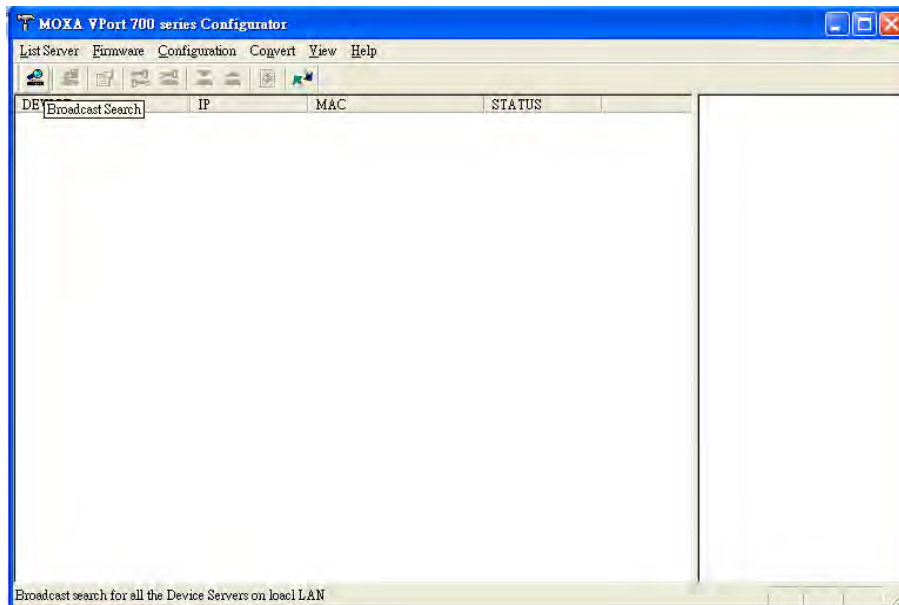
**NOTE** You may download the VPort 700 Utility software from Moxa's website at [www.moxa.com](http://www.moxa.com).

**NOTE** Please do not change the VPort 700 Utility's installation folder; this is because the NPort Windows Driver Manager is in this path.

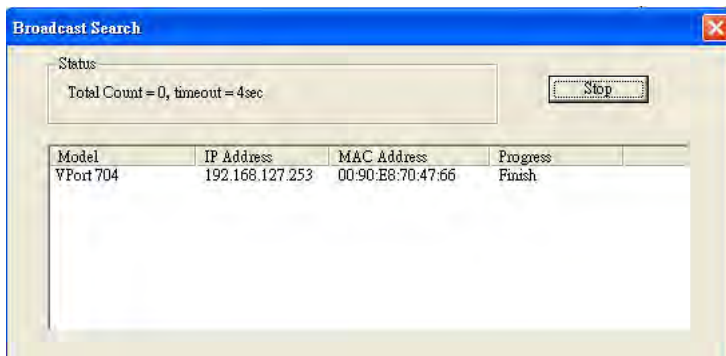
2. Run the **VPort700Utility**.



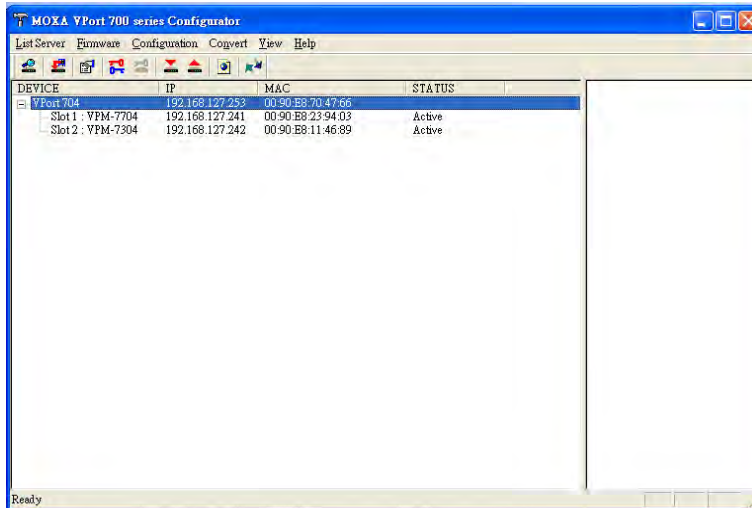
3. After the Utility window opens, select or click on **Broadcast Search**, which is located under the List Server menu, to initiate a search for the VPort 704 and the VPM modules. (note that you can also click on Broadcast Search  icon to initiate a search).



4. The Broadcast Search window will show a list of all switches and VPorts located on the network. The progress of the search will also be indicated.



- When the search has ended, the Device, IP address, MAC address, and Status of VPort 704 and VPM series will be listed in the Utility window.

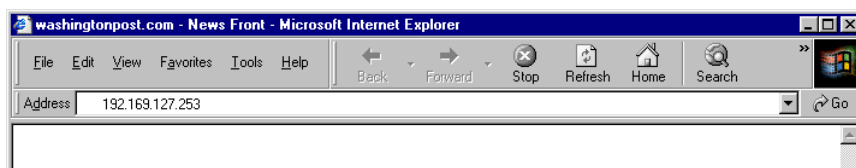


- Select the VPort 704 and click on the Web Console button, or use Internet Explorer to access the VPort 704's web-based manager (web console).

## Network Environment without DHCP Server

Perform the following steps to access the VPort 704's web browser interface.

- Open Internet Explorer and type VPort 704's IP address in the **Address** field. Press **Enter** to establish the connection.



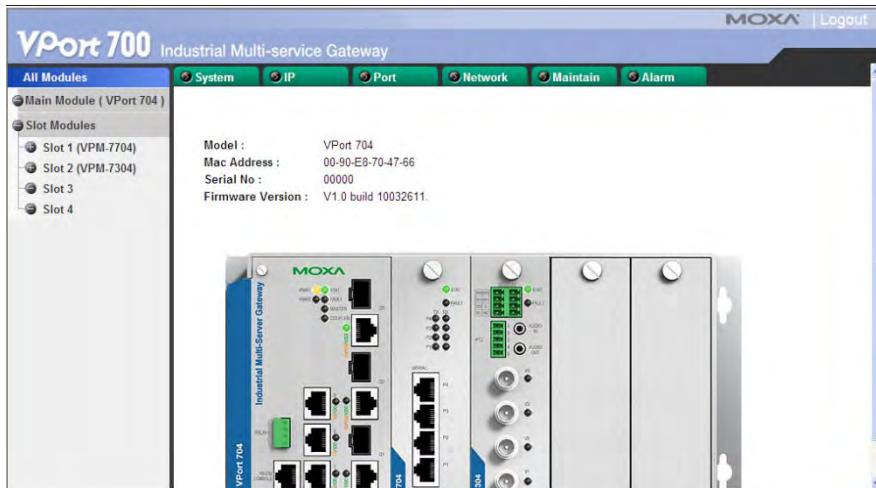
- The web login page will open. Select the login account (Admin) and enter the **Password** (this is the same as the Console password), and then click **Login** to continue. Leave the **Password** field blank if a password has not been set.



### ATTENTION

The VPort 704's default Password is not set (i.e., is blank). If a Password is already set, then you will be required to type the Password when logging into the RS-232 console or web console interface. All slot modules also use this account name and password for the login.

3. You may need to wait a few moments for the web page to be downloaded to your computer. Use the menu tree on the top of the window to open the function pages to access each of the VPort 704's functions.



## Featured Functions

---

In this chapter, we explain how to access the VPort 704's configuration options, perform monitoring, and use administration functions.

The following topics are covered in this chapter:

- ❑ **System Configuration by Web Console**

# System Configuration by Web Console

The web console includes the most commonly used settings required by administrators to maintain and control the VPort 704 and slot modules. "Slot module" refers to the modules plugged in to the VPort 704. Two modules currently available are the VPM-7304 and VPM-7704.

## Homepage

Once you log in to the homepage of the VPort 704's web console, the VPort 704's front panel image will be shown, and the system will detect automatically what kind of slot modules are currently being used. The VPort 704's and slot modules' LED indicators of will also be shown, indicating the current status of the modules.



## All Module List

A device tree is listed on the left side of the homepage. The device tree shows basic information, including Module Name, IP address, MAC address, and Status (Non, Plug In, Booting, Init, Active, Power down), of the main module and current slot modules that were detected.



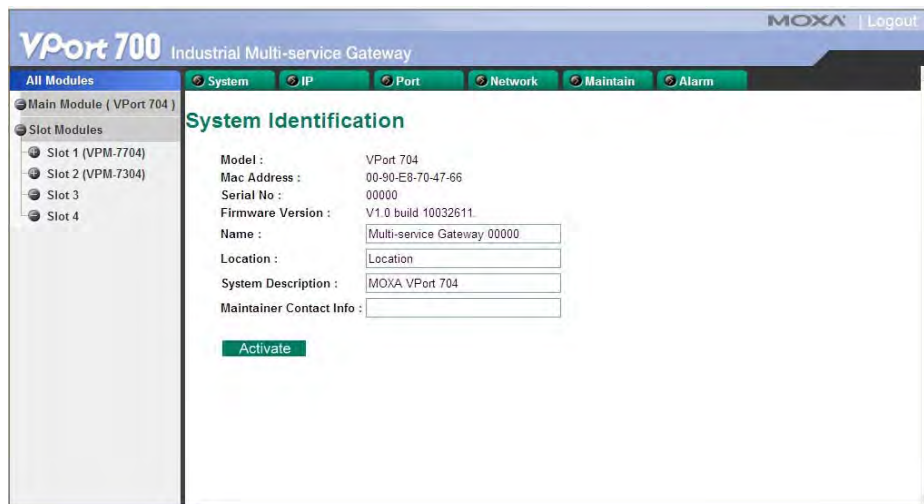
## Slot Module Information

Click on a slot module in the device list to see that module's slot module information. You can directly click on the IP address to link to the slot module configuration page.



## System Information

Click on **System Information** in the System menu. The Model, Mac Address, Serial No. and firmware version of this VPort 704 will be shown. You can also configure the Name, Location, System description, and Maintainer Contact Info. on this page.



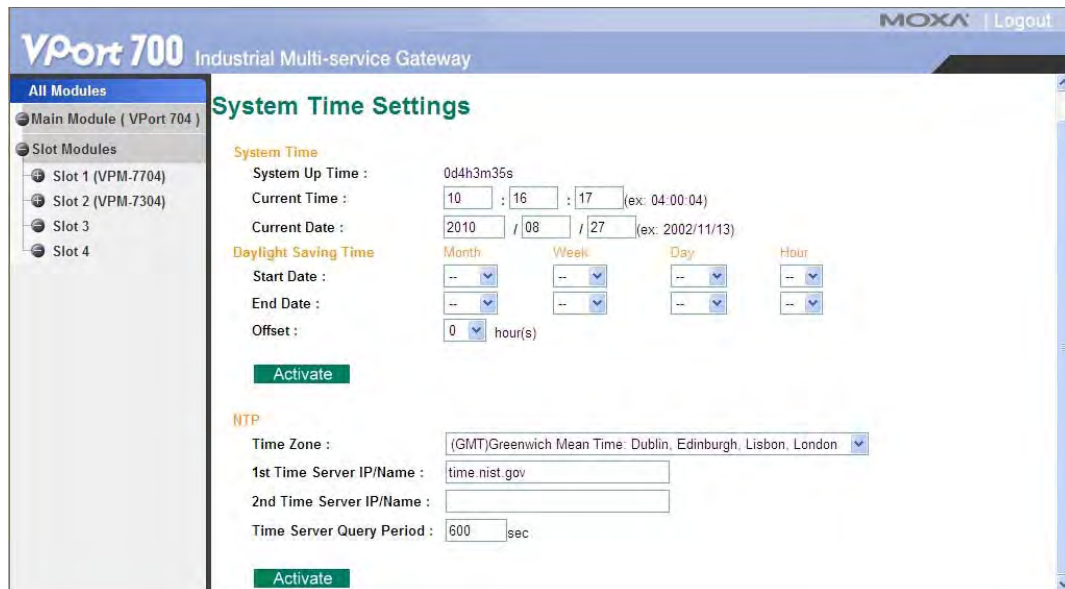
Setting	Description	Factory Default
Name	Name of this VPort, 30 character max.	Multi-service gateway
Location	Identifies the location of this VPort, 80 characters max.	Location
System Description	System description, 30 characters max.	MOXA VPort 704
Maintainer Contact Info	Key administrator information, 30 characters max.	



## System Time

Click **System Time** in the System menu to configure the system time. The configuration methods include manual setup and synchronization with an NTP server. Once the configuration is done, click on **Activate** to activate the new settings.

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



The VPort 704 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 VPort 704 does not have a real time clock. The user must update the Current Time and Current Date to set the initial time for the VPort 704 after each reboot, especially when the network does not have an Internet connection for an NTP server or there is no NTP server on the LAN.

### System Time

Setting	Description	Factory Default
System Up Time	Show how much time this VPort is activated	

### 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 (usually 1 hour) during the summer to provide an extra hour of daylight in the afternoon.

**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 ends.	None

**Offset**

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

## NTP

Setup the NTP server to synchronize the system time.

**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 (Greenwich Mean Time)

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

**Time Server IP/Name**

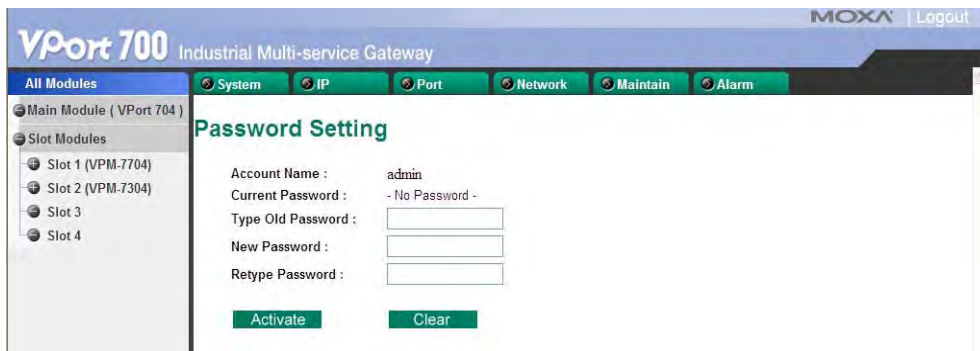
Setting	Description	Factory Default
1st Time Server IP/Name	IP or Domain address (e.g., 192.168.1.1 or time.stdtime.gov.tw or time.nist.gov).	None
2nd Time Server IP/Name	The VPort 704 will try to locate the 2nd NTP Server if the 1st NTP Server fails to connect.	

**Time Server Query Period**

Setting	Description	Factory Default
Query Period	This parameter determines how frequently the time is updated from the NTP server.	600 seconds

## Account

Click **Account** in System menu. Only one administrator account is required for accessing the VPort 704 and all slot modules, allowing the administrator to use a single login mechanism.



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



**ATTENTION**

Since there is only one admin account for accessing the VPort 704 and all slot modules, the administrator should memorize the password carefully. If you forget the password, contact a Moxa technical service engineer for assistance.

## Accessible IP

Click **Accessible IP** in the System menu. The VPort 704 uses an IP address-based filtering method to control access to VPort 704 units.



Accessible IP Settings allow you to add or remove “Legal” remote host IP addresses to prevent unauthorized access. Access to the VPort 704 is controlled by IP address. If a host’s IP address is in the accessible IP table, then the host will be allowed access to the VPort 704. You can choose from one of the following cases to set this parameter:

- **Only one host with the specified IP address can access the VPort 704**  
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 the VPort 704**  
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 VPort 704**  
Disable this function by deselecting the **Enable the accessible IP list** option.

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

## SNMP

Click **SNMP** in the System menu. VPort supports three SNMP protocols: SNMP V1, SNMP V2c, and SNMP V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string public/private (default value). SNMP V3, which requires that you select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security. The SNMP security modes and security levels supported by VPort are shown in the following table. Select one of these options to communicate between the SNMP agent and manager.

Protocol Version	Security Mode	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication
SNMP V3	No-Auth	No	No	Uses account with admin or user to access objects
	MD5 or SHA	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	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.

## Configuring SNMP Settings

The following figures indicate which SNMP parameters can be configured. A more detailed explanation of each parameter is given below the figure



## SNMP Read/Write Settings

### *SNMP Versions*

Setting	Description	Default
V1, V2c, V3	Select SNMP Versions V1, V2c, V3 protocol to manage the switch	V1, V2c
V1, V2c	Select SNMP Versions V1, V2c protocol to manage the switch	
V3 only	Select SNMP Versions V3 protocol only to manage the switch	

### *V1, V2c Read Community*

Setting	Description	Default
V1, V2c Read Community	Uses a community string match for authentication, which means that the SNMP agent accesses all objects with read-only permissions using the community string public.	public (max. 30 characters)

### *V1, V2c Read/Write Community*

Setting	Description	Default
V1, V2c Read/Write Community	Uses a community string match for authentication, which means that the SNMP agent accesses all objects with read-only permissions using the community string public.	public (max. 30 characters)

For SNMP V3, there are two levels of privilege for different accounts to access the VPort. Admin privilege allows access and authorization to read and write MIB files. User privilege only allows reading the MIB file, but does not authorize writing to the file.

### *Root Auth. Type (For SNMP V1, V2c, V3 and V3 only)*

Setting	Description	Default
No-Auth	Use admin. account to access objects. No authentication	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA- Auth	Provide authentication based on the MAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

### *Root Data Encryption Key (For SNMP V1, V2c, V3 and V3 only)*

Setting	Description	Default
Enable	The encryption key has an 8-character minimum and a 30-character maximum.	No
Disable	No data encryption	No

### *User Auth. Type (For SNMP V1, V2c, V3 and V3 only)*

Setting	Description	Default
No-Auth	Use account of admin or user to access objects. No authentication.	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA- Auth	Provide authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

**User Data Encryption Key (For SNMP V1, V2c, V3 and V3 only)**

Setting	Description	Default
Enable	8-character data encryption key is the minimum requirement for data encryption. Maximum 30-character encryption key	No
Disable	No data encryption	No

**Trap Settings**

Setting	Description	Default
Trap Server IP/Name	Enter the IP address or name of the Trap Server used by your network.	No
Trap Community	Use a community string match for authentication; Maximum of 30 characters.	No

**Private MIB information**

The private SNMP Object ID of the VPort is the enterprise value: 8691.8.3.1. This number cannot be changed.

## MAC Address

Click **MAC Address** in the System menu. This section explains the information provided by the VPort 704's MAC address table.



The MAC Address table can be configured to display the following VPort 704 MAC address groups.

