



COMMANDO Soldier E3000 Series Managed Switch Web GUI Guide

SoldierOS Version 3K.v1.10 onwards

© 2024 COMMANDO Networks Inc., USA and/or its affiliates. All rights reserved.
No part of this document may be reproduced or transmitted in any form or by any
means without prior written consent of COMMANDO Networks Inc., USA.

Trademarks and Permissions

COMMANDO Networks trademarks are trademarks of COMMANDO Networks Ltd and/or its affiliates. The COMMANDO trademarks, service marks ("Marks") and other COMMANDO trademarks are the property of COMMANDO Networks. COMMANDO Soldier Switch Series products are trademarks or registered trademarks of COMMANDO Networks Ltd. You are not permitted to use these Marks without the prior written consent of COMMANDO Networks. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between COMMANDO Networks and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS-IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

TABLE OF CONTENTS

Introduction

1.COMMANDO Solider OS

1.1 Web Interface

1.2 Menu Description

2. Status

2.1 System Information.....

2.2 Logging Message.....

2.3 Port

2.3.1Statistics

2.3.2 Error Disabled

2.3.3Bandwidth Utilization

2.4 Link Aggregation.....

2.5 MAC Address Table.....

3. Network

3.1 DNS.....

3.2 Hosts.....

4. Port

4.1 Port Setting.....

4.2 Link Aggregation.....

4.2.1 Group

4.2.2 Port Setting.....

4.2.3 LACP.....

4.3 EEE.....

4.4 Jumbo Frame.....

4.5 Port Security.....

4.6 Protected Port.....

4.7 Storm Control.....

5. VLAN

5.1 VLAN.....	
5.1.1 Create VLAN	
5.1.2 VLAN Configuration.....	
5.1.3 Membership.....	
5.1.4 Port Setting.....	
5.2 Voice VLAN.....	
5.2.1 Property.....	
5.2.2 Voice OUI.....	
5.3 Protocol VLAN.....	
5.3.1 Protocol Group.....	
5.3.2 Group Binding	
5.4 MAC VLAN.....	
5.4.1 MAC Group.....	
5.4.2 Group Binding	
5.5 Surveillance VLAN.....	
5.5.1 Property.....	
5.5.2 Surveillance OUI.....	
5.6 GVRP.....	
5.6.1 Property.....	
5.6.2 Membership.....	

6. MAC Address Table

6.1 Dynamic Address.....	
6.2 Static Address.....	
6.3 Filtering Address.....	
6.4 Port Security Address.....	

7. Spanning Tree

7.1 Property.....	
7.2 Port Setting.....	
7.3 MST Instance.....	
7.4 MST Port Setting.....	

7.5 Statistics.....

8. Discovery

8.1 LLDP.....

8.1.1 Port Setting.....

8.1.2 MED Network Policy.....

8.1.3 MED Port Setting.....

8.1.4 Packet View.....

8.1.5 Local Information.....

8.1.6 Neighbor.....

8.1.7 Statistics.....

9. DHCP

9.1 Property.....

9.2 IP Pool Setting.....

9.3 VLAN IF Address Group Setting.....

9.4 Client List.....

9.5 Client Static Binding Table.....

10. Multicast

10.1 General.....

10.1.1 Property.....

10.1.2 Group Address.....

10.1.3 Router Port.....

10.1.4 Forward All.....

10.1.5 Throttling.....

10.1.6 Filtering Profile.....

10.1.7 Filtering Binding.....

10.2 IGMP Snooping.....

10.2.1 Property

10.2.2 Querier.....

10.2.3 Statistics.....

10.3 MLD Snooping.....

- 10.3.1 Property.....
- 10.3.2 Statistics.....
- 10.4 MVR.....
- 10.4.1 Property.....
- 10.4.2 Port Setting.....
- 10.4.3 Group Address.....

11. Routing

- 11.1 IPv4 Management and Interfaces.....
- 11.1.1 IPv4 Interface.....
- 11.1.2 IPv4 Routes.....
- 11.1.3 ARP.....
- 11.2 IPv6 Management and Interfaces.....
- 11.2.1 IPv6 Interface.....
- 11.2.2 IPv6 Addresses.....
- 11.2.3 IPv6 Routes.....
- 11.2.4 IPv6 Neighbors.....
- 11.3 RIP Routes Management.....
- 11.3.1 RIP Routes Setting
- 1.4 OSFP Routes Management.....
- 11.4.1 OSFP Routes Setting

12. Security

- 12.1 RADIUS.....
- 12.2 TACACS+.....
- 12.3 AAA.....
- 12.3.1 Method List.....
- 12.3.2 Login Authentication.....
- 12.4 Authentication Manager.....
- 12.4.1 Property.....
- 12.4.2 Port Setting.....
- 12.4.3 MAC-Based Local Account.....
- 12.4.4 WEB-Based Local Account.....

- 12.4.5 Sessions
- 12.5 DoS.....
- 12.6 Dynamic ARP Inspection.....
- 12.7 DHCP Snooping.....
- 12.7.1 Property.....
- 12.7.2 Statistics.....
- 12.7.3 Option82 Property.....
- 12.7.4 Option82 Circuit ID.....
- 12.8 IP Source Guard.....
- 12.9.1 IMPV Binding.....
- 12.9.2 Save Database.....

13. ACL

- 13.1 MAC ACL.....
- 13.2 MAC ACE.....
- 13.3 IPv4 ACL.....
- 13.4 IPv4 ACE.....
- 13.5 IPv6 ACL.....
- 13.6 IPv6 ACE.....
- 13.7 ACL Binding.....

14. QoS

- 14.1 General.....
- 14.1.1 Property.....
- 14.1.2 Queue Scheduling.....
- 14.1.3 CoS Mapping.....
- 14.1.4 DSCP Mapping.....
- 14.1.5 IP Precedence Mapping.....
- 14.2 Rate Limit.....
- 14.2.1 Ingress / Egress Port.....
- 14.2.2 Egress Queue.....

