



EX24000 Switch

User's Guide

FastFind Links

Product Overview

Unpacking and Installation

Computer Setup

Setting the initial IP address



All Rights Reserved

Dissemination or reproduction of this document, or its contents, is not authorized except where expressly permitted. Violators are liable for damages. All rights reserved, for the purposes of patent application or trademark registration.

Disclaimer of Liability

The information contained in this document is subject to change without notice. EtherWAN is not liable for any errors or omissions contained herein or for resulting damage in connection with the information provided in this manual.

Registered Trademarks

The following words and phrases are registered Trademarks of EtherWAN Systems Inc. EtherOS[™] Ethernet to the World[™]

All other Trademarks are property of their respective owners.

Warranty

For details on the EtherWAN warranty replacement policy, please visit our web site at: https://kb.etherwan.com/index.php?View=entry&EntryID=27

Products Supported by this Manual:

EX24000

Contact EtherWAN Systems

Corporate Headquarters EtherWAN Systems Inc. 4570 E. Eisenhower Circle Anaheim, CA 92807 Tel: (714) 779 3800 Fax: (714) 779 3806 Email: support@etherwan.com

TABLE OF CONTENTS

Fable of Contents	
Table of Figures	xi
Preface	xiv
Changes in this Revision	xiv
Document Conventions	XV
Safety and Warnings	XV
Typographic Conventions	xv
Product Overview	
EX24000 Switch	
Product Highlights	17
Unpacking and Installation	
Package Contents	
Unpacking	
Required Equipment and Software	19
Computer Setup	
Management Methods and Protocols	20
Default IP	21
Login Process and Default Credentials	21
Setting the initial IP address	
Simple IP Addressing	22
CLI Command Usage	
Navigating the CLI Hierarchy	24
CLI Keyboard Shortcuts	
CLI Command modes	
General Configuration Mode	
MSTP Configuration Mode	
Interface Configuration Mode	27
VLAN Database Configuration Mode	27
Saving a Configuration from the CLI	

System Menu	
System Information	
System Name/Password	
IP Address	
Static IP	
DHCP Client	
Default Gateway	
DNS Server	
Management Interface	
HTTPS	
Telnet	
SSH (Secure Shell)	
Save Configuration Page	
Save Configuration	
Load Configuration	35
Backup Configuration	
Restore Default	
Auto Save	
Firmware Upgrade	
Reboot	
Logout	
Diagnostics	39
	20
System Log	
Pemote Logging	
ARP Table	
Route Table	
Port	45
Configuration	45
Port Status	47
Rate Control	
RMON Statistics	49
Per Port VLAN Activities	50
Port Security Dynamic-MAC	51
Port Configuration Examples Using CLI Commands	54
Setting the Port Description	54
Enable or Disable a Port	54
Setting the Port Speed	55
Setting Port Duplex	55
Enable or Disable Port FlowControl	56
Display Port Status	

	Setting a Ports Rate Control	56
	Display a Ports RMON Statistics	57
	Display a Ports VLAN Activities	57
	Setting Dynamic MAC Port Security	57
Switc	hing	59
	Bridging	59
	Aging Time	60
	Port Isolation	60
	Block Multicast	60
	Loopback Detect	62
	Enabling Loopback Detection (Global)	62
	Changing the Loopback Detect Action	62
	Changing the Loopback Detect Recovery Time	62
	Changing the Polling Interval	63
	Enabling Loopback Detection (Per Port)	64
	Storm Detect	65
	Enabling Storm Detect Configuration (Global)	65
	Changing the Storm Detect Interval	65
	Changing the Storm Detect Error Disable Recovery Time	65
	Static MAC Entry	68
	Adding a Static MAC Address to a Port	68
	Removing a Static MAC Address from a Port	69
	Adding a MAC to the Static-MAC-Entry Discard Table	69
	Removing a MAC address from the Static-MAC-Entry Discard Table	70
	Port Mirroring	71
	Link State Tracking	73
	Enable/Disable Link State Tracking	73
	Port Settings	74
	PoE 75	
	Changing the System Power Budget (Global)	75
	Enabling Enable Mode (Per Port)	75
	Changing the Fixed Power Limit (Per Port)	75
	Enabling Power Priority (Per Port)	75
	PoE Scheduling	76
	Enabling PoE Scheduling (Per Port)	76
	Switch Configuration Examples Using CLI Commands	78
	Setting the Aging Time Value	78
	Enabling Port Isolation	78
	Enabling Block Multicast	79
	Setting Storm Detect by Utilization	79
	Enabling Loopback Detect (Global)	80
	Setting the Loopback Detect Action	80

Setting the Loopback Detect Recovery Time	80
Setting the Loopback Detect Polling Interval	81
Enabling Loopback Detect (Port)	81
Adding a MAC Address for Static-MAC-Entry Forwarding	82
Adding a MAC Address for Static-MAC-Entry Discarding	
Configuring Port Mirroring	83
Enabling a Link State Tracking Group	83
Assigning a Port to a Link State Tracking Group	
Setting the System Power Budget	84
Trunking	85
Overview	85
Static Channel Trunking	
Link Aggregation Control Protocol	
Port Trunking	
LACP Trunking	
Trunking Configuration Examples Using CLI Commands	
Adding an Interface to a Static Trunk	
Adding an Interface to a LACP Trunk	
Setting the LACP Port Priority	90
Setting the LACP Timeout	90
STP/Ring Page – Overview	
STP/Ring Page – Overview Choosing the Spanning Tree Protocols	91 91
STP/Ring Page – Overview Choosing the Spanning Tree Protocols Spanning Tree Protocol (STP)	
STP/Ring Page – Overview Choosing the Spanning Tree Protocols Spanning Tree Protocol (STP) Rapid Spanning Tree protocol (RSTP)	91 91 91 91
STP/Ring Page – Overview Choosing the Spanning Tree Protocols Spanning Tree Protocol (STP) Rapid Spanning Tree protocol (RSTP) Multiple Spanning Tree Protocol (MSTP)	
STP/Ring Page – Overview	
STP/Ring Page – Overview	
 STP/Ring Page – Overview	91 91 91 91 91 91 91 92 92 92
 STP/Ring Page – Overview	91 91 91 91 91 91 92 92 92 92
 STP/Ring Page – Overview	91 91 91 91 91 91 91 92 92 92 92 92 92 92
 STP/Ring Page – Overview	91 91 91 91 91 91 92 92 92 92 92 92 94 94
 STP/Ring Page – Overview	91 91 91 91 91 91 92 92 92 92 92 92 92 92 92 92 92 92 92
 STP/Ring Page – Overview Choosing the Spanning Tree Protocols	91 91 91 91 91 91 92 92 92 92 92 92 92 92 92 92 92 92 92
 STP/Ring Page – Overview Choosing the Spanning Tree Protocols	91 91 91 91 91 91 92 92 92 92 92 92 92 92 92 92 92 92 92
 STP/Ring Page – Overview Choosing the Spanning Tree Protocols	91 91 91 91 91 91 92 92 92 92 92 92 92 92 92 92 92 92 92
 STP/Ring Page – Overview Choosing the Spanning Tree Protocols. Spanning Tree Protocol (STP) Rapid Spanning Tree protocol (RSTP). Multiple Spanning Tree Protocol (MSTP) STP/Ring Page - Configuring RSTP Global Configuration Page Enabling the RSTP Protocol. Additional Global Configuration page settings. The Root Bridge & Backup Root Bridge Setting the MAX Age, Forward Delay and Hello Timer RSTP Port Setting Page. Spanning Tree Port Roles Path Cost & Port Priority. Point to Point Link. Edge Port. 	91 91 91 91 91 91 92 92 92 92 92 92 92 92 92 92 92 92 92
 STP/Ring Page – Overview Choosing the Spanning Tree Protocols	91 91 91 91 91 91 92 92 92 92 92 92 92 92 92 92 92 92 92
 STP/Ring Page – Overview Choosing the Spanning Tree Protocols	91 91 91 91 91 91 92 92 92 92 92 92 92 92 92 92 92 92 92
 STP/Ring Page – Overview Choosing the Spanning Tree Protocols	91 91 91 91 91 91 92 92 92 92 92 92 92 92 92 92 92 92 92

Manually Setting a Port to be a Shared or Point to Point Link	
Enabling/Disabling a port to be an Edge Port	104
STP/Ring Page - Configuring MSTP	105
Global Configuration Page	
Enabling the MSTP Protocol	
The CIST Root Bridge & Backup CIST Root Bridge	
Setting Bridge Priority	
Configuring the CST Network Diameter	
MSTP Properties Page	
Configuring an MSTP Region	
Configuring the IST Network Diameter	111
MSTP Instance Setting Page	
Setting an MSTP Instance	
Modifying MSTP parameters for load balancing	
MSTP Port Setting page	115
Adjusting the blocking port in a MSTP network	115
MSTI Instance Port Membership	
MSTP Configuration Examples Using CLI Commands	119
Enabling Spanning Tree for MSTP	
Bridge Priority, Max Age, Forward Delay, and Hello Time	119
IST MAX Hops	
MSTP Regional Configuration Name and the Revision Level	
Creating an MSTI Instance	121
Setting MSTI Priority	
Modifying CIST Port Priority and Port Path Cost	121
Adding a Port to an MSTI Instance	
STP/Ring Page - Alpha Ring	123
Alpha Ring Setting Page	
EtherWAN α-Ring Technology	
Implementing a Simple α-Ring	
Connecting two α-Ring Networks together	
Chain Setting Page	
Chain Protocol	
VLAN (Global)	
Priority (Global)	
Timeout Count (Global)	
Enabling Storm Control (Broadcast and Multicast) (Global)	
Chain Pass-Through Setting Page	
Implementing a Chain Pass-Through	
Advanced Setting	
Advanced Bridge Configuration	

Advanced Per Port Configuration	131
Configuring Spanning Tree Advanced Settings using CLI commands	133
Enabling BPDU Guard Globally	133
Enabling BPDU Guard on a Port	133
Enabling BPDU Guard Error Disable-timeout	134
	425
VLAN	135
Port Based VLAN vs. Tagged Based VLAN	135
Configuring VLANs in Port Based VLAN Mode	135
Enabling Port Based VLAN	135
Port Based VLAN Configuration Examples	136
Port Based VLAN Configuration Examples using CLI Commands	138
VLAN Configuration in 802.1Q Tag Based VLAN Mode	140
General Overview	140
Enabling 802.1Q Tagged Based VLAN	141
Configuring 802.1Q VLAN Database	142
802.1Q Tag Based VLAN Configuration Examples Using CLI Commands	143
Configuring a 802.1Q VLAN	143
Configuring an IP Address for a Management VLAN	143
Removing an IP Address from a Management VLAN	144
Configuring an Access Port	144
Configuring a Trunk Port	145
Add an IP to the Management VLAN	146
Configuring the Port Type and the PVID setting	147
Configuring the VLAN Egress (outgoing) Member Ports	148
QoS	150
	100
Global Configuration Page	151
	153
Configuring the Egress Expedite Queue	
802.1p Priority Page	
Web GUI Interface	156
802.1p Priority Submenu – CLI Interface	
DSCP Page – HTTP Interface	158
DSCP Submenu – CLI Interface	159
QoS Interface Commands – CLI Interface	
SNMP	161
SNMP General Settings	161
Configuring SNMP v1 & v2 Community Groups	164
Configuring SNMP v3 Users	165

Adding SNMP v3 Users to the switch	
Deleting SNMP v3 Users from the switch	
SNMP Configuration Examples Using CLI Commands	
Enabling SNMP and configuring general settings	
Configuring SNMP Traps	171
Configuring SNMP v1 & v2 Community Groups	173
Adding SNMP v3 Users	173
IEEE 802.1X	174
Configuring 802.1X from the GUI system	
Enabling Radius	
Adding a Radius Server	
Enabling 802.1X on a Port	176
LLDP	178
LLDP General Settings	
Enable/Disable LLDP	
Holdtime Multiplier	
Global TLV Setting	
LLDP Ports Settings	
Enabling LLDP transmission for a specific Port	
Enabling LLDP Reception for a specific Port	
Enabling Notifications	
LLDP Neighbors	
LLDP Statistics	
LLDP Configuration Examples Using CLI Commands	
Enable/Disable LLDP	
LLDP Holdtime Multiplier	
LLDP Transmit Interval	
Enable/Disable Global LLDP TLVs	
Enabling LLDP Transmit on a Port	
Enabling LLDP Receive on a Port	
Enabling LLDP Notify	
Enabling Transmission of the Management IP	
Enabling Specific TLV's on a Port	
Other Protocols	192
GVRP	192
General Overview	
Enabling the GVRP Protocol at the Global Level	
Enabling the GVRP Protocol at the Port Level	
GVRP Configuration Examples Using CLI Commands	
IGMP Snooping	

General Overview	202
Enabling the IGMP Snooping Modes	203
Configuring IGMP Snooping General properties	203
Configuring IGMP Passive Mode Specific properties	204
Configuring IGMP Querier Mode Specific properties	205
Configuring IGMP Unknown Multicast Forwarding	206
Monitoring Registered Multicast Groups	211
IGMP Configuration Examples Using CLI Commands	212
Network Time Protocol	220
Enabling NTP	220
Setting the NTP Server IP Address	220
Setting the Timezone	220
Setting the Polling Period	220
Manually Syncing Time	221
Daylight Savings Time - Weekday Mode	221
Daylight Savings Time – Date Mode	222
Network Time Protocol Configuration Examples Using CLI Commands	224
GMRP	227
General Overview	227
GMRP Normal mode	227
GMRP Fixed mode	227
GMRP Forbidden mode	228
GMRP Forward All mode	228
GMRP Disabled mode	228
Enabling the GMRP Feature Globally on the Switch	. 228
Configuring the GMRP Feature Per Port	229
GMRP Configuration Examples Using CLI Commands	232
DHCP Server	234
General Overview	234
Configuring the DHCP Server	234
DHCP Configuration Examples Using CLI Commands	237

TABLE OF FIGURES

Figure 1: Front view	. 16
Figure 2: Back view	. 16
Figure 3: Login screen	21
Figure 4: Assigning an IP address	23
Figure 5: Saving the Configuration	24
Figure 6: System Information	29
Figure 7: System Name/Password	30
Figure 8: IP Address	32
Figure 9: Management Interface	34
Figure 10: Save Configuration Page	36
Figure 11: Firmware Upgrade Page	37
Figure 12: Utilization Page	39
Figure 13: System Log	40
Figure 14: Remote Logging Page	42
Figure 15: ARP Table	43
Figure 16: Route Table	44
Figure 17: Port Configuration	46
Figure 18: Port Status	48
Figure 19: Rate Control	49
Figure 20: RMON Page	50
Figure 21: Port VLAN Activities	51
Figure 22: Port Security	. 53
Figure 23: Bridging	. 61
Figure 24: Loopback Detection	63
Figure 25:Loopback Detection (port)	64
Figure 26: Storm Detect	67
Figure 27: MAC Static Entry	68
Figure 28: Removing a Static MAC	69
Figure 29: Adding a MAC – Static-MAC-Entry Table	70
Figure 30: Deleting a MAC – Static-MAC-Entry Table	70
Figure 31: Port Mirroring	72
Figure 32: Disabling Port Mirroring	73
Figure 33: Link State Tracking	74
Figure 34: Link State Tracking – Port Settings	74
Figure 35: PoE	76
Figure 36: PoE Scheduling	. 77
Figure 37: Port Trunking	87

Figure 38: LACP Trunking	
Figure 39: STP/Ring Global Configuration	93
Figure 40: Bridge ID	94
Figure 41: Bridge ID Display	95
Figure 42: Max Age, Hello Timer & Forward Delay	97
Figure 43: Spanning Tree Port Roles	
Figure 44: Port ID	99
Figure 45: Port Priority and Path Cost	
Figure 46: Enabling MSTP	106
Figure 47: Bridge ID	
Figure 48: Bridge ID Display	107
Figure 49: Max Age, Hello Timer & Forward Delay	109
Figure 50: MSTP Region and Revision Level	110
Figure 51: MSTP Properties – Max Hops	111
Figure 52: VLAN Instance Configuration	113
Figure 53: VLAN Instance ID	113
Figure 54: Setting the MSTI Regional Root Bridge	114
Figure 55: Port Cost & Priority	116
Figure 56: Port Instance Configuration	118
Figure 57: Port Instance - Adding Ports	118
Figure 58: α-Ring Settings	124
Figure 59: Ring Coupling	126
Figure 60: Chain Settings	128
Figure 61: Chain Pass-Through Settings	129
Figure 62: Advanced Bridge Configuration	131
Figure 63: Advanced Per Port Configuration	132
Figure 64: Port Based VLAN	136
Figure 65: Port Based VLAN – Example 1	137
Figure 66: Port Based VLAN – Example 2	138
Figure 67: Tag-based VLAN	141
Figure 68: Add VLAN	142
Figure 69: Add VLAN Page	142
Figure 70: Management VLAN IP Address	146
Figure 71: VLAN Port Setting	147
Figure 72: VLAN Links	148
Figure 73: VLAN Ports	149
Figure 74: Tag or Untag ports	149
Figure 75: Global Configuration	151
Figure 72: 802.1p Priority	156
Figure 77: DSCP	158
Figure 78: SNMP General Settings	163
Figure 79: Community Name V1/V2c	164
Figure 80: Add User	165

Figure 81: SNMP v3 Settings	166
Figure 82: User name & Access Mode	166
Figure 83: Auth Password	167
Figure 84: Privacy PassPhrase	168
Figure 85: Delete User	168
Figure 86: Select User	169
Figure 87: Enable Radius	175
Figure 88: Radius Setup	176
Figure 89: Resulting Radius Server Setup	176
Figure 90: Enabling 802.1X on a Port	177
Figure 91: LLDP Global Settings	181
Figure 92: LLDP Ports Settings	183
Figure 93: LLDP Neighbors	184
Figure 94: LLDP Statistics	185
Figure 95: GVRP	193
Figure 96: GVRP Configuration Distribution Switch	196
Figure 97: GVRP Configuration Access Switch	197
Figure 98: GVRP Per Port Settings	198
Figure 99: IGMP Mode	203
Figure 100: IGMP General Properties	204
Figure 101: IGMP Passive Mode	205
Figure 102: Querier Mode Properties	206
Figure 103: Disabled Mode Forwarding Port	207
Figure 104: PassiveForwardMode	208
Figure 105: ForceForwardMode	209
Figure 106: IGMP Querier Mode Forwarding	210
Figure 107: Current Multicast Groups	211
Figure 108: NTP Settings	221
Figure 109: Daylight Savings – Weekday Mode	222
Figure 110: Daylight Savings – Date Mode	223
Figure 111: GMRP Global Setting	229
Figure 112: DHCP Server	235
Figure 113: DHCP Bindings	236
Figure 114: DHCP Binding Table	237

PREFACE

Audience

This guide is designed for the person who installs, configures, deploys, and maintains the Ethernet network. This document assumes the reader has moderate hardware, computer, and Internet skills.

Document Revision Level

This section provides a history of the revision changes to this document.

Revision	Document Version	Date	Description
А	Version 1	05/09/2014	Initial release

Changes in this Revision

N/A - this is first version of this document.

Document Conventions

This guide uses the following conventions to draw your attention to certain information.

Safety and Warnings

This guide uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
	Note	Notes emphasize or supplement important points of the main text.
	Тір	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Warning	Warnings indicate that failure to take a specified action could result in damage to the device, or could result in serious bodily injury.
	Electric Shock Hazard	This symbol warns users of electric shock hazard. Failure to take appropriate precautions such as not opening or touching hazardous areas of the equipment could result in injury or death.

Typographic Conventions

This guide also uses the following typographic conventions.

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user.
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Italic font is also used to indicate variables.
[] square brackets	Indicates optional values.
{ } braces	Indicates required or expected values.
vertical bar	Indicates that you have a choice between two or more options or arguments.



PRODUCT OVERVIEW

EX24000 Switch

The EX24000 Switch Provides the 16-port 10/100BASE-TX (PoE) and 2 combo Gigabit SFP ports. The EX24000 Switch is a fully managed switch.



Figure 1: Front view



Figure 2: Back view

Product Highlights

Basic Features:

- 16 x 10/100BASE (PoE) ports
- Provides up to two combo Gigabit SFP ports
- Supports 8192 MAC addresses, Provides 2M bits memory buffer
- Store-and-forward mechanism, Full wire-speed forwarding rate
- Supports IEEE802.3af Power over Ethernet (PoE) Power Sourcing Equipment (PSE)
- Supports Max. 15.4W power for each PSE/PoE port
- RS-232 console, Telnet, SNMP V1, V2c & V3, RMON, Web Browser, and TFTP Management
- Supports Command Line Interface from RS-232 Console
- α-ring and RSTP/MSTP/STP for Ethernet redundancy
- IP Multicast Filtering
- Port-based VLAN, IEEE802.1Q VLAN Tagging and GVRP
- IEEE802.1p QoS with four priority queues
- MAC-based trunking with automatic link fail-over
- Supports IEEE802.1X Security
- Bandwidth Rate Control
- Per-port programmable MAC address locking
- Up to 24 Static Secure MAC addresses per port
- Port mirroring
- Supports NTP
- Supports IEEE802.3/802.3u/802.3ab/802.3z/802.3x
- 1000Mbps-Full-duplex, 10/100Mbps-Full/Half-duplex, Auto-Negotiation, Auto-MDI/MDIX
- Alarms for port and power failure by relay output
- Power Supply: 100~240VAC, 50~60Hz internal universal PSU
- Power consumption: 12W Max. (Without PoE)
- Power budget: 195W Max
- Push and hold the reset button for less than 10 seconds: system reboot
- Push and hold the reset button for more than 10 seconds: reset to default password
- 0°C to 45°C (32°F to 113°F) operating temperature range
- Supports Rack Mounting installation

UNPACKING AND INSTALLATION

This chapter describes how to unpack and install the EX24000 Switch

The topics covered in this chapter are:

- □ Package Contents (Page <u>18</u>)
- □ Unpacking (Page <u>18</u>)
- □ Required Equipment and Software (Page <u>19</u>)
- □ Computer Setup (Page <u>20</u>)
- □ Management Methods and Protocols (Page <u>20</u>)
- Default IP (Page 21)
- □ Login Process and Default Credentials (Page 21)
- □ Setting the initial IP address (Page <u>22</u>)

Package Contents

When you unpack the product package, you will find the items listed below. Please inspect the contents, and report any apparent damage or missing items immediately to your authorized reseller.

- This Management Switch
- User's Manual
- External power adapter

Unpacking

Follow these steps to unpack the EX24000 Switch and prepare it for operation:

- 1. Open the shipping container and carefully remove the contents.
- 2. Return all packing materials to the shipping container and save it.
- 3. Confirm that all items listed in the "Package Contents" section are included in the shipment. Check each item for damage. If any item is damaged or missing, notify your authorized EtherWAN representative.

Required Equipment and Software

The following hardware and software are needed in order to manage the switch from the web interface:

• Computer with an Ethernet Interface (RJ-45)

Managing the switch requires a personal computer (PC) or notebook computer equipped with a 10/100base-TX Ethernet interface and a physical RJ-45 connection. The preferred operating system for the computer is Microsoft Windows XP/Vista/7. It is possible to use Apple OSX or Linux systems as well, but, for the sake of brevity, all web configurations in this manual will be shown using Windows 7 as the underlying operating system.

• Cat 5+ Ethernet Cables

An Ethernet cable of at least Category 5 rating is required to connect your computer to the switch. The cable can be configured as "straight-through" or crossover.

• TFTP Server Software

Trivial file transfer protocol (TFTP) server software is needed to update the switch firmware and to upload/download configuration files to the switch. Users not performing these tasks do not need TFTP software installed. Several good TFTP servers are available for free online. The server that will be used in this manual is TFTPD32 by Philippe Jounin.

Web Browser Software

The end user can employ any of the following web browsers during switch configuration: Internet Explorer, Firefox, or Chrome. Internet Explorer is the preferred browser for EtherWAN switch configuration. If there is trouble with other browsers while attempting to program the switch, Internet Explorer should be used.

COMPUTER SETUP

The end user's management computer may need to be reconfigured prior to connecting to the switch in order to access the switch's web interface through its default IP address (See <u>Default IP</u>).

Management Methods and Protocols

There are several methods that can be used to manage the switch. This manual will show the details of configuring the switch using a web browser. Each section will be followed by the CLI (Command Line Interface) commands needed to achieve the same results as described in that section.

The methods available to manage the EX24000 Switch include:

- SSH Secure Shell CLI that is accessible over TCP/IP networks which and is generally regarded as the most secure method of remotely accessing a device.
- **Telnet** is like SSH in that it allows a CLI to be established across a TCP/IP network, but it does not encrypt the data stream.
- **HTTP** (Hypertext Transfer Protocol) is the most popular switch management protocol involving the use of a web browser.
- RS232 The EX24000 Switch is equipped with a RS232 serial port that can be used to access the switches CLI. The Serial port is DCE DB9F. A straight through serial cable is used to connect to a typical computer serial port.

Default IP

The switch's default IP address is 192.168.1.10. The user will need to modify the management computer so that it is on the same network as the switch. For example, the user could change the IP address of the management computer to 192.168.1.100 with a subnet mask of 255.255.255.0.

Login Process and Default Credentials

Once a compatible IP address has been assigned to the management computer, the user is ready to log in to the switch. To log in, type the URL http://192.168.1.10/ into the address field of the browser and hit return. The following will appear in the browser window (See Figure 3)

- The Default Login is root (case sensitive)
- There is no password by default
- Enter the login number and onex the Login battering
 Enter root for the login name
 Leave the password field blank
 Click the Login button
- Enter the login name and click the Login button

Figure 3: Login screen

SETTING THE INITIAL IP ADDRESS

Once logged in the user can now configure the switch per the network requirements. The two major addressing options are:

- Simple IP addressing
- Multiple VLAN addressing (See Add an IP to the Management VLAN on page 146).

Simple IP Addressing

A new IP address can now be assigned to the switch. From the System Information screen, go to the left hand navigation menu.

- 1. Click on the + next to System
- 2. Click on IP address
- 3. Enter the desired IP address and subnet mask in the **IP Address/Subnet Mask** fields associated with VLAN 1
- 4. Click the **Submit** button (See Figure 4)

Management Switch	Static IP:			1 Olish on the Location
System Information	VLAN ID	IP Address	IP Subnet Mask	1. Click on the + next to
System Name Password	1	192.168.2.50	255.255.255.0	System
Management Interface Save Configuration			3 Submit	2. Click on IP Address
Einmware Upgrade			(4)	
- Reboot - Logout	DHCP Client:			3. Enter the IP address
User Account	DHCP Client		Disable 🗸	and subnet mask
User Privilege	VLAN ID	IP Address	IP Subnet Mask	
Diagnostics Port	DHCP Disable			1 Click on the Submit
Switching Trunking		1	Submit	button
🖲 🧰 STP/Ring	.L			
ULAN	Default Gateway	Enable	✓ 10.58.7.1	
Cos SNMP S021X			Submit	
ELDP	DNS Server	Disable	~	
🖽 🗀 Others Protocols			Submit	
	MAC Address	00e0.1	b333.07bc	

Figure 4: Assigning an IP address

Note: The user should be prepared to change the IP address of the management computer to one compatible with the new IP address assigned to the switch immediately after clicking the Submit button. If the IP address change was done in error, simply cycle the power to the switch and the default IP address will be restored.

To save the configuration changes:

- 5. Change the IP address of the management computer to one on the same subnet that the switch was changed to.
- 6. Restart your Web Browser
- 7. Enter the new IP address of the switch into the Browser
- 8. Login using the user name root
- 9. Click on the + next to System
- 10. Click on Save configuration
- 11. Click on the Save Configuration button (See Figure 5)

Management Switch	Action		File	
Sustan Information	Load Config from TFTP Server	TFTP Server:	FILE:	Load
System Name/Password	Backup Config to TFTP Server	TFTP Server:	FILE:	Backup
IP Address	Save Configuration	-11		
Management Interface				
Save Configuration < (10)	Restore Default			
Firmware Upgrade				
Reboot			0.011.1.1	5 1 1 1 1 P 2 1
Logout			9. Click the	e + next to
User Account	Auto Save Config	guration	system	
User Privilege	Auto Save	Disable 🗸	2	
Diagnostics	Auto Save Interval (5~65535 sec)		10. Click on	Save
J Port		Subr	t Configu	ration
Trunking				-
STP/Ring			11. Click the	e Save
VLAN			Configu	ration button

Figure 5: Saving the Configuration

CLI COMMAND USAGE

This chapter describes accessing the EX24000 Switch by using Telnet, SSH, or serial ports to configure the switch, navigating the Command Line Interface (CLI), typing keyboard shortcuts, and moving between the levels. This chapter assumes the user has a working understanding of Telnet, SSH and Terminal emulation applications.

Note: For a serial port connection use a standard DB9F to DB9M Modem Cable. The default Serial port parameters are 115200, 8 None 1, No Flow Control.

Navigating the CLI Hierarchy

The CLI is organized into a hierarchy of levels. Each level has a group of commands for a specific purpose. For example, to configure a setting for the VLAN server, one would navigate to the VLAN level, which is under the config level.

CLI Keyboard Shortcuts

- Ctrl + a: place cursor at the beginning of a line
- Ctrl + b: backspace one character
- Ctrl + d: delete one character
- Ctrl + e: place cursor at the end of the line
- Ctrl + f: move cursor forward one character
- Ctrl + k: delete from the current position to the end of the line
- Ctrl + I: redraw the command line
- Ctrl + n: display the next line in the history
- Ctrl + p: display the previous line in the history
- Ctrl + u: delete entire line and place cursor at start of prompt
- Ctrl + w: delete one word back

CLI Command modes

Throughout this manual, each section that has CLI commands relevant to that section requires that the CLI be in a specific configuration mode. This section shows the main CLI commands to needed to enter a specific mode.

General Configuration Mode

To set the EX24000 Switch to General configuration mode, run the following commands from the CLI:

- 1. enable
- 2. configure terminal

Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#
```

MSTP Configuration Mode

To set the EX24000 Switch to General MSTP configuration mode, run the following commands from the CLI:

- 1. enable
- 2. configure terminal
- 3. spanning-tree mst configuration

```
Example:
switch_a>enable
switch_a#configure terminal
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#
```

Interface Configuration Mode

Interface mode on the EX24000 Switch is used to configure the Ethernet ports and VLAN information. Valid interfaces are:

- fe<port #> 100mb ports use fe followed by the port number. Example: fe1
- ge<port #> Gigabit ports use ge followed by the port number. Example: ge1
- vlan1.<vlan#> VLAN's use vlan. Followed by the VLAN ID. Example: vlan1.10

```
Example 1 configures 100mb port 1
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fel
switch_a(config-if)
```

```
Example 2 configures VLAN ID 9
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.9
switch_a(config-if)
```

VLAN Database Configuration Mode

VLAN Database Configuration Mode on the EX24000 Switch is used to configure the VLAN settings.

Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#vlan database
switch_a(config-vlan)#
```

Saving a Configuration from the CLI

Example: switch_a>enable switch a#write r

switch_a#write memory
Building configuration....
[OK]
switch a#>

SYSTEM MENU

System Information

The System information link on the Left menu of the Web Configuration page takes you to a page that shows the following (see <u>Figure 6</u>):

- System Name
 - The System name is typically used by network administrators. If SNMP is enabled on the switch, the system name can be found using MIB II (RFC1213) in the sysName property.