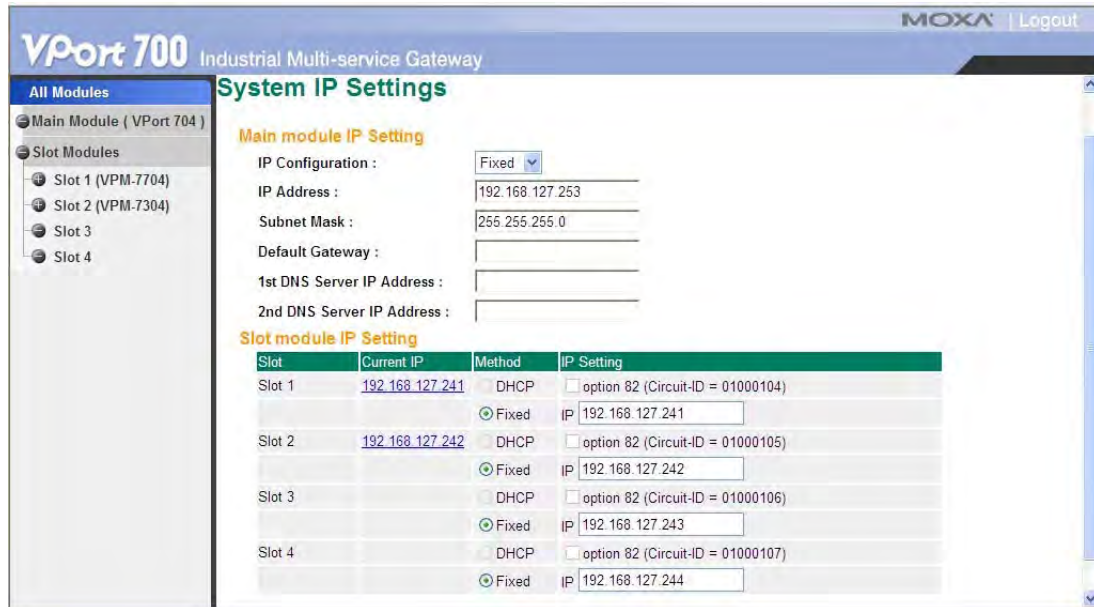
ALL	Select this item to show all VPort 704 MAC addresses
ALL Learned	Select this item to show all VPort 704 Learned MAC addresses
ALL Static	Select this item to show all VPort 704 Static/Static Lock /Static Multicast MAC addresses
ALL Static Multicast	Select this item to show all VPort 704 Static Multicast MAC addresses
Port x	Select this item to show all MAC addresses of dedicated ports

The table will display the following information:

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

# System IP

Click **System IP** in the IP menu. This section provides the IP address setting of the VPort 704 and the slot modules.



### Main Module IP Setting

Setting	Description	Default
IP Configuration	2 types: DHCP and Fixed IP. DHCP: The VPort's IP address will be assigned by DHCP server Fixed: The VPort's IP address will be fixed based on the IP listed below	Fixed
IP address	Identifies the VPort on a TCP/IP network.	192.168.127.253
Subnet mask	Identifies the type of network to which the VPort is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0
Default Gateway	The IP address of the router that connects the LAN to an outside network.	None
1st DNS Server's IP Address	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the VPort's URL (e.g., www.VPort 704.company.com) in your browser's address field, instead of entering the IP address.	None
2nd DNS Server's IP Address	The IP address of the DNS Server used by your network. The VPort's will try to locate the 2nd DNS Server if the 1st DNS Server fails to connect.	None

### Slot Module IP Setting

Setting	Description	Factory Default
Slot	The VPort 704 will automatically detect which slot (1, 2, 3, or 4) is used.	
Current IP	The current IP address of the slot module.	Slot 1: 196. 168.127.241 Slot 2: 196. 168.127.242 Slot 3: 196. 168.127.243 Slot 4: 196. 168.127.244
Method	Define the IP configuration method of the slot module: DHCP or Fixed.	Fixed

IP Setting	Define the slot module's IP configuration method. <b>Option 82:</b> except for the general DHCP, the administrator can setup the slot module to use the Option 82 method to get a fixed DHCP's IP address <b>IP:</b> Manually key in the IP address	Slot 1: 196. 168.127.241 Slot 2: 196. 168.127.242 Slot 3: 196. 168.127.243 Slot 4: 196. 168.127.244
------------	---	--

**NOTE** We strongly recommend that the administrator assign a fixed IP address to the VPort, since all of the functions and applications provided by the VPort are active when the VPort is connected to the network.

**NOTE** Use DHCP to determine if the VPort's IP address may change when then network environment changes, or the IP address is occupied by other clients. The administrator can choose Option 82 to get a fixed IP from the DHCP server. For the configuration of option 82, refer to the configuration of the DHCP relay agent.

## Device IP Settings

Click on Device IP Settings in the IP's menu. VPort 704 has built-in 6 Ethernet ports: 3 gigabit ports, and 3 10/100Mbps ports. This section provides the IP address setting of the devices these Ethernet ports connect.

### Using Device IP Settings

To reduce the effort required to set up IP addresses, the VPort 704 comes equipped with DHCP/BOOTP server and RARP protocol to set up IP addresses of Ethernet-enabled devices automatically.

When enabled, the **device IP settings** function allows the VPort 704 to assign specific IP addresses automatically to connected devices that are equipped with *DHCP Client* or *RARP* protocol. In effect, the VPort 704 acts as a DHCP server by assigning a connected device with a specific IP address stored in its internal memory. Each time the connected device is switched on or rebooted, the VPort 704 sends the device the desired IP address.

Perform the following steps to use the **device IP settings** function:

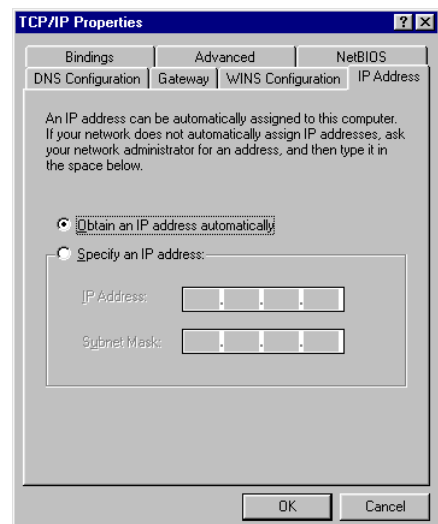
#### STEP 1

Set up those Ethernet-enabled devices connected to the VPort 704 for which you would like IP addresses to be assigned automatically. The devices must be configured to obtain their IP address automatically.

The devices' configuration utility should include a setup page that allows you to choose an option similar to Obtain an IP address automatically.

For example, Windows' TCP/IP Properties window is shown at the right. Although your device's configuration utility may look quite a bit different, this figure should give you some idea of what to look for.

You also need to decide to which of the VPort 704's ports your Ethernet-enabled devices will be connected. You will need to set up each of these ports separately, as described in the following step.



#### STEP 2

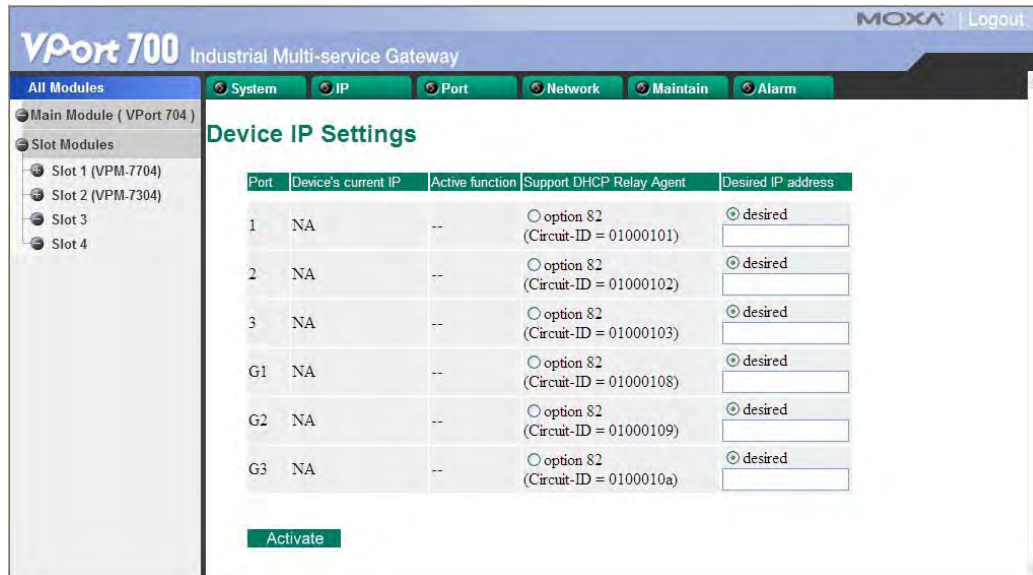
Configure the VPort 704's **device IP settings** function, either from the Console utility or from the Web Browser interface. In either case, you simply need to enter the **Desired IP** for each port that neVPort 704 to be configured.



**STEP 3**

Be sure to activate your settings before exiting.

- When using the Web Browser interface, activate by clicking **Activate**.
- When using the Console utility, activate by first highlighting the **Activate** menu option, and then press **Enter**. You should receive the **device IP settings are now active! (Press any key to continue)** message.

**Configuring Device IP Settings****Device IP Settings**

Setting	Description	Factory Default
Support DHCP Relay Agent	Can choose the Option 82 IP configuration method	None
Desired IP Address	Set the desired IP of connected devices.	None

**DHCP Relay Agent**

Click **DHCP Relay Agent** in the IP menu. The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

**DHCP Relay Agent (Option 82)**

Option 82 is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

When Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains 2 sub-options: Circuit ID and Remote ID, which define the relationship between end device IP and the DHCP Option 82 server. The "Circuit ID" is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID. The format of the "Circuit ID" is as described below:

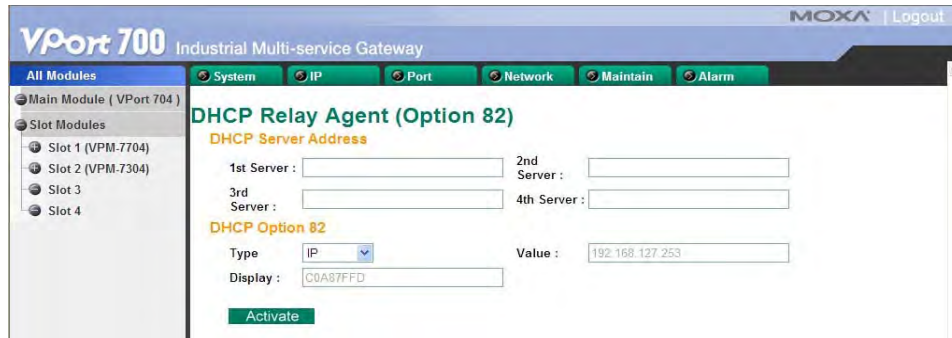
**FF-VV-VV-PP**

Where the first byte “FF” is fixed to “01”, the second and the third byte “VV-VV” is formed by the port VLAN ID in hex, and the last byte “PP” is formed by the port number in hex. For example,

**01-00-0F-03** is the “Circuit ID” of port number 3 with port VLAN ID 15.

The **Remote ID** identifies the relay agent itself; it can be one of the following:

1. The IP address of the relay agent.
2. The MAC address of the relay agent.
3. A combination of IP address and MAC address of the relay agent.
4. A user-defined string.



### Server IP Address

*1st Server*

Setting	Description	Factory Default
IP address for the 1st DHCP server	This assigns the IP address of the 1st DHCP server that the switch tries to access.	None

*2nd Server*

Setting	Description	Factory Default
IP address for the 2nd DHCP server	This assigns the IP address of the 2nd DHCP server that the switch tries to access.	None

*3rd Server*

Setting	Description	Factory Default
IP address for the 3rd DHCP server	This assigns the IP address of the 3rd DHCP server that the switch tries to access.	None

*4th Server*

Setting	Description	Factory Default
IP address for the 4th DHCP server	This assigns the IP address of the 4th DHCP server that the switch tries to access.	None

### DHCP Option 82

*Type*

Setting	Description	Factory Default
IP	Use switch IP address as the remote ID sub-option.	IP
MAC	Use switch MAC address as the remote ID sub-option.	IP
Client-ID	Use the combination of switch MAC address and IP address as the remote ID sub-option.	IP
Other	Use the user-defined value as the remote ID sub-option.	IP

**Value**

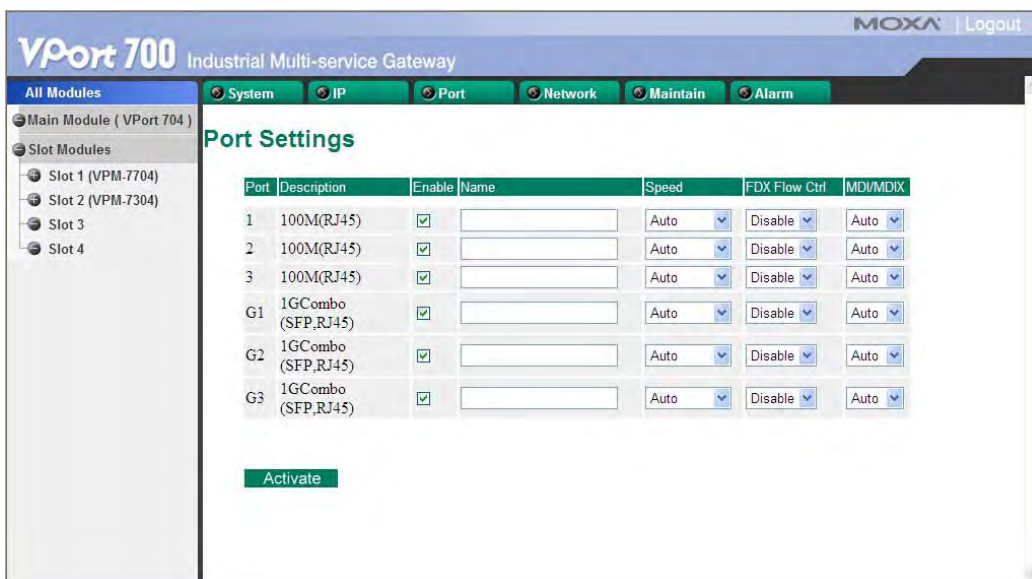
Setting	Description	Factory Default
Max. 12 characters	Displays the value which you've set. If you set the type as Other, you will have to fill it.	switch IP address

**Display**

Setting	Description	Factory Default
	The actual hexadecimal value set at the DHCP server for the Remote-ID. This value is automatically generated according to the Value field. Users can not modify it.	COA87FFD

## Port Configuration

Click on Port Configuration in the Port's menu. **Port Configuration** settings are included to give the user control over Port Access, Port Transmission Speed, Flow Control, and Port Type (MDI or MDIX). An explanation of each configuration item follows:



**Enable**

Setting	Description	Factory Default
checked	Allows data transmission through the port.	enabled
unchecked	Immediately shuts off port access.	



**ATTENTION**

If a connected device or sub-network is wreaking havoc on the rest of the network, the **Disable** option under **Advanced Settings/Port** gives the administrator a quick way to shut off access through this port immediately.

**Description**

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

**Name**

Setting	Description	Factory Default
Max. 63 Characters	Specify an alias for each port, and assist the administrator in remembering important information about the port. E.g., PLC 1	None

**Speed**

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection. Choose one of these fixed speed options if the opposing Ethernet device has trouble auto-negotiating line speed.	Auto
100M-Full		
100M-Half		
10M-Full		
10M-Half		
1G-Full		
1G-Half		

**FDX Flow Ctrl**

Setting	Description	Factory Default
Enable	Enables flow control for this port when in auto-negotiate mode.	Disable
Disable	Disables flow control for this port when in auto-negotiate mode.	

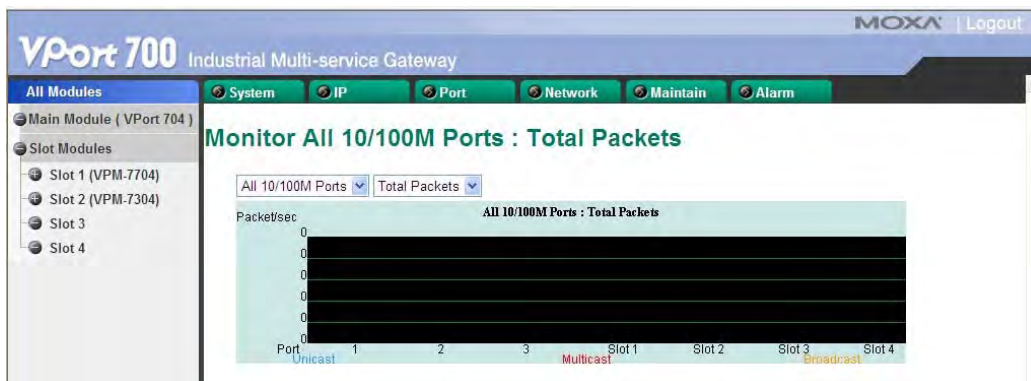
This setting enables or disables the flow control capability of this port when the “port transmission speed” setting is in “auto” mode. The final result will be determined by the “auto” process between the VPort 704 and connected devices.

**MDI/MDIX**

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

## Port Monitor

Click on Port Monitor in the Port’s menu. Access the Port Monitor function by selecting **ALL 10/100M or 1G Ports** or **Port *i***, in which *i*= **1, 2, ..., G3**, from the left pull-down list. The **Port *i*** options are identical to the Monitor by System function discussed above, in that users can view graphs that show All Packets, TX Packets, RX Packets, or Error Packets activity, but in this case, only for an individual port. The **All Ports** option is essentially a graphical display of the individual port activity that can be viewed with the Console Monitor function discussed above. The All Ports option shows three vertical bars for each port. The height of the bar represents **Packets/s** for the type of packet, at the instant the bar is being viewed. That is, as time progresses, the height of the bar moves up or down so that the user can view the change in the rate of packet transmission. The blue colored bar shows **Unicast** packets, the red colored bar shows **Multicast** packets, and the orange colored bar shows **Broadcast** packets. The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



# Mirror Port

Click on Mirror Port in the Port's menu.



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

Perform the following steps to set up the **Mirror Port** function:

## STEP 1

Configure the VPort 704's **Mirror Port** function from Web Console. You will need to configure three settings:

Monitored Port	Select the port number of the port whose network activity will be monitored.
Mirror Port	Select the port number of the port that will be used to monitor the activity of the monitored port.
Watch Direction	Select one of the following three watch direction options: <ul style="list-style-type: none"> <li>• Input data stream Select this option to monitor only those data packets coming in through the VPort 704's port.</li> <li>• Output data stream Select this option to monitor only those data packets being sent out through the VPort 704's port.</li> <li>• Bi-directional Select this option to monitor data packets both coming into, and being sent out through, the VPort 704's port.</li> </ul>

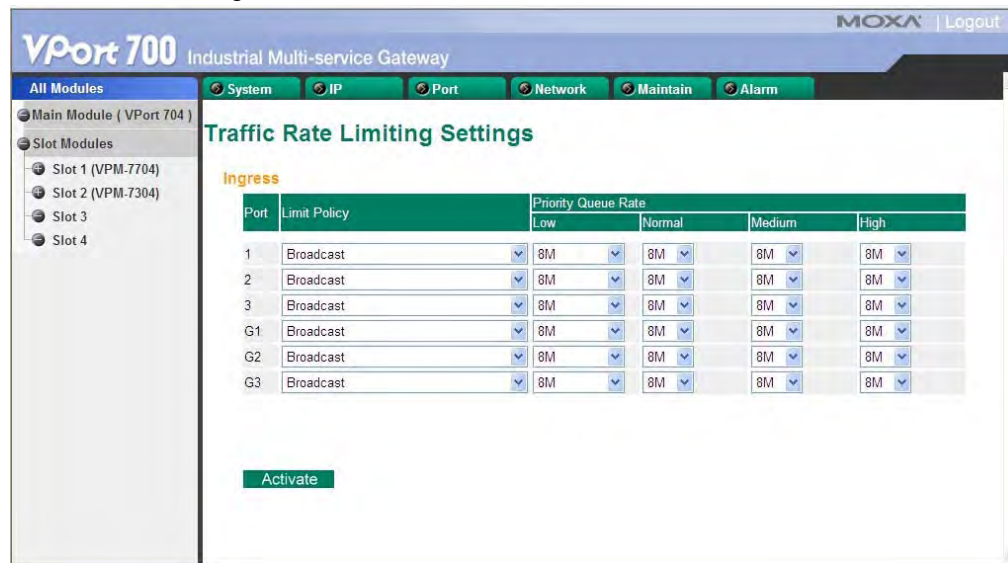
## STEP 2

Be sure to activate your settings before exiting.