15. Diagnostics

- 15.1 Logging.....
- 15.1.1 Property.....
- 15.1.2 Remote Server.....
- 15.1.3 Mirroring.....
- 15.1.4 Ping.....
- 15.1.5 Trace route.....
- 15.1.6 Copper Test.....
- 15.1.7 Fiber Module.....
- 15.2 UDLD
- 15.2.1 Property.....
- 15.2.2 Neighbor.....

16. Management

- 16.1 User Account.....
- 16.2 Management Access.....
- 16.2.1 Management VLAN.....
- 16.2.2 Management Service.....
- 16.2.3 Management ACL.....
- 16.2.4 Management ACE.....
- 16.3 Firmware.....
- 16.3.1 Upgrade.....
- 16.3.2 Active Image
- 16.3 Configuration.....
- 16.4.1 Upgrade.....
- 16.4.2 Save Configuration.....
- 16.5 SNMP
- 16.5.1 View.....
- 16.5.2 Group.....
- 16.5.3 Community.....
- 16.5.4 User.....
- 16.5.5 Engine ID.....
- 16.5.6 Trap Event.....
- 16.5.7 Notification.....

16.6 RMON.....

16.5.1 Statistics.....

16.5.2 History.....

16.5.3 Event.....

16.5.4 Alarm.....

16.6 Restore Factory Default.....

17. POE

17.1 PoE Port Setting.....

17.2 PoE Port Schedule Setting.....

Chapter 1 Introduction

COMMANDO Soldier E3000 Series Switches offers a state of art quality product that can serve on real time high-speed Performance with input power AC as well as DC, covers larger physical distance up to 250 meters with copper cables as compared to other brands best switches. This series is having advance L3 features, which are highly reliable, conformance to international open standards, durable, serviceable, aesthetics, perceived quality, enhanced performance with larger range with copper cables and usability leads to value to money. Easy Management via lots of options like RIP V1/2, OSPF, Advanced Web-based Graphical User Interface (Web GUI), Industry standard Command Line interface (CLI), RADIUS/TACACS+, LLDP/LLDP-MED, Time based PoE/PoE+ Scheduling, DHCP server as well as zero touch provisioning whichever is suitable to our esteem customers.

COMMANDO Soldier E3000 Series switches are L3 Aggregation and Access Series Routing Switches are fully managed L3 having 4, 24 and 48 GE switch ports or 24/48 SFP ports with perpetual PoE/PoE+ IEEE 802.3 af/at (15.4W, 30W) compliant or Non PoE models plus additional fixed 10G or 1G fiber/ 10GE or 1GE copper uplink ports as per requirement with perpetual PoE/PoE+ for no power downtime required for network resiliency and high availability which delivering robust performance and intelligent switching for growing networks. This series switches are easy to deploy, use, manage and designed exclusively for enterprise-class aggregation layer and as edge networks Switches, specially built for Security, IoT, and Cloud networking needs of growing businesses, high-end campus networks for Small-Medium Business (SMB). Designed for operational simplicity to lower total cost of ownership, they enable scalable, secure, and energy-efficient business operations with intelligent and automated services. This intelligent managed routing switches designed for networks requiring High performance, High port density, High uplink bandwidth, Flexibility, Fault Tolerance, and Advanced Software features for maximum Return on Investment (ROI). Switch models are designed for full PoE capability on all ports, power and fan redundancy, Layer 3 feature support static and dynamic routing, these are optimized for today's surveillance, mobile and IoT needs. Designed for operational simplicity to lower total cost of ownership, they enable scalable, secure, and energy-efficient business operations with intelligent and automated services.

It has high performance fixed uplink with fiber/copper 10G, 1G/10GE, 1GE ports fixed uplink which helps it to meet the requirement of high-end campus LAN, Metro/Enterprise networks. Each switch is capable to deliver 15.4W PoE and 30W PoE+ along with automated power (ON/OFF) scheduling with perpetual IEEE 802.3af compliant PoE (Power over Ethernet), 802.3at compliant PoE+ (Power over Ethernet plus) and having power budget up to 800W. Switches are PoE/PoE+ capable to provide power across all access ports for wireless APs, security cameras, and other IoT devices which are used in surveillance. These switches are powerful and flexible enough for users to deploy PoE/PoE+ standard supplies up to 30W of power per port which is backward compatible with 15.4W PD which makes it ideal for applications using high power wireless access points, PTZ (Pan Tilt Zoom) IP cameras, Surveillance cameras, VoIP telephony systems, kiosks, POS terminals, thin client, 802.11ac and 802.11ax access points, small cells, and connected LED lighting devices over longer distances up to 250 meters. It's software includes OSPF, RIP, Static route, QoS Traffic classification based on Layer 2, Layer 3, Layer 4, and priority information Actions including ACL, CAR, and re-marking, Queue scheduling modes such as PQ, WFQ and PQ+WRR, Congestion avoidance mechanisms, including WRED and tail drop, Traffic shaping, SNMPv1/v2c/v3, Zero Touch Provisioning (ZTP), 802.1x authentication, RADIUS and TACACS+ authentication for login, DoS, ARP, MAC address attacks, broadcast storms, and heavy-traffic and ICMP attack defenses, Remote Network Monitoring (RMON).

These switches have advanced Security features, and advanced Quality of Service (QoS), ideal for all organizations considering reliable, affordable hardware with well-known CLI and simple Web managed real time interface. Automated PoE/PoE+ scheduling, Scripting capabilities, Layer 3 routing, Automatic MDIX and Auto-negotiation on all ports select the right transmission modes (half or full duplex) as well as data transmission for crossover or straight-through cables dynamically. Moreover, with its innovative energy-efficient technology, can save up to 58% of power consumption, making it an eco-friendly perfect solution for your business network. These switches come with lifetime free software upgrades and patching to enhance features and supports patching, which provides fixes for critical bugs and security vulnerabilities between regular maintenance upgrades. This support allows customers to add new features and upgrades without having to pay a single dollar.