• Firmware Version

- If SNMP is enabled on the switch, the Firmware version can be found using MIB II in the sysDesc property
- System Time
 - System time can be change using NTP
- MAC Address
 - The hardware (MAC) address of the Management interface

• Default Gateway

- The IP address of your networks Gateway (Typically a Router on your network)
- DNS Server
 - The Dynamic Name Server (DNS) for your network
- VLAN ID
 - One or more listings depending on the number o VLANs defined on the switch
 - Lists VLAN ID, IP address, and subnet mask of the VLAN Interface(s)
- Current User Information

o Lists the current the currently logged in user and their user privileges

Svistan	5	S	ystem Informat	ion	
System	System Na	System Name		switch_a	
System Name/Password	Firmware Ve	Firmware Version		1.94c. 08/16/13 17:17:06	
TP Address	System Ti	System Time		Tue Sep 10 10:52:09 PDT 2013	
Management Interface	MAC Add	MAC Address		00e0.b333.07bc	
Save Configuration	Default Gate	eway		None	
Firmware Upgrade	DNS Server		None		
Reboot					
Logout	VLAN ID	IP	Address	IP St	ibnet Mask
<u>"User Account</u> " <u>User Privilege</u>	1	192	.168 <mark>.2</mark> .50	255.	255.255.0
Diagnostics Port		Cun	rent User Inform	nation	
Switching		Current Username			root
Trunking	C	Current User privi			Admin
STP/Ring				110	

Figure 6: System Information

System Name/Password

The System name is typically used by network administrators to make it easier to document a networks infrastructure and locate equipment on large networks. If SNMP is enabled on the switch, the system name can be found using MIB II (RFC1213) in the sysName property. To change the system name:

- 1. Click on the + next to **System**.
- 2. Click on System Name/Password (see Figure 7).
- 3. Use your mouse to place the cursor in the System Name text box.
- 4. Replace the existing name with the name you want to assign to the switch.
- 5. Click on the **Update Setting** button.

By default there is no password assigned to the switch. To add or change a password:

- 1. Click on the + next to **System**.
- 2. Click on System Name/Password (see Figure 7).
- 3. Use your mouse to place the cursor in the **Password** text box.
- 4. Enter the new password.
- 5. Retype the password in the Retype Password text box.
- 6. Click on the **Update Setting** button below the **Retype Password** text box.

Management Switch	System Name :	switch_a
<u>System Name/Password</u> <u>IP Address</u> Management Interface		Update Setting
"Save Configuration "Firmware Upgrade	Password:	
<u>Reboot</u> <u>Logout</u>	Retype Password :	
User Account User Privilege		Update Setting
 Diagnostics Port 		
🗄 🧰 Switching		

Figure 7: System Name/Password

IP Address

To navigate to the IP Address page:

- 1. Click on the + next to System
- 2. Click on IP Address (see Figure 8)

There are 4 settings on this page:

Static IP (see <u>Simple IP Addressing</u>)

DHCP Client

Use this to enable or disable DHCP on a VLAN. To enable the DHCP Client:

- 1. Use the drop down box to enable the DHCP client on a particular VLAN
- 2. Click the Submit Button

Default Gateway

If DHCP is enabled, the gateway setting is controlled by the DHCP server. The setting will be grayed out and the gateway supplied by the DHCP server will be displayed. The default gateway setting can be used when using a Static IP address. To enable the default gateway:

- 1. Use the dropdown box to enable the default gateway.
- 2. Type in the default gateway in the Default Gateway text box.
- 3. Click on the **Submit** button.

DNS Server

If DHCP is enabled, the DNS Server setting is controlled by the DHCP server. The setting will be grayed out and the DNS Server supplied by the DHCP server will be displayed. The DNS Server setting can be used when using a Static IP address. To enable the DNS Server:

- 1. Use the dropdown box to enable the DNS Server.
- 2. Type in the default gateway in the Default Gateway text box.
- 3. Click on the **Submit** button.

Note: After making changes to settings in the IP address section, The configuration needs to be saved using the System/Save configuration page (See <u>Save Configuration</u>)

Management Switch	Static IP:		
🖯 🍊 System			
System Information	VLAN ID	IP Address	IP Subnet Mask
Dystem Name/Password	1	192.168.1.62	255.255.255.0
Management Interface			Submit
Save Configuration			
Ennovare Opgrade Reboot Lopout	DHCP Client		
User Account	DHCP Client		Disable 💌
E C Diagnostics	VLAN ID	IP Address	IP Subnet Mask
Dert Port	DHCP Disab	le	
11 🔁 Switching			Submit
E C VLAN			
🕂 🧰 QoS	Default Gateway	y Enable	192.168.1.1
E CONTRACTOR			Submit
Others Protocols	DNS Server	Enable •	n 192.168.1.1
			Submit
	MAC Address	00e0	1.b332.01a4

Figure 8: IP Address

Management Interface

To navigate to the Management Interface page:

- 1. Click on the + next to System
- 2. Click on Management Interface

The Management Interface configuration page has three settings that allow the user to configure the methods available to manage the EX24000 Switch.

HTTPS

HTTPS (Hypertext Transfer Protocol Secure) allows the user to determine what method, if any, is used to configure the EX24000 Switch. The default is unencrypted HTTP (see Figure 9).

To disable the Web interface:

- 1. Uncheck Http and Https.
- 2. Click on the **Update setting** button.

Warning! Once the Submit button is pressed, the Web console will no longer function. As a safety precaution, the configuration is not saved by default. Rebooting the EX24000 Switch will restore the Web Console. To save the configuration, connect using the new IP address.

To enable the Web Interface:

- 1. Check **HTTP**, **HTTPS** or both
- 2. Click on the **Update Setting** button.
- 3. Save the Configuration (see Save Configuration)

Telnet

Telnet is a network protocol that allows a remote computer to log into the EX24000 Switch to access its CLI (Command Line Interface). The CLI can be access using Telnet, SSH and the serial port on the EX24000 Switch. The secure method of accessing the CLI over a network is SSH.

To enable or disable Telnet:

 Click the Enable or Disable radio button in the Telnet section on the Management Interface page (see <u>Figure 9</u> below)

- 2. Click on the **Update Setting** button
- 3. Save the Configuration (see Save Configuration)

SSH (Secure Shell)

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices such as a computer and the EX24000 Switch. SSH is disabled by default on the EX24000.

To enable or disable SSH:

- Click the Enable or Disable radio button in the SSH section on the Management Interface page (see Figure 9)
- 2. Click on the **Update Setting** button
- 3. Save the Configuration (see Save Configuration)

Management Switch	1	HTTPS
System System	WEB Agent	🗹 Http 🔲 Https
System Name/Password		Update Setting
<u>IP Address</u> <u>Management Interface</u>		TELNET
Save Configuration	Telnet	Disable Enable
<u>Firmware Upgrade</u>		Update Setting
Logout		SSH
User Account	SSH	Disable C Enable
Diagnostics		Update Setting
Dort Port		
C Switching		
🛅 Trunking		
C STP/Ring		

Figure 9: Management Interface

Save Configuration Page

To navigate to the Save Configuration page:

- 1. Click on the + next to System
- 2. Click on Save Configuration

The Save Configuration page contains the following configuration functions (see Figure 10):

Save Configuration

To save the currently running configuration to the flash memory on the EX24000 Switch:

- 1. Click the **Save Configuration** button
- 2. If the save is successful you will see the message: Building configuration.... [OK]

Load Configuration

This function is used to load a previously saved configuration. Backing up and loading a configuration is achieved using a TFTP server.

To load a configuration:

- 1. Enter the IP address of your TFTP server in the **TFTP Server** text box
- 2. Enter the name of the configuration file in the **FILE** text box
- 3. Click on the Backup button
- 4. If the file is successfully loaded the following message will be shown: Success! System reboot is required!

Backup Configuration

This function is used to backup the current configuration of the EX24000 Switch. Backing up the configuration is achieved using a TFTP server such as TFTPD32.

To backup a configuration:

- 1. Enter the IP address of your TFTP server in the TFTP Server text box
- 2. Enter the name of the configuration file in the **FILE** text box
- 3. Click on the **Backup** button
- 4. If the backup is successful the following message will be shown: tftp <filename> to ip <ip address> success!!

Restore Default

To restore the EX24000 to factory defaults:

1. Click on the **Restore Default** button.

Auto Save

The Auto Save function is used to set the switch to automatically save the configuration to flash. If the saved configuration is the same as the running configuration then a save is not made. The Auto Save interval is used to determine how often the running configuration is checked for changes.

To set the Auto Save function:

- 1. Click the dropdown box next to Auto Save.
- 2. Set the Auto Save interval (5~65535 sec)

Note: If a Firewall is running on the PC that is running the TFTP server it may need to be temporarily disabled.

System Information System Name Password	Load Config from TFTP Server	TFTP Server:	FILE:	Lord
System Name/Password	Bachum Config to TETP Server			LUau
P Address	Duckup coming to 11 11 oction	TFTP Server.	FILE.	Backup
Janagement Interface	Save Configuration			
eve Configuration irmware Uperade	Restore Default	-		
Reboat				
Logout				
-User Account	25			
User Privilege	Auto Save Conf	iguration		
Diagnostics	Auto Save	Disable 💌		
Switching	Auto Save Interval (5~65535 sec)			
) Trunking		Submit	1	
STP/Ring				

Figure 10: Save Configuration Page
Firmware Upgrade

To navigate to the Firmware Upgrade page:

- 1. Click on the + next to System
- 2. Click on Firmware Upgrade

To upgrade the firmware on the EX24000 Switch, a TFTP server is required. The firmware file for the EX24000 is in a .TGZ format. This is a compressed file; however, it does not need to be decompressed before updating the EX24000.

To update the firmware on the EX24000 Switch (see Figure 11):

- 1. Copy the firmware file to the correct directory for your TFTP server. The correct directory depends on your TFTP server settings
- 2. Enter the filename of the firmware in the Filename text box.
- 3. Enter the IP Address of your TFTP server in the **TFTP Server IP** text box.
- 4. Click on the **Upgrade** button.
- 5. During the firmware upgrade you will see the following messages. Do not reboot or unplug the switch until the final message is received.
 - **a**. Downloading now, please wait...
 - b. tftp <filename>.tgz from ip <ip address> success!!
 Install now. This may take several minutes, please wait...
 - C. Firmware upgrade success!

Note: If a Firewall is running on the PC that is running the TFTP server it may need to be temporarily disabled.

System	Firmware Version	1.94E. 09/10/13 18:55:46
System Information	Filename	
System Name/Password	TFTP Server IP	
IP Address		ehernoll
"Management Interface		opgrade
Save Configuration	L	
Firmware Upgrade		
Reboot		

Figure 11: Firmware Upgrade Page

Reboot

To navigate to the **Reboot** page:

- 1. Click on the + next to **System**
- 2. Click on **Reboot**

To reboot the EX24000 Switch:

- 1. Click on the **Reboot** button.
- 2. Click OK on the popup message.

Logout

To logout of the Web Configuration Console:

- 1. Click on the + next to System
- 2. Click on Logout

DIAGNOSTICS

Utilization

To navigate to the Utilization page:

- 1. Click on the + next to **Diagnostics**.
- 2. Click on Utilization.

The **Utilization** page shows (see Figure 12):

- CPU Utilization Current and Max Utilization
- Memory Utilization Total, Used and Free Memory
- **Port Utilization** Received(%), Transmit(%), RX Broadcast (Packets/s) and RX Multicast (Packets/s)

🕜 Management Switch		CP	U Utilization			
System Diamontian	(Current utilization				
Utilization		Max utiliza	tion	44%		
<u>System Log</u> Remote Logging		Memory Utilization				
ARP Table	To	otal	Used	Free	2	
Route Table	6320	63200 KB 4864		14552	KB	
🗄 🧰 Port						
🗄 🗀 Switching				Port	Utilization	
E 🛅 Trunking E 🛅 STP/Ring	Port	Receive(%) Trans	smit(%)	RX Broadcast (packets/s)	RX Multicast (packets/s)
I 🔂 VLAN	1	3.47	0	.13	1	3
CoS	2	0.14	3	.47	0	0
SNMP	3	0.00	0	00	0	0

Figure	12:	Utilization	Page
--------	-----	-------------	------

System Log

To navigate to the System Log page:

- 1. Click on the + next to **Diagnostics**.
- 2. Click on **System Log**.

The System Log shows the data and time of port links going up or down (see Figure 13)

tinent ownen		System Log					
nem .	1	At Jan 01 2010 20:00:20 (00:00:56) : Link up on Port 25					
ation	2	At Jan 01 2010 20:00:20 (00:00:56) : Link up on Port 26					
Log	3	At Jan 02 2010 00:56:49 (04:57:25) : Link down on Port 26					
Logging	4	At Jan 02 2010 00:56:52 (04:57:28) : Link up on Port 16					
able	5	At Jan 02 2010 00:56:56 (04:57:32) : Link down on Port 25					
able	6	At Jan 02 2010 00:57:00 (04:57:36) : Link up on Port 24					
	7	At Jan 02 2010 00:57:05 (04:57:41) : Link down on Port 16					
ning	8	At Jan 02 2010 00:57:08 (04:57:44) : Link up on Port 14					
ing	9	At Jan 02 2010 00:57:09 (04:57:45) : Link down on Port 24					
Ring	10	At Jan 02 2010 00:57:12 (04:57:49) : Link up on Port 19					

Figure 13: System Log

Remote Logging

To navigate to the **Remote Logging** page:

- 1. Click on the + next to **Diagnostics**.
- 2. Click on **Remote Logging**.

Remote Logging to a Syslog server allows administrators to log important system and debugging information. The Remote Logging configuration page allows reporting to a Syslog server to be enabled or disabled as well as management of a list of Syslog servers to report to (see Figure 14).

To configure the Remote Logging on the EX24000 Switch:

- 1. Click on the **Enable** or **Disable** radio button under Remote Logging.
- 2. Click on the **Update Setting** button.

To add a Syslog server:

- 1. Enter the IP Address of the Syslog Server in the Syslog Server IP text box.
- 2. Click on the Add Syslog Server button.

To delete a Syslog server from the list of servers currently on the switch:

1. Select the Syslog server from the Drop down box

Syslog Server IP List	[192.168.1.12	•	
		192.168.1.11		
		192.168.1.12		er
		192.168.1.13		

2. Click on the Delete Syslog Server button

Syslog Server IP List	192.168.1.12 💌				
	Delete Syslog Server				

Management Switch	Rem	ote Logging					
System Diagnostics	Status	Status					
Utilization		Update Setting					
System Log		-					
Remote Logging	Syslog Server IP						
<u>ARP Table</u> Route Table		Add Syslog Server					
Port	Syslog Server IP Li	ist 192.168.1.11 💌					
Trunking		Delete Syslog Server					
C STP/Ring							
🔁 VLAN							
200 63							

Figure 14: Remote Logging Page

ARP Table

To navigate to the **ARP Table** page:

- 1. Click on the + next to **Diagnostics**.
- 2. Click on ARP Table.

The ARP Table page shows ARP (Address Resolution Protocol) entries that are stored in the Switches ARP Table. This is useful for System Administrators for troubleshooting purposes. The information shown is:

- IP Address of the listed device
- Hardware Address For Ethernet devices this will always be 1.
- Flags
 - **2** = Device responded to ARP Request
 - **0** = No response to ARP Request
- Hardware Address MAC Address of the listed device
- VLAN The VLAN that the listed device is on

Management Switch		ARP Table							
Diagnostics	IP Address	Hardware Type	Flags	Hardware Address	Mask	VLAN			
Statem Log	10.58.7.114	1	2	00:18:8B:5B:B7:11	*	1			
-Remote Logging	10.58.7.112	1	2	90:18:7C:1F:D0:2B	*	1			
ARP Table	10.58.7.113	1	2	BC:30:5B:C7:43:49	*	1			
Route Table	10.58.7.119	1	2	5C:51:4F:10:E9:01	*	1			
Port	10.58.7.117	1	2	2C:B4:3A:EB:7C:AE	*	1			
🗄 🛅 Switching	10.58.7.81	1	2	00:25:64:50:82:37	*	1			
Trunking	10.58.7.105	1	0	00:00:00:00:00:00	*	1			
🗄 🛅 STP/Ring	10.58.7.32	1	2	9C:93:4E:19:38:57	*	1			
🗋 🛅 VLAN	10.58.7.107	1	2	00:50:B6:65:2A:22	*	1			
∃ 🔂 QoS	10.58.7.106	1	2	00:26:B9:88:49:4B	*	1			
t 🗀 SNMP	10.58.7.7	1	2	B8:A3:86:56:E2:9E	*	1			
	10.58.7.109	1	2	00:18:8B:5B:B2:AA	*	1			
	10 50 7 1	1	2	00100000011	*	4			

Figure 15: ARP Table

Route Table

To navigate to the Route Table page:

- 1. Click on the + next to **Diagnostics**.
- 2. Click on Route Table.

The Route Table lists the routes to network destinations and metrics (distances) that are associated with those routes. The Route Table contains information about the topology of the network around it.

Management Switch	Route Table											
Diamostics	Destination	Gateway	Genmask	Flags	Metric	Ref	Use	VLAN				
Utilization	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	2				
System Log	10.58.7.0	0.0.0.0	255.255.255.0	U	0	0	0	1				
Remote Logging	0.0.0.0	10.58.7.1	0.0.0.0	UG	0	0	0	1				
ARP Table Route Table Port												

Figure 16: Route Table

PORT

Configuration

To navigate to the **Configuration** page:

- 1. Click on the + next to Port.
- 2. Click on **Configuration**.

Port configuration contains such useful features as flow control, port speed, and duplex settings. Some users will find these settings very valuable such as when the switch is connect to a latency-critical device such as a VOIP phone or IP camera or video multiplexor. In these cases and others the ability to alter the port settings can make the difference between a poorly responding device and one that functions without loss of data or clarity.

.The Configuration page shows (see Figure 17):

- Port Number Current and Max Utilization
- Link Status Operational State of the Port's Link (Read-Only)
- Port Description User-supplied Port Description
- Admin Setting Administratively Enable or Disable the Port.
- Speed Speed and Duplex Settings for Port.
- Flow Control State of Flow Control for the Port.

To provide a description to a port on the EX24000 Switch:

- 1. Click in the **Description** text box for the appropriate port.
- 2. Type in the description of the port.
- 3. Click on the **Submit** button.

To enable or disable a port on the EX24000 Switch:

- 1. Click on the drop-down box under Admin Setting and select either Link Up or Link Down.
- 2. Click on the **Submit** button.

To set the Port Speed and/or Port Duplex Settings on the EX24000 Switch:

- Click on the drop-down box under Speed and select the desired port speed / duplex settings for that port. Please note, not all port types will have the same options. For example, 100Mb fiber ports will typically be limited to a single option of 100M/FD (100Mbps and Full Duplex) while running 1Gb UTP ports will have six options for speed/duplex.
- 2. Click on the **Submit** button.

To enable or disable a port's Flow Control settings on the EX24000 Switch:

- 1. Click on the drop-down box under Flow Control and select either Enable or Disable.
- 2. Click on the **Submit** button.

Management Switch	Port	Link Status	Port Description	Admin Setting	Speed	Flow Control
B G System B G Diamostics	1	running		Link Up 🔻	Auto 🔻	Enable 🔻
Port	2	running		Link Up 🔻	Auto 🔻	Enable T
Configuration	3	down		Link Up 🔻	Auto 🔻	Enable 🔻
Rate Control	4	down		Link Up 🔻	Auto 🔻	Enable 🔻
RMON Statistics	5	down		Link Up 🔻	Auto 🔻	Enable v
Per Port VLAN Activities	6	down		Link Up 🔻	Auto 🔻	Enable 🔻
Switching	7	down		Link Up 🔻	Auto 🔻	Enable 🔻
Tronking	8	down		Link Up 🔻	Auto 🔻	Enable v
D STF/Ring	9	down		Link Up 🔻	Auto 🔻	Enable *
		1.	1	[]		(

Figure 17: Port Configuration

Port Status

To navigate to the **Port Status** page:

- 1. Click on the + next to **Port**.
- 2. Click on Port Status.

This page is a read-only page that lists the settings described in the previous section. It is useful if all the user intends to do is read the values of the port settings, not modify the port settings. .The Port Status page shows (see Figure 18):

- **Port Number** Current and Max Utilization
- Link Status Operational State of the Port's Link.
- **Port Description** User-supplied Port Description
- Admin Setting Administratively State of the Port.
- **Speed** Speed and Duplex Settings for Port.
- Flow Control State of Flow Control for the Port.

Management Switch Port	Link Status	Port Description	Speed	Duplex	Flow Control
System 1	down		100M	Full	Enable
2 Diagnostics	down		100M	Full	Enable
3	down		100M	Full	Enable
Post Status 4	down		100M	Full	Enable
Rate Control 5	down		100M	Full	Enable
MON Statistics 6	down		100M	Full	Enable
r Fort VLAN Activities 7	down		100M	Full	Enable
nt Security Dynamic-Mac 8	down		100M	Full	Enable
Switching 9	down		100M	Full	Enable
Trunking 10	down		100M	Full	Enable
STP/Ring 11	down		100M	Full	Enable
VLAN 12	down		100M	Full	Enable
Qu6 13	down		100M	Full	Enable
SNMP 14	down		100M	Full	Enable
8021X 15	down		100M	Full	Enable
10P 16	down		100M	Full	Enable
their Protocols 17	down		100M	Fall	Enable
18	down		100M	Full	Enable
19	down		100M	Full	Enable
20	down		100M	Full	Enable
21	down		100M	Full	Enable
22	down		100M	Full	Enable
23	down		100M	Full	Enable
24	down		100M	Full	Enable
25	running		1000M	Full	Enable
26	running		1000M	Full	Enable
27	running	0	1000M	Full	Enable
28	down	2	1000M	Full	Enable

Figure 18: Port Status

Rate Control

To navigate to the Rate Control page:

- 1. Click on the + next to **Port**.
- 2. Click on Rate Control.

The Rate Control page allows the user to set the maximum throughput on a port or ports on both packets entering the port (from the connected device) or packets leaving the port.

The **Ingress** text box controls the rate of data traveling into the port while the **Egress** text box controls the rate of data leaving the port.

Note: Entries will be rounded down to the nearest acceptable rate value. If the value entered is below the lowest acceptable value then the lowest acceptable value will be used.

The Rate Control page is shown below (see Figure 19):

To provide either an ingress or egress rate control for a port on the EX24000 Switch:

- 1. Click in the Ingress or Egress Text Box for the appropriate port.
- 2. Type in the ingress/egress rate for the port according to the values listed above.
- 3. Click on the **Update Setting** button.

Management Switch	Port	Ingre	ess	Egr	ess
± ☐ System	1	0	kbps	0	kbps
Port	2	0	kbps	0	kbps
Configuration	3	115187	kbps	38375	kbps
Rate Control	4	0	kbps	0	kbps
RMON Statistics	5	0	kbps	0	kbps
Per Port VLAN Activities	6	0	kbps	0	kbps
E C Switching	7	0	kbps	0	kbps
🗄 🧰 Trunking	8	0	kbps	0	kbps
E C STP/Ring	9	0	kbps	0	kbps
E C QoS	10	0	kbps	0	kbps

Figure	19:	Rate	Control
<u> </u>			

RMON Statistics

To navigate to the **RMON Statistics** page:

- 1. Click on the + next to **Port**.
- 2. Click on RMON Statistics.

RMON Statistics gives a detailed listing of the types and quantity of packets that a particular port has seen since the last reboot of the switch (see <u>Figure 20</u>).

To view the RMON statistics for a particular port on the EX24000 Switch:

1. Click on the link to the port at the top of the RMON Statistics page.

To clear the RMON statistics for a particular port on the EX24000 Switch:

- 1. Click on the link to the port at the top of the RMON Statistics page.
- 2. Click on the Clear button at the bottom of the page.
- 3. The statistics for the port will update every ten seconds.

Pay particular attention to the values for CRC/Alignment errors and collisions. Nonzero values for these fields can indicate that a port speed or duplex mismatch exists on the port.

Drop Events	0
Broadcast Packets Received	8208
Multicast Packets Received	17830
Undersize Packets Received	0
Oversize Packets Received	0
Fragments Packets Received	0
64-byte Packets Received	11239
65 to 127-byte Packets Received	13812
128 to 255-byte Packets Received	3928
256 to 511-byte Packets Received	5903
512 to 1023-byte Packets Received	2047
1024 to 1518-byte Packets Received	41004
Jabber Packets	0
Bytes Received	67912940
Packets Received	77933
Collisions	0
CRC/Alignment Errors Received	0
TX No Errors	37441
RX No Errors	77933



Per Port VLAN Activities

To navigate to the Per Port VLAN Activities page:

- 1. Click on the + next to **Port**.
- 2. Click on Per Port VLAN Activities.

This is a read-only page that will allow the user to see what devices are connected to a particular port and the vlan associated with that device and port.

To clear the MAC addresses for a particular port on the EX24000 Switch (see Figure 21):

- 1. Click on the link to the port at the top of the Per Port VLAN Activities page.
- 2. Click on the Clear MAC button at the bottom of the page.
- 3. The statistics for the port will update every ten seconds.

🏠 Management Switch				1	4	1		1	· · · · · · · · · · · · · · · · · · ·
😐 🔂 System	<u>fe1</u>	fe2	fe3	fe4	<u>fe5</u>	fe6	fe7	fe8	<u>fe9</u>
🕀 🧰 Diagnostics		2.2			0.004	0101201			
🖻 🛄 Port	<u>fe10</u>	<u>fe11</u>	<u>fe12</u>	<u>fe13</u>	<u>fe14</u>	<u>fe15</u>	<u>fe16</u>	ge1	ge2
Configuration	-								
" <u>Port Status</u>	Port 1/fe1 sta	atus							
<u>Rate Control</u>	-				1				
<u>RMON Statistics</u>	-	Total VL	AN Count	1.0			1		
Per Port VLAN Activities	Т	otal MAC A	Address Cou	nt			1		
Port Security		VLAN M	embership			M	AC Address		
🕀 🧰 Switching		VL	AN1			6cf	0.495e.23c7		
🖲 🧰 Trunking									
🕀 🧰 STP/Ring									
🕀 🧰 VLAN									
🕀 🔂 QoS									
🕀 🔂 SNMP									
🕀 🧰 802.1X				-					
🕀 🔂 LLDP					Clear MAC				
🗄 🛅 Others Protocols									
Done						Ta 🖨 Inter	net		100% •

Figure 21: Port VLAN Activities

Port Security Dynamic-MAC

To navigate to the Port Security Dynamic-MAC page:

- 1. Click on the + next to **Port**.
- 2. Click on Port Security Dynamic-MAC.

The Port Security Dynamic-MAC submenu allows the user to control access to the ports on the switch based on the source MAC addresses of the network devices. You specify the maximum number of source MAC addresses that ports can learn. Ports that learn their maximum number of addresses discard packets that have new, unknown addresses, preventing access to the switch by any additional devices.

The Error Disable Recovery time value is a global value and represents the time that must elapse for a port to return to a normal operating state after an MAC access error is detected on that port.

To update the Error Disable Recovery time on the EX24000 Switch (see Figure 22):

- 1. Click in the **Error Disable Recovery** text box at the top of the Port Security Dynamic-MAC page.
- 2. Type in the desired value. Values can be from 0 to 65535 seconds. A value of 0 indicates that a port in an error condition is not to return to normal operating condition until an administrator resets the port or the switch is restarted..
- 3. Click on the **Update Setting** button at the bottom of the page.

To set the Dynamic MAC Security for a port on the EX24000 Switch (see Figure 22):

- 1. Click the **Enable** checkbox for the port or ports that are to be protected.
- 2. Type in a value for the **Max-Counts** field for the protected ports. This is the number of dynamically learned MAC addresses that can be accommodated by the port. For example, if the **Max-Counts** field is set to five, the port can learn up to five MAC addresses.
- 3. Select a Violation action from the Violation drop-down menu. The options are::
 - a. **Shutdown** When an unknown MAC address arrives at the port, the port is disabled and a SNMP trap is generated.
 - b. **Restrict** The port discard those frames that have unknown MAC addresses and an SNMP trap is generated when a packet with an unknown MAC address shows up on the port.
 - c. **Protect** The port discards those frames that have unknown MAC addresses.
- 4. Click on the **Submit** button.

Management Switch	Gene	ral Settino	8				
🕂 🚞 System	Error	Disable R	ecovery				
Diagnostics	(0-65	535 secon	ds, 0: no recov	ery)			
Port				Update	Setting		
Configuration							
Port Status	Dynar	nic Mac A	ddress Setting				
Rate Control		Enable	Max-Counts	Violation	Cur-Counts		
Per Port VLAN Activities	Port		1	Shutdown ‡	0		
Port Security Dynamic-Mac	Port 2	Θ	1	Shutdown ‡	0		
Trunking	Port 3		1	Shutdown +	0		
🔁 VLAN	Port 4		1	Shutdown ‡	0		
2 SNMP	Port 5	0	1	Shutdown ‡	0		
Cithers Protocols	Port 6	0	1	Shutdown ‡	0		
	Port 7		1	Shutdown ‡	0		
	Port 8		1	Shutdown ‡	0		
	Port 9		1	Shutdown ‡	0		
	Port 10		1	Shutdown ‡	0		
	Port 11		1	Shutdown ‡	0		
	Port 12		1	Shutdown ‡	0		
	Port 13	91	1	Shutdown ‡	0		

Figure 22: Port Security

Port Configuration Examples Using CLI Commands

For more information on CLI command usage see <u>CLI Command Usage</u>.