- When using the Web Browser interface, activate by clicking **Activate**.
- When using the Console utility, activate by first highlighting the Activate menu option, and then press **Enter**. You should receive the **Mirror port settings are now active! (Press any key to continue)** message.

## Rate Limiting

Click on Rate Limiting in the Port's menu.



### Ingress

Setting	Description	Factory Default
Ingress rate	Select the ingress rate for all packets from the following options: Not Limited, 128K, 256K, 512K, 1M, 2M, 4M, 8M	8M

## IEEE 802.1X

The IEEE 802.1X standard defines a protocol for client/server-based access control and authentication. The protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet, and which otherwise would be readily accessible. The purpose of the authentication server is to check each client that requests access to the port. The client is only allowed access to the port if the client's permission is authenticated.

### The IEEE 802.1X Concept

Three components are used to create an authentication mechanism based on 802.1X standards: Client/Supplicant, Authentication Server, and Authenticator.

**Supplicant:** The end station that requests access to the LAN and switch services and responds to the requests from the switch.

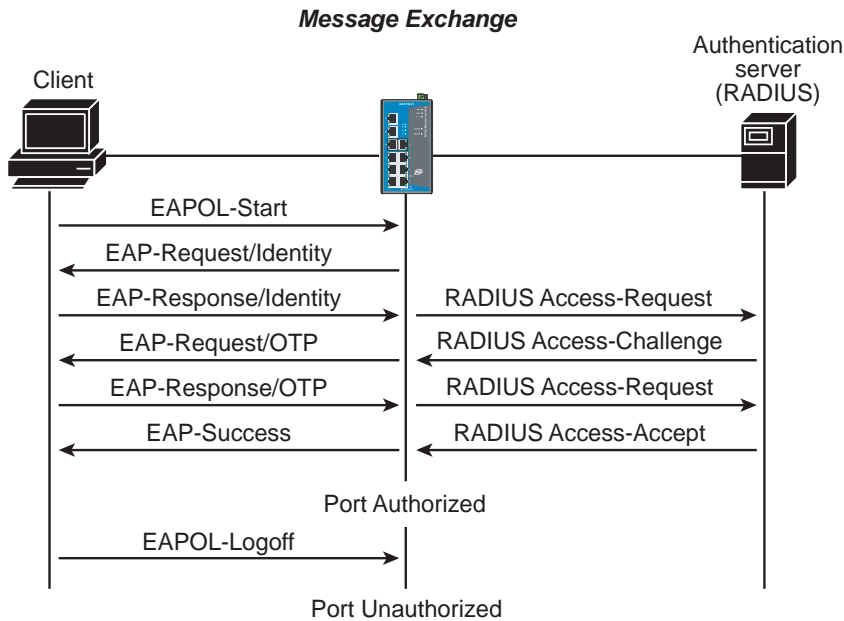
**Authentication server:** The server that performs the actual authentication of the supplicant.

**Authenticator:** Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant.

The VPort 704 acts as an authenticator in the 802.1X environment. A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server, or implement the authentication server in the VPort 704 by using a Local User Database as the authentication look-up table. When we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames between each other.

Authentication can be initiated either by the supplicant or the authenticator. When the supplicant initiates the authentication process, it sends an "EAPOL-Start" frame to the authenticator. When the authenticator initiates

the authentication process or when it receives an "EAPOL Start" frame, it sends an "EAP Request/Identity" frame to ask for the username of the supplicant. The following actions are described below:



When the supplicant receives an "EAP Request/Identity" frame, it sends an "EAP Response/Identity" frame with its username back to the authenticator.

If the RADIUS server is used as the authentication server, the authenticator relays the "EAP Response/Identity" frame from the supplicant by encapsulating it into a "RADIUS Access-Request" frame and sends to the RADIUS server. When the authentication server receives the frame, it looks up its database to check if the username exists. If the username is not present, the authentication server replies with a "RADIUS Access-Reject" frame to the authenticator if the server is a RADIUS server or just indicates failure to the authenticator if the Local User Database is used. The authenticator sends an "EAP-Failure" frame to the supplicant.

The RADIUS server sends a "RADIUS Access-Challenge," which contains an "EAP Request" with an authentication type to the authenticator to ask for the password from the client. RFC 2284 defines several EAP authentication types, such as "MD5-Challenge," "One-Time Password," and "Generic Token Card." Currently, only "MD5-Challenge" is supported. If the Local User Database is used, this step is skipped.

The authenticator sends an "EAP Request/MD5-Challenge" frame to the supplicant. If the RADIUS server is used, the "EAP Request/MD5-Challenge" frame is retrieved directly from the "RADIUS Access-Challenge" frame.

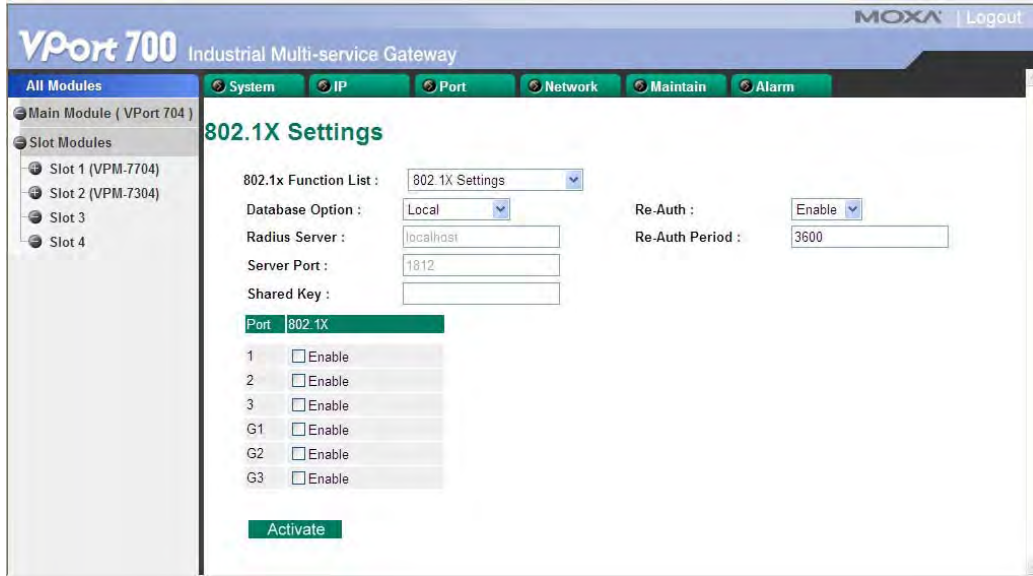
The supplicant responds to the "EAP Request/MD5-Challenge" by sending an "EAP Response/MD5-Challenge" frame that encapsulates the user's password using the MD5 hash algorithm.

If the RADIUS server is used as the authentication server, the authenticator relays the "EAP Response/MD5-Challenge" frame from the supplicant by encapsulating it into a "RADIUS Access-Request" frame along with a "Shared Secret," which must be the same within the authenticator and the RADIUS server, and sends the frame to the RADIUS server. The RADIUS server checks against the password with its database, and replies with "RADIUS Access-Accept" or "RADIUS Access-Reject" to the authenticator. If the Local User Database is used, the password is checked against its database and indicates success or failure to the authenticator.

The authenticator sends "EAP Success" or "EAP Failure" based on the reply from the authentication server.

## Configuring IEEE 802.1X

Click on 802.1X in the Port's menu.



### Database Option

Setting	Description	Factory Default
Local (Max. 32 users)	Select this option when setting the Local User Database as the authentication database.	Local
Radius	Select this option to set an external RADIUS server as the authentication database. The authentication mechanism is "EAP-MD5."	Local
Radius, Local	Select this option to make an external RADIUS server as the authentication database with first priority. The authentication mechanism is "EAP-MD5." The first priority is to set the Local User Database as the authentication database.	Local

### Radius Server

Setting	Description	Factory Default
IP address or domain name	The IP address or domain name of the RADIUS server	localhost

### Server Port

Setting	Description	Factory Default
Numerical	The UDP port of the RADIUS Server	1812

### Shared Key

Setting	Description	Factory Default
alphanumeric (Max. 40 characters)	A key to be shared between the external RADIUS server and the VPort 704. Both ends must be configured to use the same key.	None

### Re-Auth

Setting	Description	Factory Default
Enable/Disable	Select to require re-authentication of the client after a preset time period of no activity has elapsed.	Disable



**Re-Auth Period**

Setting	Description	Factory Default
Numerical (60-65535 sec.)	Specify how frequently the end stations need to reenter usernames and passwords in order to stay connected.	3600

**802.1X**

Setting	Description	Factory Default
Enable/Disable	Select the option under the 802.1X column to enable IEEE 802.1X for one or more ports. All end stations must enter usernames and passwords before access to these ports is allowed.	Disable

## Port Lock

Click on Port Lock in the Port’s menu. The VPort 704 can also be configured to protect static MAC addresses for a specific port. With the Port Lock function, these locked ports will not learn any additional addresses, but only allow traffic from preset static MAC addresses, helping to block crackers and careless usage.



**Port Lock**

Setting	Description	Factory Default
MAC Address	Add the static unicast MAC address into the address table.	None
Port	Fix the static address with a dedicated port.	1

## Port Access Table

Click **Port Access Table** in the Port menu. The port status will indicate whether the access is authorized or unauthorized.



## Communication Redundancy

### Using Communication Redundancy

Setting up Communication Redundancy on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum.

The Communication Redundancy function allows the user to set up *redundant loops* in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable. For example, if the VPort 704 is used as a key communications component of a production line, several minutes of downtime could cause a big loss in production and revenue. VPort 704 supports three different protocols to support this communication redundancy function— **Rapid Spanning Tree/ Spanning Tree Protocol (IEEE 802.1W/1D)**, **Turbo Ring** and **Turbo Ring V2**.

When configuring a redundant ring, all switches on the same ring must be configured to use the same redundancy protocol. You cannot mix the “Turbo Ring,” “Turbo Ring V2,” and STP/RSTP protocols on the same ring. The following table lists the key differences between each feature. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network.

	Turbo Ring V2	Turbo Ring	STP	RSTP
Topology	Ring	Ring	Ring, Mesh	Ring, Mesh
Recovery Time	< 50 ms	< 300 ms	Up to 30 sec.	Up to 5 sec

**NOTE** Most of Moxa’s managed switches now support 2 proprietary Turbo Ring protocols:

- **Turbo Ring** refers to the original version of Moxa’s proprietary redundant ring protocol, which has a recovery time of under 300 ms.
- **Turbo Ring V2** refers to the new generation Turbo Ring, which has a recovery time of under 50 ms.

In this manual, we use the terminology “Turbo Ring” ring and “Turbo Ring V2” ring to differentiate between rings configured for one or the other of these protocols.

### The STP/RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures in a network, and provide protection from loops. Networks that have a complicated architecture are prone to broadcast storms caused by unintended loops in the network. Moxa VPort 704’s STP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every VPort 704 connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE Std 802.1w-2001. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy. For example:

Defaults to sending 802.1D style BPDUs if packets with this format are received.

STP (802.1D) and RSTP (802.1w) can operate on different ports of the same VPort 704. This feature is particularly helpful when VPort 704-510A ports connect to older equipment, such as legacy switches.

You get essentially the same functionality with RSTP and STP. To see how the two systems differ, see the *Differences between RSTP and STP* section in this chapter.

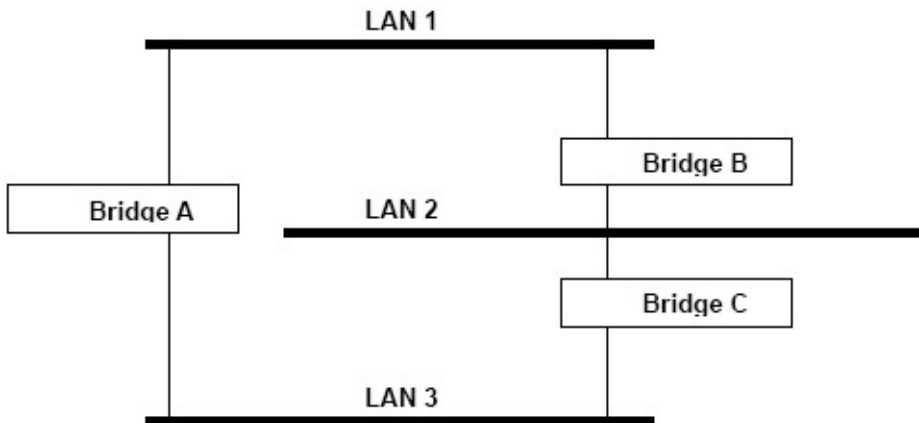
**NOTE** The STP protocol is part of the IEEE Std 802.1D, 1998 Edition bridge specification. The following explanation uses bridge instead of switch.

## What is STP?

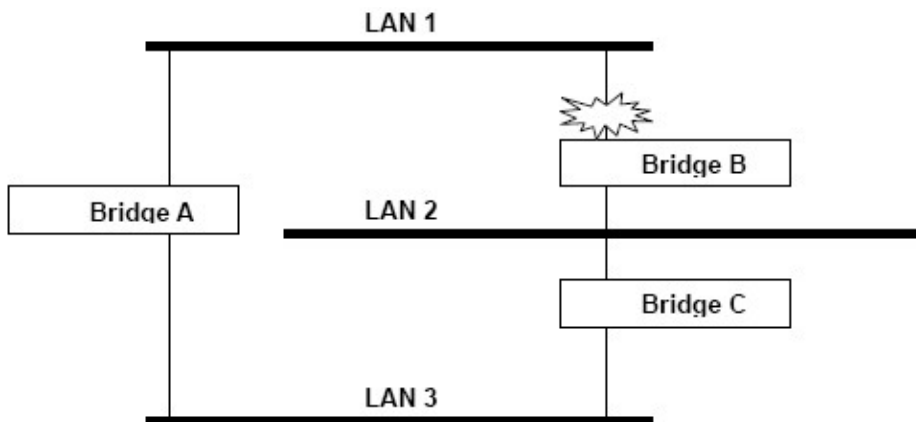
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- Locate and then disable less efficient paths (i.e., paths that have a lower bandwidth).
- Enable one of the less efficient paths if the most efficient path fails.

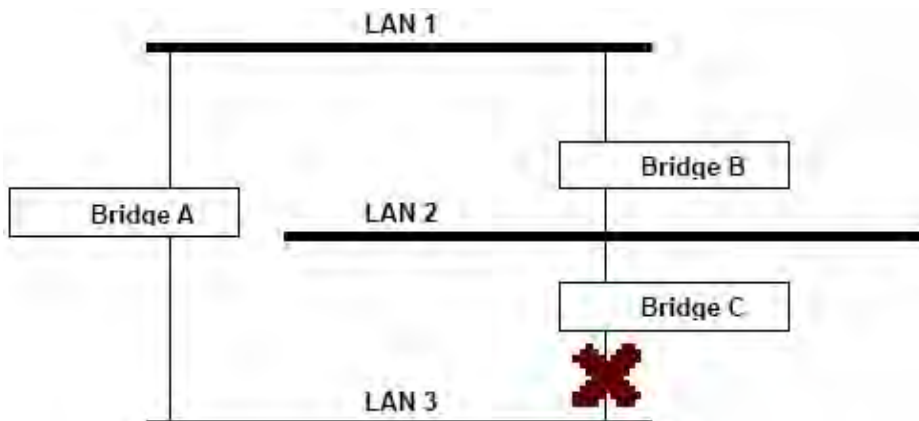
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



If STP is enabled, it will detect duplicate paths and prevent, or *block*, one of them from forwarding traffic. In the following example, STP determined that traffic from LAN segment 2 to LAN segment 1 should flow through Bridges C and A because this path has a greater bandwidth and is therefore more efficient.



What happens if a link failure is detected? As shown in next figure, the STP process reconfigures the network so that traffic from LAN segment 2 flows through Bridge B.



STP will determine which path between each bridged segment is most efficient, and then assigns a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous 3 figures, STP first determined that the path through Bridge C was the most efficient, and as a result, blocked the path through Bridge B. After the failure of Bridge C, STP re-evaluated the situation and opened the path through Bridge B.

## How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the sections below.

### STP Requirements

Before STP can configure the network, the system must satisfy the following requirements:

- Communication between all the bridges. This communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. The default priority of VPort 704 is 32768.
- Each port has a cost that specifies the efficiency of each link. The efficiency cost is usually determined by the bandwidth of the link, with less efficient links assigned a higher cost. The following table shows the default port costs for a switch:

Port Speed	Path Cost 802.1D, 1998 Edition	Path Cost 802.1w-2001
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1000 Mbps	4	20,000

### STP Calculation

The first step of the STP process is to perform calculations. During this stage, each bridge on the network transmits BPDUs. The following items will be calculated:

- Which bridge should be the Root Bridge. The Root Bridge is the central reference point from which the network is configured.
- The Root Path Costs for each bridge. This is the cost of the paths from each bridge to the Root Bridge.
- The identity of each bridge's Root Port. The Root Port is the port on the bridge that connects to the Root Bridge via the most efficient path. In other words, the port connected to the Root Bridge via the path with the lowest Root Path Cost. The Root Bridge, however, does not have a Root Port.
- The identity of the Designated Bridge for each LAN segment. The Designated Bridge is the bridge with the lowest Root Path Cost from that segment. If several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge. Traffic transmitted in the direction of the Root Bridge will flow through the Designated Bridge. The port on this bridge that connects to the segment is called the Designated Bridge Port.

### STP Configuration

After all the bridges on the network agree on the identity of the Root Bridge, and all other relevant parameters have been established, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they will not be allowed to receive or forward traffic.