It has a 4K-entry VLAN table which provides VLAN classification according to port-based, protocol-and-port-based, MAC-based, and Flow-based capability. It also supports IVL (Independent VLAN Learning), SVL (Shared VLAN Learning), and IVL/SVL (both Independent and Shared VLAN Learning) for flexible network topology architecture. It provides IEEE802.1ad (Q-in-Q) for double tag insertion and removal function. In addition, VLAN translation function is also supported for Metro Ethernet applications with up to 32K entries L2 MAC table are supported with 2-left 4-way hashing algorithm which can effectively reduce collision ratio. An independent 4K-entry Multicast table is used to support Multicast functions, such as IGMP snooping. The device supports a 4K-entry VLAN/Ingress/Egress Access Control List (ACL). The ACL function supports L2/L3/L4 match fields and performs configurable actions, such as Drop/Permit/Redirect/Mirror /Logging/Policing/Ingress VLAN conversion/Egress VLAN conversion/QoS remarking/VLAN tag status assignment. Per-port ingress/egress bandwidth control and per-queue egress bandwidth control are supported. The device provides three types of packet scheduling, including SP (Strict Priority), WFQ (Weighted Fair Queuing), and WRR (Weighted Round Robin). Each port has 8 physical queues, and each queue provides a leaky bucket to shape the incoming traffic into the average rate behavior. The Broadcast/Multicast/Unknown-Multicast/Unknown-Unicast storm suppression function can inhibit external and internal malicious attacks. The device supports 4-sets of port mirror configurations to mirror ingress and egress traffic. RSPAN, sFlow are also supported for traffic monitoring purposes. For network management purposes, complete MIB counters are supported to provide forwarding statistics in real time. The link aggregation function enhances link redundancy and increases bandwidth linearly. It offers robust QoS to optimize traffic on your Business Network, these switches provide (Port-based/802.1p/DSCP) QoS to keep latency-sensitive video and voice traffic jitter-free moving smoothly. Additionally, port-based, tag-based VLAN, Voice VLANs can improve security and meet more network segmentation requirements. This series switches also have provisioning of QOS, Static and dynamic routing for IPV6 clients.

Simplified Configuration and Management

Zero-Touch Provisioning (ZTP) simplifies installation of the switch.

Easy to manage via Console/web-Based Management (Web GUI) / Telnet / SSH / HTTPS.

Remote Manageability

Remote management is the process that allows the administrators to take full control of all operations using a remote. This remote management via Web GUI / Telnet / SSH / HTTPS will reduce time and money spent on management and maintenance and physical presence of Network Engineer.

Management by CLI - Console, Telnet (RFC854) up to 3 sessions

Management by Web GUI - HTTP, HTTPS for management Based on Remote Configuration and maintenance Using Telnet.

In this CLI guide we will understand Management by Command Line Interface (CLI) through console port, telnet management mode.

Accessing the Switch via console port

How to Login COMMANDO Series E3000 via console port?

The console interface is used by connecting the Switch to a VT100-compatible terminal or a computer running an ordinary terminal emulator program (e.g., the Hyper Terminal program included with the Windows operating system) using an RS-232C serial cable. Your terminal parameters will need to be set to:

- VT-100 compatible
- 115200 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

Users may also access the same functions over a Telnet interface. Once you have set an IP address for your Switch, you can use a Telnet program (in VT-100 compatible terminal mode) to access and control the Switch. All the screens are identical, whether accessed from the console port or from a Telnet interface.

Step 1: Connect the Switch console port with PC/Laptop via console cable.

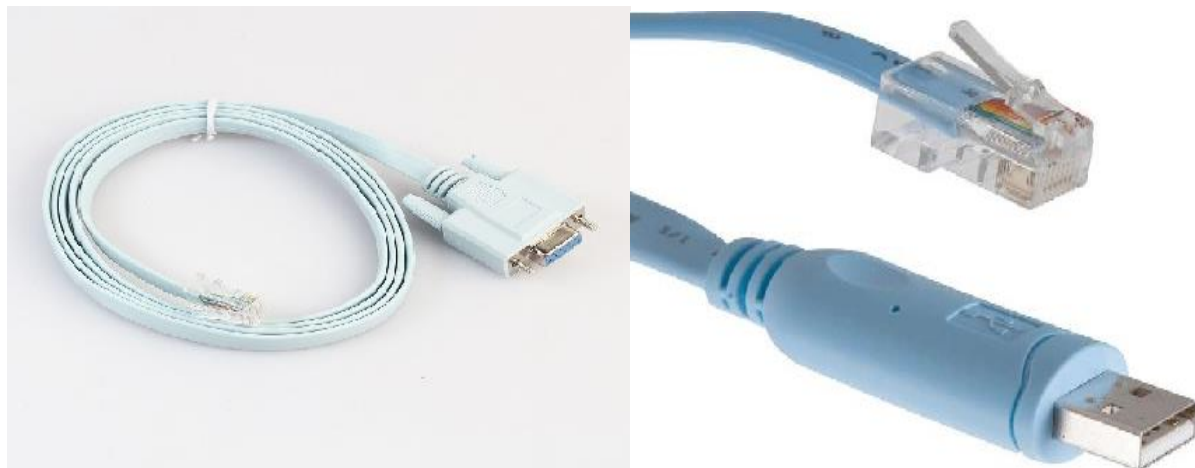
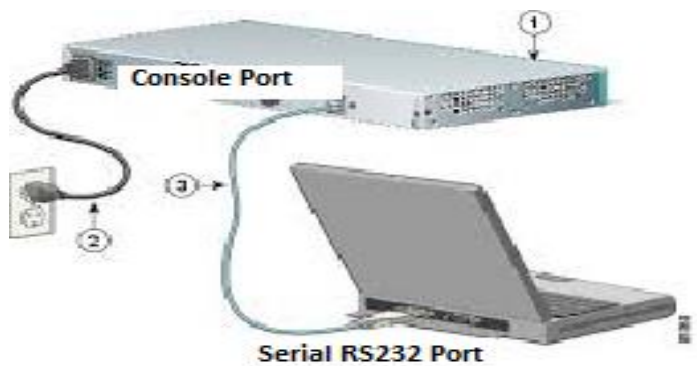


Fig-1. Connection of console port with PC/Laptop via console cable.