Setting the Port Description

To provide a description of a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: description <description text>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)#description A_Port_Description
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Enable or Disable a Port

To administratively enable or disable a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: shutdown no shutdown

Usage Example 1: Disabling a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)#shutdown
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Usage Example 2: Enabling a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)#no shutdown
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Setting the Port Speed

To set the port speed for a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: bandwidth <1-1000000000 bits> (usable units : k, m, g)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)#bandwidth 100m
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Setting Port Duplex

To set the duplex for a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: duplex <full | half | auto>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)#duplex full
switch_a(config)#q
```

```
switch_a(config)#g
switch_a#
```

Enable or Disable Port FlowControl

To enable or disable flowcontrol for a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: flowcontrol on

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)#flowcontrol on
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Display Port Status

To display the port status for a port use the CLI commands below:

CLI Command Mode: Privileged Exec Mode

CLI Command Syntax: show interface <ifname>

Usage Example:

switch_a>enable
switch_a#show interface fel

Setting a Ports Rate Control

To set a ports rate control use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: rate-control <ingress | egress> value <value in kbps>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)#rate-control ingress value 100000
```

```
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Display a Ports RMON Statistics

To display a ports RMON statistics use the CLI commands below:

CLI Command Mode: Privileged Exec Mode

CLI Command Syntax: show interface statistics <interface name>

Usage Example:

```
switch_a>enable
switch_a#show interface statistics fel
switch_a#
```

Display a Ports VLAN Activities

To display a port's VLAN activities use the CLI commands below:

CLI Command Mode: Privileged Exec Mode

CLI Command Syntax: show bridge interface <interface name>

Usage Example:

```
switch_a>enable
switch_a#show bridge interface fel
switch_a#
```

Setting Dynamic MAC Port Security

To set Dynamic MAC port security use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: port-security dynamic-mac enable

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)# port-security dynamic-mac enable
switch_a(config)#q
```

```
switch_a(config)#q
switch_a#
```

To set Dynamic MAC maximum number of addresses use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: port-security dynamic-mac maximum <value>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)# port-security dynamic-mac maximum 32
switch_a(config)#q
switch_a(config)#q
switch_a#
```

SWITCHING

Bridging

To learn MAC addresses, a switch reads all packets that it detects on the LAN or on the local VLAN, looking for MAC addresses of sending nodes. It places these addresses into its Ethernet Switching table, along with the interface on which the traffic was received and the time when the address was learned. When the switch receives traffic on an interface, it searches the Ethernet switching table for the MAC address of the destination. If the MAC address is not found, the traffic is flooded out all of the other interfaces associated with the VLAN. If traffic is received on an interface that is associated with VLAN 1 and there is no entry in the Ethernet switching table for VLAN 1, then the traffic is flooded to all access and trunk interfaces that are members of VLAN 1.

Flooding allows the switch to learn about destinations that are not yet in its Ethernet switching table. If a certain destination MAC address is not in the Ethernet switching table, the switch floods the traffic to all interfaces except the interface on which it was received. When the destination node receives the flooded traffic, it sends an acknowledgment packet back to the switch, allowing the switch to learn the MAC address of the node and to add the address to its Ethernet switching table.

The switch uses a process called aging to keep the Ethernet switching table current. For each MAC address in the Ethernet switching table, the switch records a timestamp of when the information about the network node was learned. Each time the switch detects traffic from a MAC address that is in its Ethernet switching table, it updates the timestamp of that MAC address. A timer on the switch periodically checks the timestamp, and if it is older than the value set for **mac-table-aging-time**, the switch removes the node's MAC address from the Ethernet switching table. This aging process ensures that the switch tracks only active MAC addresses on the network and that it is able to flush out from the Ethernet switching table MAC addresses that are no longer available.

The user can configure:

- How long MAC addresses remain in the Ethernet switching table
- Add a MAC address permanently to the switching table
- Prevent a MAC address from ever being registered in the switching table.

To navigate to the **Bridging** page:

1. Click on the **+** next to **Switching**.

2. Click on Bridging.

Aging Time

The Aging Time value is a global value and represents the time that a networked device's MAC address will live in the switch's memory before being removed. The default value is 300s (5 minutes) (see Figure 23).

To update the Aging Time value on the EX24000 Switch:

- 1. Click in the Error Disable Recovery text box at the top of the Port Security Dynamic-MAC page.
- 2. Type in the desired value. Values can be from **0 to 65535 seconds**. A value of **0** indicates that the port is not to return to normal operating condition until an administrator resets the port or the switch is restarted.
- 3. Click on the **Update Setting** button.

Port Isolation

The **Port Isolation** setting is a **per port value**. Port Isolation can be used to isolate a port or ports so that only the isolated ports can communicate with one another (see Figure 23).

To update the Port Isolation value for a port on the EX24000 Switch:

- 1. Click on the **Port Isolation** drop-down box for the port to be isolated.
- 2. Select the value **enable** on the Port Isolation drop-down box.
- 3. Click on the **Update Setting** button.
- 4. Repeat as necessary for all ports that are to be isolated.

Block Multicast

The Block Multicast setting is a per port value. Block Multicast is a straight-forward description of a feature that is used to block multicast traffic from accessing a port (see Figure 23).

To update the **Block Multicast** value for a port on the EX24000 Switch:

- 1. Click on the **Block Multicast** drop-down box for the port to be isolated.
- 2. Select the value **enable** on the Block Multicast drop-down box.
- 3. Click on the **Update Setting** button.
- 4. Repeat as necessary for all ports that are to have multicast traffic blocked.

) System	Ageing T	ime (seconds)	3	300
Diagnostics			Upda	te Setting
) Port				
Switching Bridging	Port	Threshold Level (0.1-100)	Storm Control Enabled Type	Port Isolation
Loopback Detect	fe1	Level	Broadcast DLE-Multicast	Disable V
Storm Detect	fe2	Level	Broadcast DLF-Multicast	Disable 🗸
Static MAC Entry	fe3	Level	Broadcast DLF Multicast	Disable V
Fort Mirroring Link State Tracking	fel	Level	Proadcast DLF -Multicast	Disable -
PoE	fa5	Level		
PoE Scheduling	fac	Level		Disable V
Trunking	100	Level		Disable V
STP/Ring	Ie/	Level	Broadcast DLF-Multicast	Disable Y
Oo\$	fe8	Level	Broadcast DLF-Multicast	Disable 🚩
SNMP	fe9	Level	Broadcast DLF-Multicast	Disable 🚩
802.1X	fe10	Level	Broadcast DLF-Multicast	Disable 🚩
LLDP	fel1	Level	Broadcast DLF-Multicast	Disable 🚩
Others Protocols	fe12	Level	Broadcast DLF-Multicast	Disable 💌
	fe13	Level	Broadcast DLF-Multicast	Disable 💌
	fe14	Level	Broadcast DLF-Multicast	Disable 💌
	fe15	Level	Broadcast DLF-Multicast	Disable 💌
	fe16	Level	Broadcast DLF-Multicast	Disable 💌
	ge1	Level	Broadcast DLF-Multicast	Disable 💌
	ge2	Level	Broadcast DLF-Multicast	Disable 🗸
				Jpdate Setting

Figure 23: Bridging

Loopback Detect

Loopback detection is quite simply the ability of the switch to detect when a port on the switch has been connected directly (or "looped back") to another port on the switch. This configuration would likely lead to a broadcast storm on the switch which would cause network performance to suffer. Loopback detection offers the ability of the switch to detect this condition and shutdown the loop-backed port before any disruption of network traffic occurs.

To navigate to the Loopback Detect page:

- 1. Click on the + next to **Switching**.
- 2. Click on Loopback Detect.

Enabling Loopback Detection (Global)

To globally enable the Loopback Detect feature of the EX24000 Switch (see Figure 24):

- 1. Click on the Loopback Detect drop-down box.
- 2. Select **Enable** from the drop down list.
- 3. Click on the **Update Setting** button.

Changing the Loopback Detect Action

To change the action that the switch takes when a loopback condition is detected (see Figure 24):

- 1. Choose an action from the **Loopback Detect Action** dropdown list. The available options are **None** and **Error Disable**.
- 2. Click on the **Update Setting** button.

Changing the Loopback Detect Recovery Time

To change the length of time that the **Loopback Detect Action** will stay in effect (see <u>Figure</u> <u>24</u>):

1. Enter a value in the text box next to **Error Disable Recovery**. Valid values range from **0 to 65535 seconds**.

2. Click on the **Update Setting** button.

Changing the Polling Interval

To change the polling interval of the Loopback Detect function (see Figure 24):

- 1. Enter a value in the text box next to **Interval**. Valid values range from **1 to 65535** seconds.
- 2. Click on the **Update Setting** button.

LoopBack Detect	Enable ‡
LoopBack Detect Action	Error Disable +
Error Disable Recovery (0-65535 seconds)	10
Interval (1-65535 seconds)	1
	Update Settin

Figure 24: Loopback Detection

Enabling Loopback Detection (Per Port)

To enable **Loopback Detection** for a particular port or ports on the EX24000 switch (see Figure 25):

- 1. Select the value **Enable** from the **Mode** drop down list for a port on the Loopback Detect page.
- 2. Click on the **Update Setting** button.

Port	Mode	State
1	Disable (default) ‡	
2	Disable (default) 🗘	
3	Disable (default) 🗘	
4	Disable (default) 💠	
5	Disable (default) 🗘	
6	Disable (default) 💠	
7	Disable (default) 💠	2 ¹¹⁷
8	Disable (default) ‡	
9	Disable (default) 💠	
10	Disable (default) 🗘	
11	Disable (default) 💠	
12	Disable (default) 💠	
13	Disable (default) 💠	
14	Disable (default) 💲	
15	Disable (default) 💠	1777:
16	Disable (default) 💠	
17	Disable (default) +	100
18	Disable (default) +	
19	Disable (default) ‡	
20	Disable (default) 💠	
21	Disable (default) 💠	
22	Disable (default) 💠	
23	Disable (default) ‡	9 ⁷⁷⁸
24	Disable (default) ‡	
25	Enable ‡	Normal
26	Enable ‡	Errdisabled
27	Disable (default) ‡	
28	Disable (default) ‡	
20	Disable (deladit) +	

Figure 25:Loopback Detection (port)

Storm Detect

This feature allows the user to regulate the reception rate of broadcast and multicast packets on a port-by-port basis. This setting can be useful in allowing a user to prevent a switch port from being overwhelmed with broadcast or multicast traffic (see Figure 26).

To navigate to the Storm Detect page:

- 1. Click on the **+** next to **Switching**.
- 2. Click on Storm Detect.

Enabling Storm Detect Configuration (Global)

To globally enable the **Storm Detect Configuration** feature of the EX24000 Switch (see Figure 26):

- 1. Click on the **Loopback Detect Configuration** drop-down box.
- 2. Select Enable from the drop down list.
- 3. Click on the **Submit** button.

Changing the Storm Detect Interval

To change the interval of the Storm Detect function (see Figure 26):

- 1. Enter a value in the text box next to **Interval**. Valid values range from **2 to 65535** seconds.
- 2. Click on the **Submit** button.

Changing the Storm Detect Error Disable Recovery Time

To change the length of time that the **Storm Detect Error Disable Recovery** will stay in effect (see Figure 26):

- 1. Enter a value in the text box next to **Error Disable Recovery**. Valid values range from **0 to 65535 seconds**.
- 2. Click on the **Submit** button.

To update the Storm Detect by utilization (%) of a port on the EX24000 Switch:

- 1. Click in the **By Utilization** text box for a particular port.
- 2. Type in the desired value. Values can be from **0 to 100**. This value is a percentage of allowable storm traffic for this port. Once this percentage of traffic is exceeded, all storm traffic beyond this percentage is dropped.
- 3. Click on the **Submit** button.

To update the Storm Detect by Broadcast (or Multicast + Broadcast) packets per second of a port on the EX24000 Switch:

- 1. Click on the Loopback Detect By Broadcast / Multicast + Broadcast Packets Per Second drop-down box.
- 2. Select **BC** (Broadcast) or **MC-BC** (Multicast + Broadcast) from the drop down list.
- 3. Click in the **By Broadcast / Multicast + Broadcast Packets Per Second** text box for a particular port.
- Type in the desired value. Values can be from 0 to 100000. This value is an allowable Broadcast (or Multicast + Broadcast) packets per second for this port. Once this value of traffic is exceeded, all Broadcast (or Multicast + Broadcast) traffic beyond this value is dropped.
- 5. Click on the **Submit** button.

		Bridge Storm-Detect (Configuration		
Diagnostics	Storm-D	etect configuration		Disable 💌	
🔁 Port	Storm-D	etect interval (265535 sec), Default	t: 10	10	
Switching Bridging	Storm-D recovery	etect errdisable-recovery time (065	535 sec), 0:no	0	
Loopback Detect	Storm-D	etect state of action		None	
Storm Detect		Storm-Dete	ect Per Port Configur	ation	
" <u>Static MAC Entry</u> " <u>Port Mirroring</u> "Link State Tracking	Port	State / Recovery time remains	By Utilization(%) (0-100) 0: not limited	By Broadcast / Mu Packets P (0-100000) 0	ulticast+Broadcast er Second): not limited
PoE	fe1	No Detecting	0	BC 💌	0
PoE Scheduling	fe2	No Detecting	0	BC M	0
Trunking	fe3	No Detecting	0	BC 💌	0
STP/Ring	fe4	No Detecting	0	BC 💌	0
OoS	fe5	No Detecting	0	BC 💌	0
SNMP	fe6	No Detecting	0	BC 😽	0
802.1X	fe7	No Detecting	0	BC 🖌	0
LLDP	fe8	No Detecting	0	BC 💌	0
Others Protocols	fe9	No Detecting	0	BC 💌	0
	fe10	No Detecting	0	BC 🛩	0
	fe11	No Detecting	0	BC 💌	0
	fe12	No Detecting	0	BC M	0
	fe13	No Detecting	0	BC 😽	0
	fe14	No Detecting	0	BC 💌	0
	fe15	No Detecting	0	BC 💌	0
	fe16	No Detecting	0	BC 💌	0
	ge1	No Detecting	0	BC 💌	0
	ge2	No Detecting	0	BC 💌	0
				1.11	

Figure 26: Storm Detect

Static MAC Entry

Occasionally, it may be useful to specify a MAC address on a particular port and VLAN rather than adjusting the ageing time for the entire switch. Alternatively, it is also possible and even desirable to prevent a MAC address from ever being registered with a switch. These features are offered under the **Static MAC Entry** menu.

To navigate to the Static MAC Entry menu:

- 1. Click on the + next to Switching.
- 2. Click on **Static MAC Entry.**

Adding a Static MAC Address to a Port

To add a static MAC entry for a particular port (see Figure 27):

- 1. Enter the MAC address for end the corresponding port's text box. The format of the MAC address should be in the form **aaaa:bbbb:cccc**).
- 2. Select the VLAN that this MAC address is associated with from the VLAN ID drop down list for the port.
- 3. Click on the **Submit** button.

Port	Add MAC Address (Ex: 0000.1111.2222)	VLAN ID	Delete MAC Address
1	e0b3.1234.abcf	1 \$	
2		+	(\$)
3		+	:
4		\$	\$
-			-

Static-MAC-Entry Forward

Figure 27: MAC Static Entry

Removing a Static MAC Address from a Port

To remove a static MAC entry for a particular port (see Figure 28):

- 1. For a particular port, select the MAC address to be deleted from the **Delete MAC** Address drop down box.
- 2. Click on the **Submit** button.

Port	Add MAC Address (Ex: 0000.1111.2222)	VLAN ID	Delete MAC Address
1		÷	e0b3.1234.abcf vlan 1 ‡
2		•	()
3		+	(
4		÷	
5		•	(\$
6		(÷)	:

Figure 28: Removing a Static MAC

Adding a MAC to the Static-MAC-Entry Discard Table

To add a MAC address to the Static-MAC-Entry Discard table (see Figure 29):

- 1. Enter a MAC address in the form "0000.1234.abdc" in the **Add MAC Address** text box of the **Static-MAC-Entry-Discard** section.
- 2. Select the VLAN associated with the MAC address.
- 3. It should be noted that while static MAC address for forwarding are associated with the switch on a per-port basis. Static MAC discards are associated with the switch for all ports.
- 4. Click on the **Submit** button.

Add MAC Address (Ex: 0000.1111.2222)	VLAN ID	Delete MAC Address
aabb.1289.cdf3	1 \$:

Figure 29: Adding a MAC – Static-MAC-Entry Table

Removing a MAC address from the Static-MAC-Entry Discard Table

To remove a MAC address from the Static-MAC-Entry Discard table (see Figure 30):

- 1. From the drop down box underneath **Delete MAC Address**, select the MAC address to be deleted.
- 2. Click on the **Submit** button.

П

Add MAC Address (Ex: 0000.1111.2222)	VLAN ID	Delete MAC Address
	\$	00eb.0321.45ad vlan 1 🗘

Figure 30: Deleting a MAC – Static-MAC-Entry Table

Port Mirroring

Port mirroring allows network traffic from one port to be copied or mirrored to another port. This is a very useful troubleshooting feature in that all data from one port is sent to another port which is attached to a computer or other network device that is configured to capture packets. This enables a network administrator or technician to see the traffic that is entering or leaving a particular port without disrupting normal network operations on the port that is being mirrored.

To navigate to the **Port Mirroring** menu:

- 1. Click on the + next to Switching.
- 2. Click on **Port Mirroring.**

To configure port mirroring for a port or ports on the EX24000 switch (see Figure 31):

- 1. Select the port or ports that traffic is to be mirrored from under the **Mirror From** column.
- 2. Select the destination port under the **Mirror To** drop down box.
- 3. Select the type of traffic that should be mirrored from the **Mirror Mode** drop down box. The available options are:
 - a. TX transmit only
 - b. RX Receive Only
 - c. TX/RX Transmit and Receive.
- 4. Click on the **Submit** button.

Mirror From	Mirror To	Mirror Mode
port 1		
ort 2		
J port 3		
ort 4		
port 5		
port 6		
port 7		
port 8		
port 9		
port 10		
port 11		
port 12		
port 13		
port 14	port 25 ÷	Tx/Rx +
port 15		
port 16		
port 17		
port 18		
port 19		
port 20		
port 21		
port 22		
port 23		
port 24		
port 25		
port 26		
port 27		
port 28		

Figure 31: Port Mirroring
To disable port mirroring for a port or ports on the EX24000 switch (see Figure 32):

- 1. Under the **Current Settings** section, the current port mirroring configuration should be displayed.
- 2. Click on the **Delete** button.

Mirror From	Mirror To	Mirror Mode
port1		
port2	a - +25	hash
port3	port25	DOTH
port4		

Figure 32: Disabling Port Mirroring

Link State Tracking

Link-state tracking binds the link state of multiple interfaces. Link-state tracking provides redundancy in the network when used with server network interface card (NIC) adapter teaming or bonding. When the server network adapters are configured in a primary or secondary relationship known as teaming and the link is lost on the primary interface, connectivity transparently changes to the secondary interface.

To navigate to the Link State Tracking menu:

- 1. Click on the + next to **Switching**.
- 2. Click on Link State Tracking.

Enable/Disable Link State Tracking

To enable Link State Tracking for a particular group on the EX24000 Switch (see Figure 33):

- 1. Under **Group Setting**, click the check box of the Link State groups that are to be enabled (or disabled).
- 2. Click on **Update Setting.**

ink State	Tracking	Setting								
	20		20	Gro	up Settir	ng	20		20	
	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6	Group 7	Group 8	Group 9	Group 10
Enable	2	•					0			

Figure 33: Link State Tracking

Port Settings

To configure individual ports for a Link State group on the EX24000 switch (see Figure 34):

- 1. Under **Port Setting**, select the Link State Group that the port will belong to from the Group drop down box
- 2. Select if the port is upstream or downstream from the Up/Down Stream)drop down box.
- 3. Click on **Update Setting.**

	Port Setting							
Port	Group	(Up/Down)Stream	Status					
1	1 \$	Up ‡						
2	1 ‡	Up \$						
3	÷	Up ‡						
4	÷	Up ‡						
5	\$	Up ‡						
6	()	Un ÷						

Figure 34: Link State Tracking – Port Settings

ΡοΕ

To navigate to the **PoE** page:

- 1. Click on the **+** next to **Switching**.
- 2. Click on **PoE.**

Changing the System Power Budget (Global)

To change the System Power Budget (see Figure 35):

- 1. Enter a value in the text box next to **System Power Budget**.
- 2. Click on the **Submit** button.

Enabling Enable Mode (Per Port)

To enable **Enable Mode** for a particular port or ports on the EX24000 switch (see Figure 35):

- 1. Select the value **Enable** from the **Enable Mode** drop down list for a port on the PoE page.
- 2. Click on the **Submit** button.

Changing the Fixed Power Limit (Per Port)

To change the **Fixed Power Limit** (see Figure 35):

- 1. Enter a value in the text box next to **Fixed Power Limit**.
- 2. Click on the **Submit** button.

Enabling Power Priority (Per Port)

To enable **Power Priority** for a particular port or ports on the EX24000 switch (see Figure <u>35</u>):

- 1. Select the value from the **Power Priority** drop down list for a port on the PoE page.
- 2. Click on the **Submit** button.

Diagnostics Port	Mai	- Y25.0 - 2.0 - 5.0 - 5.0						
Port		n Supply Voltage	48.00 ((V)				
Switching	Sys	tem Temperature	33.31 ((C)				
ownenning	Po	ower Allocation	0.00 (W)				
Bridging	Syste	em Power Budget	195.00	(W)				
.oopback Detect Storm Detect Static MAC Entry	The val greater Limit'	ue of 'System Pow than the sum of all	ver Budget' shou port's 'Fixed P	ıld ower				
Port Mirroring .ink State Tracking				Submit				
<u>oE</u>		<i></i>		PoE	Port Setting			
o <u>E Scheduling</u> Trunking	Port	Enable Mode	Fixed Power Limit (W)	Power Priority	Status	PD Class	Current (mA)	Consumption (W)
STP/Ring	1	Enable 💌	15.30	High 🔽	Searching	N/A	0	0
VLAN Das	2	Enable 💌	15.30	High 💌	Searching	N/A	0	0
NMP	3	Enable 💌	15.30	High 💌	Searching	N/A	0	0
02.1X	4	Enable 💌	15.30	High 🔽	Searching	N/A	0	0
LDP	5	Enable 👻	15.30	High 💙	Searching	N/A	0	0
thers Protocols	6	Enable 🗸	15.30	High 👻	Searching	N/A	0	0
	7	Enable 👻	15.30	High 💙	Searching	N/A	0	0
	8	Enable 👻	15.30	High 💌	Searching	N/A	0	0
	9	Enable 💌	15.30	High 💌	Searching	N/A	0	0
	10	Enable 💌	15.30	High 💌	Searching	N/A	0	0
	11	Enable 💌	15.30	High 💌	Searching	N/A	0	0
	12	Enable 🗸	15.30	High 💌	Searching	N/A	0	0
	13	Enable 💌	15.30	Low 💌	Searching	N/A	0	0
	14	Enable 🗸	15.30	Low 💌	Searching	N/A	0	0
	15	Enable 💌	15.30	Low 💌	Searching	N/A	0	0
	16	Enable 💌	15.30	Low 💌	Searching	N/A	0	0
								Submit

Figure 35: PoE

PoE Scheduling

To navigate to the **PoE Scheduling** page:

- 1. Click on the **+** next to **Switching**.
- 2. Click on **PoE Scheduling.**

Enabling PoE Scheduling (Per Port)

To enable **PoE Scheduling** for a particular port or ports on the EX24000 switch (see Figure 36):

1. Select the port from the **Port** drop down list for a port on the PoE Scheduling page.

- 2. Check time box from Sunday to Saturday.
- 3. Click on the **Submit** button.

Port	Port: 1	Stati	us: Not Schedu	ıled				
Switching	Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Bridging	00:00							
Loopback Detect	01:00							
Storm Detect	02:00							
Static MAC Entry	03:00							
Port Mirroring	04:00							
Link State Tracking	05:00							
PoE	06:00							
PoE Scheduling	07:00							
Trunking	08:00							
STP/Ring	09:00							
🗅 VLAN	10:00		2					
🔁 QoS	11:00							
SNMP	12:00			İ İ			ĺ	
302.1X	13:00							
LLDP	14:00							
Others Protocols	15:00							
	16:00							
	17:00							
	18:00							
	19:00							
	20:00							
	21:00							
	22:00							
	23:00							
		Select All	Select All	Select All	Select All	Select All	Select All	Select All
		Delete All					Delete All	Dalata All
		Delete All	Delete All	Delete All	Delete All	Delete All	Delete All	Delete All

Figure 36: PoE Scheduling

Switch Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

Setting the Aging Time Value

To update the **Aging Time** value on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 ageing-time (time in ms)

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 ageing time 300
switch_a(config)#q
switch_a#

Enabling Port Isolation

To enable **Port Isolation** for a port on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: port-isolation enable

```
switch_a>enable
switch_a#configure terminal
switch_a#configure interface fel
switch_a(config)#port-isolation enable
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Enabling Block Multicast

To enable **Block Multicast** for a port on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: switchport block multicast

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#configure interface fel
switch_a(config)#switchport block multicast
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Setting Storm Detect by Utilization

To set the percentage for the **Storm Detect by Utilization** of a port on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: storm-detect utilization <0-100>

```
switch_a>enable
switch_a#configure terminal
switch_a#configure interface fel
switch_a(config-if)#storm-detect utilization 10
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Enabling Loopback Detect (Global)

To enable Loopback Detect on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 loopback-detect <enable | disable>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 loopback-detect enable
switch_a(config)#q
switch_a#
```

Setting the Loopback Detect Action

To set the action for **Loopback Detect** on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 loopback-detect action <err-disable | none>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 loopback-detect action err-disable
switch_a(config)#q
switch_a#
```

Setting the Loopback Detect Recovery Time

To set the recovery time for **Loopback Detect** on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 loopback-detect errdisable-recovery <0-65535>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 loopback-detect errdisable-recovery 30
switch_a(config)#q
switch_a#
```

Setting the Loopback Detect Polling Interval

To set the polling interval for **Loopback Detect** on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 loopback-detect interval <1-65535>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 loopback-detect interval 5
switch_a(config)#q
switch_a#
```

Enabling Loopback Detect (Port)

To enable **Loopback Detection** on a port on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: loopback-detect enable

```
switch_a>enable
switch_a#configure terminal
switch_a#interface fel
switch_a(config)# loopback-detect enable
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Adding a MAC Address for Static-MAC-Entry Forwarding

To add a MAC address for **Static-MAC-Entry Forwarding** for a port on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax:

bridge 1 address <mac address> forward <interface> vlan <vlan id>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 address 00e0.abcd.1245 forward fel vlan 1
switch_a(config)#q
switch_a#
```

Adding a MAC Address for Static-MAC-Entry Discarding

To add a MAC address for **Static-MAC-Entry Discarding** for a port on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 address <mac address> discard vlan <vlan id>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 address 00e0.abcd.1245 discard vlan 1
switch_a(config)#q
switch_a#
```

Configuring Port Mirroring

To configure a port for Port Mirroring on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

```
CLI Command Syntax: mirror interface <interface> direction <both | tx | rx>
```

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface gel
switch_a(config)# mirror interface fel direction both
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Enabling a Link State Tracking Group

To enable a **Link State Tracking** Group on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: link state track <group #>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# link state track 4
switch_a(config)#q
switch_a#
```

Assigning a Port to a Link State Tracking Group

To assign a port to a Link State Tracking group on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: link state group <group #> <upstream | downstream>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface fel
switch_a(config)# link state group 4 downstream
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Setting the System Power Budget

To update the **Sysem Power Budget** value on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: poe system-power-budget <LEVEL>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# poe system-power-budget 246
switch_a(config)#q
switch_a#
```

TRUNKING

Overview

Port Trunking refers to the use of multiple network connections in parallel to increase the link speed beyond the limits of any one single cable or port. This is commonly called link aggregation. These aggregated links may be used to interconnect switches or to connect high-capacity servers to a network.

The EtherWAN EX24000 Switch supports up to six trunks for 100Mbps ports and up to two gigabit trunks. Each 100Mbps trunk can be composed of up to eight 100Mbps ports while each gigabit trunk can support up to four gigabit ports.

There are two popular types of port trunking, static and link aggregation control protocol (LACP). We will take a minute to discuss both types of trunking and why one would want to use them.

Static Channel Trunking

Originally specified in the IEEE802.3AD specification and now in the IEEE 802.1AX2008 specification, this type of trunking is the most basic and easiest to understand. It simply is the aggregation of two or more Ethernet links to form a virtual link equivalent in bandwidth to the sum of its individual links. For example, if one had four 100Mbps Ethernet links composing a single static channel, the overall bandwidth of the static channel would be 400Mbps.

Prioritization of data through the channel is simple as well. When one of the links of the channel becomes saturated the excess data spills over into the remaining channels. For example, if one were sending a constant stream of data at 250Mbps through a static channel composed of 4 individual 100Mbps links, the first two links of the channel would be completely saturated while the half of the third channel would be utilized and none of the forth channel would be used.

Link Aggregation Control Protocol

Within the IEEE specification, the Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP). This means that both sides of the LACP channel must be configured for LACP which implies both devices must support it. LACP also has a couple of very important advantages over static channel:

- Failover when a link fails and there is (for example) a media converter between the devices which means that the peer will not see the link down. With static link aggregation the peer would continue sending traffic down the link causing it to be lost.
- The device can confirm that the configuration at the other end can handle link aggregation. With Static link aggregation a cabling or configuration mistake could go undetected and cause undesirable network behavior.

Port Trunking

To navigate to the **Port Trunking** menu:

- 1. Click on the + next to **Trunking**.
- 2. Click on **Port Trunking.**

To create a static trunk consisting of 100Mbps ports (see Figure 37):

- 1. Click on the checkbox for each desired port in a particular trunk.
- 2. Click on the **Submit** button.

To create a static trunk consisting of 1000Mbps ports (see Figure 37):

- 1. In the **GE Trunking** section, click on the checkbox for each desired port in a particular trunk.
- 2. Click on the **Submit** button.

									i.	Stati	c Cha	nnel	Grou	ID										
	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port	port
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Trunk 1																						0		
Trunk 2																						0		
Trunk 3																						0		
Trunk 4																						0		
Trunk 5													۷	۷	1	۷	۷					0		
Trunk 6																						0		
Note: 5	G	E Tru	Inking	g	trui																	_	Sub	mit
	po	ort 1	port 2	port 3	por 4	t																		
Trunk	7 (
Trunk 8	3 (
Note: 4	port	s ma	ximu	m pei	r trur ubmit	nk D																		

Figure 37: Port Trunking

LACP Trunking

To navigate to the LACP Trunking menu:

- 1. Click on the + next to **Trunking**.
- 2. Click on LACP Trunking.

To create a LACP trunk (see Figure 38):

- 1. In the **Trunk Configuration** section, select a port in the LACP trunk.
- 2. Select LACP from the Trunk Type dropdown box for this port.
- 3. Enter an admin key for this port in the **Admin Key** textbox. 100Mbps ports admin keys must be between 1-6 and 1Gbps ports must be between 7-8.
- 4. Select the LACP Mode to either Active or Passive.
- 5. Enter a value in the **Port Priority** textbox.
- 6. Select a Timeout value of **Short** or **Long**.
- 7. Click on the **Submit** button.
- 8. Repeat steps 1-7 for each additional port that is to be used in the trunk.