### STP Reconfiguration

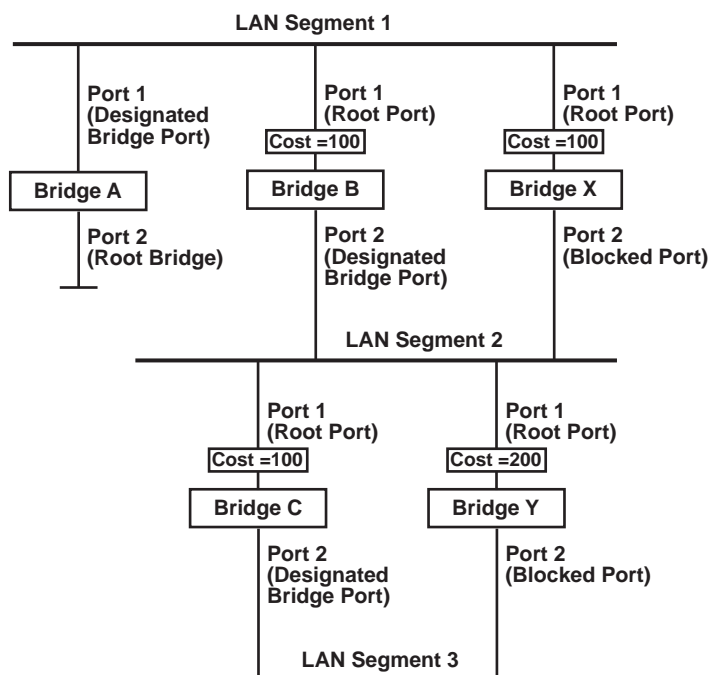
Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has gone down. This will trigger the bridge to reconfigure the network to account for the change. If you have configured an SNMP trap destination, when the topology of your network changes, the first bridge to detect the change sends out an SNMP trap.

## Differences between RSTP and STP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

## STP Example

The LAN shown in the following figure has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.

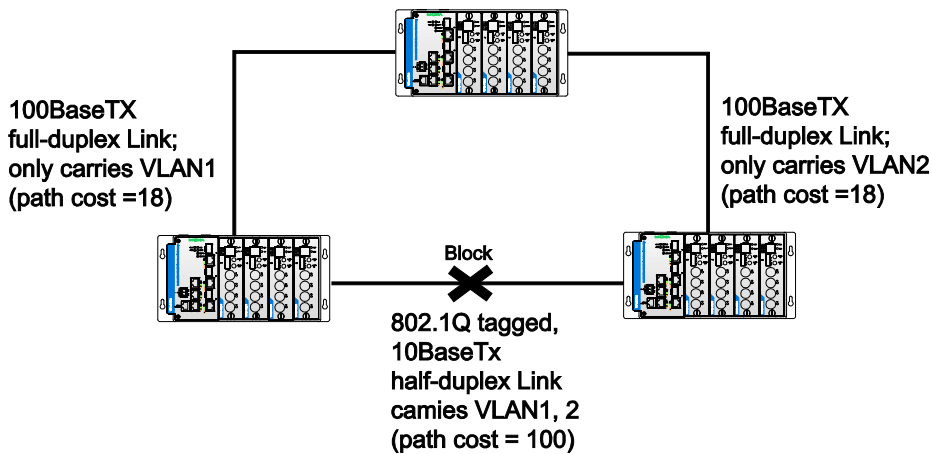


- Bridge A has been selected as the Root Bridge, since it was determined to have the lowest Bridge Identifier on the network.
- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.
- Ports 1 of Bridges B, C, X, and Y are all Root Ports since they are nearest to the Root Bridge, and therefore have the most efficient path.
- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B was selected as the Designated Bridge for that segment since it has a lower Bridge Identifier. Port 2 on Bridge B is selected as the Designated Bridge Port for LAN Segment 2.
- Bridge C is the Designated Bridge for LAN segment 3, because it has the lowest Root Path Cost for LAN Segment 3:
  - The route through Bridges C and B costs 200 (C to B=100, B to A=100)
  - The route through Bridges Y and B costs 300 (Y to B=200, B to A=100)
- The Designated Bridge Port for LAN Segment 3 is Port 2 on Bridge C.

## Using STP on a Network with Multiple VLANs

IEEE Std 802.1D, 1998 Edition, does not take into account VLANs when calculating STP information—the calculations only depend on the physical connections. Consequently, some network configurations will result in VLANs being subdivided into a number of isolated sections by the STP system. You must ensure that every VLAN configuration on your network takes into account the expected STP topology and alternative topologies that may result from link failures.

The following figure shows an example of a network that contains VLANs 1 and 2. The VLANs are connected using the 802.1Q-tagged link between Switch B and Switch C. By default, this link has a port cost of 100 and is automatically blocked because the other Switch-to-Switch connections have a port cost of 36 (18+18). This means that both VLANs are now subdivided—VLAN 1 on Switch units A and B cannot communicate with VLAN 1 on Switch C, and VLAN 2 on Switch units A and C cannot communicate with VLAN 2 on Switch B.



To avoid subdividing VLANs, all inter-switch connections should be made members of all available 802.1Q VLANs. This will ensure connectivity at all times. For example, the connections between Switches A and B, and between Switches A and C should be 802.1Q tagged and carrying VLANs 1 and 2 to ensure connectivity.

See the “Configuring Virtual LANs” section for more information about VLAN Tagging.

## Configuring STP/RSTP

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

Port	Enable RSTP	Port Priority	Port Cost	Status
1	<input type="checkbox"/>	128	200000	---
2	<input type="checkbox"/>	128	200000	---
3	<input type="checkbox"/>	128	200000	---
G1	<input type="checkbox"/>	128	20000	---
G2	<input type="checkbox"/>	128	20000	---
G3	<input type="checkbox"/>	128	20000	---

Activate

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

**Now Active:**

This will show which communication protocol is being used—Turbo Ring, RSTP, or neither.

**Root/Not Root**

This field will appear only when selected to operate in RSTP mode. It indicates whether or not this VPort 704 is the Root of the Spanning Tree (the root is determined automatically).

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

**Protocol of Redundancy**

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

**Bridge priority**

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

**Forwarding Delay**

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

**Hello time (sec.)**

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

**Max. Age (sec.)**

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

**Enable STP per Port**

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

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

**Port Priority**

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

**Port Cost**

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

**Port Status**

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

### Configuration Limits of RSTP/STP

The Spanning Tree Algorithm places limits on three of the configuration items described previously:

[Eq. 1]:  $1 \text{ sec} \leq \text{Hello Time} \leq 10 \text{ sec}$

[Eq. 2]:  $6 \text{ sec} \leq \text{Max. Age} \leq 40 \text{ sec}$

[Eq. 3]:  $4 \text{ sec} \leq \text{Forwarding Delay} \leq 30 \text{ sec}$

These three variables are further restricted by the following two inequalities:

[Eq. 4]:  $2 * (\text{Hello Time} + 1 \text{ sec}) \leq \text{Max. Age} \leq 2 * (\text{Forwarding Delay} - 1 \text{ sec})$

Moxa VPort 704's firmware will alert you immediately if any of these restrictions are violated. For example, setting

Hello Time = 5 sec, Max. Age = 20 sec, and Forwarding Delay = 4 sec does not violate Eqs. 1 through 3, but does violate Eq. 4, since in this case,

$2 * (\text{Hello Time} + 1 \text{ sec}) = 12 \text{ sec}$ , and  $2 * (\text{Forwarding Delay} - 1 \text{ sec}) = 6 \text{ sec}$ .

You can remedy the situation in many ways. One solution is simply to increase the Forwarding Delay value to at least 11 sec.

*HINT:* Perform the following steps to avoid guessing:

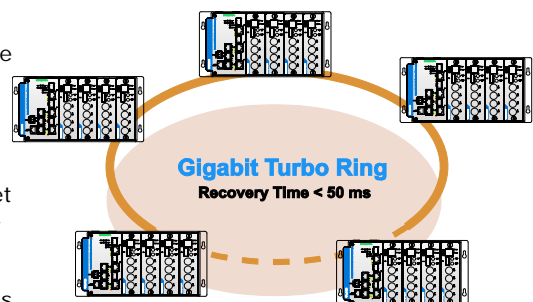
**Step 1:** Assign a value to "Hello Time" and then calculate the left most part of Eq. 4 to get the lower limit of "Max. Age."

**Step 2:** Assign a value to "Forwarding Delay" and then calculate the right most part of Eq. 4 to get the upper limit for "Max. Age."

**Step 3:** Assign a value to "Forwarding Delay" that satisfies the conditions in Eq. 3 and Eq. 4.

### Gigabit Ethernet Redundant Ring Capability (< 50 ms)

Ethernet has become the default data communications medium for industrial automation applications. In fact, Ethernet is often used to integrate video, voice, and high-rate industrial application data transfers into one network. The VPort 704, which comes equipped with a redundant gigabit Ethernet protocol called Gigabit Turbo Ring, gives system maintainers a convenient means of setting up a versatile yet stable gigabit Ethernet network. With Gigabit Turbo Ring, if any segment of the network gets disconnected, your automation system will be back to normal in less than 300 ms (Turbo Ring) or 50 ms (Turbo Ring V2).



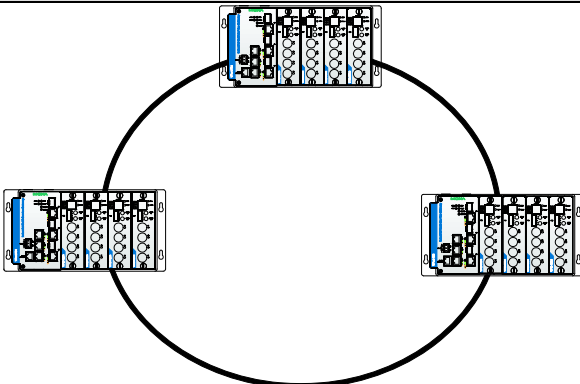


**NOTE** Port trunking and Turbo Ring can be enabled simultaneously to form a backbone. Doing so will increase the bandwidth of the backbone, and also provide redundancy. For example, suppose that two physical ports, 1 and 2, are trunked to form trunk group Trk1, and then Trk1 is set as one Turbo Ring path, if port 1 gets disconnected, the remaining trunked port, port 2, will share the traffic. If port 1 and port 2 are both disconnected, Turbo Ring will create the back up path within 300 ms.

## The Turbo Ring Concept

Moxa developed the proprietary Turbo Ring protocol to optimize communication redundancy and achieve a faster recovery time on the network.

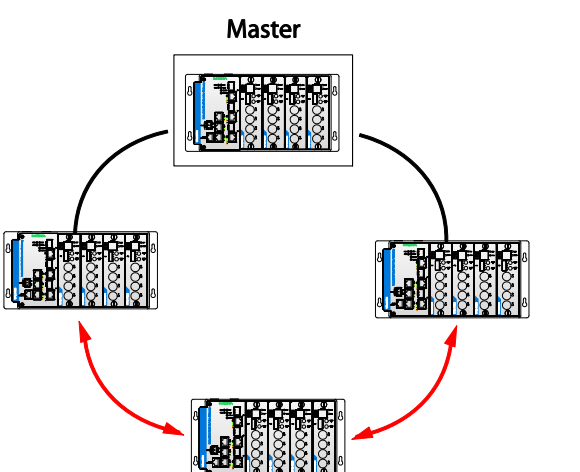
The Turbo Ring and Turbo Ring V2 protocols identify one switch as the *master* of the network, and then automatically block packets from traveling through any of the network’s redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network.

Initial setup of a “Turbo Ring” or “Turbo Ring V2” ring	
	<p>Select any two ports as redundant ports. Connect the redundant ports to form the Turbo Ring</p>

The user does not need to configure any of the switches as the master to use Turbo Ring or Turbo Ring V2. If none of the switches in the ring is configured as the master, then the protocol will automatically assign master status to one of the switches. In fact, the master is only used to identify which segment in the redundant ring acts as the backup path. In the following subsections, we explain how the redundant path is selected for rings configured for Turbo Ring, and Turbo Ring V2.

### Determining the Redundant Path of a “Turbo Ring” Ring

In this case, the redundant segment (i.e., the segment that will be blocked during normal operation) is determined by the number of VPort 704 units that make up the ring, and where the ring master is located.

When the number of VPort 704 units in the Turbo Ring is even.	
<p><b>Master</b></p> 	<p>If there are 2N VPort 704 units (an even number) in the “Turbo Ring” ring, then the backup segment is one of the two segments connected to the (N+1)st VPort 704 (i.e., the VPort 704 unit directly opposite the master).</p>

When the number of VPort 704 units in the Turbo Ring is odd.	
	<p>If there are <math>2N+1</math> VPort 704 units (an odd number) in the "Turbo Ring" ring, with VPort 704 units and segments labeled counterclockwise, then segment <math>N+1</math> will serve as the backup path.</p> <p>For the example shown here, <math>N=1</math>, so that <math>N+1=2</math>.</p>

Determining the Redundant Path of a "Turbo Ring V2" Ring	
	<p>For a "Turbo Ring V2" ring, the backup segment is the segment connected to the 2nd redundant port on the master.</p> <p>See Configuring "Turbo Ring V2" in the Configuring "Turbo Ring" and "Turbo Ring V2" section below.</p>

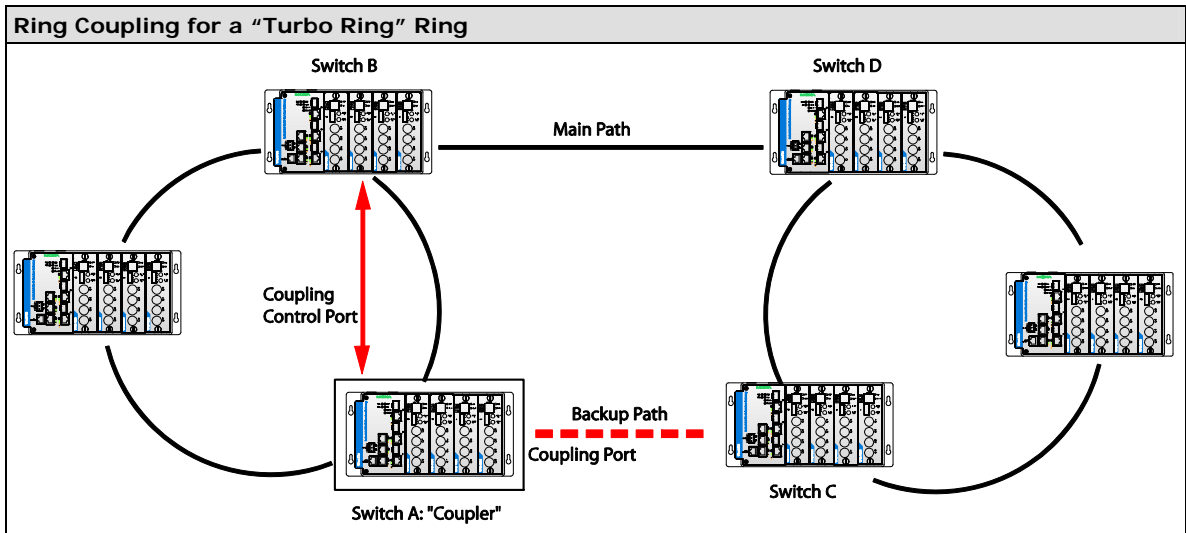
### Ring Coupling Configuration

For some systems, it may not be convenient to connect all devices in the system to create one BIG redundant ring, since some devices could be located in a remote area. For these systems, "Ring Coupling" can be used to separate the devices into different smaller redundant rings, but in such a way that they can still communicate with each other.



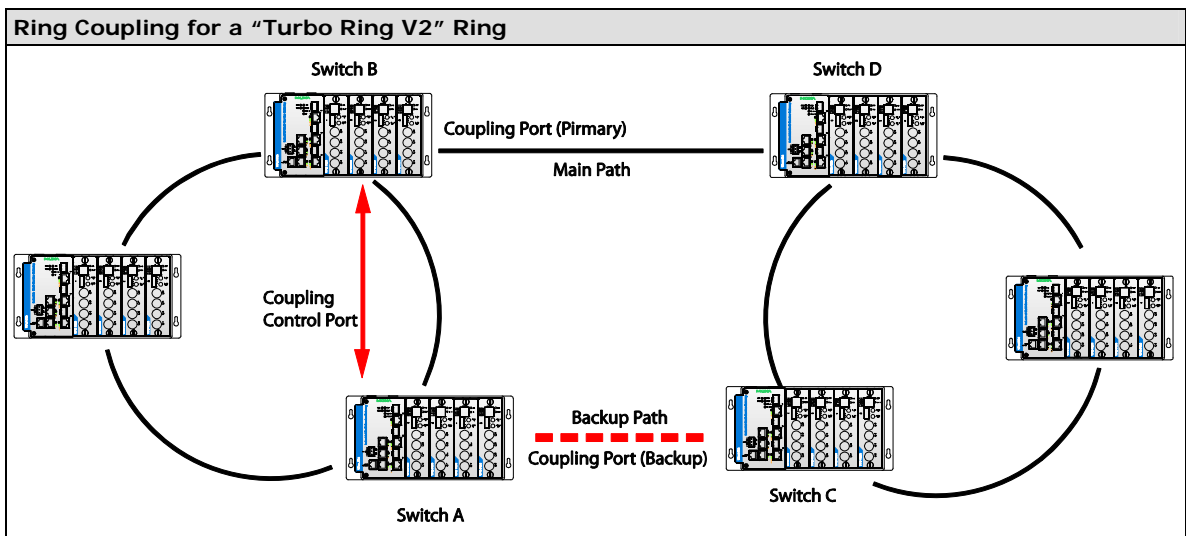
#### ATTENTION

In a VLAN environment, the user must set "Redundant Port" "Coupling Port" and "Coupling Control Port" to join all VLANs, since these ports act as the "backbone" to transmit all packets of different VLANs to different VPort 704 units.



To configure the Ring Coupling function for a **“Turbo Ring”** ring, select two VPort 704 units (e.g., Switch A and B in the above figure) in the ring, and another two VPort 704 units in the adjacent ring (e.g., Switch C and D). Decide which two ports in each switch are appropriate to be used as coupling ports, and then link them together. Next, assign one VPort 704 (e.g., VPort 704 A) to be the **“coupler”** and connect the coupler’s coupling control port with VPort 704 B (for this example).

The coupler switch (i.e., VPort 704 A) will monitor VPort 704 B through the coupling control port to determine whether or not the coupling port’s backup path should be recovered.



Note that the ring coupling settings for a **“Turbo Ring V2”** ring are different from a **“Turbo Ring”** ring. For Turbo Ring V2, Ring Coupling is enabled by configuring the **“Coupling Port (Primary)”** on VPort 704 B, and the **“Coupling Port (Backup)”** on VPort 704 A only. You do not need to set up a coupling control port, so that a **“Turbo Ring V2”** ring does not use a coupling control line.

The **“Coupling Port (Backup)”** on VPort 704 A is used for the backup path, and connects directly to an extra network port on VPort 704 C. The **“Coupling Port (Primary)”** on VPort 704 B monitors the status of the main path, and connects directly to an extra network port on VPort 704 D. With ring coupling established, VPort 704 A can activate the backup path as soon as it detects a problem with the main path.