Step 2: The communication parameters configuration of the Putty Terminal with console is shown below Baud rate (Speed):**115200**

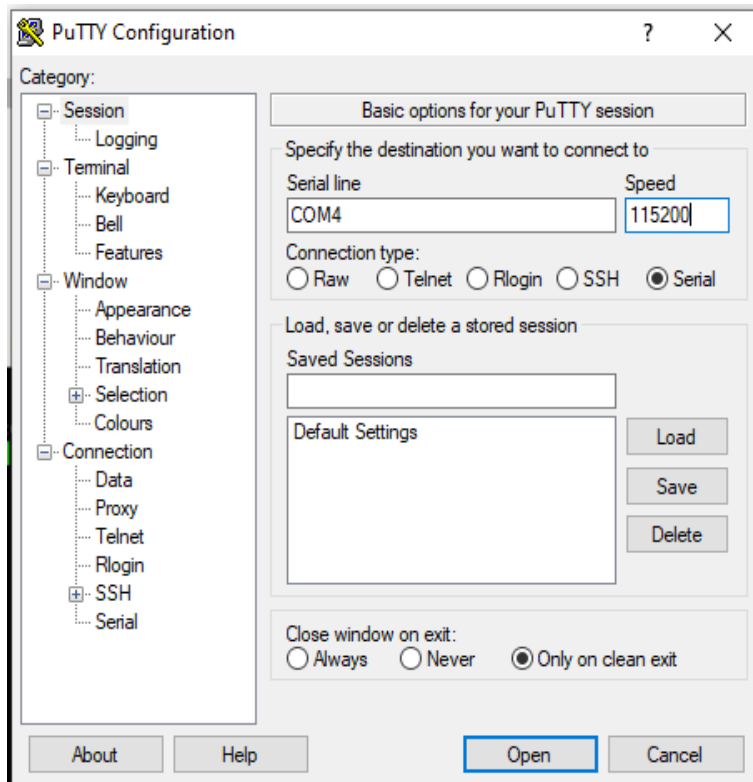


Fig-2. Putty configuration in PC for console port access

Step 3: Click on **“Open”**. You will get following window.

With the console port properly connected to a management computer, the following screen should be visible.



Fig-3. COMMANDO Series E3000 Switch CLI access via console port

How to Login COMMANDO Series E3000 Web GUI and Enable Telnet?

Before Accessing Command Line Interface via telnet, you have to login to Web GUI of COMMANDO E3000 Switch. Connect one Ethernet port to your system with RJ45 LAN cable.

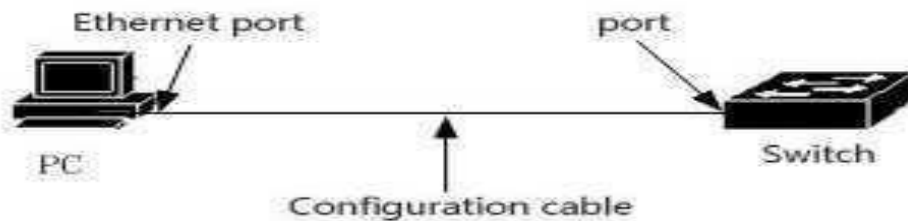


Fig-4. COMMANDO Series E3000 Switch port connected with PC via RJ45 LAN cable.

In PC following LAN setting required.

- Open **Network and sharing center**.
- Click **change Adapter** settings.
- Double click on **Local Area Connection**.
- Click **Properties**.
- Double click on **Internet Protocol Version 4 (TCP/IPv4)** option and set default IP as shown below.

IP Address: 192.168.0.(2-254)

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

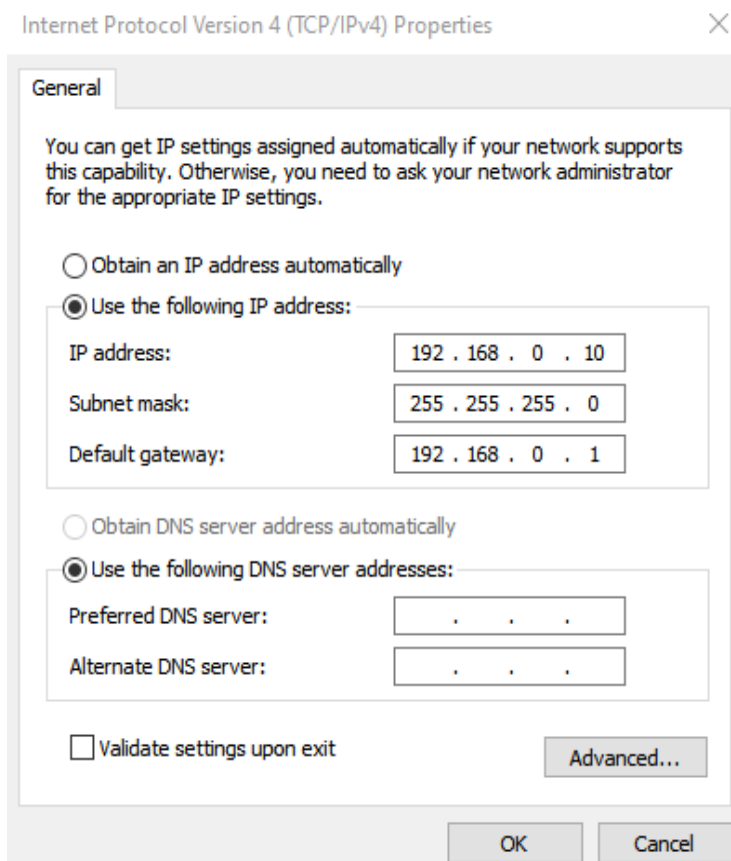


Fig-5. Local Area Connection properties for Web Interface

Now Open any web browser type <http://192.168.0.1> and hit **“Enter”** following window will appear.

Use following login details to enter in Web GUI mode,

Username: admin

Password: ****

(Note: Password is mentioned on backside of device)

Enter the login button. COMMANDO E3000 series switch starting Page appears.