Port	Trunk Type	Admin Key	LACP Mode	LACP Port Priority	LACP Timeout	LACP Sync	LACP Sync Port
1	None	None	None	None	None	None	None
2	None	None	None	None	None	None	None
3	None	None	None	None	None	None	None
4	Static	2	None	None	None	None	None
5	Static	2	None	None	None	None	None
6	Static	2	None	None	None	None	None
7	Static	3	None	None	None	None	None
8	Static	3	None	None	None	None	None
9	Static	3	None	None	None	None	None
10	Static	4	None	None	None	None	None
11	Static	4	None	None	None	None	None
12	Static	4	None	None	None	None	None
13	Static	5	None	None	None	None	None
14	Static	5	None	None	None	None	None
15	Static	5	None	None	None	None	None
16	Static	5	None	None	None	None	None
17	Static	5	None	None	None	None	None
18	Static	5	None	None	None	None	None
19	Static	6	None	None	None	None	None
20	Static	6	None	None	None	None	None
21	Static	6	None	None	None	None	None
22	None	None	None	None	None	None	None
23	None	None	None	None	None	None	None
24	None	None	None	None	None	None	None
25	None	None	None	None	None	None	None
26	LACP	7	active	1	long	Not Sync	NA
27	None	None	None	None	None	None	None
28	LACP	7	active	1	long	Not Sync	NA
k Confi	guration :	ala di					
ort	Trunk Type	Admin Key (FE ports:1-6) (GE ports:7-8)	LACP Mode	LACP Port Priority (Set 0 for None)	LACP Timeout		
8 \$	LACP \$	7	Active	\$	Long ‡		
e: 8 por	rts maximum per t	runk			Update Setting		

Figure 38: LACP Trunking

Trunking Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

Adding an Interface to a Static Trunk

To add an interface to a static trunk on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode CLI Command Syntax: static-channel-group <static channel> (1-6 for 100Mbps, 7-8 for 1Gbps ports)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fe1
switch_a(config)#static-channel-group 1
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Adding an Interface to a LACP Trunk

To add an interface to a LACP trunk on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: **channel-group** *<LACP Channel>* **mode** *<active | passive>* (LACP Channel is 1-6 for 100Mbps, 7-8 for 1Gbps ports)

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fe1
switch_a(config)# channel-group 2 mode passive
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Setting the LACP Port Priority

To set the port priority for an interface attached to a LACP trunk on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: lacp port-priority <1 - 65535>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fe1
switch_a(config)# lacp port-priority 1
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Setting the LACP Timeout

To set the timeout for an interface attached to a LACP trunk on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: lacp timeout <long | short>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fe1
switch_a(config)# lacp timeout long
switch_a(config)#q
switch_a(config)#q
switch_a#
```

STP/RING PAGE – OVERVIEW

Choosing the Spanning Tree Protocols

The Spanning Tree algorithm works by designating a single switch (The Root Bridge) in the network, as the root or the parent to all the switches. All the switches in the network will use the same algorithm to form unique paths all the way back to the Root Bridge. Some switches establish a blocking point (a port on a switch) somewhere along the path to prevent a loop. There are 3 versions of the Spanning Tree protocol, STP, RSTP, MSTP, and they are all backwards compatible with each other.

Spanning Tree Protocol (STP)

This is the original Spanning Tree protocol, and it has been supersede by both the RSTP and MSTP protocol. It is based on a network with a maximum diameter of no more than 17 switches. It uses timers to synchronize any changes in the network topology, and this could take minutes. It is not recommended that you use this version of the Spanning Tree protocol.

Rapid Spanning Tree protocol (RSTP)

The RSTP protocol is the new enhanced version of the original STP protocol. It uses an enhanced negotiation mechanism to directly synchronize any topology changes between switches; it no longer uses timers as in the original STP protocol, which results in a faster re-convergence time. The maximum allowed network diameter for the RSTP protocol is 40 switches.

Multiple Spanning Tree Protocol (MSTP)

The MSTP protocol extends the RSTP protocol by simultaneously running multiple instances of the Spanning Tree Protocol and mapping different VLANs to each instance, thus providing load balance across multiple switches. The MSTP protocol accomplishes this by creating new extended sections within the RSTP protocol, called Regions. Each region runs its own instance of the Spanning Tree Protocol. Within each Region, the MSTP protocol can accommodate a network diameter of up to 40 switches. There can be a maximum of 40 Regions in a single MSTP network.

Note: If a faster recovery time is required, EtherWAN's proprietary α -Ring provides a recovery time of <15MS with up to 250 switches. See <u>STP/Ring Page -</u> Alpha Ring_on page <u>123</u> for more information.

STP/RING PAGE - CONFIGURING RSTP

Global Configuration Page

To navigate to the STP/Ring Global Configuration page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on Global Configuration.

Enabling the RSTP Protocol

RSTP is enabled by Default. If RSTP has been disabled and you wish to enable it (see Figure 39):

- 1. Click the dropdown box next to **Spanning Tree** Protocol and choose **Enable**.
- 2. Click on the dropdown box next to **STP Version** and select **RSTP**.
- 3. Click on the **Update Setting** button.

Additional Global Configuration page settings

- **Bridge Priority** Bridge Priority is used to set the Root and backup Root Bridge. For more details see <u>The Root Bridge & Backup Root Bridge</u>.
 - Default is 32768. Range is 0 to 61440.
- Hello Time This tells how often a BPDU (Bridge Protocol Data Unit) is sent (see <u>Bridge Protocol Data Units</u>). Default is 2 seconds. Range is 1 to 10 seconds.
- Max Age Default is 20. Hop count limit for BPDU packets (see <u>Setting the MAX</u> Age, Forward Delay and Hello Timer),
- Forward Delay Default is 15 sec.
- Note: Bridge Protocol Data Units (BPDUs) are frames that contain information about the Spanning tree protocol (STP). Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC (01:80:C2:00:00:00). There are three kinds of BPDUs:
- Configuration BPDU, used by Spanning Tree Protocol to provide information to all switches.
- TCN (Topology change), tells about changes in the topology.
- TCA (Topology change Acknowledgment), confirm the reception of the TCN.

		Update Setting					
	STP Version	RSTP					
🕀 🧰 802.1X	Forward Delay (430 sec)	15					
E C SNMP	Max Age (040 sec)	20					
		2					
Advanced Setting	Hello Time (1, 10 sec)						
Chain Pass-Through Setting	Bridge Priority (0, 61440)	32768					
Chain Setting	Spanning Tree Protocol	Enable 🗸					
Ring Setting	Set	Setting					
MSTP Port Setting	Time Since Last Topology Change	Thu Jan 22 20:27:09 2009					
MSTP Instance Setting	Topology Change Count	0					
-MSTP Properties	Current Forward Delay (sec)	15					
RSTP Port Setting	Current Hello Time (sec)	20					
Global Configuration	Current Max Age (cec)	20					
🗄 🧰 Trunking	Root Port	0					
🗄 🧰 Switching	Reg Root ID						
🗄 🔂 Port	Designated Root	800000e0b3556677					
🗉 🧀 Diagnostics	Bridge ID	800000e0b3556677					
🕀 🧰 System	Sta	itus					

Figure 39: STP/Ring Global Configuration

The Root Bridge & Backup Root Bridge

To configure the Spanning Tree protocol on your network, you will need to setup a Root Bridge and Backup Root Bridge. In order to configure a switch to be the Root Bridge of a Spanning Tree network, you have to make sure that the Bridge Priority (which is the most significant 4 bits of the Bridge ID) of the switch is the lowest among any of the switches on the network. Similarly for the Backup Root Bridge, it must have the next lowest Bridge Priority of all the switches.

Note: Since the Bridge Priority is the most significant 4 bit of the Bridge ID, the lowest Bridge Priority will always be the Root Bridge and the second lowest Bridge Priority will be the Backup Root Bridge. If all switches have the same Bridge Priority, then The 12 bit System ID or MAC Address (if the system ID's are the same) will be used to determine the Root and Backup Root Bridge (See 41).

Figure 40: Bridge ID

Bridge ID is a concatenation of 3 values: a 4 bit Bridge Priority (most significant), a 12 bit System ID (less significant), and the 48 bit MAC address of the local switch (least significant).

Setting the Root Bridge and Backup Root Bridge

To navigate to the STP/Ring Global Configuration page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on Global Configuration.

To set the Bridge Priority:

- Enter the Bridge Priority ID in the text box to the right of Bridge Priority (0..61440)
- 2. Click on the **Update Setting** button.

Note: The valid values for this parameter are from 0 to 61440, in increments of 4096; you will see this value reflected in the first hexadecimal digit of the **Bridge ID** field after you click the **Update Setting** button (See Figure 41). Set this value to be less than any other switch on the network, in order to make this switch the Root Switch. To set a

± 🔂 Svstem	Stat	his
± 🔂 Diagnostics	Bridge ID	800000e0b3556677
🗄 🛅 Port	Designated Root	800000e0b3556677
🗄 🛅 Switching	Reg Root ID	
🗄 🛅 Trunking	Root Port	0
STP/Ring	Root Path Cost	0
Global Configuration	Current Max Age (sec)	20
RSTP Port Setting	Current Hello Time (sec)	2
<u>MSTP Properties</u>	Current Forward Delay (sec)	15
MSTP Instance Setting	Topology Change Count	0
MSTP Port Setting	Time Since Last Topology Change	Thu Jan 22 20:27:09 2009
Ring Setting	Sett	ing
Chain Setting	Spanning Tree Protocol	Enable 💌
Advanced Setting	Bridge Priority (061440)	32768
D 🔂 VLAN	Hello Time (110 sec)	2
🗄 🛅 QoS	Max Age (640 sec)	20
E 🔁 SNMP	Forward Delay (430 sec)	15
	STP Version	RSTP
Others Protocols		Update Setting
one		😜 Internet 🥢 🔹 🔨 100%

Backup Root Bridge set the **Bridge ID** to be between the **Root Bridge** and the rest of the network switches.

Figure 41: Bridge ID Display

Setting the MAX Age, Forward Delay and Hello Timer

To navigate to the STP/Ring Global Configuration page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on Global Configuration.

The Network Diameter

The Diameter of a network depends on the type of topology your network uses. In a ring topology, the Network Diameter is the total number of switches in a network minus the Root Bridge. In a star topology, the Network Diameter is the maximum number of hops to get from Root Bridge to the switch that is the most hops away. the In the RSTP protocol, the **Max Age** parameter is used as a hop count limit on how far the Spanning Tree protocol packet can propagate throughout the network topology, therefore, it must be configured with a value that is greater than the network diameter.

Relationship between Max Age, Forward Delay and Hello Time

The following rules must be followed when setting the **Max Age**, **Forward Delay** and **Hello Timer**:

- Max Age >= 2 × (Hello Time + 1.0 second)
- 2 × (Forward Delay 1.0 second) >= Max Age

To change the Max Age, Forward Delay and Hello Timer (see Figure 42):

- 1. Enter the Max Age in the text box to the right of Max Age (6..40 sec) label.
- 2. Enter the **Hello Time** in the text box to the right of the Hello Time (1..10 sec) label.
- 3. Enter the **Forward Delay** in the text box to the right of the Forward Delay (4..30 sec) label.
- 4. Click on the **Update Setting** button.
- 5. Save the configuration (see the Save Configuration Page)

🙆 Management Switch		
🖻 🗀 System	Sta	tus
🕀 🗀 Diagnostics	Bridge ID	800000e0b3556677
🗉 🧰 Port	Designated Root	800000e0b3556677
🗉 🧰 Switching	Reg Root ID	
🗉 🗀 Trunking	Root Port	0
🖻 🙆 STP/Ring	Root Path Cost	0
Global Configuration	Current Max Age (sec)	20
RSTP Port Setting	Current Hello Time (sec)	2
MSTP Properties	Current Forward Delay (sec)	15
MSTP Instance Setting	Topology Change Count	0
MSTP Port Setting	Time Since Last Topology Change	Thu Jan 22 20:27:09 2009
<u>Ring Setting</u>	Sett	ting
Chain Setting	Spanning Tree Protocol	Enable 💌
Advanced Setting	Bridge Priority (061440)	32768
🕀 🔂 VLAN	Hello Time (110 sec)	2
🗄 🧰 QoS	Max Age (640 sec)	20
E C SNMP	Forward Delay (430 sec)	15
	STP Version	RSTP
Others Protocols		Update Setting
Done		😌 Internet 🦷 🔹 🍕 100% 🔹 🖉

Figure 42: Max Age, Hello Timer & Forward Delay

RSTP Port Setting Page

To navigate to the STP/Ring RSTP Port Setting page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on **RSTP Port Setting.**

Spanning Tree Port Roles

In a stable RSTP topology, each port on a switch can function in any one of 4 different Spanning Tree port roles. These Spanning Tree port roles are (see <u>Figure 43</u>):

- Root Port
- Designated Port
- Alternate Port
- Backup Port

System Diamostics	Port	Port Status	Priority	Path Cost	Point to Point Lin	ık Edg	ge Port
Distances	fe1	Designated(Forwarding)	128	200000	Point to Point	Conf. Auto	/ Curr. Portfast
Switching	fe2	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
Trunking	fe3	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
STP/Ring	fe4	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
Global Configuration	fe5	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
RSTP Port Setting	fe6	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
MSTP Properties	fe7	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
MSTP Instance Setting	fe8	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
MSTP Port Setting	fe9	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
Ring Setting	fe10	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
Chain Setting	fel1	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
Chain Pass-Through Setting	fe12	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
Advanced Setting	fe13	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
VLAN	fe14	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
QoS	fe15	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
) SNMP	fe16	Disabled(Discarding)	128	200000	Shared	Conf. Auto	Curr. Edge off
802.1X	ge1	Disabled(Discarding)	128	20000	Shared	Conf. Auto	Curr. Edge off
) LLDP	ge2	Disabled(Discarding)	128	20000	Shared	Conf. Auto	Curr. Edge off
	RSTP P	ort Configuration	v 16)	Admin	Path Cost	Point to Point Link	Edge Port
	fe1	▼ 128		2000	00	Enable 💙	Auto 🗸
						(Update Setting

Figure 43: Spanning Tree Port Roles

Path Cost & Port Priority

By default, each port on a Spanning Tree switch will be assigned a **Path Cost** based on the port's transmission speed according to the IEEE standard below:

Link speed	Recommended value
Less than or equal 100Kb/s	200,000,000
1 Mb/s	20,000,000
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200
1 Tb/s	20
10 Tb/s	2

By default each port on a Spanning Tree switch will be assigned a Port Priority of 128, according to the IEEE standard. This Port Priority is part of the Port ID, which is a concatenation of 2 values: Port Priority (4 bits) + Interface ID (12 bits) (see ± 1)

Port ID	Priority	ID (Interface Number)	
	4 Bits	12 Bits	

Figure 44: Port ID

Port Priority is part of the Port ID, which is a concatenation of 2 values: Port Priority (4 bits) + Interface ID (12 bits).

The default values will work fine in most scenarios; however, there are times when you may need to adjust these values manually in order to influence the location of the Alternate Port, the Root Port or the Backup Port.

To adjust the Port Priority value or the Path Cost value on a port:

- 1. Choose the correct port from the drop down list under **Port** (see ± 1)
- 2. Enter the proper value under the Priority (Granularity 16)
 - a. The Port Priority range is between 0 and 240 in multiples of 16.
- 3. Enter the proper value under the Admin. Path Cost text entry box.
 - a. The Path Cost range is between 1 and 200,000,000.
- 4. Click on the **Update Setting** button
- 5. Save your configuration (see the Save Configuration Page).

 System Diamostics 	Port	Port Status	Priority	Path Cost	Point to Point Lin	k Edg	e Port
Diagnostics Port	fe1	Designated(Forwarding)	128	200000	Point to Point	Conf. Auto	Curr. Portfast
Switching	fe2	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
Trunking	fe3	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
STP/Ring	fe4	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
Global Configuration	fe5	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
RSTP Port Setting	fe6	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
MSTP Properties	fe7	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
MSTP Instance Setting	fe8	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
MSTP Port Setting	fe9	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
Ring Setting	fe10	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
Chain Setting	fe11	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
Chain Pass-Through Setting	fe12	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
Advanced Setting	fe13	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
VLAN	fe14	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
	fe15	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
SNMP	fe16	Disabled(Discarding)	128	200000	Shared	Conf. Auto /	Curr. Edge off
0 802.1X	ge1	Disabled(Discarding)	128	20000	Shared	Conf. Auto /	Curr. Edge off
	ge2	Disabled(Discarding)	128	20000	Shared	Conf. Auto /	Curr. Edge off
C Others Protocols	RSTP P	ort Configuration	v 16)	20000	Path Cost 1	Point to Point Link	Edge Port
	fol	128	, 10)	2000	00	Enable V	Auto
	liei	120	1	2000			Lindote Cotting
						L	opdate Setting

Figure 45: Port Priority and Path Cost

Point to Point Link

By default, RSTP will assume any full-duplex link as a **Point to Point Link**, but if the switch detects that the neighbor switch is not running the RSTP protocol, it will assume the port to be a **Shared Port**. You can force a port to be a **Shared Port**, if you know in advance that there will be more than one switch connecting to this link (through an unmanaged switch, for example), or if you know in advance that the other switch on this link will be running the older STP protocol.

To manually force a port to be a **Shared Port** or a **Point to Point Link**:

- 1. Choose the correct port from the drop down list under **Port**, and choose **Enable** or **Disable** under **Point to Point Link** (see <u>Figure 45</u>).
- 2. Click on the **Update Setting** button.
- 3. Save the configuration (see the Save Configuration Page)

Edge Port

By enabling the **Edge Port** feature on a port, the switch will stop reacting to any linkup event on this port, and will not send out any Topology Change notification to the neighbor bridges.

- 1. Choose the correct port from the drop down list under **Port**, and choose **Enable** or **Disable** under **Edge Port** (see <u>Figure 45</u>).
- 2. Click on the **Update Setting** button.
- 3. Save the configuration (see the Save Configuration Page)

RSTP Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

Enabling the Spanning Tree Protocol

To enable the Spanning Tree function on a switch, use the following CLI commands:

CLI Command Mode: General Configuration Mode CLI Command Syntax: no bridge shutdown 1 bridge 1 protocol rstp vlan-bridge

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)#no bridge shutdown 1
switch_a(config)#bridge 1 protocol rstp vlan-bridge
switch_a(config)#q
switch_a#

Bridge Priority, Max Age, Forward Delay, and Hello Time

To configure the Bridge Priority, Max Age, Forward Delay, and Hello Time of a Spanning Tree Bridge, please use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 priority <0-61440> bridge 1 max-age <6-40> bridge 1 forward-time <4-30> bridge 1 hello-time <1-10>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 priority 4096
switch_a(config)#bridge 1 max-age 20
switch_a(config)#bridge 1 forward-time 15
switch_a(config)#bridge 1 hello-time 2
```

```
switch_a(config)#g
switch_a#
```

Modifying the Port Priority and Path Cost

To modify the Port Priority and Path Cost on a switch, use the below CLI commands:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: bridge-group 1 path-cost <1-200000000> bridge-group 1 priority <0-240>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fe1
switch_a(config-if)#bridge-group 1 path-cost 200000
switch_a(config-if)#bridge-group 1 priority 128
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Manually Setting a Port to be a Shared or Point to Point Link

To manually force a port to be a **shared** link or **Point-to-point** link, use the below CLI commands:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: spanning-tree link-type point-to-point spanning-tree link-type shared

Usage Example 1: Setting port 1 to be point-to-point:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fe1
switch_a(config-if)#spanning-tree link-type point-to-point
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Usage Example 2: Setting port 1 to be shared:

```
switch_a>enable
switch_a#configure terminal
```

```
switch_a(config)#interface fel
switch_a(config-if)#spanning-tree link-type shared
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Enabling/Disabling a port to be an Edge Port

To manually enable or disable a port to be an **Edge Port**, use the following CLI commands:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: spanning-tree spanning-tree edgeport no spanning-tree spanning-tree edgeport

Usage Example 1: Enabling edge port on port 1:

switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fel
switch_a(config-if)#spanning-tree edgeport
switch_a(config-if)#q
switch_a(config)#q
switch_a#

```
Usage Example 2: Disabling edge port on port 1:
```

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fel
switch_a(config-if)#no spanning-tree edgeport
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

STP/RING PAGE - CONFIGURING MSTP

The MSTP protocol adds a new concept called a **Region** to the Spanning Tree algorithm. Unlike RSTP and STP, inside each MSTP Region, there can be more than one instance of Spanning Tree Protocol running simultaneously. The MSTP protocol can then map multiple VLANs to each instance of Spanning Tree protocol to provide load balancing among the switches. Between Regions, the MSTP runs a single instance of Spanning Tree similar to, and is backward compatible with, the RSTP protocol.

Global Configuration Page

Enabling the MSTP Protocol

Navigate to the STP/Ring Global Configuration page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on **Global Configuration**.
- 3. Verify that the Spanning Tree Protocol is enabled (see <u>Figure 46</u>), if not, choose **Enabled** from the **Spanning Tree Protocol** drop down list.
- 4. Choose **MSTP** in the **STP Version** drop down list.
- 5. Click on the **Update Setting** button.
- 6. Save the configuration (see the Save Configuration Page).

🟠 Management Switch	Sta	tus		
Diagnostics Bridge ID		800000e0b3556677		
E Port	Designated Root	800000e0b3556677 800000e0b3556677 0		
🕀 🧰 Switching	Reg Root ID			
🖽 🧰 Trunking	Root Port			
🛱 🙆 STP/Ring	Root Path Cost	0		
Global Configuration	Current Max Age (sec)	20		
RSTP Port Setting	Current Hello Time (sec)	2		
<u>MSTP Properties</u> <u>MSTP Instance Setting</u> <u>MSTP Port Setting</u>	Current Forward Delay (sec)	15		
	Topology Change Count	0		
	Time Since Last Topology Change	Fri Jan 23 04:29:44 2009		
<u>Ring Setting</u>	Setting			
Chain Setting	Spanning Tree Protocol	Enable 💌		
Advanced Setting	Bridge Priority (061440)	32768		
🕀 🔂 VLAN	Hello Time (110 sec)	2		
🖽 🔂 QoS	Max Age (640 sec)	20		
	Forward Delay (430 sec)	15		
	STP Version	MSTP		
Others Protocols		Update Setting		
	<u></u>			
Done		🜍 Internet 🦷 🔹 🍕 100% 🔹		

Figure 46: Enabling MSTP

The CIST Root Bridge & Backup CIST Root Bridge

In order to configure a switch to be the CIST Root Bridge of a Spanning Tree network, you just have to make sure that the Bridge Priority (which is the most significant 4 bits of the Bridge ID) of the switch is the lowest among any of the switches on the network. Similarly for the Backup CIST Root Bridge, it must have the next lowest Bridge Priority of all the switches. This Bridge ID is a concatenation of 3 values: a 4 bit Bridge Priority (most significant), a 12 bit System ID (less significant), and the 48 bit MAC address of the local switch (least significant) (see <u>m</u>).

←		Bridge ID ———	\longrightarrow
Bridge Priority	System ID Ext.	MAC Address	
4 bits	12 bits	6 bytes	

Figure 47: Bridge ID

Setting Bridge Priority

To set the Bridge Priority:

- 1. Enter the **Bridge Priority ID** in the text box to the right of **Bridge Priority** (0..61440)
- 2. Click on the **Update Setting** button.

Note: The valid values for this parameter are from 0 to 61440, in increments of 4096; you will see this value reflected in the first hexadecimal digit of the **Bridge ID** field after you click the **Update Setting** button (See Figure 48). Set this value to be less than any other switch on the network, in order to make this switch the Root Switch. To set a **Backup Root Bridge** set the **Bridge ID** to be between the **Root Bridge** and the rest of the network switches.

🟠 Management Switch				
🕀 🧰 System	Sta	tus		
Diagnostics Bridge ID		800000e0b3556677		
Port Designated Root		800000e0b3556677		
🗄 🗀 Switching	Reg Root ID	800000e0b3556677		
🖻 🛅 Trunking	Root Port	0		
Root Path Cost		0		
Global Configuration	Current Max Age (sec)	20		
RSTP Port Setting	Current Hello Time (sec)	2		
MSTP Properties	Current Forward Delay (sec)	15		
MSTP Instance Setting	Topology Change Count	0		
MSTP Port Setting	Time Since Last Topology Change	Fri Jan 23 04:29:44 2009		
Ring Setting	Setting			
Chain Setting <u>Chain Pass-Through Setting</u> <u>Advanced Setting</u> Diana VLAN	Spanning Tree Protocol	Enable 💌		
	Bridge Priority (061440)	32768		
	Hello Time (110 sec)	2		
🕂 🧰 QoS	Max Age (640 sec)	20		
	Forward Delay (430 sec)	15		
STP Version		MSTP		
🗄 🛅 Others Protocols		Update Setting		
	L			
Done		🜍 Internet 🦓 🔹 🍕 100% 🔹		

Figure 48: Bridge ID Display

Configuring the CST Network Diameter

When using MSTP, the **Max Age** parameter is used for the CST (Common Spanning Tree) topology simply as a hop count limit on how far the Spanning Tree protocol packet can propagate throughout the CST topology, therefore, the Max Age must be configured with a value that is greater than the network diameter of the CST topology. The Max Age parameter will need to be configured correctly on both the CIST Root Bridge as well as on the Backup CIST Root Bridge (in the event when the CIST Root Bridge fails).

Setting the MAX Age, Forward Delay and Hello Timer

Navigate to the STP/Ring Global Configuration page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on Global Configuration.

Relationship between Max Age, Forward Delay and Hello Time

The following rules must be followed when setting the **Max Age**, **Forward Delay** and **Hello Timer**:

- Max Age >= 2 × (Hello Time + 1.0 second)
- 2 × (Forward Delay 1.0 second) >= Max Age

To change the Max Age, Forward Delay and Hello Timer (see Figure 49):

- 1. Enter the **Max Age** in the text box to the right of Max Age (6..40 sec) label.
- 2. Enter the **Hello Time** in the text box to the right of the Hello Time (1..10 sec) label.
- 3. Enter the **Forward Delay** in the text box to the right of the Forward Delay (4..30 sec) label.
- 4. Click on the **Update Setting** button.
- 5. Save the configuration (see the <u>Save Configuration Page</u>)
| Management Switch | Sta | tuc | | | | |
|-----------------------|---------------------------------|--------------------------|--|--|--|--|
| 🖽 🗀 System | Bridge ID | 800000e0b3556677 | | | | |
| Diagnostics Port | Designated Root | 800000e0b3556677 | | | | |
| E C Switching | Reg Root ID | 800000e0b3556677 | | | | |
| E 🔂 Trunking | Root Port | 0 | | | | |
| STP/Ring | Root Path Cost | 0 | | | | |
| Global Configuration | Current Max Age (sec) | 20 | | | | |
| RSTP Port Setting | Current Hello Time (sec) | 2 | | | | |
| MSTP Properties | Current Forward Delay (sec) | 15 | | | | |
| MSTP Instance Setting | Topology Change Count | 0 | | | | |
| MSTP Port Setting | Time Since Last Topology Change | Fri Jan 23 04:29:44 2009 | | | | |
| Ring Setting | Setting | | | | | |
| Chain Setting | Spanning Tree Protocol | Enable 💌 | | | | |
| Advanced Setting | Bridge Priority (061440) | 32768 | | | | |
| 🕀 🦳 VLAN | Hello Time (110 sec) | 2 | | | | |
| 🖽 🧰 QoS | Max Age (640 sec) | 20 | | | | |
| E C SNMP | Forward Delay (430 sec) | 15 | | | | |
| E C LLDP | STP Version | MSTP V | | | | |
| E C Others Protocols | | Update Setting | | | | |
| | | | | | | |
| | | | | | | |
| Done | | 🌍 Internet 🦷 🔹 🍕 100% 🔹 | | | | |

Figure 49: Max Age, Hello Timer & Forward Delay

MSTP Properties Page

Configuring an MSTP Region

In order to form a MSTP Region, the switches that will be connected together to form the MSTP Region must have the same values for the configuration parameters listed below. Two of the parameters can be configured directly, the third parameter (Configuration Digest) will be automatically calculated by the switch based on the VLAN to MSTI (Multiple Spanning Tree Instance) mapping. The VLAN to MSTI instance mapping must be the same for all the switches within the same MSTP Region (see <u>MSTP Instance Setting Page</u>

Setting an MSTP Instance).

- Region name
- Revision level
- Configuration Digest

To navigate to the STP/Ring MSTP Properties page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on **MSTP Properties.**

To configure both the MSTP Regional Configuration Name and the Revision Level for each of the switches located in the same MSTP Region (see 41):

- 1. Enter the **Region Name** of the Region that the switch will belong to in the **Region Name** text entry box,
- 2. Enter the **Revision Level** value for the corresponding Region in the **Revision Level** text entry box,
- 3. Click on the **Update Setting** button.
- 4. Save the configuration (see the <u>Save Configuration Page</u>)

	MSTP Properties
Region Name	Region_1
Revision Level	0
Max Hops	20
Digest	0x0A93D2F3DF9DA7495DB99A256750491A
CIST Root ID	100000e0b32103de
CIST Reg Root ID	100000e0b32103de
CIST Bridge ID	100000e0b32103de
	Update Setting

Figure 50: MSTP Region and Revision Level

Configuring the IST Network Diameter

To navigate to the **STP/Ring MSTP Properties** page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on **MSTP Properties.**

In the MSTP protocol, the **Max Hops** parameter is used for the **IST** (Internal Spanning Tree) and the **MSTI** (Multiple Spanning Tree Instance) topology as a hop count limit on how far the Spanning Tree protocol packet can propagate inside of a MSTP Region, therefore, it must be configured with a value that is greater than the network diameter of the **IST/MSTI** topology. The **Max Hops** parameters should be configured correctly on the CIST Root and the Backup CIST Root switch and on all of the Boundary switches of a MSTP Region (if there are multiple Regions within your MSTP network).

Follow the steps below to configure the **Max Hops** parameter:

- 1. Enter the desired hop count in the text entry box next to Max Hops
- 2. Click on the **Update Setting** button (see $\underline{\#}$).
- 3. Save the configuration (see the Save Configuration Page)

	MSTP Properties	
Region Name	Region_1	
Revision Level	0	
Max Hops	30	
Digest	0x0A93D2F3DF9DA	7495DB99A256750491A
CIST Root ID	100000e0b32103de	
CIST Reg Root ID	100000e0b32103de	
CIST Bridge ID	100000e0b32103de	

Figure 51: MSTP Properties – Max Hops

MSTP Instance Setting Page

Setting an MSTP Instance

Navigate to the STP/Ring MSTP Instance Setting page:

- 1. Click on the + next to STP/Ring.
- 2. Click on MSTP Instance Setting.

To create the Spanning Tree instances to be run inside a MSTP Region and its VLAN mappings, follow the below steps.

- 1. Click on the VLAN Instance Configuration button (see Figure 52),
- 2. Choose the **VLAN** that you want to map to a MSTI instance from the **VLAN ID** drop down box (see Figure 53).
- 3. Enter the **Instance ID** that you want the VLAN to map to In the text entry box next to **Instance ID (1..15)**.
- 4. Click on the **Update Settings** button.
- 5. Save the configuration (see the Save Configuration Page)

Note: You can enter a new instance number here, which is how a new MSTI instance is created. You can use an existing MSTI instance if it has already been created on another switch.

Management Switch	VLAN Instance Configuration]	
Diagnostics	Inclu	ded VLANs	
Switching	Instance ID		
🗄 🗀 Trunking	Included VLAN	*	
🛱 🙆 STP/Ring	Insta	ance Setting	
Global Configuration	Bridge Priority (061440)		
RSTP Port Setting	Root ID		
MSTP Properties	Root Port		
MSTP Instance Setting	Root Path Cost		
Ring Setting	Bridge ID		
Chain Setting			Update Setting
Chain Pass-Through Setting			
Advanced Setting			
🖻 🧰 VLAN			
🕀 🔂 QoS			
🕀 🔂 SNMP			
🕀 🛅 802.1X			
🕀 🛅 LLDP			
⊡ ☐ Others Protocols			
Done		🗔 🌍 Internet	🖌 🔹 🔍 100% 🔹 💡

Figure 52: VLAN Instance Configuration

VI	AN Instance Configuratio	n
VLAN ID	101 🔻	
Instance ID (115)	1	
	ľ.	Update Setting

Figure 53: VLAN Instance ID

Modifying MSTP parameters for load balancing

To navigate to the **STP/Ring MSTP Instance Setting** page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on MSTP Instance Setting.

To load balance switches within a MSTP Region, set different switches within the MSTP Region to be the Root Bridge for different MSTI instances. A Root Bridge in a particular MSTI instance is called a MSTI Regional Root Bridge.

To designate a specific switch in a MSTP Region to be the Root Bridge in a specific MSTI instance, the bridge priority must be set to be the lowest number of all the switches in a particular MSTI instance.

To set the bridge priority on the switch for a specific MSTI Instance (see Figure 54):

- 1. Choose the particular instance in the **Instance ID** drop down list for which the switch will be a MSTI Regional Root Bridge;
- 2. Enter the desired value in the **Bridge Priority** text box
- 3. Click on the **Update Setting** button. The valid values for this parameter are from 0 to 61440, in increments of 4096.
- 4. Save the configuration (see the <u>Save Configuration Page</u>)

Ir	ncluded VLANs
Instance ID	1 -
Included VLAN	•
I	nstance Setting
Bridge Priority (061440)	4096
Root ID	100100e0b32103e4
Root Port	0
Root Path Cost	0
Bridge ID	100100e0b32103e4

Figure 54: Setting the MSTI Regional Root Bridge

MSTP Port Setting page

Adjusting the blocking port in a MSTP network

To navigate to the **STP/Ring MSTP Port Setting** page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on **MSTP Port Setting.**

You can adjust the location of the blocking port in a MSTP network by modifying the **Port Priority** and the **Path Cost** of the ports on the switch. Modifying the **Port Priority** adjusts the blocking port between two switches. Modify the **Port Cost** adjusts the location of the blocking port in a MSTP loop.

To modify the Port Priority and the Path Cost of the ports on a MSTP switch for the MSTI instance only, please follow the below steps:

- 1. Choose the correct MSTI Spanning Tree instance from the drop down list under **Instance ID** (see <u>Figure 55</u>).
- 2. Choose the correct port number from the drop down list under **Port**, and enter the proper value under the **Priority** and the **Admin. Path Cost** text box,
- 3. Click on the Update Setting button (see Figure 55).
- 4. Save the configuration (see the <u>Save Configuration Page</u>)

Port	Port State	Role	Priority	Path Cost	Designated Bridge ID	Designated Port ID	Designated Root ID	Designated Path Cost
1	Forwarding	Designated	128	200000	100100e0b32143b4	8001	100100e0b32143b4	0
2	Discarding	Disabled	112	100000	000000000000000000000000000000000000000	0	000000000000000000000000000000000000000	0
3	Discarding	Disabled	128	200000	000000000000000000000000000000000000000	0	000000000000000000000000000000000000000	0
4	Discarding	Disabled	128	200000	000000000000000000000000000000000000000	0	000000000000000000000000000000000000000	0
5	Discarding	Disabled	128	200000	000000000000000000000000000000000000000	0	000000000000000000000000000000000000000	0
6	Discarding	Disabled	128	200000	000000000000000000000000000000000000000	0	000000000000000000000000000000000000000	0
7	Discarding	Disabled	128	200000	000000000000000000000000000000000000000	0	000000000000000000000000000000000000000	0
8	Discarding	Disabled	128	200000	000000000000000000000000000000000000000	0	000000000000000000000000000000000000000	0
<u>AST</u>	P Port Confi	guration				;		
Port	:	Priority	(Granular	ity 16)		I	Admin. Path Cost	
2 -		112			0	10	00000	

Figure 55: Port Cost & Priority

MSTI Instance Port Membership

To navigate to the STP/Ring MSTP Port Settings page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on **MSTP Port Setting.**

If changes have been made to the port membership of a VLAN, you must also reconfigure the MSTI port membership for the MSTI instance that the VLAN maps to.

To reconfigure the MSTI instance port membership:

- 1. Click on the **Port Instance Configuration** button (see Figure 56)
- Choose the correct MSTI instance from the drop down list next to Instance ID (see Figure 57).
- 3. Check the box next to all the ports that should be part of this instance
- 4. Click on the **Update Setting** button.
- 5. Save the configuration (see the <u>Save Configuration Page</u>)

rt	mstand				D d	D 1		D 1	D .
ritching	Port	Port State	Role	Priority	Path Cost	Designated Bridge ID	Designated Port ID	Designated Root ID	Designated Path Cost
P.Ring	fe1								
al Configuration	fe2			1			1		
P Port Setting	fe3								
IP Properties	fe4								
TP Instance Setting	fe5								
IP Port Setting	fe6								
Setting	fe7								
in Setting	fe8								
n Pass-Through Setting	fe9								
anced Setting	fe10								
AN	fe11								
n m	fe12								
	fe13			_					
DP	fe14						_		
hers Protocols	fe15								
	fe16								
	ge1			1					
	ge2								
	MSTP	Port Configura	tion						
	Port		Priority	y(Granularity	16)		Ad	lmin. Path Cost	
	fe1	~							
									adata Catting

Figure 56: Port Instance Configuration

Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8

Figure 57: Port Instance - Adding Ports

MSTP Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

Enabling Spanning Tree for MSTP

To enable the Spanning Tree function on a switch use the below CLI commands.:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: no bridge shutdown 1 bridge 1 protocol mstp

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)#no bridge shutdown 1
switch_a(config)#bridge 1 protocol mstp
switch_a(config)#q
switch_a#

Bridge Priority, Max Age, Forward Delay, and Hello Time

To configure the CIST Bridge Priority, Max Age, Forward Delay, and Hello Time of a Spanning Tree Bridge, use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 priority <0-61440> bridge 1 max-age <6-40> bridge 1 forward-time <4-30> bridge 1 hello-time <1-10>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 priority 4096
switch_a(config)#bridge 1 max-age 20
switch_a(config)#bridge 1 forward-time 15
switch_a(config)#bridge 1 hello-time 2
```

```
switch_a(config)#q
switch_a#
```