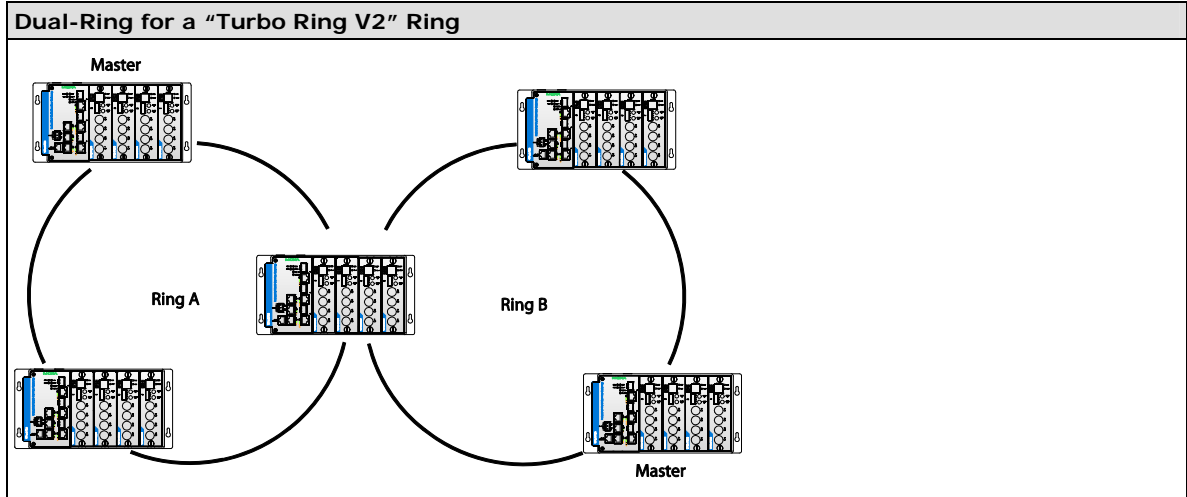
**ATTENTION**

Ring Coupling only neVPort 704 to be enabled on one of the switches serving as the Ring Coupler. The Coupler must designate different ports as the two Turbo Ring ports and the coupling port.

**NOTE** You do not need to use the same VPort 704 unit for both Ring Coupling and Ring Master.

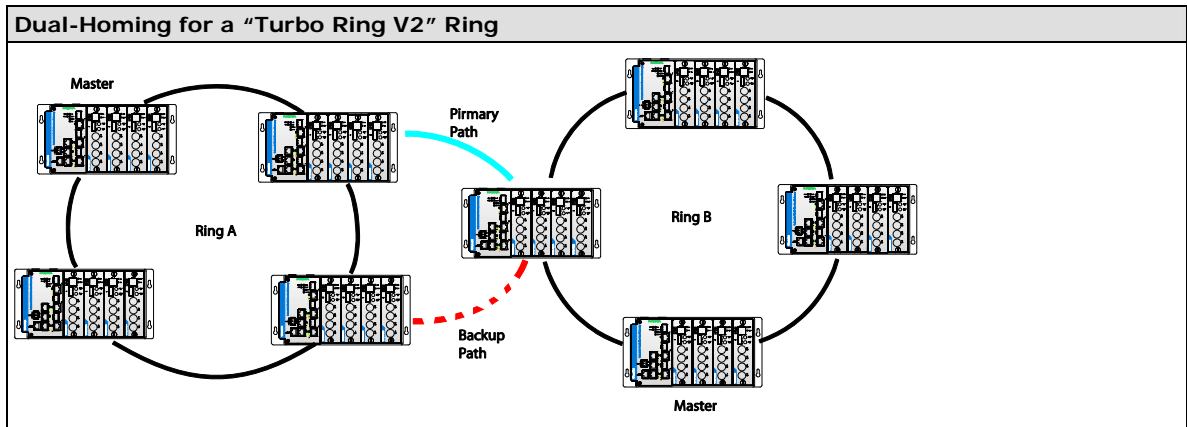
### Dual-Ring Configuration (applies only to “Turbo Ring V2”)

The “**dual-ring**” option provides another ring coupling configuration, in which two adjacent rings share one switch. This type of configuration is ideal for applications that have inherent cabling difficulties.



### Dual-Homing Configuration (applies only to “Turbo Ring V2”)

The “**dual-homing**” option uses a single VPort 704 to connect two networks. The primary path is the operating connection, and the backup path is a back-up connection that is activated in the event that the primary path connection fails.

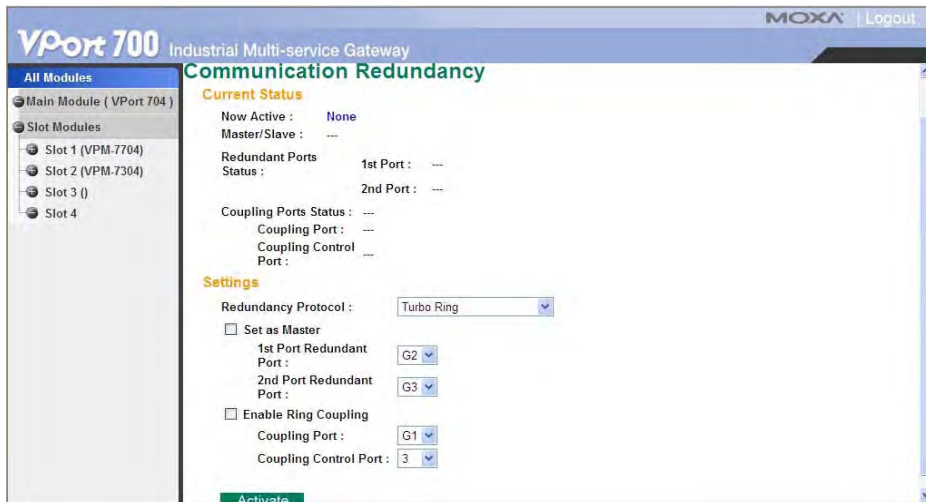


**NOTE** The design of communication redundancy of VPort 704 is as same as Moxa EDS switches, which means you can put VPort 704 on the same network of Moxa EDS switch to build the same redundancy network.

## Configuring “Turbo Ring” and “Turbo Ring V2”

Use the **Communication Redundancy** page to configure select “Turbo Ring” or “Turbo Ring V2” Note that configuration pages for these two protocols are different.

### Configuring “Turbo Ring”



#### Explanation of “Current Status” Items

##### **Now Active**

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

##### **Master/Slave**

Indicates whether or not this VPort 704 is the Master of the Turbo Ring. (This field appears only when selected to operate in Turbo Ring or Turbo Ring V2 mode.)

**NOTE** The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the VPort 704 units in the ring. The master is only used to determine which segment serves as the backup path.

##### **Redundant Ports Status (1st Port, 2nd Port)**

##### **Ring Coupling Ports Status (Coupling Port, Coupling Control Port)**

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

#### Explanation of “Settings” Items

##### **Redundancy Protocol**

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

##### **Set as Master**

Setting	Description	Factory Default
Enabled	Select this VPort 704 as Master	Not checked
Disabled	Do not select this VPort 704 as Master	

**Redundant Ports**

Setting	Description	Factory Default
1st Port	Select any port of the VPort 704 to be one of the redundant ports.	port G2
2nd Port	Select any port of the VPort 704 to be one of the redundant ports.	port G3

**Enable Ring Coupling**

Setting	Description	Factory Default
Enable	Select this VPort 704 as Coupler	Not checked
Disable	Do not select this VPort 704 as Coupler	

**Coupling Port**

Setting	Description	Factory Default
Coupling Port	Select any port of the VPort 704 to be the coupling port	port G1

**Coupling Control Port**

Setting	Description	Factory Default
Coupling Control Port	Select any port of the VPort 704 to be the coupling control port	Port 3

**Configuring “Turbo Ring V2”**



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

**Explanation of “Current Status” Items**

**Now Active**

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

**Ring 1/2—Status**

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

**Ring 1/2—Master/Slave**

Indicates whether or not this VPort 704 is the Master of the Turbo Ring. (This field appears only when selected to operate in Turbo Ring or Turbo Ring V2 mode.)

**NOTE** The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the VPort 704 units in the ring. The master is only used to determine which segment serves as the backup path.

#### ***Ring 1/2—1st Ring Port Status***

#### ***Ring 1/2—2nd Ring Port Status***

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

#### ***Coupling—Mode***

Indicates either **None**, **Dual Homing**, or **Ring Coupling**.

#### ***Coupling—Coupling Port status***

Indicates either **Primary**, or **Backup**.

#### **Explanation of “Settings” Items**

##### ***Redundancy Protocol***

<b>Setting</b>	<b>Description</b>	<b>Factory Default</b>
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

##### ***Enable Ring 1***

<b>Setting</b>	<b>Description</b>	<b>Factory Default</b>
Enabled	Enable the Ring 1 settings	Not checked
Disabled	Disable the Ring 1 settings	

##### ***Enable Ring 2\****

<b>Setting</b>	<b>Description</b>	<b>Factory Default</b>
Enabled	Enable the Ring 2 settings	Not checked
Disabled	Disable the Ring 2 settings	

**\*You should enable both Ring 1 and Ring 2 when using the Dual-Ring architecture.**

##### ***Set as Master***

<b>Setting</b>	<b>Description</b>	<b>Factory Default</b>
Enabled	Select this VPort 704 as Master	Not checked
Disabled	Do not select this VPort 704 as Master	

##### ***Redundant Ports***

<b>Setting</b>	<b>Description</b>	<b>Factory Default</b>
1st Port	Select any port of the VPort 704 to be one of the redundant ports.	port G2
2nd Port	Select any port of the VPort 704 to be one of the redundant ports.	port G3

##### ***Enable Ring Coupling***

<b>Setting</b>	<b>Description</b>	<b>Factory Default</b>
Enable	Select this VPort 704 as Coupler	Not checked
Disable	Do not select this VPort 704 as Coupler	

**Coupling Mode**

Setting	Description	Factory Default
Dual Homing	Select this item to change to the Dual Homing configuration page	Primary Port: port 2 Backup Port: port 1
Ring Coupling (backup)	Select this item to change to the Ring Coupling (backup) configuration page	port 2
Ring Coupling (primary)	Select this item to change to the Ring Coupling (primary) configuration page	port 2

**Primary/Backup Port**

Setting	Description	Factory Default
Primary Port	Select any port of the VPort 704 to be the primary port.	port 2
Backup Port	Select any port of the VPort 704 to be the backup port.	port 1

**QoS**

Click on the QoS in Network's menu. Quality of Service (QoS) provides a traffic prioritization capability to ensure that important data is delivered consistently and predictably. EDS-510A Series can inspect IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information, to provide a consistent classification of the entire network. VPort 704' QoS capability improves your industrial network's performance and determinism for mission critical applications..



Moxa VPort 704 supports inspection of layer 3 TOS and/or layer 2 CoS tag information to determine how to classify traffic packets.

**Queuing Mechanism**

Setting	Description	Factory Default
Weighted Fair	VPort 704 has 4 priority queues. In the weighted fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair



Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures all high priority frames to egress the switch as soon as possible.	
--------	---	--

**Port Highest Priority**

Setting	Description	Factory Default
Low/Normal/ Medium/High	Set the Port Default Priority of the ingress frames to different priority queues. If the received packets are not equipped with any tag information (CoS, TOS) the default port priority will take effect.	Normal

**Inspect TOS**

Setting	Description	Factory Default
Enable/Disable	Select the option to enable VPort 704 to inspect the Type of Service (TOS) bits in IPV4 frame to determine the priority of each frame.	Enable

**Inspect COS**

Setting	Description	Factory Default
Enable/Disable	Select the option to enable VPort 704 to inspect the 802.1p COS tag in the MAC frame to determine the priority of each frame.	Enable

**NOTE** The priority of an ingress frame is determined in order by:

1. Inspect TOS
2. Inspect CoS
3. Port Highest Priority

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

## CoS Mapping

### Mapping Table of CoS Value and Priority Queues

QoS Function List CoS Mapping Settings

CoS	Priority Queue
0	Low <input type="button" value="v"/>
1	Low <input type="button" value="v"/>
2	Normal <input type="button" value="v"/>
3	Normal <input type="button" value="v"/>
4	Medium <input type="button" value="v"/>
5	Medium <input type="button" value="v"/>
6	High <input type="button" value="v"/>
7	High <input type="button" value="v"/>

**QoS Function List**

Setting	Description	Factory
Low/Normal/ Medium/High	Set the mapping table of different CoS values to 4 different egress queues.	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

**TOS/DiffServ Mapping**

**Mapping Table of ToS (DSCP) Value and Priority Queues**

QoS Function List ToS Mapping Settings ▾

ToS	Level	ToS	Level	ToS	Level	ToS	Level
0x40(17)	Normal ▾	0x44(18)	Normal ▾	0x48(19)	Normal ▾	0x4C(20)	Normal ▾
0x50(21)	Normal ▾	0x54(22)	Normal ▾	0x58(23)	Normal ▾	0x5C(24)	Normal ▾
0x60(25)	Normal ▾	0x64(26)	Normal ▾	0x68(27)	Normal ▾	0x6C(28)	Normal ▾
0x70(29)	Normal ▾	0x74(30)	Normal ▾	0x78(31)	Normal ▾	0x7C(32)	Normal ▾
0x80(33)	Medium ▾	0x84(34)	Medium ▾	0x88(35)	Medium ▾	0x8C(36)	Medium ▾
0x90(37)	Medium ▾	0x94(38)	Medium ▾	0x98(39)	Medium ▾	0x9C(40)	Medium ▾
0xA0(41)	Medium ▾	0xA4(42)	Medium ▾	0xA8(43)	Medium ▾	0xAC(44)	Medium ▾
0xB0(45)	Medium ▾	0xB4(46)	Medium ▾	0xB8(47)	Medium ▾	0xBC(48)	Medium ▾
0xC0(49)	High ▾	0xC4(50)	High ▾	0xC8(51)	High ▾	0xCC(52)	High ▾
0xD0(53)	High ▾	0xD4(54)	High ▾	0xD8(55)	High ▾	0xDC(56)	High ▾
0xE0(57)	High ▾	0xE4(58)	High ▾	0xE8(59)	High ▾	0xEC(60)	High ▾
0xF0(61)	High ▾	0xF4(62)	High ▾	0xF8(63)	High ▾	0xFC(64)	High ▾

**Activate**

**ToS Mapping Settings**

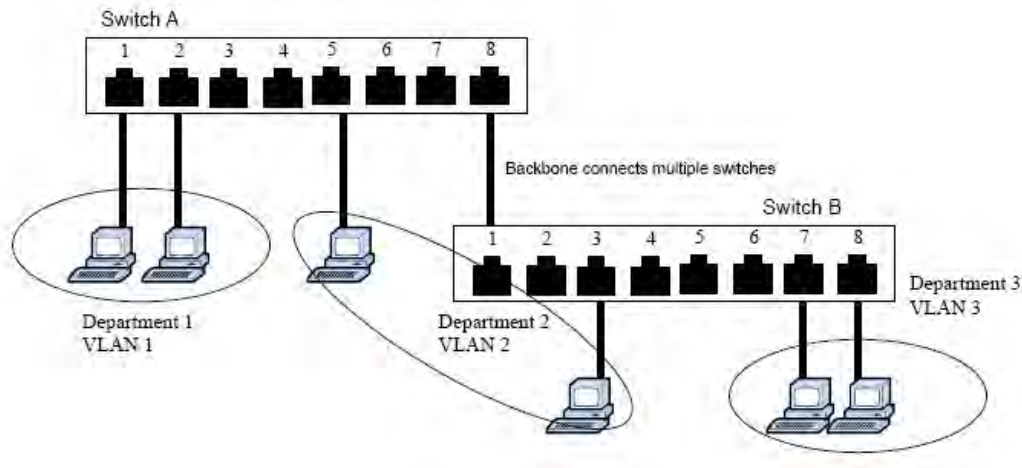
Setting	Description	Factory Default
Low/Normal/ Medium/High	Set the mapping table of different TOS values to 4 different egress queues.	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

**VLAN**

Click on the VLAN in Network’s menu.

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

- **Departmental groups**—You could have one VLAN for the Marketing department, another for the Finance department, and another for the Development department.
- **Hierarchical groups**—You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—You could have one VLAN for e-mail users, and another for multimedia users.



## VLANs and Moxa VPort 704

Your VPort 704 provides support for VLANs using IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-1998 standard allows each port on your VPort 704 to be placed in:

- Any one VLAN defined on the VPort 704.
- Several VLANs at the same time using 802.1Q tagging.

The standard requires that you define the *802.1Q VLAN ID* for each VLAN on your VPort 704 before the switch can use it to forward traffic:

## Managing a VLAN

A new or initialized VPort 704 contains a single VLAN—the Default VLAN. This VLAN has the following definition:

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

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the VPort 704 over the network.

## Communication between VLANs

If devices connected to a VLAN need to communicate to devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

## VLANs: Tagged and Untagged Membership

The VPort 704 supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical (backbone, trunk) link. When setting up VLANs you need to understand when to use untagged and tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, tagged membership must be defined.

A typical host (e.g., clients) will be untagged members of one VLAN, defined as “Access Port” in the VPort 704, while inter-switch connections will be tagged members of all VLANs, defined as “Trunk Port” in the VPort 704.

The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs to. If a frame is carrying the additional information, it is known as a *tagged* frame.

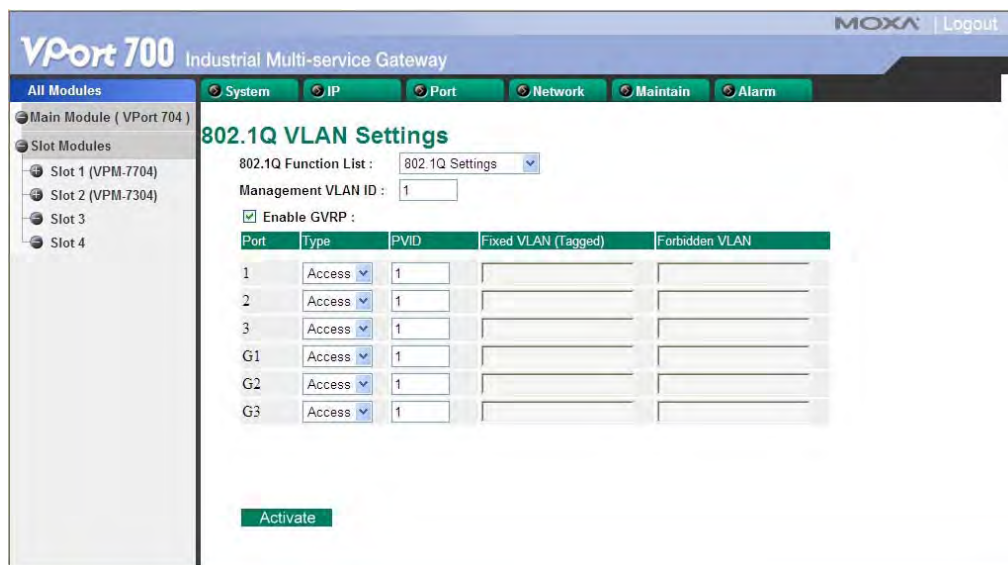
To carry multiple VLANs across a single physical (backbone, trunk) link, each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong to which VLAN. To communicate between VLANs, a router must be used.

The VPort 704 supports two types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that determines to which VLAN the device belongs. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the VPort 704 will insert this PVID into this packet to help the next 802.1Q VLAN switch recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices/tagged devices and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the port default PVID as its VID.

## Configuring Virtual LAN

To configure the VPort 704's **802.1Q VLAN**, use the VLAN Settings page to configure the ports.