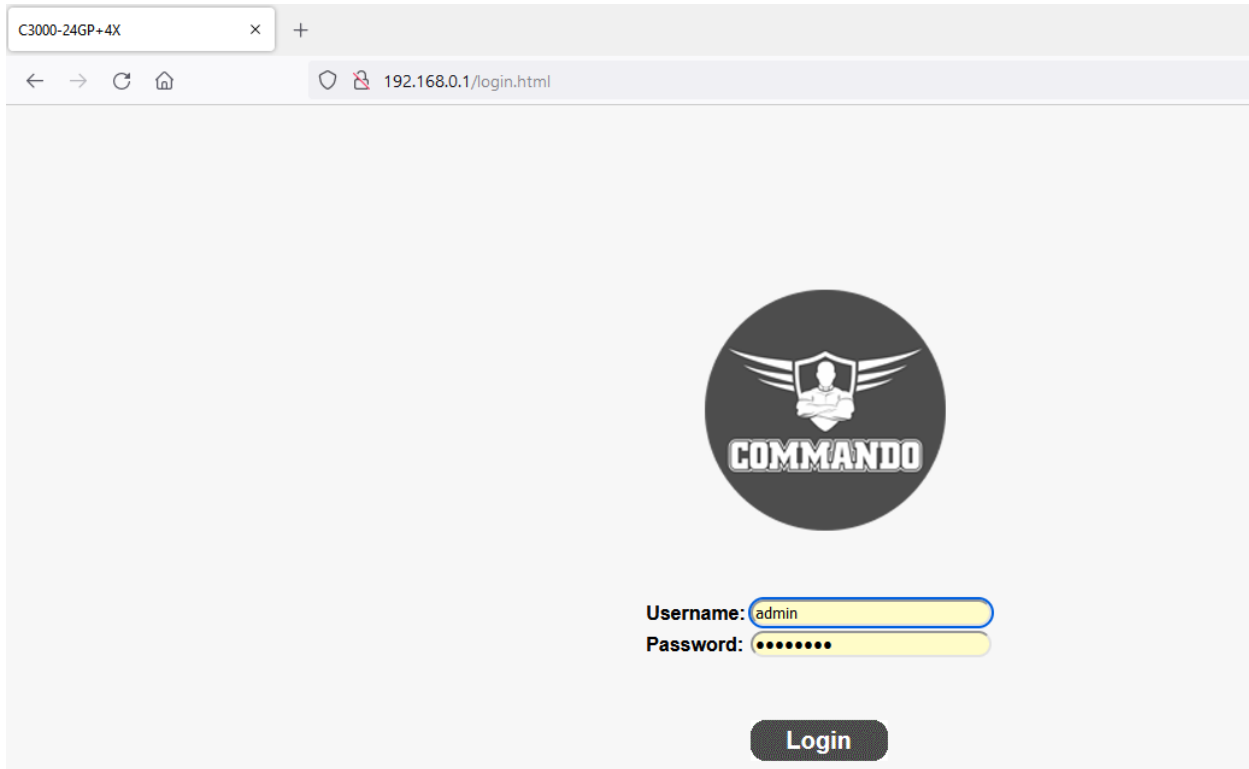


Fig-6. COMMANDO E3000 Switch Web GUI Administrator Login Page

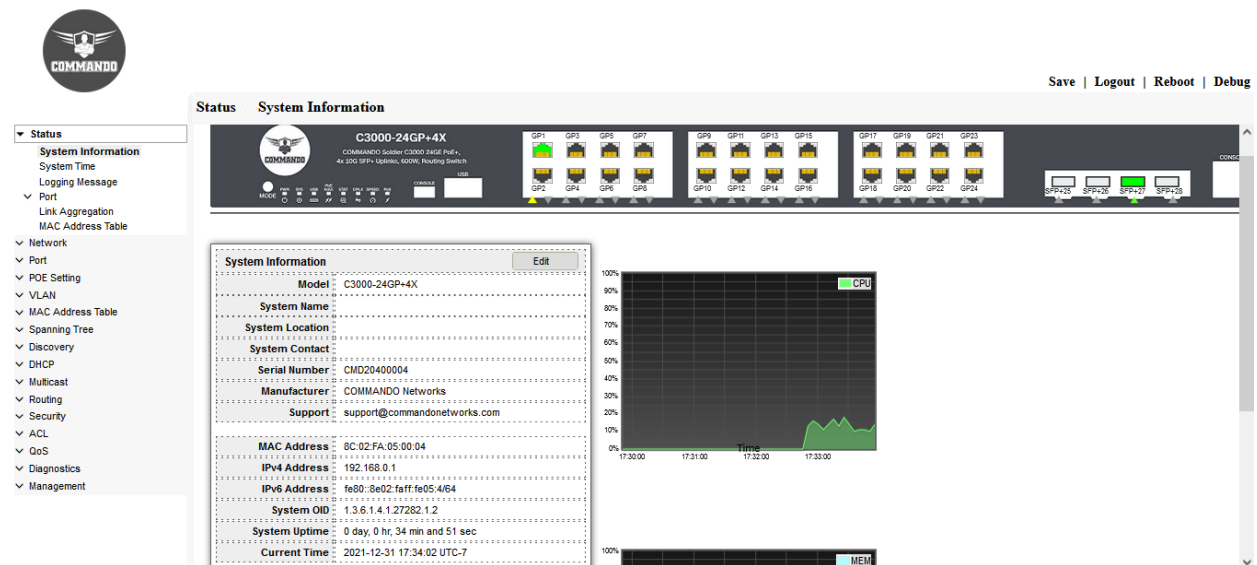


Fig-7. COMMANDO E3000 Switch Web GUI starting Page

Following steps are required to access CLI via telnet lines.

Management>>Management Access>>Management Service

Click on **Management**

Click on **Management Access**

Click on **Management Services**

Telnet Click on

“Apply” and “Save” the configuration.

This is required stage before accessing COMMANDO E3000 Switch Command Line Interface (CLI) to enable “Telnet”. By default, “Telnet” service is disabled by default, so you must enable it manually.

Management >>Management Access>>Management Service is very important page to enable and disable Telnet, SSH, HTTP, HTTPS, SNMP and Set Session Timeout (By default 10min), Password Retry Count (By default 3), Silent Time (To block all further login attempts until the timer expires By default is 0 second) .