IST MAX Hops

To configure the IST Max Hops parameter on a switch, use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 max-hops <1-40>

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 max-hops 20
switch_a(config)#q
switch_a#

MSTP Regional Configuration Name and the Revision Level

To configure both the MSTP Regional Configuration Name and the Revision Level on a switch, use the following CLI commands:

CLI Command Mode: MSTP Configuration Mode

CLI Command Syntax: bridge 1 region <region_name> bridge 1 revision <revision_number>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 region R1
switch_a(config-mst)#bridge 1 revision 0
switch_a(config-mst)#q
switch_a(config)#q
switch_a#
```

Creating an MSTI Instance

To create a MSTI instance and map it to a VLAN, use the following CLI commands:

- CLI Command Mode: MSTP Configuration Mode
- CLI Command Syntax: bridge 1 instance <1-15> vlan <vlan_ID>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 instance 1 vlan 10
switch_a(config-mst)#q
switch_a(config)#q
switch_a#
```

Setting MSTI Priority

To set the MSTI priority of a switch in a MSTP Region, use the following CLI commands:

- CLI Command Mode: General Configuration Mode
- CLI Command Syntax: bridge 1 instance <1-15> priority <0-61440>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 instance 1 priority 0
switch_a(config)#q
switch_a#
```

Modifying CIST Port Priority and Port Path Cost

To modify the CIST Port Priority and CIST Port Path Cost on a switch, use the below CLI commands:

CLI Command Mode: Interface Configuration Mode (port)

CLI Command Syntax: bridge-group 1 path-cost <1-200000000>; bridge-group 1 priority <0-240> Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fel
switch_a(config-if)#bridge-group 1 path-cost 200000
switch_a(config-if)#bridge-group 1 priority 128
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

To modify the MSTI Port Priority and MSTI Port Path Cost for an Instance on a switch, please use the below CLI commands:

CLI Command Mode: Interface Configuration Mode

```
CLI Command Syntax:
bridge-group 1 instance <1-15> path-cost <1-200000000>
bridge-group 1 instance <1-15> priority <0-240>
```

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fel
switch_a(config-if)# bridge-group 1 instance 1 path-cost 20000
switch_a(config-if)# bridge-group 1 instance 1 priority 128
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Adding a Port to an MSTI Instance

To add a port to a MSTI instance (this port must be a member port of the VLAN that is mapped to the MSTI instance), please use the below CLI commands:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: bridge-group 1 instance <1-15>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fe1
switch_a(config-if)#bridge-group 1 instance 1
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

STP/RING PAGE - ALPHA RING

Alpha Ring Setting Page

To navigate to the STP/Ring α -Ring Settings page:

- 1. Click on the + next to STP/Ring.
- 2. Click on **α-Ring Setting.**

EtherWAN α-Ring Technology

The α -Ring protocol was designed and developed by EtherWAN to overcome traditional STP and RSTP's inability to provide fast network recovery and minimize packet loss caused by link failure. Among the advantages of α -Ring are:

- High-speed Recovery Less than 15 milliseconds
- Flexibility for Network Deployment Coexistence with STP, RSTP and MSTP
- Ring Coupling Smaller rings coupled together to increase network efficiency

Implementing a Simple α-Ring

- 1. Change the **Ring State** to **Enabled**
- 2. Click on the **Update Setting** button.

Next, the ports that will be used to connect this switch to the α -Ring need to be assigned to provide the connection redundancy (see Figure 58).

1. Change **Ring Port 1** to the port you will be using for the first redundant connection

- 2. Change **Ring Port 2** to the port you will be using for the second redundant connection.
- 3. Click on the **Update Setting** button.
- 4. Save the configuration (see the <u>Save Configuration Page</u>)

 Management Switch 	Ring State	[Disable 💌	Update :	Setting
P 🔂 Port				22.45 10.54 10.54	
🕀 🧰 Switching	Set Ring Port	Ring I	Port 1 fe1 🞽	Ring Port 2	fe2 🚩
🕀 🧰 Trunking	Ring Port State	DO	OWN	DOWN	
🛱 🦾 STP/Ring				Updat	e Setting
Global Configuration	<u>4.</u>				
RSTP Port Setting				Upda	ate Setting
MSTP Properties	Ring Coupling St	tate	Disable 🎽		
MSTP Instance Setting				1.	26
<u>MSTP Port Setting</u> <u>Ring Setting</u>	Set Ring Coupling	Port	Ring Coupling Po	rt 1 Ring Co	upling Port 2
Chain Setting Chain Pass Through Setting	Ring Coupling Port	State	DOWN	DC	WN
Advanced Setting				Upd	ate Setting
🕀 🔂 VLAN					
🕀 🛅 QoS					
🖻 🛅 SNMP					
🖻 🧰 802.1X					
🖻 🦳 LLDP					
🗄 🚞 Others Protocols					
Done			👩 🌍 Internet		🗛 🔹 🔍 100% 🔹 👖

Figure 58: α-Ring Settings

Connecting two α -Ring Networks together

To navigate to the STP/Ring α -Ring Settings page:

- 1. Click on the + next to STP/Ring.
- 2. Click on **α-Ring Setting.**

As additional switches are added to a network, it may become necessary to connect multiple α -Ring networks together. This is called **Ring-coupling** and uses two additional Ethernet ports on the switch. To setup Ring-coupling (see Figure 59):

- 1. Change the **Ring-coupling** state to **Enable**.
- 2. Click on the **Update Setting** button next to the Ring-coupling state.
- 3. Choose the desired port from the dropdown list under Ring Coupling Port 1
- 4. Choose the desired port from the dropdown list under Ring Coupling Port 2
- 5. Click on the **Update Setting** button.
- 6. Save the configuration (see the <u>Save Configuration Page</u>)

🚷 Management Switch	1					
🕀 🔂 System	Ring State		Disable 🗸	Up	odate Setting	
🕂 🗀 Diagnostics	Tung State	L				
🗉 🛅 Port						
🗉 🛅 Switching	Set Ring Port	Ring	Port 1 fe1 💌	Ring	Port 2 fe2 💌	
🖻 🛅 Trunking	Ring Port State	D	OWN	D	OWN	
🛱 🙆 STP/Ring					Update Setting	
Global Configuration	<u>+</u>					
RSTP Port Setting	1				Update Setting	
MSTP Properties	Ring Coupling S	tate	Disable 🎽	-		
MSTP Instance Setting				1		
MSTP Port Setting		1000	Ring Coupling Po	rt 1 Ri	ng Coupling Port 2	
Ring Setting	Set Ring Coupling	Port	fe3 🗸		fe4 🖌	
Chain Setting	Ring Coupling Port	t State	DOWN		DOWN	
Advanced Setting					Update Setting	
E C VLAN	1					
🕀 🔂 QoS						
🕀 🛅 SNMP						
🗄 🛅 802.1X						
🖻 🛅 LLDP						
🗄 🛅 Others Protocols						_
Done			👩 🌏 Internet		🖌 🔹 🔍 100%	•

Figure 59: Ring Coupling

Chain Setting Page

To navigate to the STP/Ring Chain Settings page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on **Chain Setting.**

Chain Protocol

To enable or disable Chain Protocol settings for a port on the EX24000 Switch:

- 1. Click on the check box under Chain Protocol to select Enable.
- 2. Click on the **Submit** button.

VLAN (Global)

To set the VLAN for Chain Protocol on the EX24000 Switch. The VLAN ID value can be from 1 to 4094. Default VLAN ID is 1.

- 1. Click in the **VLAN** text box for Chain Protocol.
- 2. Type in the VLAN ID for Chain Protocol.
- 3. Click on the **Submit** button.

Priority (Global)

To set the Priority value for Chain Protocol on the EX24000 Switch. The Priority value can be from 0 to 255. Default Priority is 128.

- 1. Click in the **Priority** text box for Chain Protocol.
- 2. Type in the Priority value for Chain Protocol.
- 3. Click on the **Submit** button.

Timeout Count (Global)

To set the Timeout Count for Chain Protocol on the EX24000 Switch. The Timeout Count value can be from 3 to 255. Default Timeout Count is 5.

- 1. Click in the **Timeout Count** text box for Chain Protocol.
- 2. Type in the Timeout Count value for Chain Protocol.
- 3. Click on the **Submit** button.

Enabling Storm Control (Broadcast and Multicast) (Global)

To globally enable the **Storm Control** feature of the EX24000 Switch:

- 1. Click on the **Storm Control** drop-down box.
- 2. Select **Enable** from the drop down list.
- 3. Click on the **Submit** button.

E 🔂 System		Chain	Protocol	
Diagnostics	Port	Enable	Role	State
Port	fe1		None	None
C Switching	fe2		None	None
🗋 🛅 Trunking	fe3		None None	None
STP/Ring	fe4			None
Global Configuration	fe5		None	None
RSTP Port Setting	fe6		None	None
- <u>MSTP Properties</u> - <u>MSTP Instance Setting</u> - <u>MSTP Port Setting</u> - <u>Ring Setting</u> - <u>Chain Setting</u> - <u>Chain Setting</u> - <u>Advanced Setting</u> - <u>Advanced Setting</u> ULAN - <u>Chain QoS</u>	fe7		None	None
	fe8		None None None None None None None None None None None	None
	fe9			None
	fe10			None None
	fe11			
	fe12			None
	fe13 fe14			None None None
9 🛅 802.1X	fe16			
C LLDP	ge1		None	None
Others Protocols	ge2		None	None
		<i></i>		Submit
		Globa	d Setting	
	VLAN (1-4094, def	ault:1)		1
	Priority (0-255, defa	ult:128)		128
	Timeout Count (3-25	5, default:5)		5
	Storm Control (broad	dcast and multicast)		Enable 💌
				Submit

Figure 60: Chain Settings

Chain Pass-Through Setting Page

To navigate to the STP/Ring Chain Pass-Through Settings page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on Chain Pass-Through Setting.

Implementing a Chain Pass-Through

- 1. Change **Chain Pass-Through Port 1** to the port you will be using for the first Chain Pass-Through connection
- 2. Change **Chain Pass-Through Port 2** to the port you will be using for the second Chain Pass-Through connection.
- 3. Click on the **Update Setting** button.
- 4. Save the configuration (see the <u>Save Configuration Page</u>)

🟠 Management Switch				1	
🗄 🔂 System	Set Chain Pass-	Chain Pas	s-Through Port 1	Chain Pas	s-Through Port 2
🕀 🧰 Diagnostics	I hrough Port		*		×
🗄 🛅 Port	Chain Pass-				
E Constraint	Through Fort State			Disable	Lindote Catting
🗄 🧰 Trunking				Disable	Opdate Setting
두 🎦 STP/Ring					
Global Configuration					
RSTP Port Setting					
MSTP Properties					
MISTP Instance Setting					
Ding Satting					
Chain Satting					
Chain Pass-Through Setting					
Advanced Setting					
E C VLAN					
🕀 🛅 QoS					
🖻 🧰 SNMP					
🗄 🧰 802.1X					
🗄 🧰 LLDP					
🗄 🛅 Others Protocols					
Done			ı 🚱 🛐	nternet	🖌 🔹 🔍 100% 🔹 🚲

Figure 61: Chain Pass-Through Settings

Advanced Setting

To navigate to the **STP/Ring Advanced Setting** page:

- 1. Click on the + next to **STP/Ring**.
- 2. Click on Advanced Setting.

Advanced Bridge Configuration

The Advanced Setting Page contain several settings to determine how the switch will handle BPDU packets.

- **Bridge bpdu-guard configuration** When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have **bpdu-guard** set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed.
- Error disable timeout configuration Enabling this allows a Disabled port to reenable itself automatically after the specified Interval.
- **Interval** Default is 300 seconds. This is the length of time a port will remain disabled after shutting down due to the **bpdu-guard**.

🕜 Management Switch		Advnced Bridge Config	uration			
 Diagnostics 	Bridge I	Disable 🗸				
E 🔂 Port	Error di	Disable 🗸				
🗄 🧰 Switching	Interval	Interval (10, 1000000 sec) Default: 300				
🗄 🧰 Trunking		A dranged Par Dort Configuration				
C STP/Ring	Port	BPDU-mard configuration				
Global Configuration	fel	Disable Enable / Curr OFE				
MSTP Properties	fal	Disable O Enable / Curr OFF	Default V			
MSTP Instance Setting	1C2	Disable O Enable / Curr. OFF	Default V			
MSTP Port Setting	Ies C.A	Disable C Enable Curr. OFF	Default			
Ring Setting	fe4	Disable O Enable / Curr. OFF				
<u>Chain Setting</u>	fe5	◎ Disable ○ Enable / Curr. OFF	Default 🚩			
Chain Pass-Through Setting	fe6	⊙ Disable ○ Enable / Curr. OFF	Default 🞽			
Advanced Setting	fe7	⊙ Disable ○ Enable / Curr. OFF	Default 🚩			
	fe8	⊙ Disable ○ Enable / Curr. OFF	Default 💌			
I 🔂 SNMP	fe9	Oisable ○ Enable / Curr. OFF	Default 💌			
602.1X	fe10	⊙ Disable ○ Enable / Curr. OFF	Default 💌			
	fe11	💿 Disable 🔘 Enable / Curr. OFF	Default 😽			
Chers Protocols	fe12	💿 Disable 🔘 Enable / Curr. OFF	Default 💌			
	fe13	⊙ Disable ○ Enable / Curr. OFF	Default 💌			
	fe14	⊙ Disable ○ Enable / Curr. OFF	Default 🖌			
	fe15	⊙ Disable ○ Enable / Curr. OFF	Default 🗸			
	fe16	⊙ Disable ○ Enable / Curr. OFF	Default 🗸			
	ge1	⊙ Disable ○ Enable / Curr. OFF	Default 💌			
	ge2	⊙ Disable ○ Enable / Curr. OFF	Default 🗸			
	Note: Per port BPDU-guard configuration takes precedence over bridge configuration					
			Submit			
one		👩 🔐 Internet	<i>4</i> ₂ → € 100% →			

Figure 62: Advanced Bridge Configuration

Advanced Per Port Configuration

- **Portfast Configuration / status –** Enabling this for Edge ports (ports connecting to an end device as opposed to another switch) protect the
- **BPDU-Guard Configuration –** When set to **Default** the port will default to the Advanced Bridge Configuration settings. **Enable** or **Disable** to override the Bridge BPDU-Guard

🗄 🧀 System	Advnced Bridge Configuration				
🗄 🛅 Diagnostics	Bridge I	Disable 💌			
🖸 🛅 Port	Error di	Error disable timeout configuration			
🗄 🛅 Switching	Interval	Interval (101000000 sec), Default: 300			
Trunking	Advanced Per Port Configuration				
Global Configuration	Port	BPDU-guard configuration			
RSTP Port Setting	fe1	⊙ Disable ○ Enable / Curr. OFF	Default 💌		
MSTP Properties	fe2	⊙ Disable ○ Enable / Curr. OFF	Default 👻		
MSTP Instance Setting	fe3	⊙ Disable ○ Enable / Curr. OFF	Default 👻		
MSTP Port Setting	fe4	⊙ Disable ○ Enable / Curr. OFF	Default 💌		
Chain Setting	fe5	⊙ Disable ○ Enable / Curr. OFF	Default 💌		
Chain Pass-Through Setting	fe6	⊙ Disable ○ Enable / Curr. OFF	Default 🖌		
Advanced Setting	fe7	⊙ Disable ○ Enable / Curr. OFF	Default 😽		
Han VLAN	fe8	⊙ Disable ○ Enable / Curr. OFF	Default 💙		
	fe9	⊙ Disable ○ Enable / Curr. OFF	Default 👻		
S02.1X	fe10	Disable Enable / Curr. OFF	Default 👻		
	fe11	Disable Enable / Curr. OFF	Default 👻		
Chers Protocols	fe12	Disable Enable / Curr. OFF	Default 👻		
	fe13	Disable Enable / Curr. OFF	Default 👻		
	fe14	Disable Enable / Curr. OFF	Default 💙		
	fe15	⊙ Disable ○ Enable / Curr. OFF	Default 🗸		
	fe16	⊙ Disable ○ Enable / Curr. OFF	Default 🗸		
	ge1	⊙ Disable ○ Enable / Curr. OFF	Default 🗸		
	ge2	Disable () Enable / Curr OFF	Default V		
	Note: P	er port BPDU-guard configuration takes p ation.	precedence over bridge		
			Submit		

Figure 63: Advanced Per Port Configuration

Configuring Spanning Tree Advanced Settings using CLI commands

For more information on CLI command usage see <u>CLI Command Usage</u>.

Enabling BPDU Guard Globally

To enable the BPDU Guard feature **globally** on the switch use the below CLI commands (for more information on CLI command usage and typographic conventions please click here):

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 spanning-tree portfast bpdu-guard

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 spanning-tree portfast bpdu-guard
switch_a(config)#q
switch_a#
```

Enabling BPDU Guard on a Port

To enable the BPDU Guard feature on a **individual** switch port use the CLI commands below:

CLI Command Mode: Switch-Port Interface Configuration Mode

CLI Command Syntax: spanning-tree portfast; spanning-tree portfast bpdu-guard enable

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fel
switch_a(config-if)#spanning-tree portfast
switch_a(config-if)#spanning-tree portfast bpdu-guard enable
switch_a(config-if)#q
```

```
switch_a(config)#g
switch_a#
```

Enabling BPDU Guard Error Disable-timeout

To enable the BPDU Guard Error Disable-timeout feature on a switch port, and set the timeout interval, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: bridge 1 spanning-tree errdisable-timeout enable bridge 1 spanning-tree errdisable-timeout interval 300

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 spanning-tree errdisable-timeout enable
switch_a(config)#bridge 1 spanning-tree errdisable-timeout interval
300
switch_a(config)#q
switch_a#
```

VLAN

Port Based VLAN vs. Tagged Based VLAN

The EX24000 Switch can be configured to operate in one of two VLAN modes: Port based VLAN mode or Tagged based VLAN mode. In Port based VLAN mode, packets from different VLANs can only be segregated from one another while within a single switch, but not when the packets travel to other switches in the network. The VLAN association rule for all incoming packets in Port based VLAN mode is determined only by the VLAN ID that is associated with the port when a packet enters the switch.

In Tagged based VLAN mode, traffic from different VLANs can be segregated from one another even after it travels to another switch. This is done by "tagging" (inserting information inside a packet) a packet with the VLAN ID that the packet belongs to when the packet exits the switch. The VLAN association rule for incoming packets in Tag based VLAN mode can either be based on the VLAN ID that is assigned to the port (PVID) when a packet enters the switch (in the event when the packet does not contain a VLAN ID), or it can be determined from the packet itself (when the packet does contains a VLAN ID).

Configuring VLANs in Port Based VLAN Mode

Enabling Port Based VLAN

To navigate to the VLAN Mode Setting page:

- 1. Click on the + next to VLAN.
- 2. Click on VLAN Mode Setting.

To enable Port Based VLAN on the switch:

- 1. Select Port-based VLAN from the dropdown box (see \underline{mr})
- 2. Click on the **Submit** button.
- 3. Save the configuration (see the <u>Save Configuration Page</u>)





Port Based VLAN Configuration Examples

To navigate to the **Port Based VLAN** page:

- 1. Click on the + next to **VLAN**.
- 2. Click on Port Based VLAN.

In Port Based VLAN mode, you can configure a port to be a member for a single VLAN or multiple VLANs. By default, all the ports on the switch are all members of a single VLAN (VLAN 1).

 $\underline{\forall l}$ is an example on how to configure two groups of ports, with each port being a member of a single VLAN. Since no ports are members of more than one VLAN, the ports in different groups cannot communicate with each other.

🏠 Management Switch ▣ 🫅 System	VLAN	/LAN Mode 2 : Port-Based VLAN				
Diagnostics		VLAN	VLAN	VLAN	VLAN	VLAN
🖽 🗀 Port		1	2	3	4	2
 Switching Trunking 	Port 1	V				
🕀 🦳 STP/Ring 🖻 📋 VLAN	Port 2					
<u>VLAN Mode Setting</u> <u>802.1Q VLAN Setting</u>	Port 3					
<u>B02.1Q Port Setting</u> Port Based VLAN	Port 4					
⊕ 🔂 QoS ⊕ 🛅 SNMP	Port 5					
 ➡ ➡ 8021X ➡ ➡ LLDP 	Port 6					
🗄 🛅 Others Protocols	Port 7					
	Port 8					

Figure 65: Port Based VLAN – Example 1

In the example \underline{mr} , ports 1 through 6 are all on their own VLAN and cannot communicate with each other. Port 7 and 8 are members of all 6 VLANS and therefore can communicate with all ports that are in any of the VLANs that they share membership with.

Management Switch ⊕	VLAI	N Mode 2 : I	Port-Based V	LAN			
 Diagnostics Diagnostics 		VLAN 1	VLAN 2	VLAN 3	VLAN 4	VLAN 5	VLAN 6
Switching Trunking	Port 1		(III)	F	F	F	
STP/Ring	Port 2						
<u>VLAN Mode Setting</u> <u>802.1Q VLAN Setting</u>	Port 3				<u>I</u>	1	
<u>B02.1Q Port Setting</u> Port Based VLAN	Port 4						
Cos Cos SNMP	Port 5				1		F
 □ □ \$021X □ □ LLDP 	Port 6						
Others Protocols	Port 7			V	V	V	
	Port 8						

Figure 66: Port Based VLAN – Example 2

To add or remove ports from a specific VLAN:

- 1. Select or deselect the checkbox to the right of the Port and below the VLAN ID for the port you want to add or remove from a VLAN.
- 2. Click on the **Submit** button.
- 3. Save the configuration (see the <u>Save Configuration Page</u>)

Port Based VLAN Configuration Examples using CLI Commands

To configure port based VLANs use the following CLI commands (for more information on CLI command usage see <u>CLI Command Usage</u>)

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: switchport portbase add vlan <1 - 16>

Usage Example (to add a port to a single VLAN):

switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fe1
switch_a(config-if)#switchport portbase add vlan 1

```
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Usage Example (to add a port to multiple VLANs):

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fel
switch_a(config-if)#switchport portbase add vlan 1
switch_a(config-if)#switchport portbase add vlan 2
switch_a(config-if)#switchport portbase add vlan 3
switch_a(config-if)#switchport portbase add vlan 4
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

VLAN Configuration in 802.1Q Tag Based VLAN Mode

General Overview

802.1Q VLAN configuration consists of the following four elements:

- 1. Creating all VLANs in the VLAN database.
- 2. Configuring an incoming untagged packet's VLAN association rule: this is accomplished by configuring the PVID setting on each individual port.
- 3. Configuring the ports that are associated with a VLAN to allow the packets that belong to that VLAN to exit and enter the switch through that port.
- 4. Configuring the tag action on the outgoing packets for each VLAN, that is to say, deciding on whether or not an outgoing packet will be tagged with the VLAN number that the packet belongs to.

All ports on the EX24000 Switch can be configured with different Port Types that have different tagging restrictions as defined below.

- Access Port If a port is configured to be an Access Port, then this port can only be a member of a single VLAN based on the Access Port's PVID VLAN setting, and this port's outgoing packets cannot be modified to contain a VLAN Tag.
- Trunk Port If a port is configured to be a Trunk Port, then this port can be a
 member of multiple VLANs. This port's outgoing packets will be automatically
 modified to contain a VLAN tag of the VLAN that the packet belongs to, with the
 exception of the PVID VLAN on that port. The PVID VLAN on a Trunk Port will not be
 automatically modified to contain a VLAN tag of the PVID VLAN.
- **Hybrid Port** A Hybrid Port has no restriction on it. If a port is configured to be a Hybrid Port, then this port can be a member of multiple VLANs, and this port's outgoing packets can be configured to be either with or without a VLAN tag of the VLAN that the packet belongs to, including the PVID VLAN of the Hybrid Port.

For all three types of ports above, if an incoming packet contains a VLAN tag, then the packet's VLAN association rule will be based on the VLAN Tag.

Enabling 802.1Q Tagged Based VLAN

To navigate to the VLAN Mode Setting page:

- 1. Click on the + next to VLAN.
- 2. Click on VLAN Mode Setting.

To enable 802.1Q Tagged Based VLAN on the switch:

- 1. Select Tag-based VLAN from the dropdown box (see 如下)
- 2. Click on the **Submit** button.
- 3. Save the configuration (see the <u>Save Configuration Page</u>)





Configuring 802.1Q VLAN Database

To navigate to the 802.1Q VLAN Setting page:

- 1. Click on the + next to VLAN.
- 2. Click on 802.1Q VLAN Setting.

To configure the 802.1Q VLAN Database, please do the following:

1. Click on the Add VLAN button (see Figure 68).

VLAN Setting		Add VLAN	Delete VLAN
VLAN ID	VLAN NAME		
VLAN1	default		

Figure 68: Add VLAN

- 2. Enter the VLAN ID.
- 3. Enter the VLAN Name.
- 4. Select Attach or Detach for the CPU Port.
 - a. Attaching the CPU to a VLAN is typically done on the Management VLAN.
- 5. Select the ports to be a member of the VLAN (see <u>Configuring the VLAN Egress</u> (outgoing) Member Ports)
- 6. Click on **Submit** button.
- 7. Repeat for all the VLANs that are needed.
- 8. Save the configuration (see the Save Configuration Page)

🏠 Management Switch 🗇 🍋 System	VLAN ID(24094)	100	VLAN Name	Managemnet
E 🗀 Diagnostics	CPU Port	Attach 💌		
E 🔁 Port	VLAN Setting	·		
E C Trunking	PORT	VLAN Memb	er	Tag or Untag
I A VLAN	1	m		Untag 💌
-VLAN Mode Setting	2	100 A		Untag 💌
802 1Q VLAN Setting	3	[[]]		Untag 💌
- S02.1Q Port Setting	4			Untag 💌
TOLEDASSO VERIN				1

Figure 69: Add VLAN Page

802.1Q Tag Based VLAN Configuration Examples Using CLI Commands

Configuring a 802.1Q VLAN

To configure a 802.1Q VLAN on a switch use the following CLI commands (for more information on CLI command usage see <u>CLI Command Usage</u>)

CLI Command Mode: VLAN Database Configuration Mode

CLI Command Syntax: switchport portbase add vlan <1 – 16> vlan <1 – 4094> bridge 1 name VLAN NAME state enable

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#vlan database
switch_a(config-vlan)#vlan 100 bridge 1 name Management state enable
switch_a(config-vlan)#vlan 200 bridge 1 name Accounting state enable
switch_a(config-vlan)#vlan 300 bridge 1 name Sales state enable
switch_a(config-vlan)#q
switch_a(config)#q
switch_a#
```

Configuring an IP Address for a Management VLAN

To configure the IP address for the management VLAN use the following CLI commands

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: ip address IP_ADDRESS/PREFIX [e.g. 10.0.0.1/24]

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.100
switch_a(config-if)#ip address 192.168.100.10/24
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Removing an IP Address from a Management VLAN

To removed an IP address from a management VLAN use the following CLI commands

- CLI Command Mode: Interface Configuration Mode
- CLI Command Syntax: no ip address

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.100
switch_a(config-if)#no ip address
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Configuring an Access Port

To configure an Access Port use the following CLI commands:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: switchport mode access

CLI Command Syntax: switchport access vlan <1 - 4094>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fel
switch_a(config-if)#switchport mode access
switch_a(config-if)#switchport access vlan 100
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```
Configuring a Trunk Port

To configure a Trunk Port use the following CLI commands:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: switchport mode trunk

- CLI Command Syntax: switchport trunk allowed vlan add 100,200,300
- CLI Command Syntax: switchport trunk native vlan 1

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fe7
switch_a(config-if)#switchport mode trunk
switch_a(config-if)#switchport trunk allowed vlan add 100,200,300
switch_a(config-if)#switchport trunk native vlan 1
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Add an IP to the Management VLAN

To navigate to the System/IP Address page:

- 1. Click on the + next to System.
- 2. Click on IP Address.

To add an IP for a Management VLAN:

- 1. Enter the IP address and subnet mask for the management VLAN
- 2. Click on the **Submit** button (see $\underline{\forall \square \vdash}$).
- 3. Save the configuration (see the <u>Save Configuration Page</u>)

stem Information	VLAN ID	IP Address	IP Subnet Mask
tem Name/Password Address	1	192.168.1.12	255.255.255.0
anagement Interface	100	192.168.100.12	255.255.255.0
iware Upgrade	200		
<u>t</u>	300		

Figure 70: Management VLAN IP Address

To delete an IP from a VLAN (the default VLAN, for an example):

- 1. Delete the IP and the subnet mask of the default VLAN and leave it as blank
- 2. Click on the **Submit** button.

Warning: Before completing the above steps, make sure that you have already set up another management IP on another VLAN, and have set up a port properly for accessing that VLAN.

Configuring the Port Type and the PVID setting

To navigate to the 802.1Q Port Setting page:

- 1. Click on the + next to VLAN.
- 2. Click on 802.1Q Port Setting.

To configure the proper port type and the PVID setting for each switch port:

- 1. Choose the port type for each port in the drop-down list (see <u>General Overview</u> for port type details).
- 2. Enter the **PVID VLAN** for each port (see below).
- 3. Enter the Priority Level (optional).
- 4. Click on the **Update Setting** button.
- 5. Save the configuration (see the <u>Save Configuration Page</u>)

Warning: Modifying the Port Type using the Web GUI will cause that switch port to lose all its current VLAN membership and become a member port for the PVID VLAN only. You will lose your current connection to the switch, should you choose to modify the PVID of the port that connects your Computer to the switch.