### Management VLAN ID

Setting	Description	Factory Default
VLAN ID ranges from 1 to 4094	Set the management VLAN of this EDS-510A.	1

### Enable GVRP

Setting	Description	Factory Default
Enable/Disable	Select the option to enable/disable the GVRP function.	Enable

### Port Type

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

**ATTENTION**

For communication redundancy in the VLAN environment, set "Redundant Port," "Coupling Port," and "Coupling Control Port" as "Trunk Port," since these ports act as the "backbone" to transmit all packets of different VLANs to different VPort 704 units.

**Port PVID**

Setting	Description	Factory Default
VID range from 1 to 4094	Set the port default VLAN ID for untagged devices that connect to the port.	1

**Fixed VLAN List (Tagged)**

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

**Forbidden VLAN List**

Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the "Trunk" port type. Set the VLAN IDs that will not be supported by this trunk port. Use commas to separate different VLANs.	None

**VLAN Table****VLAN Table**

VLAN Mode            802.1Q VLAN  
 Management VLAN    1

Index	VID	Joined Access Port	Joined Trunk Port
1	1	1, 2, 3, G1, G2, G3,	

In 802.1Q VLAN table, you can review the VLAN groups that were created, Joined Access Ports, and Trunk Ports, and in Port-based VLAN table, you can review the VLAN group and Joined port.

**NOTE** The physical network can have a maximum of 64 VLAN settings.

**IGMP**

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your VPort 704.

**The Concept of Multicast Filtering****What is an IP Multicast?**

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

bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

## Benefits of Multicast

The benefits of using IP multicast are that it:

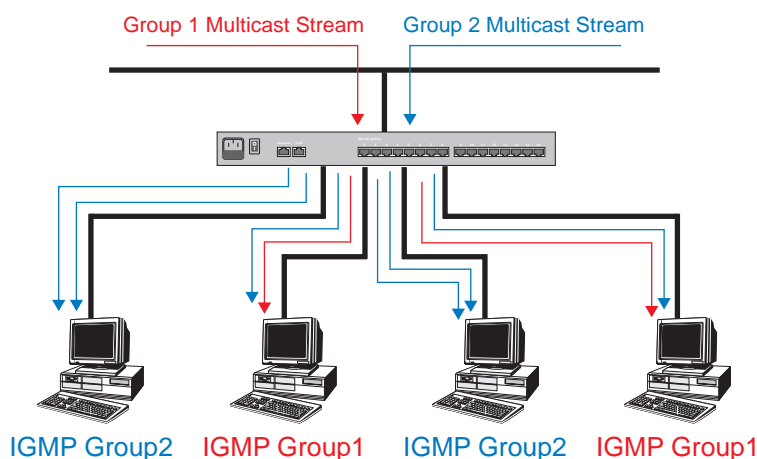
- Uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- Reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- Makes efficient use of network bandwidth and scales well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

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

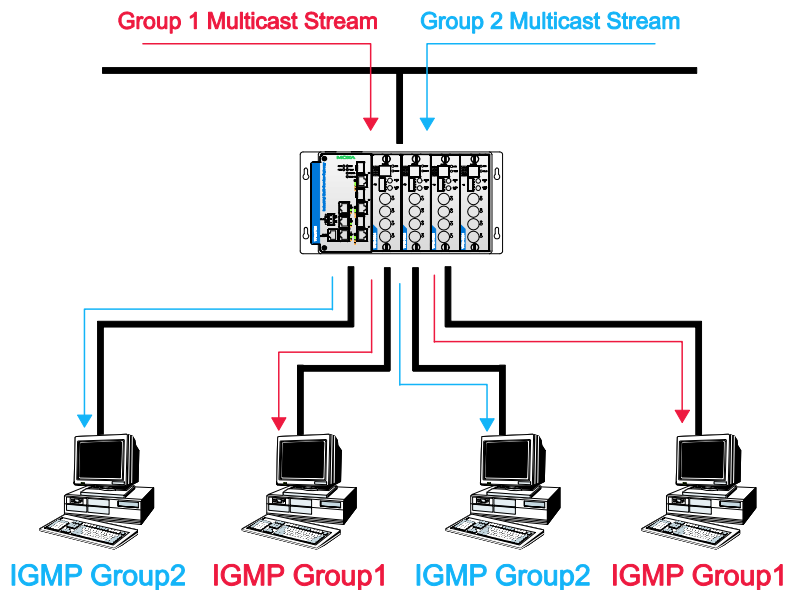
## Multicast Filtering

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

### Network without multicast filtering



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

**Network with multicast filtering**

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

## Multicast Filtering and VPort 704

The VPort 704 has three ways to achieve multicast filtering: IGMP (Internet Group Management Protocol) Snooping, GMRP (GARP Multicast Registration Protocol), and adding a static multicast MAC manually to filter multicast traffic automatically.

### IGMP (Internet Group Management Protocol)

#### *Snooping Mode*

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

#### *Query Mode*

Query mode allows the VPort 704 to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs. IGMP querying is enabled by default on the VPort 704 to help prevent interoperability issues with some multicast routers that may not follow the lowest IP address election method. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers).

**NOTE** The VPort 704 is compatible with any device that conforms to the IGMP v2 device protocol.

## IGMP Multicast Filtering

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

The IP router (or querier) periodically sends *query* packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with IP address lower than the IP address of any other IGMP queriers connected to the LAN or VLAN can become the IGMP querier.

When an IP host receives a query packet, it sends a *report* packet back that identifies the multicast group that the end-station would like to join.

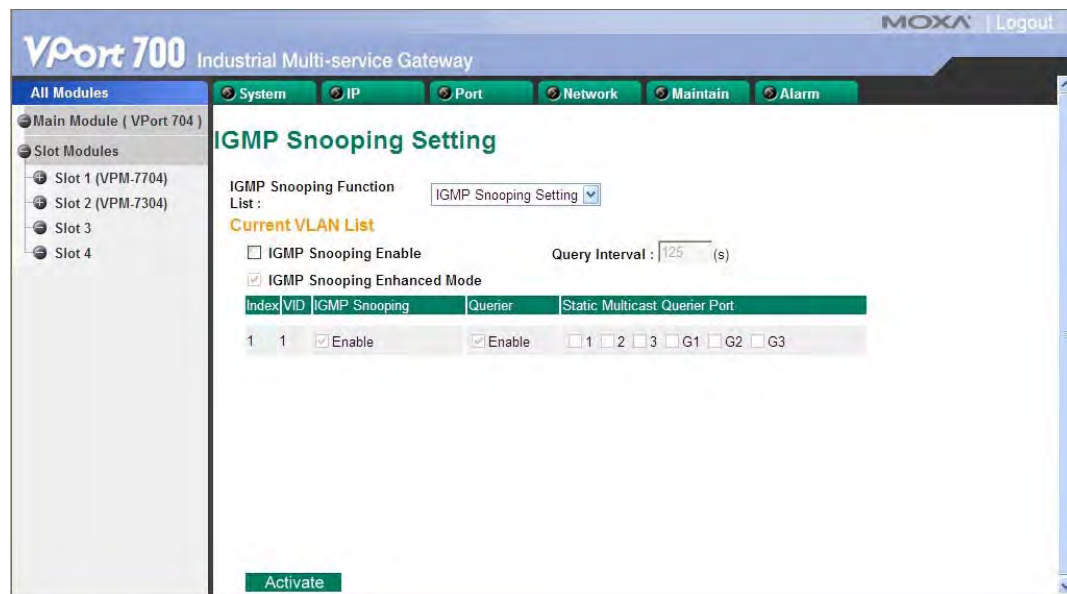
When the report packet arrives at a port on a switch with *IGMP Snooping* enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.

When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.

When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

## Configuring IGMP Snooping

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



### IGMP Snooping Enable

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the IGMP Snooping function globally.	Disabled

### IGMP Snooping Enhanced Mode

Setting	Description	Factory Default
Enable	IGMP Multicast packets will forward to : Learned Multicast Querier Ports Member Ports	Enable
Disable	IGMP Multicast packets will forward to : Learned multicast Querier Ports Static Multicast Querier Ports Querier Connected Ports Member Ports	

### Query Interval

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



**IGMP Snooping**

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the IGMP Snooping function per VLAN.	Enabled if IGMP Snooping Enabled Globally

**NOTE** We suggest the following IGMP Snooping configurations-

**When the network is mixed with third party switches, such as Cisco:**

- IGMP Snooping Enable
- IGMP Snooping Enhanced Mode

**When the network consists entirely of Moxa switches:**

- IGMP Snooping Enable
- IGMP Snooping Enhanced Mode

**Querier**

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the VPort 704's querier function.	Enabled if IGMP Snooping is Enabled Globally

**Static Multicast Router Port**

Setting	Description	Factory Default
Select/Deselect	Select the option to select which ports will connect to the multicast routers. It's active only when IGMP Snooping is enabled.	Disabled

**NOTE** At least one switch must be designated the Querier or enable IGMP snooping and GMRP when enabling Turbo Ring and IGMP snooping simultaneously.

**IGMP Table**

The VPort 704 displays the current active IGMP groups that were detected.

**Current Active IGMP Groups**

IGMP Snooping Function List IGMP Snooping Table

	Auto Learned Multicast Querier Port	Static Multicast Querier Port	Querier Connected Port	Act as Querier	Active IGMP Groups		
					IP	MAC	Members Port
1				Yes	239.255.255.250	01-00-5E-7F-FF-FA	1

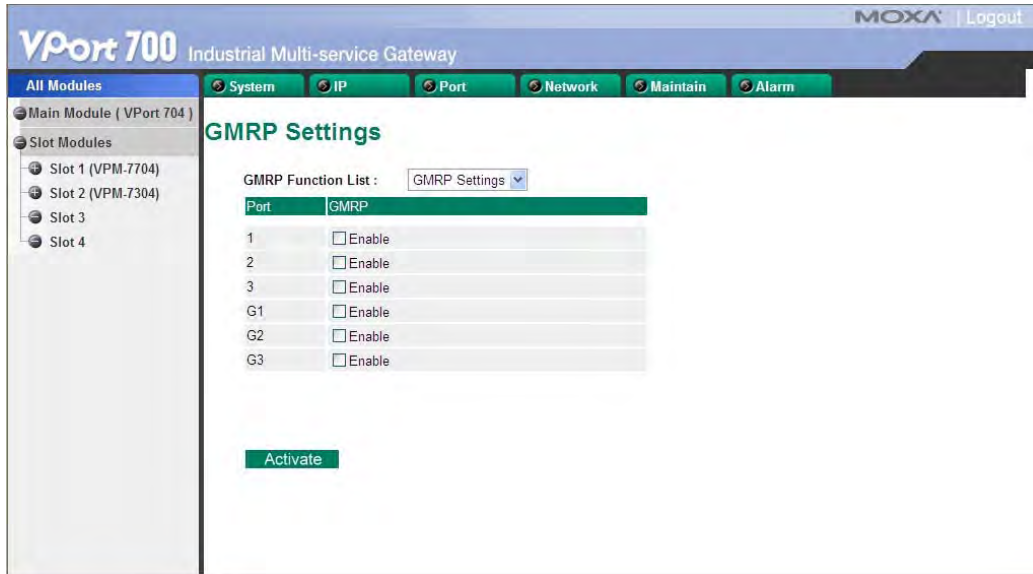
The information includes **VID**, **Auto-learned Multicast Router Port**, **Static Multicast Router Port**, **Querier Connected Port**, and the **IP** and **MAC** addresses of active IGMP groups.

**GMRP (GARP Multicast Registration Protocol)**

The VPort 704 supports IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol), which differs from IGMP (Internet Group Management Protocol). GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or de-register Group membership information dynamically. GMRP functions similarly to GVRP, except that GMRP registers multicast addresses on ports. When a port receives a **GMRP-join** message, it will register the multicast address to its database if the multicast address is not registered, and all the multicast packets with that multicast address are able to be forwarded from this port. When a port receives a **GMRP-leave** message, it will de-register the multicast address from its database, and all the multicast packets with this multicast address are not able to be forwarded from this port.

## Configuring GMRP

GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or un-register Group membership information dynamically.



### GMRP enable

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the GMRP function for the port listed in the Port column	Disable

## GMRP Table

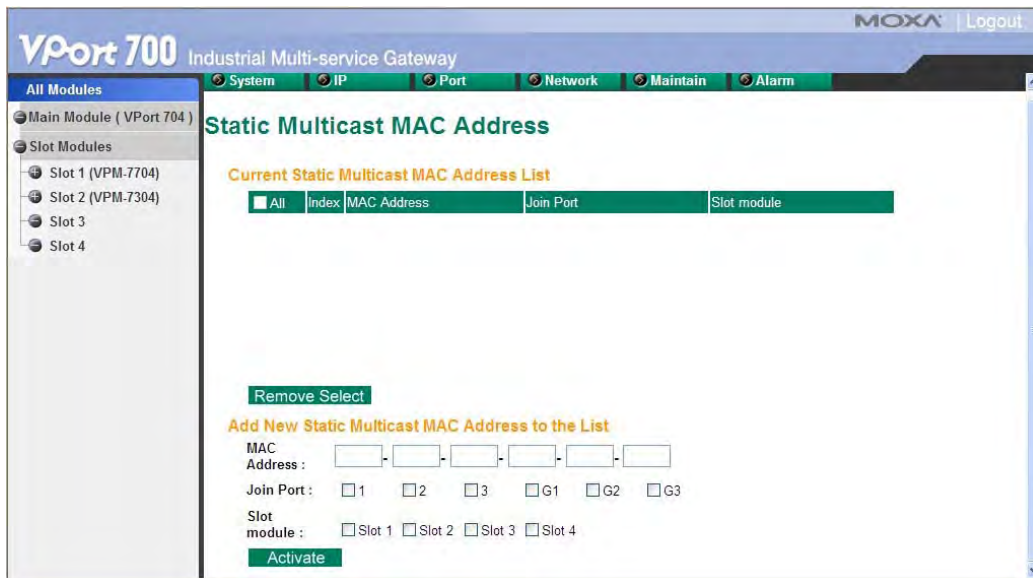
The VPort 704 displays the current active GMRP groups that were detected.

	Multicast Address	Fixed Ports	Learned Ports
1	01-00-5E-00-00-01	1,2	

Setting	Description
Fixed Ports	This multicast address is defined by static multicast.
Learned Ports	This multicast address is learned by GMRP.

## Static Multicast MAC

Click on Static Multicast MAC in Network's menu. Some devices may only support multicast packets, but not support either IGMP Snooping or GMRP. The VPort 704 supports adding multicast groups manually to enable multicast filtering.



**Add New Static Multicast Address to the List**

Setting	Description	Factory Default
MAC Address	Input the multicast MAC address of this host.	None

**MAC Address**

Setting	Description	Factory Default
integer	Input the number of the VLAN to which the host with this MAC Address belongs.	None

**Join Port**

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

## Line Swap

Click on Line Swap in Network’s menu. The Line-Swap function, which is enabled by default, allows the VPort 704 to return to normal operation extremely quickly after devices are unplugged and then re-plugged into different ports. The recovery time is on the order of a few milliseconds (compare this with standard commercial switches for which the recovery time could be on the order of several minutes). To disable the Line-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access the Web Console interface’s **Line-Swap fast recovery** page, as the following figure shows:



**Line Swap Fast Recovery**

Setting	Description	Factory Default
Enable/Disable	Select this option to enable the Line-Swap-Fast-Recovery function	Enable

## Firmware Upgrade

Click on Firmware Upgrade in Maintain's menu.



Take the following steps to upgrade the firmware:

**Step 1:** Press the **Browse** button to select the firmware file.

**NOTE** For the VPort 704, the firmware file extension should be .rom.

**Step 2:** Click on the **Upgrade** button to upload the firmware to the VPort.

**Step 3:** The system will start to run the firmware upgrade process.

**Step 4:** Once **Firmware Update Success.....Reboot....** is shown, please wait for few seconds for the VPort to reboot. The reboot process is finished once the **STAT** LED is lit continuously in green.

**NOTE** Upgrading the firmware upgrade will not change the original settings.

## Configuration Import/ Export

Click on Configuration Import/Export in Maintain's menu. Administrators can also save this information in a file (sys\_config.ini) by clicking the **Export** button, or import a file by clicking the **Browse** button to search a sys\_config.ini file and the **Import** button to update the system configuration quickly.



## Factory Default

Click on Factory Default in Maintain's menu. Click on Activate to reset the VPort to its factory default settings.



**NOTE** All parameters will be reset to factory defaults when you use the Factory Default function. For this reason, if you want to keep a digital copy of the current configuration, remember to export the sys\_config.ini file before using the Factory Default function.

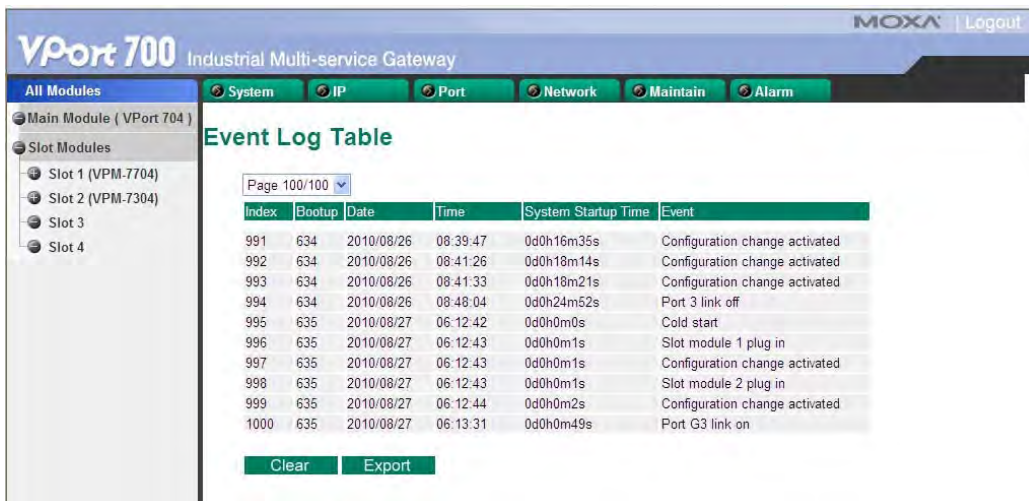
## Reboot

Click on Reboot in Maintain's menu. Click on Activate to reboot the VPort.



## Log History

Click on Log History in Alarm menu. VPort 704 can save 1000 logs in its database. These logs also can be exported as a file, or be cleared.



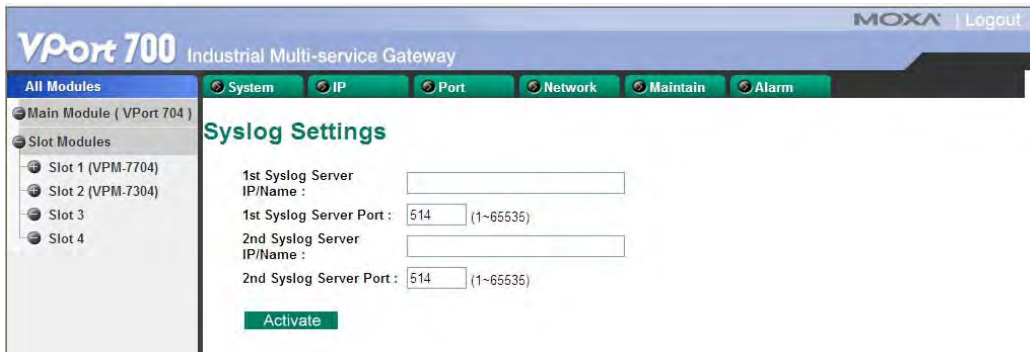
Bootup	This field shows how many times the EDS-510A has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the "Basic Setting" page.
Time	The time is updated based on how the current time is set in the "Basic Setting" page.
System Startup Time	The system startup time related to this event.
Events	Events that have occurred.