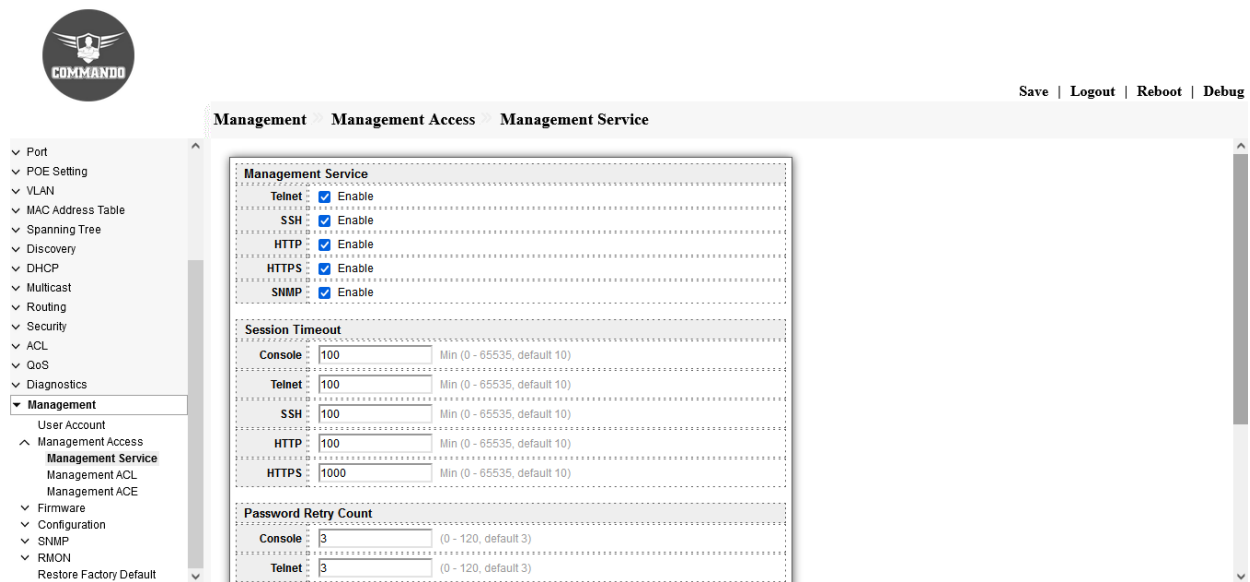


Fig-8. COMMANDO E3000 Switch Management Access service.

Users access CLI through TELNET

Following are the steps to access CLI via telnet.

Step 1: Connect the LAN port of PC/Laptop with any Ethernet port of the switch by LAN cable.

Step 2:

The communication parameters configuration of the Putty Terminal with TELNET is shown below:

IP Address: **192.168.0.1**

Port: **23**

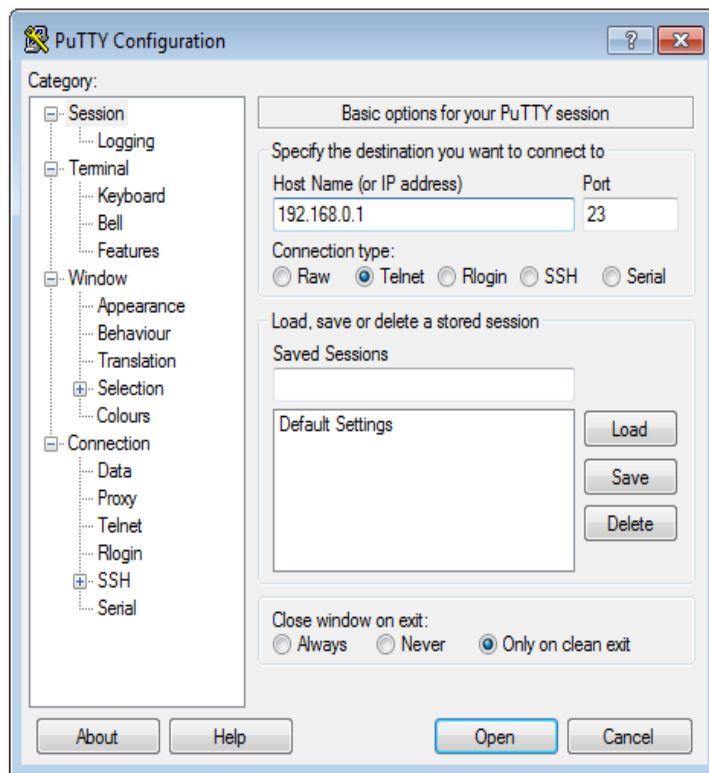


Fig-9. Putty configuration in PC for Telnet access

Step 3: Click on “**Open**”. You will get following window.

Username: **admin**

Password: *********

(Note: Password is mentioned on backside of device)