Diagnostics	Port	Mode	PVID	Priority Level
e 🔁 Port	1	Access 💌	100	0
C Switching	2	Access 💌	200	0
STP.Ring	3	Access 💌	200	0
VLAN	4	Access 💌	200	0
S02.10 VLAN Setting	5	Access 💌	300	0
802.10 Port Setting	6	Access 💌	300	0
Port Based VLAN	7	Access .	300	0
C Qos	25	Trunk 💌	1	0
302.1X	26	Trunk 💌	1	0
C LLDP	27	Trunk 💌	1	0
Others Protocols	28	Trunk 💌	1	0



Configuring the VLAN Egress (outgoing) Member Ports

To navigate to the 802.1Q VLAN Setting page:

- 1. Click on the + next to VLAN.
- 2. Click on 802.1Q VLAN Setting.

To configure the egress member ports for each VLAN:

1. Click on the VLAN link that you want to configure (see $\underline{\#}$).

Diagnostics	VLAN Sett	ing	Add VLAN	Delete VLAN
Port	VLAN ID	VLAN NAME	CPU	
C Switching	VLAN1	default		1
STP/Ring	VLAN100	Managemnet		
VLAN	VLAN200	Accounting		
VLAN Mode Setting	VLAN300	Sales		
				-
802.1Q Port Setting				
Port Based VLAN				

Figure 72: VLAN Links

- 2. Check the check box next to the port number that should be the egress member port for this VLAN
- 3. Click on the **Submit** button (see Figure 73).

Note: If an egress member port for a VLAN has the PVID set on that port to be the same as the VLAN, then that port will automatically be configured as an egress member port for the VLAN by the switch. If a check box is not checked and is grayed out, it is because that port is an Access Port with the PVID set to be a different VLAN than the current VLAN.

E C Diagnostics	VLAN ID	100		VLAN Name	Managemnet
ti 🛄 Port Film Switching	CPU Port	Attach 💌	54		
Trueking	PORT		VLAN Memb	er	Tag or Untag
Co STP Ring	1		50		Untag =
VLAN	2		E1		Untag =
VLAN Mode Setting	3				Untag +
102.10 Port Setting	4		13		Untag +
Part Based VLAN	5		El		Untag 👻
Ca QoS	25		12		Tag 💌
302.1X	26		2		Tag 💌
	27		12		Tag 💌
🖬 😋 Others Protocols	28		10		Tag



If any of the egress member ports are Hybrid ports, you must also configure the Tag action on this port (see Figure 74).

- 4. Select the correct **Tag** option in the drop down list under **Tag or Untag** for this port.
- 5. Click on the **Submit** button.

System	-			1	
B 🗀 Diagnostics	VLAN ID	400	VLAN Name	VLAN0400	
E 🗀 Switching	CPU Port	Attach 💌	1.1		
Trunking	PORT	VLAN Mem	ber	Tag or Untag	
8 🗀 STP/Ring	1			Untag 💌	
I 🙆 VLAN	2	E		Untag 💌	
VLAN Mode Setting 	3			Untag 💌	
802.10 Port Setting	4	E		Untag 💌	
Port Based VLAN	5			Untag 💌	
QoS	6			Untag 💌	
I SNMP	7	E		Untag 💌	
Co LLDP	8	E		Untag 💌	
😳 Others Protocols	9	8		Untag 💌	
	10			Untag 💌	
	11			Tag Untag	
	12	E		Untag 💌	

Figure 74: Tag or Untag ports

QOS

QoS (Quality of Service) refers to several related aspects of computer networks that allow the transport of traffic with special requirements. In particular, technology has been developed to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter service demands. Beyond the audio applications that QoS was originally intended, data traffic such as video or real-time information can benefit from QoS.

QoS as it pertains to the EX24000 Switch can be broken down into two types, CoS and DCSP. CoS or **Class of Service** operates at Layer 2 and was developed by an IEEE working group in the 1990s. CoS uses a 3-bit field called the **Priority Code Point** (PCP) within an Ethernet frame header when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value between 0 and 7, inclusive that can be used by QoS disciplines to differentiate traffic. Although this technique is commonly referred to as IEEE 802.1p, there is no standard or amendment by that name published by the IEEE. Rather the technique is incorporated into the IEEE 802.1Q standard which specifies the tag inserted into an Ethernet frame.

Eight different classes of service are available as expressed through the 3-bit PCP field in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE however has made some broad recommendations:

РСР	Priority	Acronym	Traffic Types
1	0 (lowest)	BK	Background
1	1	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Critical Applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork Control
7	7 (highest)	NC	Network Control

The above recommendations are implemented in the EX24000's 802.1p submenu.

DSPC or **Diffserv Code Point** uses the first 6 bits in the ToS field of the IP(v4) packet header. This type of QoS is primarily useful if the QoS needs to pass through a router or routers. We will touch on DSPC briefly later in this section.

Global Configuration Page

Web GUI Interface

To navigate to the **QoS Global Configuration** page (see <u>dur</u>):

- 1. Click on the + next to **QoS**.
- 2. Click on Global Configuration.

🔁 🔂 System	10	Mode				
Diagnostics	QoS	Disable 💌				
Port	Trust		DSCP			
F 🔁 Switching F 🦳 Trunking	Policy	Strict Priority(Queue3) +WRR(Queue0-2) WRR(Queue0-3)				
C STP/Ring		Weighted Round Robin				
H🛅 VLAN	Queue	Weight(1~20)				
QoS	0	1				
Global Configuration 802.1p Priority	1	2				
DSCP	2	4				
SNMP	3	8				
Haine 802.1X Haine LLDP Haine Others Protocols			Submit			

Figure 75: Global Configuration

To Enable the QoS settings:

- 1. Enable QoS, by selecting the drop-down box to the right of the QoS option.
- 2. Choose CoS and/or DSCP next to the Trust option.
- 3. Select the desired option next to Policy:
 - a. Strict Priority (Queue0-3) Packets must be emptied from the queues in order. Starting with queue 3 and ending with queue 0, the packets in each queue must be completely emptied before the next queue's packets are considered for transmission.
 - b. WRR (Queue 0 3) each queue is allowed to discharge a certain number of packets (according to the WRR weights in the Weighted Round Robin section) before moving to the next queue.

- 4. Enter the **Weight** for each queue in the Weight Round Robin section
- 5. Click on the **Submit** button.
- 6. Save the configuration (see the Save Configuration Page)

Note: Weighted Round Robin – There are four text fields, one for each queue (0 – 3). A number from 1 to 20 can be assigned for each queue. This number is used with WRR policy and is the value of the number of packets that must be emptied from the queue before the next queue is considered. By default, these values are:

Queue	Weight
0	1
1	2
2	4
3	8

QoS Global Configuration using the CLI Interface

This section gives information on Command line commands related to QoS and assumes the user has a working knowledge of connecting to the switch using Telnet, SSH or the Serial port.. Telnet is enabled by default. To enable or disable Telnet or SSH see the Management Interface section.

For more information on CLI command usage see <u>CLI Command Usage</u>.

Enabling/Disabling QoS

To get to the CLI level to configure QoS:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: mls qos enable no mls qos

Usage Example – Enabling QoS:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fel
switch_a(config-if)#mls qos enable
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Usage Example – Disabling QoS:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int fe1
switch_a(config-if)# no mls qos
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Enable/Disable QoS Trust

CLI Command Mode: General Configuration Mode

CLI Command Syntax: mls qos trust <cos/dscp> no qos trust

Usage Example – Enable QoS Trust:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#mls qos trust cos
switch_a(config)#q
switch_a#
```

Usage Example – Disable QoS Trust:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# no mls qos trust
switch_a(config)#q
switch_a#
```

Configuring the Egress Expedite Queue

CLI Command Mode: General Configuration Mode

CLI Command Syntax: priority-queue strict priority-queue out no priority-queue out mls qos <*WRR_WTS*> (4 values separated by spaces. Range is 1-20 (See the <u>Usage Example</u>).

Usage Example – Enable QoS Strict Priority (Queue 0-3):

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# priority-queue strict
switch_a(config)#q
switch_a#
```

Usage Example – Enable QoS Strict Priority (Queue 3) + WWR (Queue 0-2):

switch_a>enable
switch_a#configure terminal
switch_a(config)# priority-queue out
switch_a(config)#q
switch_a#

Usage Example – Disable QoS Strict Priority:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# no priority-queue out
switch_a(config)#q
switch_a#
```

Usage Example – The following example specifies the bandwidth ratios of the four transmit queues, starting with queue 0, on the switch. WRR_WTS Weighted Round Robin (WRR) weights for the 4 queues (4 values separated by spaces). Range is 1-20.

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#mls qos 1 2 4 8
switch_a(config)#q
switch_a#
```

802.1p Priority Page

Web GUI Interface

To navigate to the QoS 802.1p Priority page (see Figure 76):

- 1. Click on the + next to **QoS**.
- 2. Click on **802.1p Priority**.

The 802.1p Priority page allows a user to assign the queues to VLAN priorities (see <u>Global</u> <u>Configuration Page</u> for more information on queues).

Each VLAN priority is expressed as the three-bit PCP field in the 802.1Q header discussed previously. The values shown above are the default values with the higher VLAN priorities corresponding to the higher priority queues.

System Diamostics	VLAN Priority	Priority		
E C Port	0	0 ~		
🖸 🔂 Switching	1	0 ~		
🗄 🧀 Trunking	2	1 ~		
🗄 🧰 STP/Ring	3	1 -		
🗄 🧰 VLAN	4	2 ~		
- QoS	5	2 ~		
802.1p Priority	6	3 ~		
DSCP	7	3 ¥		
🗄 🛅 SNMP		Submit		
🗄 🛅 802.1X				
🗄 🔂 LLDP	<u>h.</u>			
🗄 🛅 Others Protocols				
Done			👩 🚭 Internet	🖓 🔹 🔍 100%

Figure 76: 802.1p Priority

By default, the higher priority queue 3 are assigned to VLAN priorities 6 and 7, queue 2 assigned to VLAN priorities 4 and 5; queue 1 assigned to VLAN priorities 2 and 3; and finally, queue 0 assigned to VLAN priorities 0 and 1.

After making any changes on the page, click on the **Submit** button to ensure that the changes are stored.

802.1p Priority Submenu – CLI Interface

For more information on CLI command usage see CLI Command Usage.

CLI Command Mode: General Configuration Mode

CLI Command Syntax: wrr-queue cos-map <QUEUE_ID> <COS_VALUE> Queue ID. Range is 0-3. COS_VALUE CoS values. Up to 8 values (separated by spaces).

Usage Example The following example shows mapping CoS values 0 and 1 to queue 1 on the switch:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#wrr-queue cos-map 1 0 1
switch_a(config)#q
switch_a#
```

DSCP Page – HTTP Interface

The DSCP submenu is much like the 802.1p submenu except there are many more DSCP priorities to choose from and they are all assigned to the lowest-priority queue, 0. For each DSCP priority, the user can change the value of the queue to between 0 and 3. See Figure 3 for more information:

E Gystem	DSCP Priority	Priority	DSCP Priority	Priority	DSCP Priority	Priority	DSCP Priority	Priority
Diagnostics	0	0 ~	1	0 ~	2	0 ~	3	0 ~
D G Switching	4	0 ~	5	0 ~	6	0 ~	7	0 ~
🗋 🗋 Trunking	8	0 ~	9	0 ~	10	0~	11	0 ~
🗋 🧰 STP/Ring	12	0~	13	0 ~	14	0 ~	15	0 ~
🛙 🛅 VLAN	16	0 ~	17	0~	18	0 ~	19	0 ~
Contractor	20	0 ~	21	0 ~	22	0 ~	23	0 ~
	24	0 ~	25	0 ~	26	0~	27	0 ~
DSCP	28	0 ~	29	0 ~	30	0 ~	31	0 ~
- 🔁 SNMP	32	0 ~	33	0 ~	34	0 ~	35	0 ~
1 🧰 802.1X	36	0 ~	37	0 ~	38	0 ~	39	0 ~
	40	0 ~	41	0 ~	42	0~	43	0 ~
Uthers Protocols	44	0~	45	0 ~	46	0 ~	47	0 ~
	48	0 ~	49	0 ~	50	0 ~	51	0 ~
	52	0 ~	53	0 ~	54	0 ~	55	0 ~
	56	0~	57	0 ~	58	0~	59	0 ~
	60	0~	61	0 ~	62	0~	63	0 ~
								Submit

Figure 77: DSCP

If the user changes any values on this page, clicking on the **Submit** button allows them to take effect.

DSCP Submenu – CLI Interface

For more information on CLI command usage see <u>CLI Command Usage</u>.

CLI Command Mode: General Configuration Mode

CLI Command Syntax: **mls qos map dscp-queue <dscp_value> to <queue_ID>** dscp_value: Up to 8 values (separated by spaces). Range is 0-63. queue_ID: Range is 0-3.

Usage Example The following example shows mapping DSCP values 0 to 3 to queue 1 on the switch:

switch_a>enable
switch_a#configure terminal
switch_a(config)#mls qos map dscp-queue 0 1 2 3 to 1
switch_a(config)#q
switch_a#

QoS Interface Commands – CLI Interface

For more information on CLI command usage see <u>CLI Command Usage</u>.

To assign a VLAN Priority to an Interface:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: user-priority <0-7>

Usage Example The following example shows mapping DSCP values 0 to 3 to queue 1 on the switch:

switch_a>enable
switch_a#configure terminal
switch_a(config)#interface fel
switch_a(config-if) user-priority 4
switch_a(config)#q
switch_a(config)#q
switch_a#

SNMP

SNMP is a TCP/IP application layer network management protocol that allows any TCP/IP device to be managed across a TCP/IP network. It is based on the client-server paradigm. The server (called a SNMP Agent) runs a process on the managed device that listens for a client's (a network management software running on a computer, usually called a NMS, short for Network Management Station) polling requests to fetch or to set a data item on the managed device. The SNMP Agent can also send alert messages (called Traps) to a NMS automatically, based on the occurrence of certain events on the device that the Agent resides.

SNMP General Settings

To navigate to the SNMP General Settings page:

- 1. Click on the + next to **SNMP**.
- 2. Click on SNMP General Settings.

To configure the general settings for the SNMP feature (see Figure 78):

- 1. The SNMP server on the switch can be enabled or disabled by selecting the appropriate choice from the dropdown list next to SNMP Status.
- 2. Enter a short description (up to 256 characters) into the text entry box next to Description, for the purpose of switch identification.
- 3. Enter a name into the text entry box next to Location, for the purpose of identifying the location of the switch.
- 4. Enter a name (up to 256 characters) into the text entry box next to Contact, to identify the entity that is responsible for this switch.
- 5. Enter a trap community name (up to 256 characters) into the text entry box next to any one of the 5 Trap community name entry boxes from Trap Community Name 1 to Trap Community Name 5.
 - a. Community names identify the SNMP Trap community group that the traps on this switch should be sending to. The identical Trap community names should also be set on the NMS hosts that will be receiving the traps. Each name defined corresponds with the Trap host IP address entry box with the same number. For example, Trap Community Name 1 corresponds with Trap Host 1 IP Address.

- 6. Enter an IP address, for the NMS host(s) that should be receiving traps from this switch, into the text entry box next to any one of the 5 Trap host IP address entry boxes from **Trap Host 1 IP Address to Trap Host 5 IP Address**
- 7. Enable or disable the link down trap by selecting the appropriate choice from the drop-down list next to **Link Down Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link up state to the link down state.
- 8. Enable or disable the link up trap by selecting the appropriate choice from the dropdown list next **Link Up Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link down state to the link up state.
- 9. Enable or disable the MAC notification trap by selecting the appropriate choice from the drop-down list next to **MAC Notification Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups anytime there is a change in the MAC table on certain selected ports of the switch.
- 10. Set the interval between the MAC notification traps that you want the switch to send by entering the interval (in number of seconds from 1 to 65535) into the text entry box next to **MAC Notification Interval (1 to 65535 seconds)**.
- 11. Set the size of the MAC notification history table by entering the total number of records (from 1 to 500) that the switch will keep for user to review at any one time into the text entry box next to **MAC Notification History Size (1 to 500)**.
- 12. Select which ports on the switch for which traps should be sent when there is a new MAC address added to the MAC table for the port, by checking the appropriate check boxes for these ports in the **MAC Notification Added** section.
- 13. Select which ports on the switch for which traps should be sent when there is a MAC address being removed from the MAC table for the port, by checking the appropriate check boxes for these ports in the **MAC Notification Removed** section.
- 14. Click on the **Update** button after you have finished the configuration of the SNMP Server (Agent) General Settings.
- 15. Save the configuration (see the Save Configuration Page)

Management Switch	SNMD Status 1	Enable T			
🗄 🧰 System	STATE Status				
Diagnostics	SIVINE O				
ti D Port	Description 2	Hub_Switch_1			
Tranking	Location 3	First_Floor_Closet			
E STP.Rmg	Contact 4	Administrator			
🖻 🛅 VLAN	Trap Community Name 1	Trap_Group_1			
E QoS	Trap Community Name 2	Trap_Group_2			
SNMP	Trap Community Name 3 5	Trap Group 3			
-SNMP v1/v2	Trap Community Name 4	Trap_Group_4			
E SNMP v3	Trap Community Name 5	Trap_Group_5			
	Trap Host 1 IP Address	192.168.1.100			
E Conters Protocols	Trap Host 2 IP Address	192.168.2.100			
	Trap Host 3 IP Address 6	192.168.3.100			
	Trap Host 4 IP Address	192.168.4.100			
	Trap Host 5 IP Address	192 168 5 100			
	Link Down Trap 7	Enable •			
	Link Up Trap 8	Enable			
	MAC Notification Trap 9	Enable •			
	MAC Notification Interval (1 to 65535 seconds) 10	60			
	MAC Notification History Size (1 to 500) 11	100			
	MAC Notification Added 12	P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 P11 P12 P13 P14 P15 P16 P17 P18 P19 P20 P21 P22 P23 P24 P25 P26 P27 P28 P25 P26 P27 P28			
	MAC Notification Removed 13	P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 P11 P12 P13 P14 P15 P16 P17 P18 P19 P20 P21 P22 P23 P24 P25 P26 P27 P28 P P P2 P28			
		14 Update Setting			

Figure 78: SNMP General Settings

Configuring SNMP v1 & v2 Community Groups

To navigate to the SNMP v1/v2 page:

- 1. Click on the + next to **SNMP**.
- 2. Click on SNMP v1/v2.

To configure the SNMP v1 & v2 community groups (see Figure 79):

- 1. Enter the SNMP community name into the text entry box next to **Get Community Name**. This will allow the NMS to poll status information from the switch (read only).
- 2. Enter the SNMP community name, into the text entry box next to **Set Community Name**. This will allow a NMS to change the status of a data item in the switch.
- 3. Click on the **Update Setting** button after you have finished the configuration.

Management Switch	SNMP V1/V2c Setting					
 Diagnostics 	Get Community Name	1	public			
🗉 🧰 Port	Set Community Name	2	private			
 □ □ Switching □ □ Trunking 				3 Update Setting		
Tring						
E SNMP						
SNMP General Setting						
SNMP v1/v2 SNMP v3						

4. Save the configuration (see the <u>Save Configuration Page</u>)

Figure 79: Community Name V1/V2c

Configuring SNMP v3 Users

To navigate to the SNMP v3 page:

- 1. Click on the + next to **SNMP**.
- 2. Click on SNMP v3.

Adding SNMP v3 Users to the switch

1. Click on the **Add User** button. See \underline{mr} .

🏠 Management Switch	
🕀 🧰 System	SNMPv3 Setting Add User Delete User
🕀 🧰 Diagnostics	
🗄 🛅 Port	User Name Access Mode Security Level Authentication Type Privacy Type
🗄 🛅 Switching	
🗄 🔂 Trunking	
🗄 🛅 STP/Ring	
🕀 🔂 VLAN	
🗄 🛅 QoS	
🖻 🙆 SNMP	
SNMP General Setting	
<u>"SNMP v1/v2</u>	
SNMP v3	
🗄 🛅 802.1X	
🗄 🛅 LLDP	
🗄 🛅 Others Protocols	
Done	🔀 🎱 Internet 🦓 🔹 🕄 100% 👻

Figure 80: Add User

- 2. Next, select the desired authentication/privacy protocols from the drop-down list next to "NMP Version, according to the chart below (also see <u>Figure 81</u>):
 - a. **SNMPv3 No-Auth** = Only user name match is required for SNMP access to the switch. No user authentication or data encryption will be used.
 - b. **SNMPv3 Auth-MD5** = User authentication will be required using the MD5 hashing algorithm, but no data encryption will be used.
 - c. **SNMPv3 Auth-SHA** = User authentication will be required using the SHA-1 hashing algorithm, but no data encryption will be used.

- d. **SNMPv3 Priv Auth-MD5** = User authentication will be required using the MD5 hashing algorithm, and in addition, all data in protocol message will be encrypted using 56-bit DES encryption algorithm.
- e. **SNMPv3 Priv Auth-SHA** = User authentication will be required using the SHA-1 hashing Algorithm, and in addition, all data in protocol message will be encrypted using 56-bit DES encryption algorithm.

Management Switch	SNMP V3 Setting						
	SNMP Version	SNMPv3 No-Auth					
E Port	User Name	SNMPv3 No-Auth SNMPv3 Auth-MD5					
E 🗀 Switching	Access Mode	SNMPv3 Auth-SHA					
Trunking	Auth. Password	SNMPv3 Priv Auth-ND3					
E C VLAN	Privacy PassPhrase						
		Submit					
🖻 🙆 SNMP							
SNMP General Setting							
<u>SNMP v1/v2</u>							
<u>SNMP v3</u>							

Figure 81: SNMP v3 Settings

- 3. Next, enter the desired username in the text entry box next to User Name.
- 4. Next, please select the desired access authorization for the user from the drop-down list next to **Access Mode**. See <u>Figure 82</u>.

Management Switch	SNMP V3 Setting					
	SNMP Version	SNMPv3 No-Auth				
🗄 🧰 Port	User Name	SNMP_User_1				
🗉 🫅 Switching	Access Mode	Read Only 🔻				
Trunking STP/Ring	Auth. Password					
🗉 🔂 VLAN	Privacy PassPhrase					
🗄 🧰 QoS		Submit				
🖻 🙆 SNMP	L					
SNMP General Setting						
<u>SNMP v1/v2</u>						
<u>SNMP v3</u>						

Figure 82: User name & Access Mode

 Next, if authentication is required for this user, and you have chosen an authentication protocol, then the text entry box next to **Auth. Password** will have been enabled. Enter a password for this user inside this text entry box. See <u>Figure</u> <u>83</u>.

Management Switch	SNMP V3 Setting					
 Diagnostics 	SNMP Version	SNMPv3 Auth-MD5				
E Port	User Name	SNMP_User_2				
🕀 🧰 Switching	Access Mode	Read Only 🔻				
Trunking STP/Ring	Auth. Password	User2				
E D VLAN	Privacy PassPhrase					
🕀 🧰 QoS		Submit				
SNMP						
<u>SNMP v3</u>						

Figure 83: Auth Password

 Next, if both authentication and privacy are required for this user, and you have chosen both an authentication and privacy protocol, then the text entry box next to **Privacy PassPhrase** will have been enabled. Enter a pass phrase inside this text entry box, as part of the key used to encrypt the protocol message for this user. See <u>Figure 84</u>.

🏠 Management Switch		SNMP V3 Setting					
System Diagnostics	SNMP Version	SNMPv3 Priv Auth-MD5 V					
🖽 🔂 Port	User Name	SNMP_User_3					
🗉 🧰 Switching	Access Mode	Read/Write 🔻					
Trunking STP/Ring	Auth. Password	User3					
🕂 🧰 VLAN	Privacy PassPhrase	Private_User					
⊕ 🔂 QoS ⊡ 🔂 SNMP		Submit					
<u>SNMP General Setting</u> <u>SNMP v1/v2</u>							
SNMP v3							



Deleting SNMP v3 Users from the switch

1. Go to SNMP \rightarrow SNMP v3, you should see a list of previously configured users. Next, click on the **Delete User** button. See \underline{mr} .

i Management Switch I in Constant Switch In Const	SNMPv3 Settin	g Add Use	er De	ete User	
 Diagnostics Port 	User Name	Access Mode	Security Level	Authentication Type	Privacy Type
🗉 🛅 Switching	SNMP_User_3	rw	priv	md5	des
🗉 🧰 Trunking	SNMP_User_2	ro	auth	md5	
🗄 🛅 STP/Ring	SNMP_User_1	ro	noauth		
🗉 🔂 VLAN	-				
🖻 🫅 QoS					
E C SNMP					
SNMP General Setting					
<u>SNMP v1/v2</u>					
<u>SNMP v3</u>					

Figure 85: Delete User

- 2. Next, select the user that you wish to delete from the drop-down list next to **Select User Name**.
- 3. Click on the **Submit** button. See $\underline{\#}$.



Figure 86: Select User

SNMP Configuration Examples Using CLI Commands

For more information on CLI command usage see <u>CLI Command Usage</u>.

Enabling SNMP and configuring general settings

To enable the SNMP feature of the switch, and configure its general settings (Description, Location, and Contact information), you must use the below CLI commands. (for more information on CLI command usage and typographic conventions please click here):

CLI Command Mode: General Configuration Mode

CLI Command Syntax: snmp-server enable snmp-server description <1 -256 characters> snmp-server location <1 -256 characters> snmp-server contact <1 -256 characters>

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)# snmp-server enable
switch_a(config)# snmp-server description Hub_Switch_1
switch_a(config)# snmp-server location First_Floor_Closet
switch_a(config)# snmp-server contact Administrator
switch_a(config)#q
switch_a#
```

Configuring SNMP Traps

To configure the Trap features of the SNMP protocol on the switch, you use the following CLI commands:

CLI Command Mode: General Configuration Mode Interface Configuration Mode

CLI Command Syntax: snmp-server trap-community 1 <1 -256 characters > snmp-server trap-community 2 <1 -256 characters > snmp-server trap-community 3 <1 -256 characters > snmp-server trap-community 4 <1 -256 characters > snmp-server trap-community 5 <1 -256 characters > snmp-server trap-ipaddress 1 <IP Address> snmp-server trap-ipaddress 2 </P Address> snmp-server trap-ipaddress 3 <IP Address> snmp-server trap-ipaddress 4 </P Address> snmp-server trap-ipaddress 5 < IP Address> snmp-server trap-type enable linkDown snmp-server trap-type enable linkup snmp-server trap-type enable mac-notification snmp-server mac-notification interval <1 to 65535 seconds> snmp-server mac-notification history-size <1 to 500 entries> snmp-server trap mac-notification added snmp-server trap mac-notification removed

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)# snmp-server trap-community 1 Trap_Group_1
switch_a(config)# snmp-server trap-community 2 Trap_Group_2
switch_a(config)# snmp-server trap-community 3 Trap_Group_3
switch_a(config)# snmp-server trap-community 4 Trap_Group_4
switch_a(config)# snmp-server trap-community 5 Trap_Group_5
switch_a(config)# snmp-server trap-ipaddress 1 192.168.1.100
switch_a(config)# snmp-server trap-ipaddress 2 192.168.2.100
switch_a(config)# snmp-server trap-ipaddress 3 192.168.3.100
switch_a(config)# snmp-server trap-ipaddress 4 192.168.4.100
switch_a(config)# snmp-server trap-ipaddress 5 192.168.5.100
switch_a(config)# snmp-server trap-type enable linkDown
switch_a(config)# snmp-server trap-type enable linkup
switch_a(config)# snmp-server trap-type enable mac-notification
switch_a(config)# snmp-server mac-notification interval 60
switch_a(config)# snmp-server mac-notification history-size 100
switch_a(config)#interface fe1
switch_a(config-if)#snmp-server trap mac-notification added
switch_a(config-if)#snmp-server trap mac-notification removed
switch_a(config-if)#q
switch_a(config)#q
switch a#
```

Configuring SNMP v1 & v2 Community Groups

To configure the SNMP v1 & v2 community groups to make the SNMP feature more secure, use the following CLI commands:

CLI Command Mode: General Configuration Mode CLI Command Syntax: snmp-server enable snmp-server community get <1 -256 characters> snmp-server community set <1 -256 characters>

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)# snmp-server community get public
switch_a(config)# snmp-server community set private
switch_a(config)#q
switch_a#
```

Adding SNMP v3 Users

To add SNMP v3 Users to the switch and maximize the security for the SNMP feature, you must use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: snmp-server v3-user <username> <ro|rw> noauth snmp-server v3-user <username> <ro|rw> auth <md5|sha> <password> snmp-server v3-user <username> <ro|rw> priv <md5|sha> <password> des <pass_phrase>

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)# snmp-server v3-user SNMP_User_1 ro noauth
switch_a(config)# snmp-server v3-user SNMP_User_2 ro auth md5 User2
switch_a(config)# snmp-server v3-user SNMP_User_3 rw priv md5 User3
des Private_User
```

switch_a(config)#q
switch_a#

IEEE 802.1X

EtherWAN switches support the IEEE 802.1X protocol to provide port based security on a switch port against unauthorized access. In order for this protocol to work, two additional components are required; an EAP (Extensible Authentication Protocol) compatible RADIUS server to authenticate a client station that is trying to gain access to the network through a port on the switch, and an 802.1X client software (known as the "Supplicant" software) used on the end device to communicate with the RADIUS server for the purposes of authenticating the end device that is trying to gain access to the network through the switch port.

When an end device is initially connected to a port on the EtherWAN switch where the 802.1X protocol is enabled on the port, the switch will only pass 802.1X authentication traffic (known as EAPOL traffic) on that port between the Supplicant on the end device and the RADIUS server, and will not allow any other traffic to pass. After the initial connection, the EtherWAN switch will request authentication credentials from the Supplicant in the end device that has just connected to the port. After the switch receives the proper authentication credentials from the Supplicant in the end device, the switch will sent the credentials to the EAP compatible RADIUS server that's configured in the switch for the purpose of authenticating the end device. If the end device is successfully authenticated by the RADIUS server, the RADIUS server will sent an "Access-Accept" message to the switch; at this point the EtherWAN switch will inform the Supplicant in the end device of the successful authentication and open up the port for all network traffic to pass.

Configuring 802.1X from the GUI system

To navigate to the 802.1X / Radius Configuration page:

- 1. Click on the + next to 802.1X
- 2. Click on Radius Configuration

Enabling Radius

By default, the 802.1X function is globally disabled on the EtherWAN switch. If you want to use the 802.1X port based security on a port, you must enable it globally on the switch first, and then enable it on a per port basis.

To enable the 802.1X function globally on the switch:

- 1. Choose enable from the drop down list next to Radius Status
- 2. Click on the Update Setting button. (See Figure 87)

Management Switch		Radius Server Global Setting					
Diamostics	Radius Statu	15	Ena	able 💌			
B 🗀 Port			Jpdate Setti	ing			
C Switching							
C Trunking		Rad	ius Configu	ration			
STP/Ring	A	dd Radius	Delete Radius				
C VLAN				(Carlotter			
Co QoS	Order	Radius Se	rver IP	Port	Timeout	Retransmit	Key
8021X							
Radius Configuration							
Port Authentication							



Adding a Radius Server

Next, you will need to configure the settings that the switch will need in order to connect to a RADIUS server.

- 1. Click on the **Add Radius** button (see $\underline{\#}$).
- 2. Next, enter the IP address of the RADIUS server that the switch will use in order to authenticate in the text entry box next to **Radius Server IP** (see Figure 88).
- 3. Enter the password for RADIUS server in the text entry box next to Secret Key.
- 4. Optionally, the UDP port number for the RADIUS server (if it is different from the standard default 1812) can be changed. To do this, enter the port number in the text entry box next to **Radius Server Port**.
- 5. Next, you can choose to configure the minimum time that the switch must wait, before it is allowed to retransmit a message to the RADIUS server due to no response. To do this, enter the number of seconds that the switch must wait (between 1 and 1000 seconds) into the text entry box next to Timeout <1-1000>.

6. Next, you can choose to configure the maximum number of times that the switch can attempt to retransmit a message to the RADIUS server. To do this, please enter a number (from 1 to 100) into the text entry box next to **Retransmit**.