**NOTE** The following events will be recorded into the VPort 704's Log table:

- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off ( On), Power 1/2 transition (On ( Off)
- Authentication fail
- Topology changed
- Master setting is mismatched
- DI 1/2 transition (Off ( On), DI 1/2 transition (On ( Off)
- Port traffic overload
- dot1x Auth Fail
- Port link off / on

## Sys log

Click on Sys log in Alarm menu. 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

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

### Syslog Server 2

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

## Email Alarm

Click on Email Alarm in Alarm menu. The Email Alarm 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:

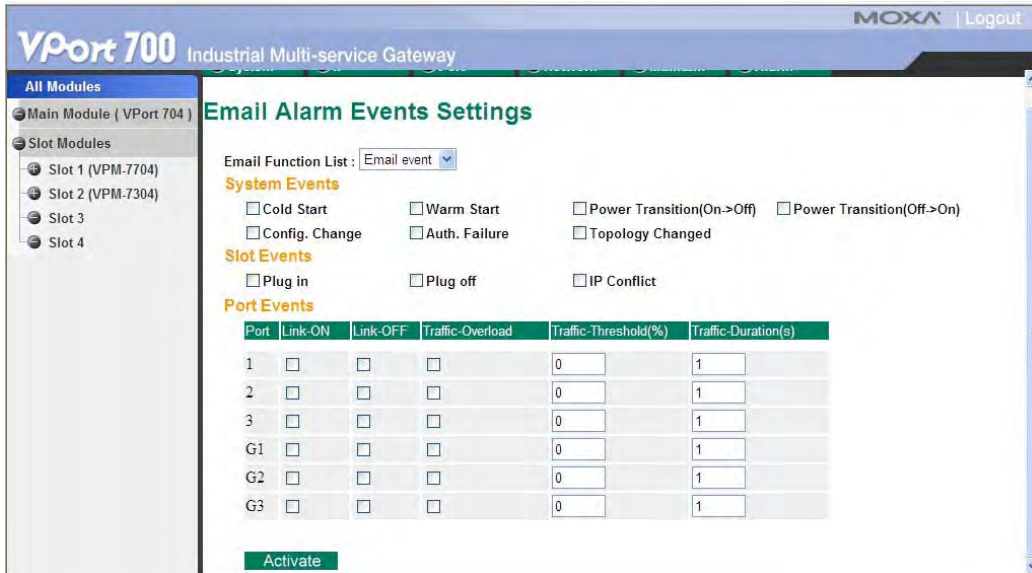
- **Configuring Email Event Types**  
Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Email Alarm Events setting* subsection).

- **Configuring Email Settings**

To configure the VPort 704's email setup from the Console interface or browser interface, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address to which warning messages will be sent.

- **Activate your settings and if necessary, test the email**

After configuring and activating your VPort 704'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 Types can be divided into three basic groups: **System Events**, **Slot Events** and **Port Events**. **System Events**

System Events	Warning e-mail is sent when...
Switch Cold Start	Power is cut off and then reconnected.
Switch Warm Start	The VPort 704 is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	The VPort 704 is powered down.
Power Transition (Off→On)	The VPort 704 is powered up.
Configuration Change Activated	A configuration item has been changed.
Authentication Failure	An incorrect password is entered.
Comm. Redundancy Topology Changed	Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). The Master of the Turbo Ring has changed or the backup path is activated.

**Slot Events**

Slot Events	Warning e-mail is sent when...
Plug-in	A slot module is plugged into VPort 704's slot
Plug off	A slot module is removed from VPort 704's slot
IP conflict	The IP address of 2 slot modules are conflicted.

**Port Events**

Port Events	Warning e-mail is sent when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a non-zero number if the port's Traffic-Overload item is Enabled.

Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.
-------------------------	--

**NOTE** The Traffic-Overload, Traffic-Threshold (%), and Traffic-Duration (sec.) Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a non-zero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

**NOTE** Warning e-mail messages will have the sender field formatted in the form:  
Moxa\_EtherDevice\_Switch\_0001@Switch\_Location  
where Moxa\_EtherDevice\_Switch is the default Switch Name, 0001 is the VPort 704's serial number, and Switch\_Location is the default Server Location.  
Refer to the Basic Settings section to see how to modify Switch Name and Switch Location.

## Email Setting

There are 2 SMTP servers can be setup for email alarm transmission. If the 1<sup>st</sup> SMTP server is failed in transmission, then the 2<sup>nd</sup> SMTP server will be activated immediately.

### Email Settings

#### 1st SMTP Server and Sender Email

Mail server

Mail account

Mail password

Change mail password

Old

New

Retype

Email address

#### 2nd SMTP Server and Sender Email

Mail server

Mail account

Mail password

Change mail password

Old

New

Retype

Email address

#### Recipient's email address

1st email address

2nd email address

3rd email address

4th email address

#### Mail Server

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

#### Mail Account

Setting	Description	Factory Default
Max. 45 Characters	Your email account name (typically your user name)	None

#### Mail Password

Setting	Description	Factory Default
Disable/Enable to change Mail Password	To reset the Password from the Web Browser interface, click the Change password check-box, type the Old Password, type the New Password, retype the New password, and then click Activate; Max. 45 Characters.	Disable
Old Password	Type the current password when changing the password	None
New Password	Type new password when enabled to change password; Max. 45 Characters.	None
Retype Password	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



**Email Address**

Setting	Description	Factory Default
Max. 30 characters	You can set up to 4 email addresses to receive alarm emails from the VPort 704.	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.

## Relay Alarm Event

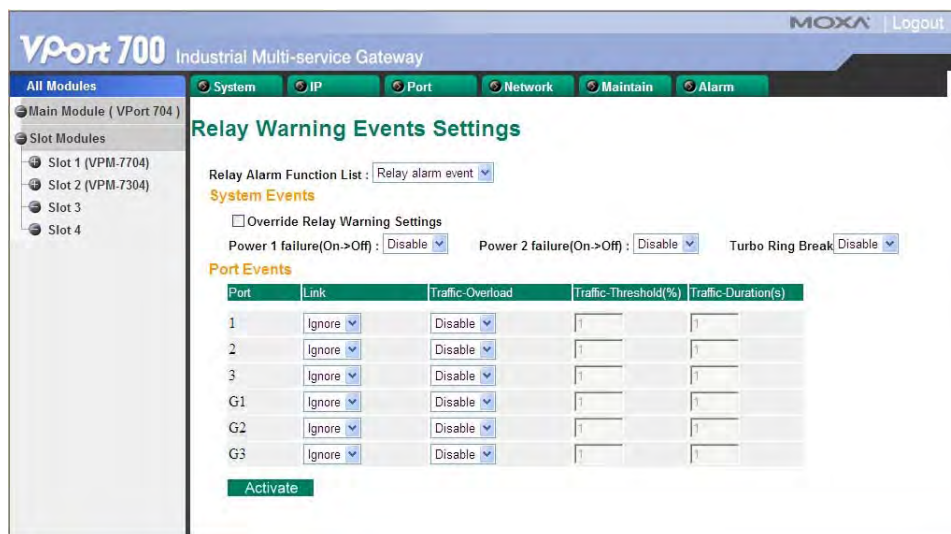
Click on Relay Alarm Event in Alarm menu. The Relay Alarm Event function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

- **Configuring Relay Event Types**

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

- **Activate your settings**

After completing the configuration procedure, you will need to activate your VPort 704'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 switch, whereas Port Events are related to the activity of a specific 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.

**System Events**

System Events	Warning Relay output is triggered when...
Power Transition (On→Off)	The VPort 704 is powered on.
Power Transition (Off→On)	The VPort 704 is powered down.
Turbo Ring Break (Ring Master Only)	When the VPort 704 is the Master of this Turbo Ring, and the Turbo Ring is disconnected.

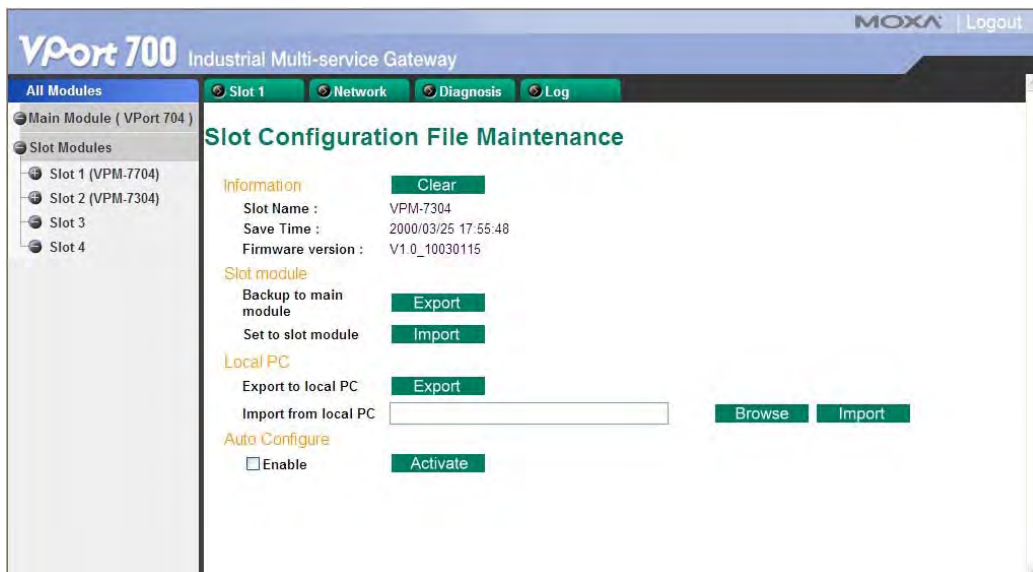
**Port Events**

Port Events	Warning e-mail is sent when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a non-zero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.

**NOTE** The Traffic-Overload, Traffic-Threshold (%), and Traffic-Duration (sec) Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a non-zero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

## Slot Configuration Maintenance

Click on Configuration Maintenance in Slot menu. For the management convenience, the configurations of slot module can be saved in VPort 704's memory for backup purpose. Once it is required to recover the original configurations, the configuration file being saved in VPory 704 can be imported to the slot module, or a new slot module. In addition, the slot module's configuration file can also be configured to be imported to the slot module automatically once the slot module is reboot.



**Information**

This information shows which slot module's configuration file currently used, and what time it is currently exported. In addition, the firmware version is also shown in case of the wrong operation in importing different firmware version's configuration file.

**Slot Module**

Setting	Description
Backup to main module	Save the current configurations to VPort 704
Set to slot module	Import the VPort 704's configuration file to the slot module

**NOTE** If you change a new slot module, please make sure its model is as same as the previous one when you use the Set to slot module function due to the VPort 704 uses the slot number as the distinguish in saving the slot module's configurations.

**Local PC**

Setting	Description
Export to local PC	Save the current configurations to the local PC
Import form Local PC	Import the local PC's configuration file to the slot module

**Auto Configure**

Setting	Description
Enable/ Disable	Enable or disable the import of slot module's configuration file being saved in VPort 704 automatically once the slot module is reboot.

**NOTE** Because some configuration changes will restart the slot module, if Auto Configure is enabled we strongly recommend backing up the slot module's configurations to the VPort 704 each time the slot module's configurations are changed.

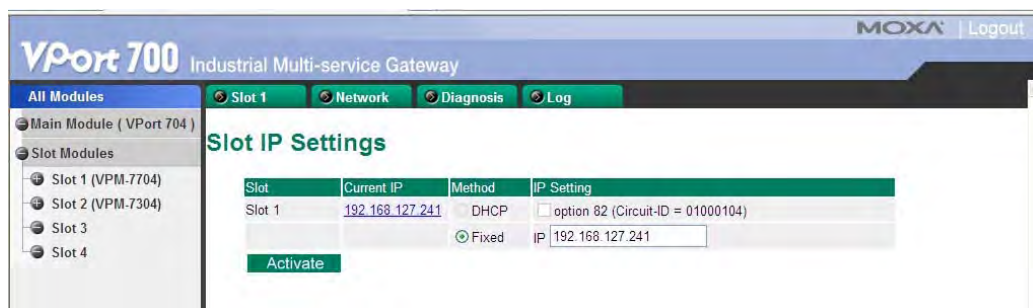
## Slot Operation

Click on Operation in Slot menu. The administrator can configure the slot module in power on, power down, return to factory default and reboot in this section.



## Slot IP Settings

Click on IP in Slot's Network menu. This section provides the IP settings for each slot module. The configuration method is as same as the IP settings of VPort 704's IP settings.



## Slot Network Configure

Click on IP in Slot's Network menu. This section provides the network parameters for each slot module. The configurations of QoS and Traffic Rate Limiting are as same as VPort 704's configurations.

### Network Parameters

#### QoS

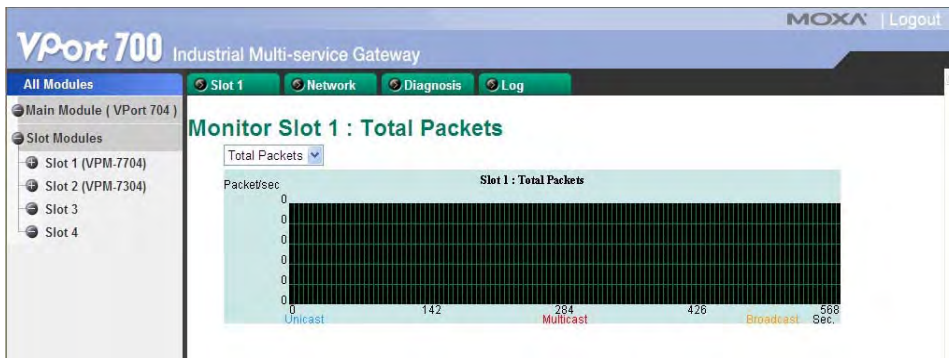
Traffic priority

#### Traffic Rate Limiting

Rate

## Slot Monitor

Click on Monitor in Slot's Diagnosis menu. This section provides the network traffic monitor for each slot module. The configurations are as same as VPort 704's network monitor.



## Slot Test

Click on Test in Slot's Diagnosis menu. This section can ping the slot module to see if its network communication is alive or not.



## Slot Event Log List

Click on Event Log List in Slot's Log menu. This section provides the log list of each slot. Each slot can have maximum 500 logs in the database. The log includes the Bootup, Date, Time, Startup Time, Model, MAC and Event. And the event includes Plug In, Plug Out, Power On, Power Down, Ready State and Operation.

Page 50/50

Index	System			Slot		Event
	Bootup	Date	Time	Model	Mac	
491	632	2010/08/23 09:01:30	0d0h40m28s	VPM-7704	00-90-E8-23-94-03	System Cold Start
492	632	2010/08/23 09:19:32	0d0h58m30s	VPM-7704	00-90-E8-23-94-03	Plug out
493	634	2010/08/26 08:39:47	0d0h16m35s	---	---	Plug in
494	634	2010/08/26 08:39:48	0d0h16m36s	---	---	Power on
495	634	2010/08/26 08:40:32	0d0h17m20s	VPM-7704	00-90-E8-23-94-03	Ready state
496	634	2010/08/26 08:40:33	0d0h17m21s	VPM-7704	00-90-E8-23-94-03	System Cold Start
497	635	2010/08/27 06:12:43	0d0h0m1s	---	---	Plug in
498	635	2010/08/27 06:12:44	0d0h0m2s	---	---	Power on
499	635	2010/08/27 06:13:28	0d0h0m46s	VPM-7704	00-90-E8-23-94-03	Ready state
500	635	2010/08/27 06:13:29	0d0h0m47s	VPM-7704	00-90-E8-23-94-03	System Cold Start

[Slot module log page](#)

Clear Export

## Slot Alarm Trigger

Click on Alarm Trigger in Slot's Log menu. This section provides the capability of sending SNMP Trap and email alarm for those slot modules, which don't have these 2 kinds of functions.

Alarm Trigger Email

Alarm Trigger Snmp Trap

Activate

## VPort 700 Utility GUI

---

VPort 700 Utility is a comprehensive Windows-based GUI that is used to configure and maintain multiple VPort 700 series . A suite of useful utilities is available to help you locate the VPort 700 series attached to the same LAN as the PC host (regardless of whether or not you know the IP addresses of the switches), connect to an VPort 700 whose IP address is known, modify the network configurations of one or multiple VPort 700 series, and update the firmware of one or more VPort 700 series. VPort 704 Utility is designed to provide you with instantaneous control of *all* of your VPort 700, regardless of location. You may download the VPort 704 Utility software from Moxa's website free of charge.

The following topics are covered in this chapter:

- ❑ **Starting VPort 700 Utility**
- ❑ **Broadcast Search**
- ❑ **Search by IP address**
- ❑ **Upgrade Firmware**
- ❑ **Modify IP Address**
- ❑ **Export Configuration**
- ❑ **Import Configuration**
- ❑ **Convert**

# Starting VPort 700 Utility

To start VPort 700 Utility, locate and then run the executable file **VPort 700Utility.exe**. Follow the installation process to install the VPort 700 utility.

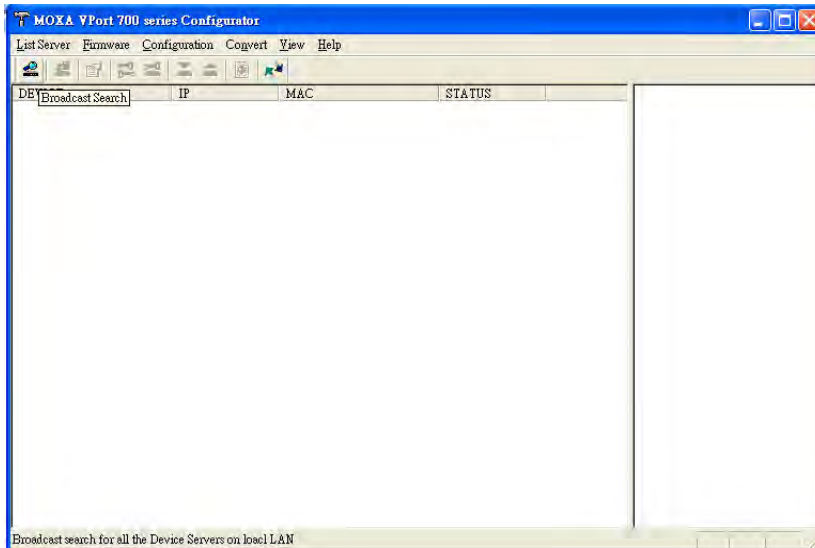
**NOTE** You may download the VPort 700 Utility software from Moxa's website at [www.moxa.com](http://www.moxa.com).