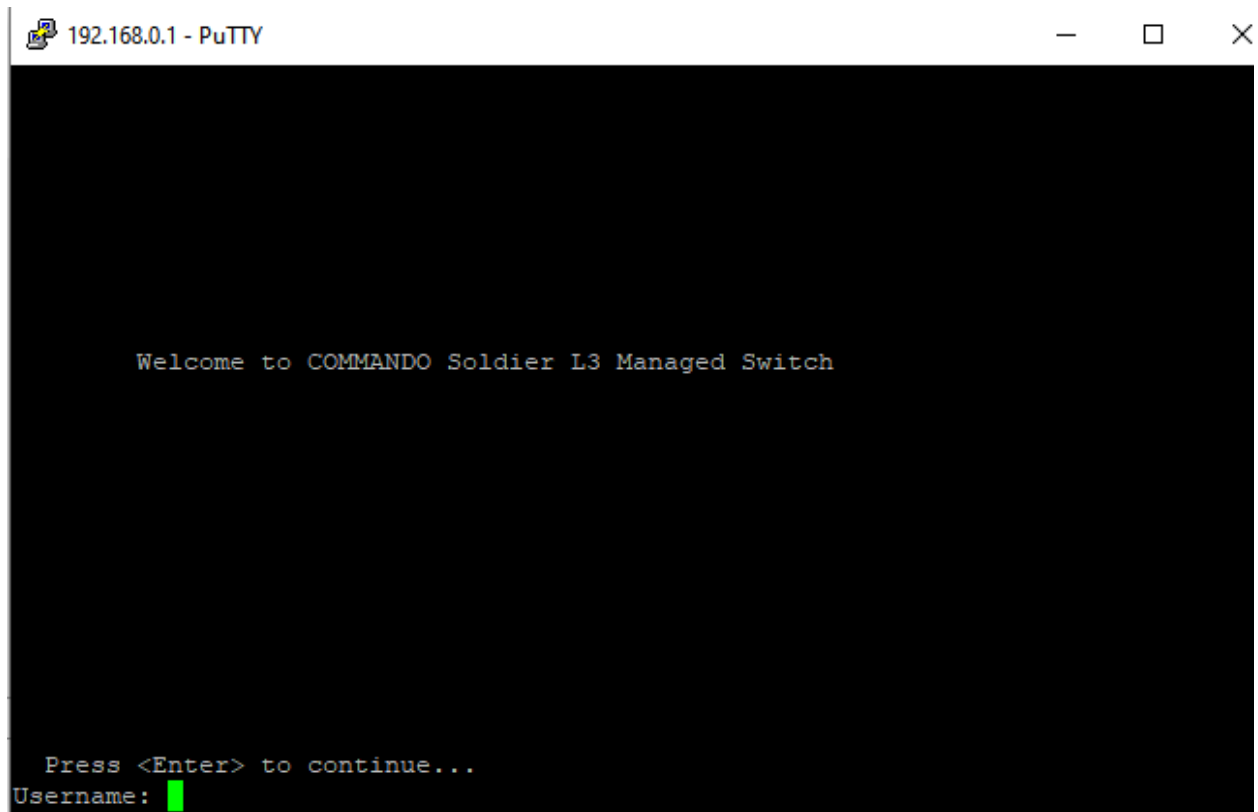
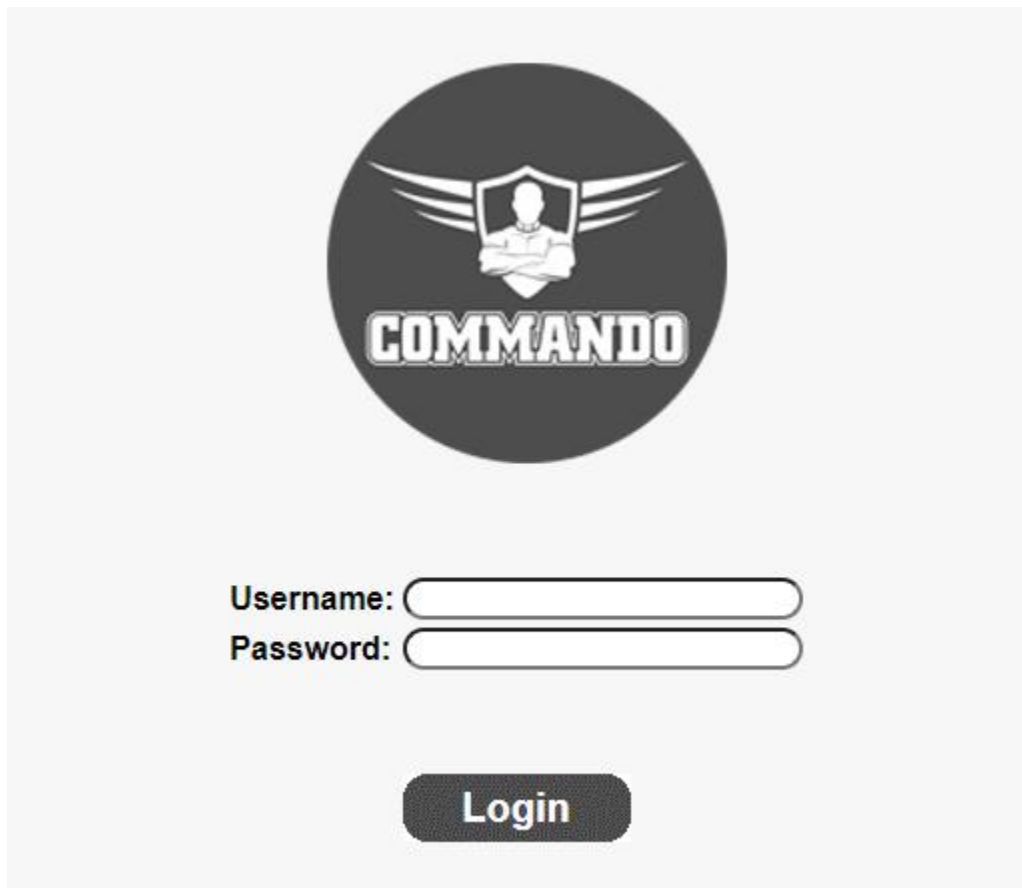


Fig-10. COMMANDO Series E3000 Switch CLI access via telnet

1.1 Web browse based graphical user interface (Web GUI)

Introduction

COMMANDO E3000 Series SoldierOS had a web browser based graphical user interface (Web GUI). This is inbuilt in each COMMANDO E3000 series switches. You can use either the CLI via Console/Telnet or Web GUI for managing E3000 Series Switches. COMMANDO Networks recommend that you use this Web GUI which can configure almost everything as you needed in simple and user-friendly manner. This Web GUI is a state of art having world class features with which you can configure basic, advance, and special feature very easily. After setting the Proper PC LAN parameter given above and in Web browser giving IP address 192.168.0.1 you will get the login page.



The image shows a login page for the COMMANDO E3000 Series Switches. At the top center is a circular logo containing a stylized soldier figure with wings and the word "COMMANDO" in a bold, blocky font. Below the logo, there are two input fields: "Username:" followed by a text box, and "Password:" followed by a text box. At the bottom center, there is a dark, rounded button labeled "Login".