Management Switch	R	Radius Server Setting				
	Radius Server IP	2	192.168.1.102			
Port Switching	Radius Server Port	4	1812			
	Secret Key	3	5678			
T C STP.Ring	Timeout <1-1000>	5	5			
VLAN	Retransmit <1-100>	6	3			
 QoS SNMP 8021X 			7 Subm			
Radius Configuration						
Port Authentication						

7. Click on the **Submit** button.

Figure 88: Radius Setup

Management Switch		Radius Server Global Setting					
Diagnostics	Radius State	ıs [)isable 💌				
Di Port		Update Se	etting				
🗀 🔂 Switching	L						
🗋 Trunking		Radius Configuration					
Gamma STP/Ring		Add Padius	Dele	to Radius			
VLAN			Dele				
	Order	Radius Server IP	Port	Timeout	Retransmit	Key	
8021X	1	192.168.1.102	1812	5	3	5678	
Radius Configuration							
Port Authentication							

Figure 89: Resulting Radius Server Setup

Enabling 802.1X on a Port

After the 802.1X port based security is enabled globally, you must enable it locally on the port.

To navigate to the 802.1X / Port Authentication page:

1. Click on the + next to **802.1X**

2. Click on Port Authentication

To enable 802.1X on a port (see Figure 90):

- 1. Choose the desired port from the drop-down list next to **Interface**, to have the 802.1X feature applied to that port.
- 2. Next, make sure **Enabled** is selected from the drop-down list next to **Authentication State**, this will enable the 802.1X function on the previously selected port.
- 3. Next, make sure that the choice **Auto** is selected in the drop-down list next to **Port Control**; this will allow the port to use 802.1X to authentic the end station.
 - a. If you choose to have the port to be always unauthorized or to be always authorized, you can choose the appropriate choice in the drop-down list.
- 4. Next, you can choose to have the end station to be re-authenticated periodically. To do this, choose **Enabled** in the drop-down list next to **Periodic Re-authentication**.
- 5. After you have enabled periodic re-authentication, you must also configure the time period interval for the re-authentication of the end station. To do this, enter the number of seconds (1-4294967295), in to the text entry box next to **Re-authentication Period**.
- 6. Next, **Update Setting** button in order to activate all the configured settings (see the below screenshot)

a Sumagement Switch		802.1x Port Setting						
Diamostics	Interfac	e			1	fe1 💌		
D Port	Authent	ication State			2	Enabled 💌]	
C Switching	Port Co	ntrol			3	Auto		_
C Trunking	Periodic	Reauthentication	1		4	Enable 💌	1	
C STP/Ring	Reauthe	ntication Period <	7295>	5	3600	(sec.)	_	
C QoS			6	Update S	etting			
SNMP								
802.1x Radius Configuration	Port	Port Enabled	Port Control		Port Status		Periodic Reauthentica	Reauthentication tion Period
Port Authentication	1							
TO LLDP	2	false	Auto		Unauthorized		enabled	3600
- Other Fronces	3							
	4							

Figure 90: Enabling 802.1X on a Port

LLDP

LLDP is a network discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about devices to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management reachability and connection endpoint information from adjacent devices.

Using LLDP, a device is able to advertise its own identification information, its capabilities and media-specific configuration information, as well as learn the same information from the devices connected to it. LLDP advertises this information over Logical Link-Layer Control frames and the information received from other agents in IEEE-defined Management Information Bases (MIB) modules.

LLDP significantly aids in the deployment of any network device that supports the protocol. As a media independent protocol intended to be run on all IEEE 802 devices, LLDP may be used to discover routers, bridges, repeaters, WLAN APs, IP telephones, network camera or any LLDP-enabled device, regardless of manufacturer. Since LLDP runs over the data-link layer only, a switch running one network layer protocol can discover and learn about an access device running a different network layer protocol.

LLDP General Settings

To navigate to the LLDP General Settings page:

- 1. Click on the + next to LLDP.
- 2. Click on General Settings.

Enable/Disable LLDP

To enable LLDP on the EX24000 Switch:

- Select Enable or Disable from the Drop Down box in the LLDP field of the LLDP Transmit Settings box (see Figure 91)
- 2. Click on the **Update Settings** button.
- 3. Save the configuration (see the <u>Save Configuration Page</u>)

Holdtime Multiplier

The Holdtime multiplier for transmit TTL is used to compute the actual time-to-live (TTL) value used in an LLDP frame. The TTL value is the length of time the receiving device should maintain the information in its MIB. To compute the TTL value, the system multiplies the LLDP transmit (TX) interval by the holdtime multiplier. For example, if the LLDP transmit (TX) interval is 30 and the holdtime multiplier for TTL is 4, then the value 120 is encoded in the TTL field in the LLDP header.

To adjust the Holdtime multiplier:

- 1. Enter a numeric value between 2 and 10 (default is 4) in the Holdtime Multiplier text box.
- 2. Click on the **Update Settings** button.

The TX Interval setting adjusts the time that LLDP information is transmitted by the switch. Values can range from 5 to 32768 seconds (default is 30 seconds).

To adjust the TX Interval setting (see Figure 91):

- 1. Enter a numeric value between 5 and 32768 (default is 30) in the TX Interval text box.
- 2. Click on the **Update Settings** button.
- 3. Save the configuration (see the <u>Save Configuration Page</u>)

Global TLV Setting

The global TLV (Time – Length – Value) settings are advertised by the switch to other LLDP devices. The TLVs supported by the EX24000 are (see <u>Figure 91</u>):

- Port Description
- System Name
- System Description
- System Capabilities
- Management Address
- Port VLAN ID
- MAC/PHY Configuration/Status
- Port And Protocol VLAN ID
- VLAN Name
- Protocol Identity
- Power Via MDI
- Link Aggregation
- Maximum Frame Size

To enable specific TLVs for the EX24000:

- 1. Select the check box for each TLV that is to be enabled or select the checkbox for the **All** option which will enable all TLVs for the switch.
- 2. Click on the **Update Settings** button.
- 3. Save the configuration (see the <u>Save Configuration Page</u>)
| System | LLDP Global Setting | | |
|-------------|----------------------------|---|--|
| Diagnostics | LLD | P Transmit Setting | |
| Port | LLDP | Enable + | |
| Trunking | Holdtime multiplier(2-10) | 4 | |
| STP/Ring | Tx interval (5, 32768 sec) | 30 | |
| | Global TLV setting | All
Port Description
System Name
System Description
System Capabilities
Management Address
Port VLAN ID
MAC/PHY Configuration/Status
Port And Protocol VLAN ID
VLAN Name
Protocol Identity
Power Via MDI
Link Aggregation
Maximum Frame Size | |
| | Update Setting | | |

Figure 91: LLDP Global Settings

LLDP Ports Settings

LLDP Ports Settings allows the individual ports on the switch to be configured for LLDP independently of one another. Each port can be configured to transmit LLDP information, receive LLDP information, and notify (via SNMP or Syslog) if there are changes in the LLDP information received from neighboring devices.

To navigate to the LLDP Port Settings page:

- 1. Click on the + next to **LLDP**.
- 4. Click on LLDP Ports Settings (see Figure 92)

Enabling LLDP transmission for a specific Port

To enable the transmission of LLDP information for a specific port:

- 1. Select Enable from the Drop Down box under the Transmit field for each port for which the transmission of LLDP information should be enabled.
- 2. Click on the **Submit** button.

Enabling LLDP Reception for a specific Port

To enable the reception of LLDP information for a specific port:

- 1. Select Enable from the Drop Down box under the Receive field for each port for which the reception of LLDP information should be enabled.
- 2. Click on the **Submit** button.

Enabling Notifications

To enable notification whenever a port receives changed LLDP information:

- 1. Select Enable from the Drop Down box under the Notify field for each port that should send a notification whenever received LLDP information changes.
- 2. Click on the **Submit** button
- 3. Save the configuration (see the <u>Save Configuration Page</u>) after making changes shown on this page.

Port	Link Status	Transmit	Receive	Notify
1	Down	Disabled \$	Disabled \$	Disabled \$
2	Down	Disabled \$	Disabled ‡	Disabled \$
3	Down	Disabled ‡	Disabled +	Disabled \$
4	Down	Disabled ‡	Disabled \$	Disabled \$
5	Down	Disabled \$	Disabled \$	Disabled \$
6	Down	Disabled ‡	Disabled ‡	Disabled \$
7	Down	Disabled ‡	Disabled ‡	Disabled \$
8	Down	Disabled ‡	Disabled +	Disabled \$
9	Down	Disabled \$	Disabled \$	Disabled \$
10	Down	Disabled ‡	Disabled ‡	Disabled \$
11	Down	Disabled ‡	Disabled +	Disabled \$
12	Down	Disabled ‡	Disabled ‡	Disabled \$
13	Down	Disabled \$	Disabled \$	Disabled \$
14	Down	Disabled ‡	Disabled ‡	Disabled \$
15	Down	Disabled ‡	Disabled +	Disabled \$
16	Down	Disabled ‡	Disabled +	Disabled \$
17	Down	Disabled \$	Disabled \$	Disabled \$
18	Down	Disabled ‡	Disabled +	Disabled \$
19	Down	Disabled \$	Disabled +	Disabled \$
20	Down	Disabled ‡	Disabled \$	Disabled \$
21	Down	Disabled \$	Disabled \$	Disabled \$
22	Down	Disabled ‡	Disabled ‡	Disabled \$
23	Down	Disabled ‡	Disabled ‡	Disabled \$
24	Down	Disabled +	Disabled +	Disabled \$
25	Running	Disabled \$	Disabled +	Disabled \$
26	Down	Disabled +	Disabled +	Disabled \$
27	Running	Disabled +	Disabled +	Disabled \$
28	Down	Disabled \$	Disabled \$	Disabled \$

Figure 92: LLDP Ports Settings

LLDP Neighbors

LLDP Neighbors is a read-only page (see <u>Figure 93</u>) that will display all the LLDP capable devices detected by the switch. The following information about connected LLDP-enabled devices is displayed in a tabular format. The columns displayed are:

- **Port** The local switch port to which the remote device is connected.
- Chassis ID The MAC address of the remote device.
- **Port ID** The port number of the remote device.
- IP Address The management IP address of the remote device.
- **TTL** Time to Live, the amount time remaining before the remote device's LLDP is aged-out from the switch.

Diagnostics	Port	System Name	Chassis ID	Port ID	IP Address	TTL
🔁 🔂 Port	1	switch_a	00:e0:b3:33:07:bc	fe5	10.58.7.199	95
🗄 🛅 Switching	5	switch_a	00:e0:b3:33:07:bc	fel	10.58.7.199	95
🗄 🛅 Trunking	28	switch a	00:e0:b3:32:01:a4	fel	10.58.7.162	100
C VLAN						
C VLAN						
 B02.1X LLDP LLDP General Settings 						
BO2.1X LLDP LLDP General Settings LLDP Ports Settings						
BO2.1X LLDP LLDP General Settings LLDP Forts Settings LLDP Neighbors						
302.1X LLDP LLDP General Settings LLDP Forts Settings LLDP Neighbors LLDP Statistics						

Figure 93: LLDP Neighbors

LLDP Statistics

This is a read-only page (see <u>Figure 94</u>) that displays LLDP device statistics and LLDP statistics on a per-port basis. The information collected on this page includes:

- Port switch port number.
- TX Total Total LLDP packets sent.
- RX Total Total LLDP packets received.
- Discards Number of LLDP packets discarded.
- Errors LLDP errors.
- Ageout LLDP information that has been aged out by the switch.
- TLV Discards TLV information discarded
- TLV Unknown TLV information that is unknown

Management Switch	LL	DP Device	Statistics]				
E Diagnostics	Last	Update	130585126	1				
🗉 🧰 Port	Tota	1 Inserts	3					
E C Switching	Total	Deletes	0					
E C STP/Ring	Tota	l Drops	0					
🗉 🧰 VLAN	Total	Ageouts	0					
			10.00	1				
 	Port	Tx Total	Rx Total	Discards	Errors	Ageout	TLV Discards	TLV Unknowns
	1	4	4	0	0	0	0	0
I DP Ports Settings	2	0	0	0	0	0	0	0
"LLDP Neighbors	3	0	0	0	0	0	0	0
LLDP Statistics	4	0	0	0	0	0	0	0
🗄 🛅 Others Protocols	5	4	4	0	0	0	0	0
	6	0	0	0	0	0	0	0
	7	0	0	0	0	0	0	0

Figure 94: LLDP Statistics

LLDP Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

Enable/Disable LLDP

To enable or disable LLDP on the EX24000 switch use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: Ildp enable no lldp enable

Usage Example – Enabling LLDP:

switch_a>enable
switch_a#configure terminal
switch_a(config)#lldp enable
switch_a(config)#q
switch_a#

Usage Example – Disabling LLDP:

switch_a>enable
switch_a#configure terminal
switch_a(config)#no lldp enable
switch_a(config)#q
switch_a#

LLDP Holdtime Multiplier

To modify LLDP holdtime multiplier use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: IIdp holdtime multiplier <1-10>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#lldp holdtime multiplier 4
switch_a(config)#q
switch_a#
```

LLDP Transmit Interval

To modify LLDP Transmit Interval use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: IIdp txinterval <5-32768>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# lldp txinterval 30
switch_a(config)#q
switch_a#
```

Enable/Disable Global LLDP TLVs

To enable or disable global LLDP TLVs use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: IIdp tlv-global <TLV>

TLV Parameters	Description
port-descr	Port Description
sys-name	System Name TLV
sys-descr	System Description TLV
sys-cap	System Capabilities
mgmt-addrs	Management Address
port-vlan-id	Port VLAN ID
mac-phy	MAC/PHY Configuration/Status
port-and-protocol	Port And Protocol VLAN ID
vlan-name	VLAN Name
protocol-identity	Protocol Identity
link-aggregation	(Link Aggregation
max-frame	Maximum Frame Size

TLV Parameters

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# lldp tlv-global mgmt-addrs
switch_a(config)#q
switch_a#
```

Enabling LLDP Transmit on a Port

To enable LLDP Transmit for a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: IIdp tx-pkt

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface fel
switch_a(config)# lldp tx-pkt
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Enabling LLDP Receive on a Port

To enable LLDP Receive for a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: IIdp rcv-pkt

```
switch_a>enable
switch_a#configure terminal
switch_a#interface fel
switch_a(config)# lldp rcv-pkt
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Enabling LLDP Notify

To enable LLDP Notify for a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: IIdp notification

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface fel
switch_a(config)# lldp notification
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Enabling Transmission of the Management IP

To enable the transmission of the management IP address through a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: IIdp mgmt-ip vlan <vlan id>

```
switch_a>enable
switch_a#configure terminal
switch_a#interface fel
switch_a(config)# lldp mgmt-ip vlan 1
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Enabling Specific TLV's on a Port

To enable specific TLVs on a port use the CLI commands below:

CLI Command Mode: Interface Configuration Mode

CLI Command Syntax: IIdp tiv-select <TLV ID> (see TLV Parameters on page 188)

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a#interface fe1
switch_a(config)# lldp tlv-select mgmt-addrs
switch_a(config)#q
switch_a(config)#q
switch_a#

OTHER PROTOCOLS

GVRP

Defined in IEEE 802.1Q, GVRP is a protocol used to dynamically create VLANs on a switch. Any IEEE 802.1Q compliant switch must implement this protocol.

To navigate to the Other Protocols / GVRP page (see Figure 95):

- 1. Click on the + next to **Other Protocols**.
- 2. Click on **GVRP**.

Diagnostics	GVRP		Disable	~		
Port	Dynamic	VLAN Creation	Disable	~		
Switching	Dynam		Disdelie	Update Setting		
STP/Ring						
VLAN	<u> </u>					
QoS	Per Port Setting (include LAG)					
NMP	Port	GVRP	GVRP Applicant	GVRP Registration		
L1X	fe1	Disable V	Normal V	Normal V		
hers Protocols	fe2	Disable 🗸	Normal 🗸	Normal		
RP	fe3	Disable 🗸	Normal 🗸	Normal		
MP Snooping	fe4	Disable 🗸	Normal 🗸	Normal 👻		
<u>P</u>	fe5	Disable 🗸	Normal 🗸	Normal 👻		
<u>RP</u> CR Sources	fe6	Disable 🛩	Normal 🗸	Normal 🗸		
or server	fe7	Disable 🛩	Normal 🖌	Normal 🗸		
	fe8	Disable 🖌	Normal 😽	Normal 💌		
	fe9	Disable 💌	Normal 🛩	Normal 👻		
	fe10	Disable 🛩	Normal 💌	Normal 💌		
	fel1	Disable 🛩	Normal 💌	Normal 💌		
	fe12	Disable 👻	Normal 💌	Normal 💌		
	fe13	Disable 👻	Normal 💌	Normal 👻		
	fe14	Disable 👻	Normal 💌	Normal 💌		
	fe15	Disable 🛩	Normal 💌	Normal 🔽		
	fe16	Disable 👻	Normal 🖌	Normal 💌		
	ge1	Disable 💌	Normal 💌	Normal 👻		
	ge2	Disable 👻	Normal 🛩	Normal 💌		
				Update Setting		

Figure 95: GVRP

General Overview

To enable the GVRP protocol on your network, you must make sure that the switches in your network are configured with the minimum requirements for each type of switches listed below:

For the Access Switches at the edge of the network, below are the minimum requirements:

- All of the user VLANs have been created in the VLAN Database.
- The IP address for the Management VLAN has been configured.
- The appropriate Port Type (Access or Trunk) and the PVID have been configured for all the ports of the switch.
- All the member Trunk ports for all the user VLANs have been configured.
- The GVRP protocol has been globally enabled, and GVRP is locally enabled on the Trunk Ports as well.

For the **Distribution Switches** in the core of the network, below are the minimum requirements:

- The Management VLAN has been created in the VLAN Database.
- The IP address for the Management VLAN has been configured.
- The appropriate Port Type (Access or Trunk) and the PVID have been configured for all the ports of the switch.
- The GVRP protocol has been globally enabled and GVRP is locally enabled on the Trunk Ports as well.
- The Dynamic VLAN Creation feature has been enabled.

Enabling the GVRP Protocol at the Global Level

To enable the GVRP protocol globally on a distribution switch (see Figure 96):

- 1. Under **GVRP Global Setting**, choose the **Enable** option from the drop-down list next to **GVRP**.
- 2. Choose the **Enable** option from the drop-down list next to **Dynamic VLAN Creation**.
- 3. Click on the **Update Setting** button.

Diagnostics	GVRP		Disable	~		
Port	Dynamic	VLAN Creation	Disable	~		
Trunking	-			Update Setting		
STP/Ring			_			
VLAN	-					
QoS	Per Port Setting (include LAG)					
SNMP	Port	GVRP	GVRP Applicant	GVRP Registration		
LLDP	fe1	Disable 🐱	Normal 🖌	Normal 👻		
Others Protocols	fe2	Disable 👻	Normal 💌	Normal 💌		
GVRP	fe3	Disable 💌	Normal 💌	Normal 👻		
IGMP Snooping	fe4	Disable 🐱	Normal 💌	Normal 💌		
NTP	fe5	Disable 💌	Normal 💌	Normal 👻		
DHCP Server	fe6	Disable 🛩	Normal 💌	Normal 👻		
	fe7	Disable 🖌	Normal 💌	Normal 👻		
	fe8	Disable 😽	Normal 🛩	Normal 🖌		
	fe9	Disable 🛩	Normal 💌	Normal 👻		
	fe10	Disable 👻	Normal 💌	Normal 👻		
	fel1	Disable 🛩	Normal 💌	Normal 👻		
	fe12	Disable 🛩	Normal 🛩	Normal 👻		
	fe13	Disable 🛩	Normal 💌	Normal 👻		
	fe14	Disable 🛩	Normal 💌	Normal 👻		
	fe15	Disable 💌	Normal 💌	Normal 👻		
	fe16	Disable 👻	Normal 💌	Normal 👻		
	ge1	Disable 👻	Normal 💌	Normal 👻		
	ge2	Disable 💌	Normal 💌	Normal 💌		
			[Update Setting		

Figure 96: GVRP Configuration Distribution Switch

To enable the GVRP protocol globally on an Access Switch (see Figure 97):

- 1. Under **GVRP Global Setting**, choose the **Enable** option from the drop-down list next to **GVRP**.
- 2. Click on the **Update Setting** button.

GVRP	Enable 💌
Dynamic VLAN Creation	Disable 💌

Figure 97: GVRP Configuration Access Switch

Enabling the GVRP Protocol at the Port Level

To navigate to the Other Protocols / GVRP page (see Figure 95):

- 1. Click on the + next to **Other Protocols**.
- 2. Click on **GVRP**.

To enable the GVRP protocol locally at the port level, for both the Access switch and the Distribution switch, apply the following procedures to all the Trunk Ports of the switch:

- 1. For all the Trunk Ports under the **Per Port Setting (include LAG)** section, choose the **Enable** option from the drop-down list under the **GVRP** column.
- 2. For all the Trunk Ports under the **Per Port Setting (include LAG)** section, choose the **Active** or **Normal** option from the drop-down list under the **GVRP Applicant** column.
 - **Active** Use this option if you want to run the GVRP protocol on that Trunk Port even if it is blocked by the STP protocol.
 - Normal Use this option if you do not wish to run the GVRP protocol on a Trunk Port when it is being blocked by the STP protocol.
- 3. For all the Trunk Ports under the **Per Port Setting (include LAG)** section, choose the **Enable** option from the drop-down list under the **GVRP Registration** column.
- 4. Click on the **Update Setting** button.
- 5. Save the configuration (see the Save Configuration Page)

Diagnostics	or ma			
D Port	GVKP		Disable	×
Switching	Dynamic	vLAN Creation	Disable	~
Trunking				Update Setting
STP/Ring				
VLAN	Per Port	Setting (include I	AG)	
I QOS SNMP	I GI I OI	Setting (include in	NO)	
802.1X	Port	GVRP	GVRP Applicant	GVRP Registration
LLDP	fe1	Disable 💌	Normal 🚩	Normal 👻
Others Protocols	fe2	Disable 🛩	Normal 💌	Normal 💌
<u> 3VRP</u>	fe3	Disable 💌	Normal 💌	Normal 💌
IGMP Snooping	fe4	Disable 🛩	Normal 💌	Normal 💌
NTP	fe5	Disable 💌	Normal 💌	Normal 👻
OHCP Server	fe6	Disable 🛩	Normal 💌	Normal 👻
	fe7	Disable 💌	Normal 💌	Normal 💌
	fe8	Disable 💌	Normal 💌	Normal 💌
	fe9	Disable 💌	Normal 💌	Normal 💌
	fe10	Disable 👻	Normal 💌	Normal 💌
	fe11	Disable 💙	Normal 💌	Normal 💌
	fe12	Disable 🛩	Normal 💌	Normal 💌
	fe13	Disable 💌	Normal 💌	Normal 👻
	fe14	Disable 🗸	Normal 💌	Normal 💌
	fe15	Disable 🗸	Normal 💌	Normal 🗸
	fe16	Disable 👻	Normal 💙	Normal 👻
	ge1	Disable 💌	Normal 💌	Normal 👻
	ge2	Disable 🗸	Normal 🗸	Normal 👻
		<u>н</u> ј		Update Setting
	4		L	oputito obtaining

Figure 98: GVRP Per Port Settings

GVRP Configuration Examples Using CLI Commands

For more information on CLI command usage see <u>CLI Command Usage</u>.

To enable or disable GVRP globally on the EtherWAN switch, use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: set gvrp enable bridge 1 set gvrp disable bridge 1

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)# set gvrp enable bridge 1
switch_a(config)# set gvrp disable bridge 1
switch_a(config)#q
switch_a#

To enable the dynamic VLAN creation feature of GVRP on the EtherWAN switch, you must use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: set gvrp dynamic-vlan-creation disable bridge 1

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set gvrp dynamic-vlan-creation disable bridge 1
switch_a(config)#q
switch_a#
```

To enable or disable GVRP locally on a port on the EtherWAN switch, you must use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: set port gvrp enable <port id> set port gvrp disable <port id>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set port gvrp enable fe1
switch_a(config)# set port gvrp disable fe1
switch_a(config)#q
switch_a#
```

By default, when GVRP is enabled on a port the **Applicant** runs in Normal mode, which means that the GVRP protocol will not send out any PDUs from a port if the port is being blocked by STP. When you enable the GVRP Applicant to run in Active mode on a port, the GVRP protocol will continue to send PDUs from a port even if the port is being blocked by STP.

The GVRP **Applicant** can be set to run in Normal or Active mode on a port by issuing the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax:

set gvrp applicant state normal <port id> set gvrp applicant state active <port id>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set gvrp applicant state normal fe1
switch_a(config)# set gvrp applicant state active fe1
switch_a(config)#q
switch_a#
```

When you enable GVRP on a port, the **Registrar** is enabled on the port by default. You can enable or disable the GVRP **Registrar** on a port by issuing the following CLI commands:

CLI Command Mode: General Configuration Mode CLI Command Syntax:

set gvrp registration normal <port id> set gvrp registration forbidden <port id>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set gvrp registration normal fe1
switch_a(config)# set gvrp registration forbidden fe1
switch_a(config)#q
switch_a#
```

IGMP Snooping

The settings in the IGMP Snooping feature of the EtherWAN switch controls how the switch forwards multicast packets.

General Overview

The EX24000 Switch has been outfitted with the IGMP Snooping function in three modes:

- Disabled:
 - The switch will forward all multicast packets according to the **Forced Forwarding Port** setting based on the following rule:
 - All multicast packets will be forwarded to only the port specified by either the PassiveForwardMode or the ForcedForwardMode function.
- Passive mode:
 - The switch will forward any multicast packets that have known receivers to the known multicast receiver ports only.
 - The switch will forward any unknown multicast packets (multicast packets without any known receivers) according to the Forced Forwarding Port setting based on the following rule:
 - When there is no Querier Port (a port that receives IGMP queries) present all unknown multicast packets will be forwarded to the port specified by either the **PassiveForwardMode** function or the **ForcedForwardMode** function.
 - When there is a Querier port present, the switch will forward all unknown multicast packets to the Querier port. In addition, all unknown multicast packets will be forwarded to the port specified by the ForcedForwardMode function as well.

• Querier mode:

- The switch will forward any multicast packets that have known receivers to the known multicast receiver ports only.
- The switch will forward any unknown multicast packets according to the Forced Forwarding Port setting based on the following rule:
 - All unknown multicast packets will be sent to only the port specified by the ForcedForwardMode function.

 The switch will also transmit IGMP Queries to the specified VLAN and according to the specified IGMP Query parameters.

Enabling the IGMP Snooping Modes

To navigate to the IGMP Snooping page:

- 1. Click on the + next to **Other Protocols**.
- 2. Click on IGMP Snooping.

To put the IGMP Snooping feature in the correct Mode, follow the steps below:

- Choose the appropriate choice from the dropdown list next to IGMP mode
- Click on the **Update Setting** button (See 如下)

🙆 Management Switch		Multicast Current Table
🗄 🧰 System	IGMP Mode	Passive -
The Diagnostics	IGWIP INIQUE	Fassive V
E C Switching		Update Setting
E 🔂 Trunking		
🗄 🫅 STP/Ring	F	
🗋 🛅 VLAN	VLAN ID	
E 🔂 QoS	ICM III I	
E 🔂 SNMP	IGINP Version	3 💌
🗄 🛅 8021X	Fast Leave	Disable 💌
🗎 🧰 LLDP	Query Interval (10~18000)	
Others Protocols GVRP	Max Response Time (1~240)	
IGMP Snooping	Report Suppression	Enable 💌
- <u>NTP</u>		Update Setting
GMRP		opulate betting
DHCP Server		



Configuring IGMP Snooping General properties

To navigate to the IGMP Snooping page:

- 1. Click on the + next to **Other Protocols**.
- 2. Click on IGMP Snooping.

To configure the general features for IGMP Snooping in either the **Passive** or **Querier** mode, follow the steps below (see <u>Figure 100</u>):

- 1. From the dropdown list next to **VLAN ID**, choose the VLAN that you want the IGMP Snooping process to run on.
- 2. From the dropdown list next to **IGMP Version**, choose the correct IGMP version to be run on this VLAN. This setting must match the IGMP version being used by the IGMP querier and the IGMP client on the network.
- 3. Choosing the appropriate choice (Enable or Disable) from the dropdown list next to **Fast Leave**.
 - If this feature is enabled on the switch, and the switch receives a request to leave a multicast stream on a port, then the switch will drop this multicast stream on that port without checking to see if there are any other multicast clients on that port that might still be interested in receiving this multicast stream. This allows the multicast stream to disappear from a port much faster.

🏠 Management Switch		Multicast Current Table
E C System	IGMR Mode	Passiva w
	IGWIP MIDde	F assive
T C Switching		Update Setting
E C Trunking		
E C STP/Ring		
🗄 🧰 VLAN	VLAN ID	
🖽 🔂 QoS		
🗄 🧰 SNMP	IGMP Version	3 -
🖽 🛅 8021X	Fast Leave	Disable 💌
	Query Interval (10~18000)	
GVRP	Max Response Time (1~240)	
IGMP Snooping	Report Suppression	Enable 💌
- <u>NTP</u>		Update Setting
GMRP		(copulation of the second of t
DHCP Server		

1. Next, click on the **Update Setting** button



Configuring IGMP Passive Mode Specific properties

To navigate to the IGMP Snooping page:

- 1. Click on the + next to **Other Protocols**.
- 2. Click on IGMP Snooping.

To configure specific properties for IGMP Passive Mode, please follow the steps below.

🕼 Management Switch		Multicast Current Table
∃ 🛅 System ∃ 🛅 Diagnostics	IGMP Mode	Passive 💌
- Port - Constraint Switching		Update Setting
🗄 🛅 Trunking		
🗄 🫅 STP/Ring		
I 🧀 VLAN	VLAN ID	
	IGMP Version	3
- 3 SIMIF	Fast Leave	Disable 💌
	Query Interval (10~18000)	
Others Protocols GVRP	Max Response Time (1~240)	
IGMP Snooping	Report Suppression	Enable 💌
- <u>NTP</u>		Update Setting
GMRP		opuato octaing
DHCP Server		

Figure 101: IGMP Passive Mode

- 1. From the dropdown list next to **VLAN ID**, choose the VLAN for which you wish to configure the Report Suppression feature.
- 2. Choose **Enable** or **Disable** in the dropdown list next to **Report Suppression**. (Note: if the switch is not in **Passive** mode, then this feature will have no effect.)

Note: If you are using IGMP version 1 or 2, the **Query Interval**, and the **Max Response Time** setting must be configured even if you are not configuring IGMP Querier mode. For IGMP version 1 and 2, the membership registration timer (used to time out the membership status on each port) is based on these two parameters on the local switch. These two parameters should configure to match that of the current active IGMP Querier. The formula for the membership registration timer is: 2 X query-interval + max-responsetime = Timeout period.

Configuring IGMP Querier Mode Specific properties

To navigate to the IGMP Snooping page:

- 1. Click on the + next to **Other Protocols**.
- 2. Click on IGMP Snooping.

To configure specific properties for IGMP Querier Mode, follow the steps below (see <u>Figure 102</u>):

- 1. In the text box next to **Query Interval**, enter a value between 10 and 18000
 - This value will represent the time interval, in seconds, between any two queries that the switch scents on to the network. It is recommended that you use the default setting of 125 seconds that are according to the IGMP standard.
- 2. In the text box next to **Max Response Time**, enter a value between 1 and 240.
 - This value represents the maximum time in seconds that a multicast client will have to respond to an IGMP query. Any response received after this time will not be accepted by the Querier. It is recommended that you use the default setting of 10 seconds according to the IGMP standard.

Management Switch		Multicast Current Table
Circle System	IGMP Mode	Querier 💌
Contemport		Update Setting
Trunking		
Fin STP/Ring Fin VLAN	VLAN ID	
Hair QoS Hair SNMP	IGMP Version	3 💌
6 8021X	Fast Leave	Disable 💌
	Query Interval (10~18000)	
GVRP	Max Response Time (1~240)	
IGMP Snooping	Report Suppression	Enable 💌
- <u>NTP</u> - <u>GMRP</u>		Update Setting
DHCP Server		

Figure 102: Querier Mode Properties

Configuring IGMP Unknown Multicast Forwarding

To navigate to the **IGMP Snooping** page:

- 1. Click on the + next to **Other Protocols**.
- 2. Click on IGMP Snooping.

With IGMP enabled, the EtherWAN switch will transmit all multicast packets to their only multicast receiver ports. However, some multicast packets will not have any known multicast receiver ports either due to IGMP Snooping being disabled on the switch, or because no multicast receiver has sent IGMP requests for these multicast packets. The multicast packets in these scenarios are referred to as **unknown multicast packets**. You can use the **Passive Mode Forwarding Port** section of the IGMP Snooping configuration page to control how the switch will forward these unknown multicast packets under different IGMP Snooping modes of the switch (see Figure 103).

Disabled Mode Forwarding Port Configuration

When IGMP is in Disabled Mode, all multicast packets are unknown multicast packets, and by default all unknown multicast packets are forwarded to all the ports of the switch. To modify the default behavior and to control how the switch will forward unknown multicast packets when the switch is in **IGMP Snooping Disabled mode**:

- 1. Select either the **PassiveForwardMode** or the **ForceForwardMode** radio button.
- 2. Make sure that only the ports that you would like to have the **unknown multicast packets** to be forwarded to, have a check mark next to it.

					Pas	sive N	lode	Forwa	urding	Port				
Constraints of the server of	Port 1 Port 15 V Note port multic	Port 2 Port 16 If IG was no cast pa assive	Port 3 Port 17 WP st ot lear acket Forwa	Port 4 Port 18 Ø noopin ned, s to pas ardMo	Pas Port 5 Port 19 Ø ng is p witch ssive n ode	Port 6 Port 20 20 will for bode f	Vode Port 7 Port 21 21 mode orward corward	Forwa Port 8 Port 22 2 e and r d unkn ding p wardly	Port 9 Port 23 V router own ort. fode	Port 10 V Port 24 V	Port 11 Port 25 V	Port 12 Port 26	Port 13 Port 27 V	Port 14 Port 28
					_							Upda	ate Se	tting

3. Then click on the **Update Setting** button.

Figure 103: Disabled Mode Forwarding Port

Passive Mode Forwarding Port Configuration

You can control how the switch forwards unknown multicast packets under **IGMP Passive mode** in two different conditions:

- When there is no IGMP Querier port (a port that receives IGMP queries) present.
- When an IGMP Querier port is present **or** when no IGMP Querier port is present.

To configure how the switch forwards unknown multicast packets when the switch is in IGMP Passive mode, follow the steps below:

No IGMP Querier port present

- 1. Under the **Passive Mode Forwarding Port** section, select the **PassiveForwardMode** radio button.
- 2. Select the checkbox under the ports that you would like to have the **unknown multicast packets** forwarded to.
- 3. Click on the "Update Setting" button.

Note: The presence of an IGMP Querier port will make the settings provided by the **PassiveForwardMode** to have no effect, and all unknown multicast packets will be forwarded to the IGMP Querier port only.

			Pas	sive N	lode	Forwa	urding	Port				
SNMP 8021X LLDP Others Protocols GVRP IGMP Snooping NTP GMRP DHCP Server Port P 15 M Port P Port P 15 M Port P Port Port P Port Port Port Port Port Port Port Port	Port Por 2 3 Port Por 16 17 f IGMP as not lea st packet siveForw	Port 4 Port 18 moopin snoopin med, s to pas ardMo	Port 5 Port 19 mg is p witch sive n ode	Port 6 Port 20 assive will fo hode f	Port 7 Port 21 mode orward corward	Port 8 Port 22 and t 1 unkn ding p wardly	Port 9 Port 23 Port 23 couter own ort. fode	Port 10 Port 24	Port 11 Port 25	Port 12 Port 26	Port 13 Port 27	Port 14 Port 28

Figure 104: PassiveForwardMode

IGMP Querier port present or no IGMP Querier port present

- 1. Under the **Passive Mode Forwarding Port** section, select the **ForceForwardMode** radio button
- 2. Select the checkbox under the ports that you would like to have the **unknown multicast packets** forwarded to.
- 3. Click on the **Update Setting** button.

Note: The settings according to the **ForceForwardMode** will always be in effect both with and without the presence of an IGMP Querier port. In addition, when an IGMP Querier port is present, all unknown multicast packets will also be forwarded to the IGMP Querier port as well, in addition to the settings in the **ForceForwardMode** function.

Constraints of the second sec	Force Forwarding Port														
	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14	
				<u>m</u>					F		100				
	Port 15	Port 16	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	Port 25	Port 26	Port 27	Port 28	
<u>IGMP Snooping</u> <u>NTP</u> <u>GMRP</u> <u>DHCP Server</u>	Note: to for Passi © Pa	Force for for ve mo assive	e swit wardi de for Forwa	ch for ng por wardi ardMo	ward of the second seco	all unk setting rt setti Forc	mown g will t ing. ceForv	multic oggle wardlv	cast pa	acket		Upda	I ate Se	tting	

Figure 105: ForceForwardMode

IGMP Querier Mode Forwarding Port Configuration

To configure how the switch forwards unknown multicast packets when the switch is in IGMP Querier mode, follow the below instructions:

- 1. Under the **Passive Mode Forwarding Port** section, select the **ForceForwardMode** radio button
- 2. Select the checkbox under the ports that you would like to have the **unknown multicast packets** forwarded to.
- 3. Click on the **Update Setting** button.

Note: When the switch is in **IGMP Snooping Querier mode**, there will not be an IGMP Querier port present, and the settings according to the **ForceForwardMode** will always be in effect.

Qos SNMP Solution Solution	Force Forwarding Port													
	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14
	Port 15	Port 16	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	Port 25	Port 26	Port 27	Port 28
	15 16 17 18 19 20 21 22 23 24 23 20 27 26 Note: Force switch forward all unknown multicast packet to force forwarding port.this setting will toggle 10<												tting	

Figure 106: IGMP Querier Mode Forwarding

Monitoring Registered Multicast Groups

To navigate to the Multicast Current Table page:

- 1. Click on the + next to **Other Protocols**.
- 2. Click on IGMP Snooping.
- 3. Click on the **Multicast Current Table** link at the top of the page.

When the switch is in IGMP Passive **or** IGMP Querier mode, registered Multicast Groups can be monitored on each port, as well as the location of the IGMP Querier port (see <u>Figure 107</u>).

- All the registered multicast Groups will be listed in the **Group Address** column.
- The port where each registered Group ID was received can be found in the **Membership** column in each registered Groups corresponding row.

Note: when an IGMP Querier port is present, all registered multicast group IDs will show up in the **Membership** column as a checked box for the IGMP Querier port, even if an **IGMP Join** was never received for that Group ID on the Querier port.

n 🛄 System		Current Multicast Groups													
Diagnostics Diagnostics Diagnostics	VLAN ID	Group Address	Group	Membership	Route Port										
E 🗀 Trunking			Ports 1-8												
B- 🗀 STP/Ring B- 🗀 VLAN	1	01:00:5e:32:d9:05	Ports 9-28		ge4										
🗄 🧰 QoS			Ports 1-8												
- SNMP 	1	01:00:5e:7c:01:01	Ports 9-28		ge4										
" LLDP " Others Protocols			Ports 1-8												
- <u>GVRP</u> IGMP Snooping	1	01:00:5e:7ffffa	Ports 9-28		ge4										
<u>NTP</u> GMRP					Refresh										
DHCP Server															



IGMP Configuration Examples Using CLI Commands

For more information on CLI command usage see <u>CLI Command Usage</u>.

To put the IGMP Snooping feature in **Disabled Mode** use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: no ip igmp snooping

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no ip igmp snooping
switch_a(config)#q
switch_a#
```

To put the IGMP Snooping feature in **Passive Mode** use the CLI commands below:

CLI Command Mode: General Configuration Mode CLI Command Syntax: ip igmp snooping enable no ip igmp snooping querier

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip igmp snooping enable
switch_a(config)#no ip igmp snooping querier
switch_a(config)#q
switch_a#
```

To put the IGMP Snooping feature in **Querier Mode** use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: ip igmp snooping enable ip igmp snooping querier

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip igmp snooping enable
switch_a(config)#ip igmp snooping querier
switch_a(config)#q
switch_a#
```

To set the IGMP version per VLAN, use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: ip igmp version <1-3>

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp version 2
switch_a(config)#q
switch_a#

To enable or disable the IGMP fast-leave feature on a VLAN, use the CLI commands below:

CLI Command Mode: VLAN Interface Configuration Mode CLI Command Syntax: ip igmp snooping fast-leave no ip igmp snooping fast-leave

Usage Example - Enabling the IGMP fast-leave feature:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp snooping fast-leave
switch_a(config)#q
switch_a#
```

Usage Example - Disabling the IGMP fast-leave feature:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)#no ip igmp snooping fast-leave
switch_a(config)#q
switch_a#
```

To enable or disable the IGMP **Report Suppression** feature on a VLAN, use the CLI commands below:

CLI Command Mode: VLAN Interface Configuration Mode

CLI Command Syntax: ip igmp snooping report-suppression no ip igmp snooping report-suppression

Usage Example - Enabling the IGMP Report Suppression feature:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)# ip igmp snooping report-suppression
switch_a(config)#q
switch_a#
```

Usage Example - Disabling the IGMP Report Suppression feature:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)#no ip igmp snooping report-suppression
switch_a(config)#q
switch_a#
```

To configure the IGMP **query-interval**, and the **max-response-time** settings per VLAN, use the CLI commands below:

CLI Command Mode: VLAN Interface Configuration Mode

CLI Command Syntax: ip igmp query-interval <10-18000> ip igmp query-max-response-time <1-240>

Usage Example - Configuring the IGMP query-interval parameter:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)# ip igmp query-interval 125
switch_a(config)#q
switch_a#
```

Usage Example - Configuring the IGMP max-response-time parameter:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)# ip igmp query-max-response-time 10
switch_a(config)#q
switch_a#
```

To control how the switch forwards unknown multicast packets when the switch is in IGMP Disabled mode, follow the instructions below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: ip igmp snooping passive-forward all ip igmp snooping passive-forward none ip igmp snooping passive-forward <ifname>,<ifname>,

Usage Example - Flood all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward all
switch_a(config)#q
switch_a#
```

Usage Example - Drop all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward none
switch_a(config)#q
switch_a#
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward fel,fe2,fe3
switch_a(config)#q
switch_a#
```
To only control how the switch will forward unknown multicast packets when the switch is in IGMP Passive mode and also without a Querier Port present, follow the below instructions:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: ip igmp snooping passive-forward all ip igmp snooping passive-forward none ip igmp snooping passive-forward <ifname>,<ifname>

Usage Example - Flood all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward all
switch_a(config)#q
switch_a#
```

Usage Example - Drop all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward none
switch_a(config)#q
switch_a#
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward fel,fe2,fe3
switch_a(config)#q
switch_a#
```

To control how the switch will forward unknown multicast packets when the switch is in IGMP Passive mode, both with or without a Querier Port present, follow the instructions below:

CLI Command Mode: General Configuration Mode CLI Command Syntax: ip igmp snooping force-forward all ip igmp snooping force-forward none ip igmp snooping force-forward <ifname>,<ifname>,<ifname>

Usage Example - Flood all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward all
switch_a(config)#q
switch_a#
```

Usage Example - Drop all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward none
switch_a(config)#q
switch_a#
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward fel,fe2,fe3
switch_a(config)#q
switch_a#
```

To control how the switch will forward unknown multicast packets when the switch is in IGMP Querier mode, follow the below instructions:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: ip igmp snooping force-forward all ip igmp snooping force-forward none ip igmp snooping force-forward <*ifname*>,<*ifname*>,<*ifname*>,

Usage Example - Flood all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward all
switch_a(config)#q
switch_a#
```

Usage Example - Drop all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward none
switch_a(config)#q
switch_a#
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward fel,fe2,fe3
switch_a(config)#q
switch_a#
```

Network Time Protocol

NTP or Network Time Protocol is a useful tool designed to update your switch with the most accurate time available from a user specified time source. This is useful for the end user in that the switch logging is noted with the actual time rather than the default switch time (begins on Jan 1st, 2010) as it can aid debugging switching related problems by showing an accurate time an event occurred.

To navigate to the NTP page:

- 1. Click on the + next to **Other Protocols**.
- 2. Click on NTP

Enabling NTP

To enable the NTP client, follow the steps below (see Figure 108):

- 1. Choose Enable from the dropdown list next to NTP Status
- 2. Click on the **Update Setting** button

Setting the NTP Server IP Address

To provide a time source for the NTP client, follow the steps below:

- 1. Enter an IP address or host name in the **NTP Server** text box.
- 2. Click on the **Update Setting** button

Setting the Timezone

To change the timezone of the switch, follow the steps below:

- 1. Select the proper timezone from the dropdown list next to **Time Zone**.
- 2. Click on the **Update Setting** button

Setting the Polling Period

To alter the polling period (how often the NTP client checks the server for the correct time), follow the steps below:

1. Enter the new polling period in the Polling Interval textbox.

2. Click on the **Update Setting** button

Manually Syncing Time

To set the time immediately using an NTP server, follow the steps below:

- 1. Enter the new polling period in the Polling Interval textbox.
- 2. Click on the **Sync Time** button in the **NTP Server** field

	NTP Setting		
NTP Status	Enable ‡		
NTP Server (IP Address or Domain Name)	time-a.nist.gov	Sync Time	
Time Zone	(GMT-06:00) Central Time (US & Canada)		
Current Time	Thu Mar 27 12:42:43 CST 2014		
Polling Interval (1-10080 min)	60		
		Update Setting	

Figure 108: NTP Settings

Daylight Savings Time - Weekday Mode

To adjust the switch's clock for Daylight Savings Time using the weekday mode, follow the steps below:

- 1. Select the option **Weekday** from the **Daylight Saving Mode** dropdown box.
- 2. Enter the value for the time offset in the Time Set Offset textbox.
- 3. Enter the name of the **Daylight Saving Timezone**.
- 4. In the Weekday Box, select the month, week, day, hour, and minute for both the

from and to fields. For example, if Daylight Saving Time begins on the second

Sunday in March at 2:00AM and ends on the first Sunday in November at 2:00AM,

then select the values as shown in Figure 109.

5. Click on the **Update Setting** button

(i)	Daylight Saving Setting
Daylight Saving Mode	Weekday ‡
Time Set Offset (1-480 min)	60
Name of Daylight Saving Timezone	CDT
weeкday From To	Month Mar Week 2 Day Sun Hour 2 Minute 0 Month Nov Week 1 Day Sun Hour 2 Minute 0
Date From To	Month Jan + Day Hour Minute Month Jan + Day Hour Minute
	Update Settin

Figure 109: Daylight Savings – Weekday Mode

Daylight Savings Time – Date Mode

To adjust the switch's clock for Daylight Savings Time using the date mode, follow the steps below:

- 1. Select the option **Date** from the **Daylight Saving Mode** dropdown box.
- 2. Enter the value for the time offset in the **Time Set Offset** textbox.
- 3. Enter the name of the **Daylight Saving Timezone**.
- 4. In the **Date section**, select the month and enter the date, hour, and minute for both the from and to fields. For example, if Daylight Saving Time begins on March 9th at 2:00AM and ends on November 2nd at 2:00AM, then select the values as shown in <u>Figure 110</u>.
- 5. Click on the **Update Setting** button

	Daylight Saving Setting
Daylight Saving Mode	Date ‡
Time Set Offset (1-480 min)	60
Name of Daylight Saving Timezone	CDT
Weekday From To	Month Jan Week Day Sun Hour Minute Month Jan Week Day Sun Hour Minute Minute
Date From To	Month Mar + Day 9 Hour 2 Minute 0 Month Nov + Day 2 Hour 2 Minute 0
	Update Setting

Figure 110: Daylight Savings – Date Mode

Network Time Protocol Configuration Examples Using CLI Commands

For more information on CLI command usage see <u>CLI Command Usage</u>.

To enable NTP on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: ntp enable

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)#ntp enable
switch_a(config)#q
switch_a#

To set the NTP server on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: ntp server <IP Address or Host Name of NTP Server>

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)#ntp server 192.168.1.126
switch_a(config)#q
switch_a#

To set the NTP polling interval on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: ntp polling-interval <time in minutes, 1-10080>

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)#ntp polling-interval 180

```
switch_a(config)#g
switch_a#
```

To have the NTP client sync the clock immediately on the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: ntp sync-time

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ntp sync-time
switch_a(config)#q
switch_a#
```

To set the current time zone for the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: clock timezone <Name of Time Zone> <UTC Offset in hh:mm format>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#clock timezone CDT -6:00
switch_a(config)#q
switch_a#
```

To set the Daylight Savings Time settings using weekday mode for the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax:

clock summer-time <Name of Time Zone> weekday <start week number> <start day> <start month> <start hour> <start minute> <end week number> <end day> <end hour> <end minute> <time offset in minutes>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# clock summer-time CDT weekday 2 Sun March 2
0 1 Sun November 2 0 60
switch_a(config)#q
switch_a#
```

To set the Daylight Savings Time settings using date mode for the EX24000 Switch, use the CLI commands below:

CLI Command Mode: General Configuration Mode

CLI Command Syntax:

```
clock summer-time <Name of Time Zone> date <start date> <start month> <start hour> <start minute> <end date> <end month> <end hour> <end minute> <time offset in minutes>
```

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# clock summer-time CDT date 9 March 2 0 2 November 2
0 60
switch_a(config)#q
switch_a#
```

GMRP

The settings in the GMRP feature controls how the switch automates the process of multicast packet forwarding, both within a single switch as wells as between switches in a bridged network. With the GMRP feature enabled, when the switch receives any GMRP multicast group registration requests from either a multicast client or a neighbor switch, the switch will register these multicast groups on these ports and will only transmit the multicast packets that belong to these groups to these ports. The switch will also automatically propagate these multicast group registrations onto the neighbor switches to allow the neighbor switches to forward the multicast packets that belong to these groups to the packets that belong to the neighbor switches to forward the multicast packets that belong to these groups to the sufficient of these groups to the set of the neighbor switches to forward the multicast packets that belong to these groups to the local switch.

To navigate to the Other Protocols / GMRP page:

- 1. Click on the + next to **Other Protocols**.
- 2. Click on **GMRP**.

General Overview

The ports on the EtherWAN switch can be configured with the GMRP feature in five modes:

- Disabled
- Normal
- Fixed
- Forbidden
- Forward All.

GMRP Normal mode

When a port is put in GMRP **Normal** mode, that port can accept both multicast group registration and multicast group deregistration from the multicast client or the neighbor switch that is residing on that port. Also, the switch will propagate all the registered multicast groups on the switch to the neighbor switch residing on that port.

GMRP Fixed mode

When a port is put in GMRP **Fixed** mode, that port can accept group registration but will not accept any group deregistration from multicast clients or neighbor switches that reside on that port. Also, the switch will be propagating all the registered multicast groups on the switch to the neighbor switch residing on that port.

GMRP Forbidden mode

When a port is put in GMRP **Forbidden** mode, all multicast groups will be deregistered on that port and that port will not be accepting any further multicast group registrations. However, the switch will still be propagating all the registered multicast groups on the switch to the neighbor switch residing on that port.

GMRP Forward All mode

When a port is put in GMRP **Forward All** mode, all the registered multicast groups on the switch will automatically be registered to this port, so the switch will be forwarding all the multicast packets that belong to these groups to this port and this port will also be propagating all the registered multicast groups on the switch to the neighbor switch residing on that port.

GMRP Disabled mode

When a port is put in GMRP **disabled** mode that port will not participate in any GMRP activities.

Enabling the GMRP Feature Globally on the Switch

To navigate to the **Other Protocols / GMRP** page:

- 1. Click on the + next to **Other Protocols**.
- 2. Click on **GMRP**.

To enable the GMRP function in the switch, follow the procedure below:

- 1. Choose the Enable option from the dropdown list next to GMRP
- 2. Click on the Update Setting button. (See Figure 111)

Diagnostics	[
D Port	GMRP		Disable	Disable Vpdate Setting		
Switching						
STP/Ring	<u>I.</u>			9		
VLAN	Per Por	t Setting (Include	LAG)			
QoS SNMP	Port	GMRP	GMRP Registration	GMRP Forward		
802.1X	fe1	Disable 💌	Normal 💌	Disable 👻		
Others Protocols	fe2	Disable 💌	Normal 💌	Disable 😽		
GVRP	fe3	Disable 💌	Normal 🖌	Disable 👻		
IGMP Snooping	fe4	Disable 💌	Normal 🖌	Disable 🛩		
NTP	fe5	Disable 💌	Normal 💌	Disable 💌		
- <u>GMRP</u> - <u>DHCP Server</u>	fe6	Disable 🛩	Normal 💌	Disable 💙		
	fe7	Disable 🖌	Normal 🔽	Disable 🖌		
	fe8	Disable 💌	Normal 💌	Disable 💌		
	fe9	Disable 💌	Normal 💌	Disable 💌		
	fe10	Disable 💙	Normal 💌	Disable 😽		
	fe11	Disable 🚩	Normal 💌	Disable 🛩		
	fe12	Disable 💌	Normal 👻	Disable 👻		
	fe13	Disable 💌	Normal 💌	Disable 💌		
	fe14	Disable 💌	Normal 💌	Disable 💙		
	fe15	Disable 🖌	Normal 💌	Disable 👻		
	fe16	Disable 💌	Normal 💌	Disable 💌		
	ge1	Disable 💌	Normal 💌	Disable 💌		
	ge2	Disable 💌	Normal 💌	Disable 🖌		
]	Update Setting		

Figure 111: GMRP Global Setting

Configuring the GMRP Feature Per Port

To navigate to the **Other Protocols / GMRP** page:

1. Click on the + next to **Other Protocols**.

2. Click on **GMRP**.

GMRP should be enabled on all the ports that could be a potential source of multicast traffic, and on the ports that are connected to multicast clients. You can also further configure each GMRP enabled port with the particular application modes described in the below configuration.

To allow a port to dynamically receive GMRP multicast group registrations and dynamically transmit the multicast packets that belong to these multicast groups on this port configure the items listed below:

- For each port that you wish to apply this application, select the **Enable** option from the drop-down list under the GMRP column.
- For each port that you wish to apply this application, select the **Normal** option from the drop-down list under the GMRP Registration column.
- For each port that you wish to apply this application, select the **Disable** option from the drop-down list under the GMRP Forward All column.
- Click on the **Update Setting** button.

To allow a port to dynamically receive GMRP multicast group registrations and then make the multicast packets that belong to these multicast groups constantly available on this port, configure the items listed below:

- For each port that you wish to apply this application, select the **Enable** option from the drop-down list under the GMRP column.
- For each port that you wish to apply this application, select the **Fixed** option from the drop-down list under the GMRP Registration column.
- For each port that you wish to apply this application, select the **Disable** option from the drop-down list under the GMRP Forward All column.
- Click on the **Update Setting** button.

If you do not wish to transmit any multicast packets on a port based on the received GMRP multicast group registrations on that port, but would like to receive multicast packets that belong to the currently registered multicast groups on the switch on that port, configure the items listed below:

- For each port that you wish to apply this application, select the **Enable** option from the drop-down list under the GMRP column.
- For each port that you wish to apply this application, select the **Forbidden** option from the drop-down list under the GMRP Registration column.

- For each port that you wish to apply this application, select the **Disable** option from the drop-down list under the GMRP Forward All column.
- Click on the **Update Setting** button.

If you wish to transmit all the multicast packets that belong to all the currently registered multicast groups on the switch on a port, configure the items listed below:

- For each port that you wish to apply this application, select the "**Enable**" option from the drop-down list under the GMRP column.
- For each port that you wish to apply this application, select the appropriate option from the drop-down list under the GMRP Registration column, according to the previous instructions.
- For each port that you wish to apply this application, select the **Enable** option from the drop-down list under the GMRP Forward All column.
- Click on the **Update Setting** button.

If you do not want a port to participate in the GMRP protocol, configure the items listed below:

- For each port that you wish to apply this application, select the **Disable** option from the drop-down list under the GMRP column.
- Click on the **Update Setting** button.

GMRP Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

To enable or disable GMRP globally on the EtherWAN switch, use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: set gmrp enable bridge 1 set gmrp disable bridge 1

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)# set gmrp enable bridge 1
switch_a(config)# set gmrp disable bridge 1
switch_a(config)#q
switch a#

To enable GMRP locally on a port on the EtherWAN switch, you must use the below CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: set port gmrp enable <port id> set port gmrp enable <port id>

Usage Example:

switch_a>enable
switch_a#configure terminal
switch_a(config)# set port gmrp enable fe1
switch_a(config)# set port gmrp disable fe1
switch_a(config)#q
switch_a#

When you enable GMRP on a port, the **Registrar** is in **Normal** mode by default. The GMRP **Registrar** on a port can be configured in 3 different modes by issuing the following CLI commands

CLI Command Mode: General Configuration Mode

CLI Command Syntax: set gmrp registration normal <port id> set gmrp registration fixed fe1 <port id> set gmrp registration forbidden <port id>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#set gmrp registration normal fe1
switch_a(config)#set gmrp registration fixed fe1
switch_a(config)#set gmrp registration forbidden fe1
switch_a(config)#q
switch_a#
```

By default when you enable GVRP on a port this feature is disabled To enable or disable the **Forward All** feature on a port, use the following CLI commands:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: set gmrp fwdall enable <port id> set gmrp fwdall disable <port id>

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#set gmrp fwdall enable fe1
switch_a(config)#set gmrp fwdall disable fe1
switch_a(config)#q
switch_a#
```

DHCP Server

DHCP is a TCP/IP application protocol that allows any TCP/IP device to dynamically obtain its initial TCP/IP configurations through the TCP/IP protocol itself (in this case, through the UDP protocol). It is based on the client-server paradigm. The EtherWAN switch can be setup as a DHCP server to allow any DHCP client to dynamically obtain its IP address, default router, and DNS servers.

General Overview

The EtherWAN switch can function as a DHCP server for a single VLAN (it can be any VLAN) on the switch. When functioning as a DHCP server, the EtherWAN switch can be configured with a range of IP addresses, default gateway and DNS servers, which will allow the switch to use the dynamic configuration function of the DHCP protocol to provide any TCP/IP device that is a DHCP client, to dynamically obtain an IP address, default router, and DNS servers. The EtherWAN DHCP server can also be configured with a lease period that the DHCP clients are allowed the use of their assigned IP address. In this simple implementation, both the DHCP Client and the DHCP Server must be on the same network (same VLAN).

Configuring the DHCP Server

To navigate to the DHCP Server page:

- 1. Click on the + next to Other Protocols
- 2. Click on DHCP Server (see Figure 112)

You can use the GUI to set the following DHCP server parameters:

- DHCP Server Enable
- DHCP VLAN.
- DHCP Client Parameters
 - o IP Address range
 - o Subnet Mask
 - o Default gateway
 - Primary and Secondary DNS.
- DHCP Client lease time

To set the DHCP server parameters:

- 1. From the drop-down list next to **DHCP Server Status**, select the VLAN that will get the DHCP provided TCP/IP Parameters.
- 2. Enter the starting and ending IP addresses for the DHCP Client IP address range, in the text boxes next to **Start IP** and **End IP**.
- 3. Enter the Subnet Mask in the text box next to Subnet Mask.
- 4. Enter the IP address for the DHCP Client default router in the text entry box next to **Gateway**.
- 5. Enter the IP addresses for the DHCP Client primary and secondary DNS servers, in the text entry box next to **Primary DNS** and **Secondary DNS**.
- 6. Enter the lease period in seconds, which the DHCP clients are allowed the use of their leased IP addresses, in the text entry box next to **Lease Time**.
- 7. Click on the **Update Setting** button.

System	DHCP Server Status	1	VI AN0100	
Port Diagnostics	DHCP Server General Setting			
🕀 🗀 Switching	Start IP 192.168.7.100		192.168.7.100	
C Trunking	End IP	2	192.168.7.107	
 VLAN QoS SNMP \$02.1X LLDP Others Protocols <u>GVRP</u> IGMP Snooping NTP GMRP 	Subnet Mask	3	255.255.255.0	
	Gateway	4	192.168.7.1	
	Primary DNS	-	5.6.7.8	
	Secondary DNS	9		
	Lease Time	6	86400 (0 to 864000,86400:default)	
			7 Update Sett	

Figure 112: DHCP Server

To check what IP addresses has been allocated to which DHCP clients:

- 1. Click on the DHCP Binding Table link (see Figure 113)
- 2. Click on the DHCP General Setting link to get back to the previous DHCP configuration Web GUI page (see <u>Figure 114</u>).

Management Switch		DHCP Binding Table		
 Diagnostics 	DHCP Server Status	VLAN0100 V		
🗄 🫅 Port	DHCP Server General Setting			
🗄 🧰 Switching	Start IP	192.168.7.100		
Trunking	End IP	192.168.7.107		
Image: Simple simple	Subnet Mask	255.255.255.0		
	Gateway	192.168.7.1		
	Primary DNS	1.2.3.4		
	Secondary DNS	5.6.7.8		
Others Protocols GVRP GO RP Security	Lease Time	86400 (0 to 864000,86400:default)		
- <u>NTP</u> - <u>GMRP</u>		Update Setting		
"" <u>DHCP server</u>				

Figure 113: DHCP Bindings

Management Switch				DHCP General Setting			
🗄 🧰 System	DHCP Binding Table						
Diagnostics	Mac Address IP-Address Expires In						
E C Switching	a4:ba:db:de:d6:2f	192.168.7.100	23 hours, 58 minutes, 0 seconds				
E 🛅 Trunking				Refresh			
E 🔂 STP/Ring				Rendon			
🗄 🛅 VLAN							
🗄 🧰 QoS							
🗉 🛅 SNMP							
🖻 🛅 802.1X							
🗄 🛅 LLDP							
🖻 Others Protocols							
GVRP							
IGMP Snooping							
NTP							
GMRP							
DHCP Server							

Figure 114: DHCP Binding Table

DHCP Configuration Examples Using CLI Commands

For more information on CLI command usage see <u>CLI Command Usage</u>.

To set the DHCP server parameters:

CLI Command Mode: General Configuration Mode

CLI Command Syntax: dhcp-server range <start IP> <end IP> dhcp-server subnet-mask <subnet mask in doted decimal notation> dhcp-server gateway <IP address> dhcp-server dns 1 <IP address> dhcp-server dns 2 <IP address> dhcp-server lease-time <0-864000>

```
switch_a> enable
switch_a#configure terminal
switch_a(config)#dhcp-server range 192.168.7.100 192.168.7.107
switch_a(config)#dhcp-server subnet-mask 255.255.255.0
switch_a(config)#dhcp-server gateway 192.168.7.1
switch_a(config)#dhcp-server dns 1 1.2.3.4
```

```
switch_a(config)#dhcp-server dns 2 5.6.7.8
switch_a(config)#dhcp-server lease-time 86400
switch_a(config)#q
switch_a#
```

To enable the DHCP server and set the DHCP VLAN:

CLI Command Mode: Interface Configuration Mode CLI Command Syntax: dhcp-server enable; no dhcp-server enable

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)#interface vlan1.100
switch_a(config-if)#dhcp-server enable
switch_a(config-if)#no dhcp-server enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

To check what IP addresses has been allocated:

CLI Command Mode: enable CLI Command Syntax: show dhcp-server binding

```
switch_a> enable
switch_a#show dhcp-server binding
Mac Address IP-Address Expires in
a4:ba:db:de:d6:2f 192.168.7.100 23 hours, 57 minutes, 15
seconds
switch a#
```

EtherWAN Corporation 17595 Mount Hermann Street Fountain Valley, CA. 92708 Phone: 714.885.6000 www.EtherWAN.com

EtherWAN has made a good faith effort to ensure the accuracy of the information in this document and disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties, except as may be stated in its written agreement with and for its customers.

EtherWAN shall not be held liable to anyone for any indirect, special or consequential damages due to omissions or errors. The information and specifications in this document are subject to change without notice.

Copyright © 2014. All Rights Reserved. All trademarks and registered trademarks are the property of their respective owners.

EtherWAN User Guide

December 16, 2014

Document version: Version 1