**NOTE** Please do not change the VPort 700 Utility's installation folder; this is because the NPort Windows Driver Manager is in this path.


1. Simply double click on the VPort700Utility to run the program.



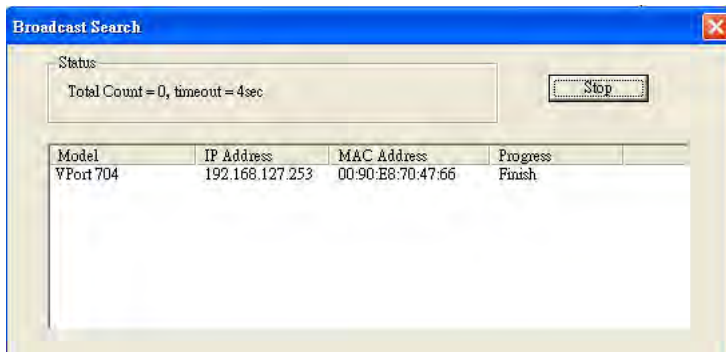
2. The VPort 700 Utility window will open, as shown below.



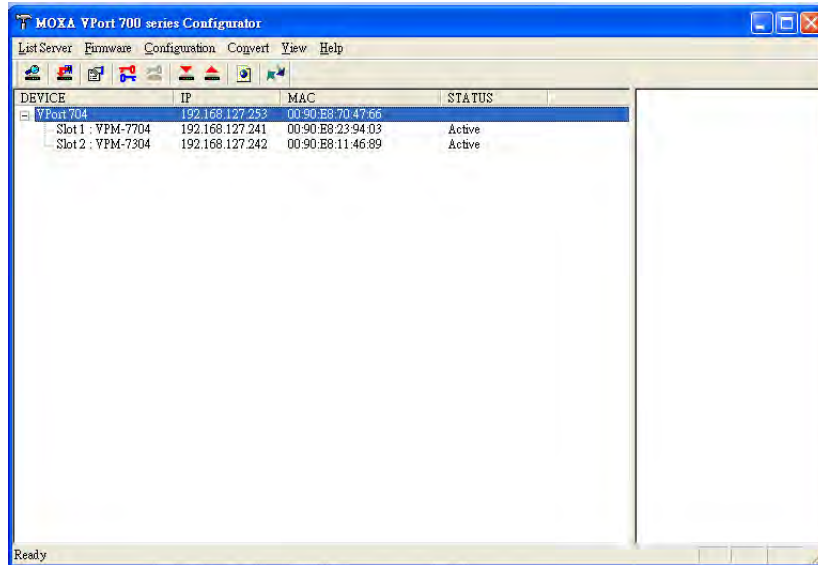
## Broadcast Search

Use the Broadcast Search utility to search the LAN for all VPort 700 series that are connected to the LAN. Note that since the search is done by MAC address, Broadcast Search will not be able to locate Moxa VPort 700 series connected outside the PC host's LAN. Start by clicking the Broadcast Search icon , or by selecting **Broadcast Search** under the **List Server** menu.


1. The Broadcast Search window will open, displaying a list of all switches located on the network, as well as the progress of the search.



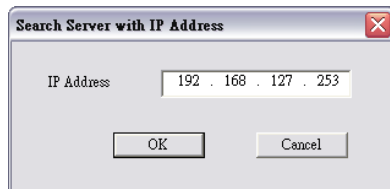
- Once the search is complete, the Utility window will display a list of all VPort 700 series that were located.



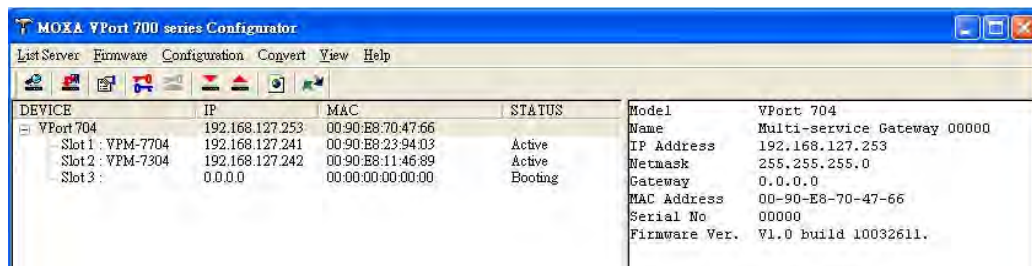
## Search by IP address

This utility is used to search for VPort 700 series one at a time. Note that the search is conducted by IP address, so you should be able to locate any VPort 700 that is properly connected to your LAN, WAN, or even the Internet. Start by clicking the Specify by IP address icon , or by selecting **Specify IP address** under the **List Server** menu.

- The **Search Server with IP Address** window will open. Enter the IP address of the VPort 700 you wish to search for, and then click **OK**.



- Once the search is complete, the Utility window will add the switch to the list of VPort 700 series.



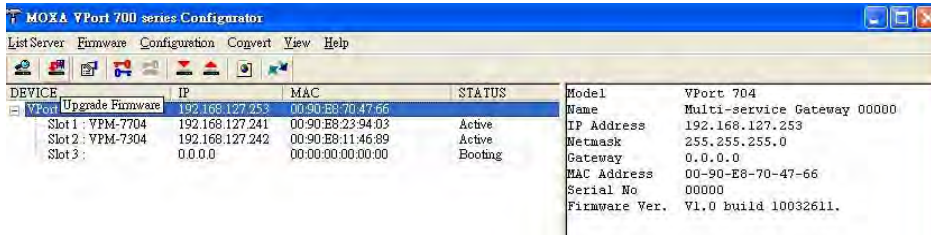
## Upgrade Firmware


Keep your VPort 700 up to date with the latest firmware from Moxa. Perform the following steps to upgrade the firmware:

- Download the updated firmware (\*.rom) file from the Moxa website ([www.moxa.com](http://www.moxa.com)).




- Click the VPort 700 whose firmware you wish to upgrade to highlight it.

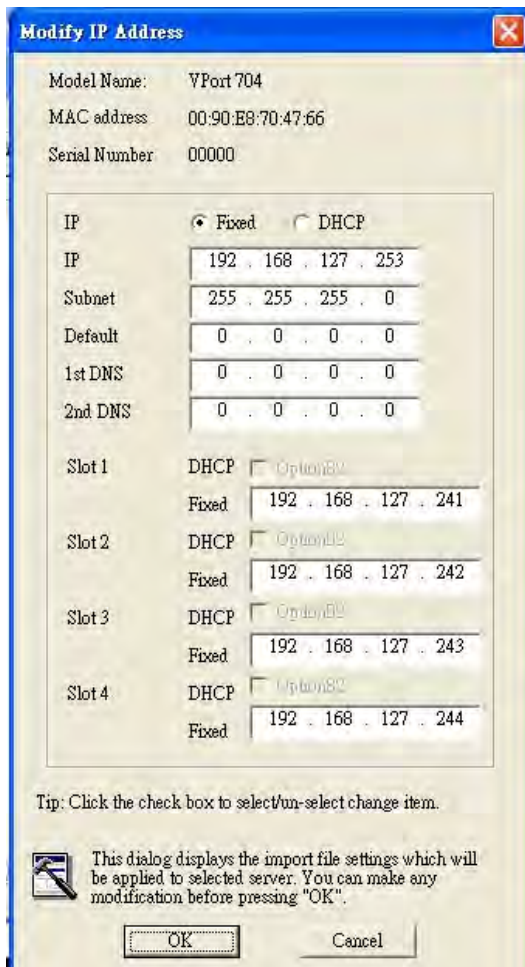


- Click the **Upgrade Firmware** toolbar icon , or select **Upgrade** under the **Firmware** menu. If the switch is Locked, you will be prompted to input the switch's User Name and Password.
- Use the **Open** window to navigate to the folder that contains the firmware upgrade file, and then click the correct **"\*.rom"** file (**VPort 704\_xxx.rom**) to select the file. Click **Open** to activate the upgrade process.

## Modify IP Address


You may use the Modify IP Address function to reconfigure VPort 700 and the slot module's network settings. Start by clicking the Modify IP address icon , or by selecting **Modify IP address** under the **Configuration** menu.

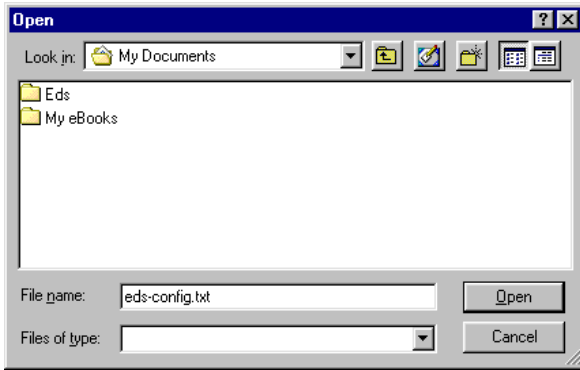
The **Setup Configuration** window will open. Checkmark the box to the left of those items that you wish to modify, and then Disable or Enable DHCP, and enter IP Address, Subnet mask, Gateway, and DNS IP. Click **OK** to accept the changes to the configuration.



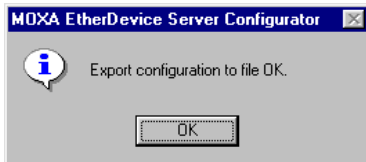
# Export Configuration

The **Export Configuration** utility is used to save the entire configuration of a particular VPort 700 to a text file. Take the following steps to export a configuration:

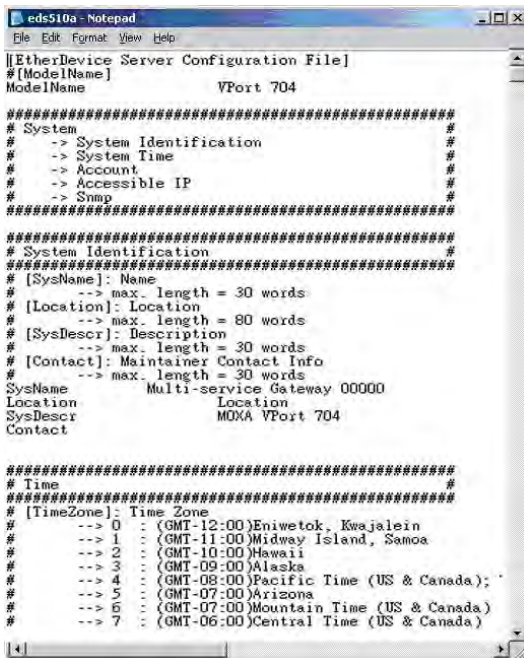
1. Highlight the switch (from the Server list in the Utility window's left pane), and then click the **Export** toolbar icon  or select **Export Configuration** from the **Configuration** menu. Use the **Open** window to navigate to the folder in which you want to store the configuration, and then type the name of the file in the File name input box. Click **Open**.



2. Click **OK** when the **Export configuration to file OK** message appears.




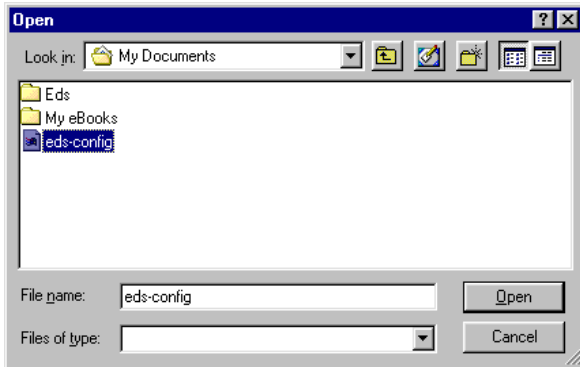
3. You may use a standard text editor, such as Notepad under Windows, to view and modify the newly created configuration file.



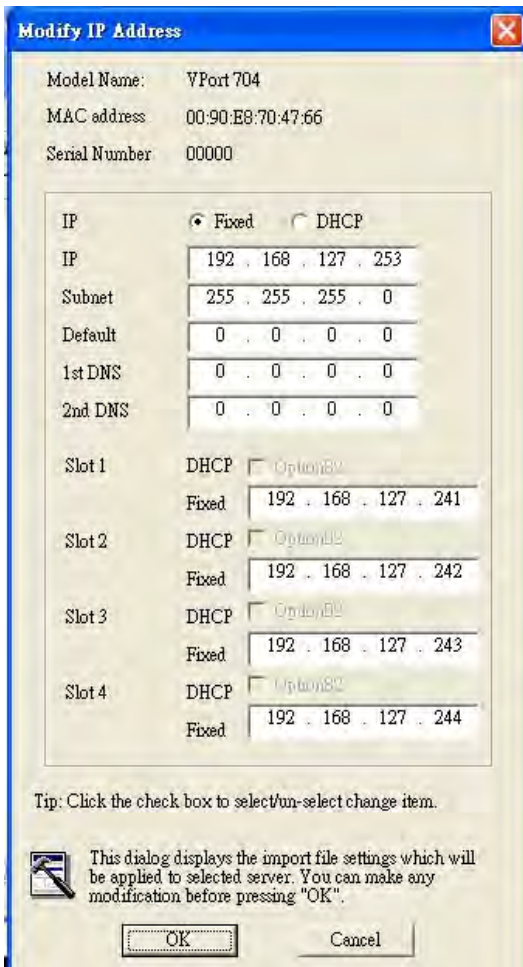
# Import Configuration

The **Import Configuration** function is used to import an entire configuration from a text file to the VPort 700. This utility can be used to transfer the configuration from one VPort 700 to another, by first using the Export Configuration function (described in the previous section) to save a switch configuration to a file, and then using the Import Configuration function. Perform the following steps to import a configuration:

1. Highlight the server, and then click the **Import** toolbar icon , or select **Import Configuration** from the **Configuration** menu.
2. Use the **Open** window to navigate to the text file that contains the desired configuration. Once the file is selected, click **Open** to initiate the import procedure.



3. The **Setup Configuration** window will be displayed, with a special note attached at the bottom. Parameters that have been changed will be activated with a checkmark. You may make more changes if necessary, and then click **OK** to accept the changes.

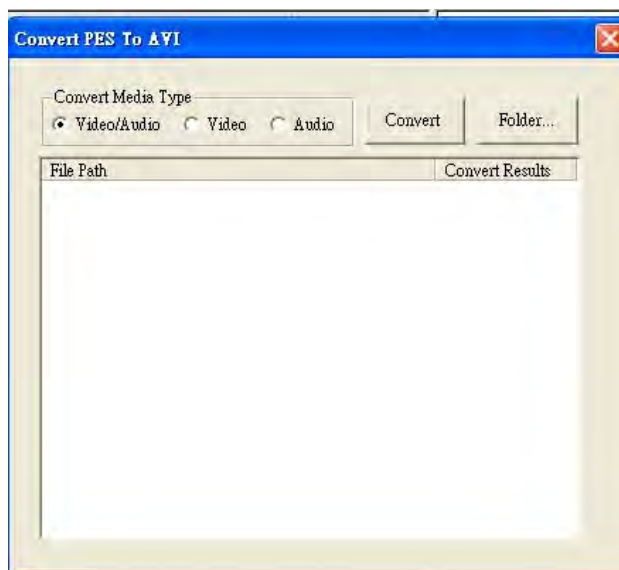


- Click **Yes** in response to the following warning message to accept the new settings.



## Convert

The Convert function is used to convert the PES Video/Audio streams, which is the recorded video stream type by VPort IP video devices (video encoder or IP camera), to the AVI format. By doing this, the user can use the general media player to playback the recorded video streams.



**NOTE** Currently, the VPM-7304, the 4-channel video encoder module for VPort 700 series, doesn't have video recording function. Therefore, this Convert function is reserved for the future use.

# A

## Modbus Address Table

---

Address	Word	Item name	
0x0000	1	Vender ID	0x1393
0x0001	1	Unit ID	0x01
0x0002	1	Product Code	0x8801
0x0010	20	Vender Name	Moxa
0x0030	20	Product Name	VPort704
0x0050	1	Serial Number	
0x0051	2	Firmware Version	
0x0053	2	Release Date	
0x0055	2	MAC Address	
0x0058	1	Power 1 status	
0x0059	1	Power 2 status	
0x005A	1	Fault Led Status	
0x0082	1	DO 1 Status	
0x1000	256	Port Link Status	
0x1100	256	Port Speed	
0x1200	256	Port Flow Control	
0x1300	256	Port MDI/MDIX	
0x1400	3072	Port Description	
0x2000	256	Port Tx Packets	
0x2100	256	Port Rx Packets	
0x2200	256	Port Tx Error Packets	
0x2300	256	Port Rx Error Packets	
0x3000	1	Redant Protocol	
0x3100	1	RTSP Root	
0x3200	256	RSTP Port Status	
0x3300	1	Master / Slave	
0x3301	1	TR Port1 Status	
0x3302	1	TR Port2 Status	
0x3303	1	TR Coupling	
0x3304	1	TR Port3 Status	
0x3305	1	TR Port4 Status	
0x3500	1	TR2 Coupling M	
0x3501	1	TR2 Coupling PS	
0x3502	1	TR2 Coupling BS	
0x3600	1	TR2 Ring 1 Status	
0x3601	1	TR2 Ring 1 Master / Slave	
0x3602	1	TR2 Ring 1 Port 1 S	
0x3603	1	TR2 Ring 1 Port 2 S	
0x3680	1	TR2 Ring 2 Status	
0x3681	1	TR2 Ring 2 Master / Slave	
0x3682	1	TR2 Ring 2 Port 1 S	
0x3683	1	TR2 Ring 2 Port 2 S	

0x4000	1	Slot module 1 Idx	
0x4001	30	Slot module 1 Module	
0x401F	30	Slot module 1 Description	
0x403D	30	Slot module 1 Name	
0x405B	2	Slot module 1 Ip	
0x405D	3	Slot module 1 Mac	
0x4060	1	Slot module 1 Serial No	
0x4061	30	Slot module 1 Firm. Ver.	
0x407F	8	Slot module 1 Status	
0x4100	1	Slot module 2 Idx	
0x4101	30	Slot module 2 Module	
0x411F	30	Slot module 2 Description	
0x413D	30	Slot module 2 Name	
0x415B	2	Slot module 2 Ip	
0x415D	3	Slot module 2 Mac	
0x4160	1	Slot module 2 Serial No	
0x4161	30	Slot module 2 Firm. Ver.	
0x417F	8	Slot module 2 Status	
0x4200	1	Slot module 3 Idx	
0x4201	30	Slot module 3 Module	
0x421F	30	Slot module 3 Description	
0x423D	30	Slot module 3 Name	
0x425B	2	Slot module 3 Ip	
0x425D	3	Slot module 3 Mac	
0x4260	1	Slot module 3 Serial No	
0x4261	30	Slot module 3 Firm. Ver.	
0x427F	8	Slot module 3 Status	
0x4300	1	Slot module 4 Idx	
0x4301	30	Slot module 4 Module	
0x431F	30	Slot module 4 Description	
0x433D	30	Slot module 4 Name	
0x435B	2	Slot module 4 Ip	
0x435D	3	Slot module 4 Mac	
0x4360	1	Slot module 4 Serial No	
0x4361	30	Slot module 4 Firm. Ver.	
0x437F	8	Slot module 4 Status	

Memory mapping from address 0x0000 to 0x43FF