Fig 1.1 Username and Password page of E3000 Series Switches

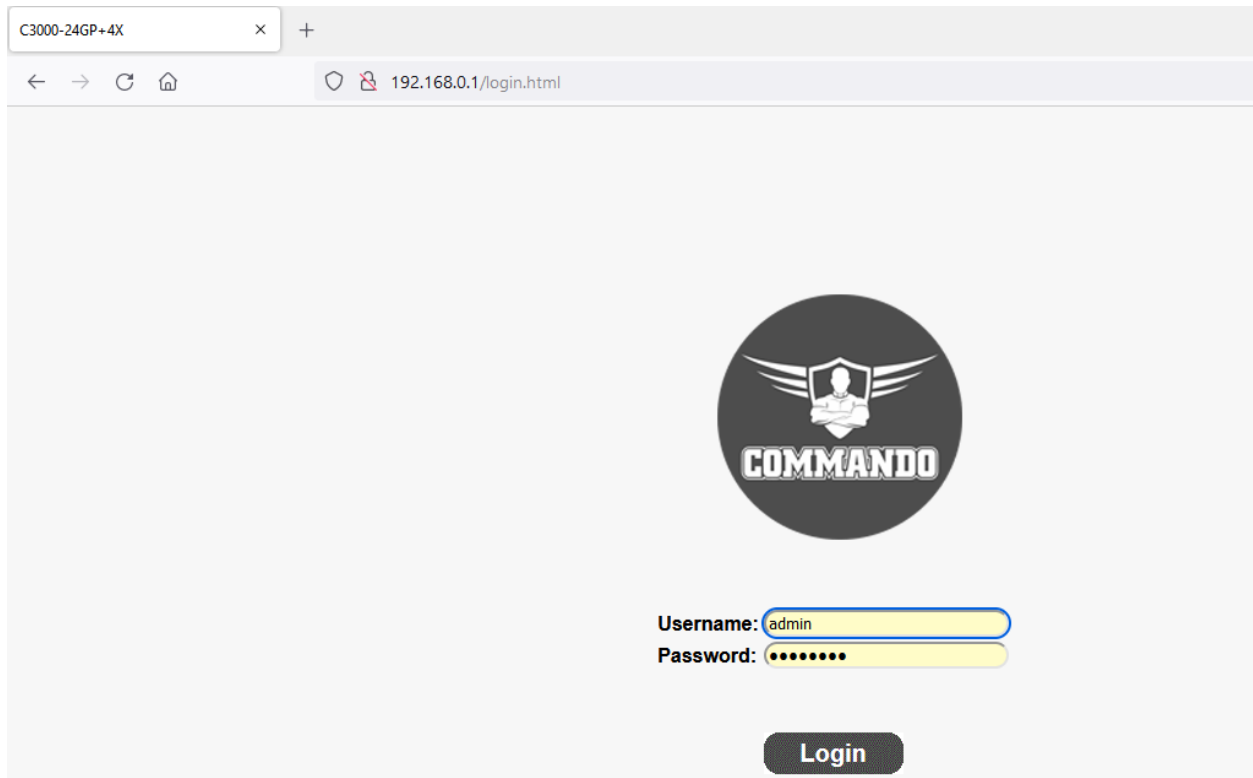


Fig 1.2 Default Login page of E3000 Series Switches

Note: With E3000 Web based Graphical User Interface (Web GUI)

1. You can change default IP 192.168.0.1 to any desired IP address.
2. You can change Factory set username--> admin and password-->*****.
3. Factory set default Password is written on the Backside of device.

After you login the web page successfully, you will see the System information page which provides you real time status of Switch. This page shows very important System information of this E3000 device which can help in troubleshooting network issues. The upper frame is the front panel frame, which shows the connection situation of each port. If a port is connected and link is up and working properly then the corresponding port on the front panel will be green.

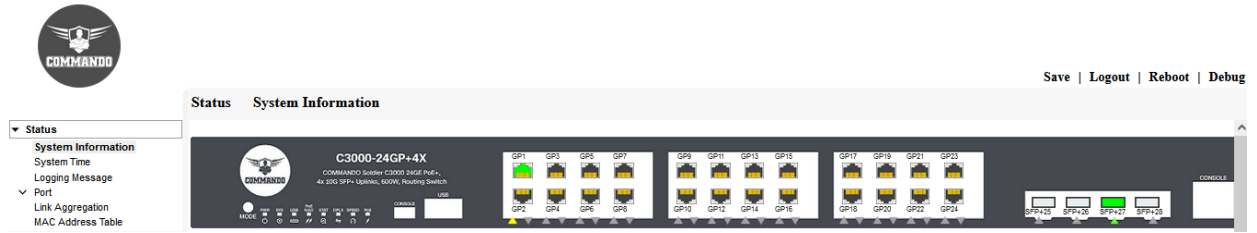


Fig 1.3 System Information page of E3000 Series Switches

1.2 Main Menu Description in Web GUI

The left-hand panel shows the configuration the configuration web pages tabs. All configuration web pages are hidden by the group head label. To expand the group head label, click the down arrow sign on the left side of main WEB page. Then this down arrow key can expand group head label to get specific Web pages for Switch to configure as per requirement of users.

In E3000 Series Switches SoldierOS comes with PoE/PoE+ as Well as Non PoE models. COMMAMDO SoldierOS has 15 Group heads for E3000 PoE based switches. Lots of functions and protocols can be easily configured by Web GUI and very handy and easy to troubleshoot any networking issue.



► Status
✓ Network
✓ Port
✓ POE Setting
✓ VLAN
✓ MAC Address Table
✓ Spanning Tree
✓ Discovery
✓ DHCP
✓ Multicast
✓ Routing
✓ Security
✓ ACL
✓ QoS
✓ Diagnostics
✓ Management

Fig 1.4 WEB Pages for E3000 Series Switches.

Quick Start Device Configuration

To simplify E3000 Series device configuration through quick navigation, the Getting Started page provides links to the most used pages.

Table 1.1 E3000 Series Switches SoldierOS Web Software Frameworks.

Group head label	Corresponding Web pages
<p>Status</p>	<p>System Information System Time Logging Message Port Statistics Error Disabled Bandwidth Utilization Link Aggregation MAC Address Table</p>
<p>Network</p>	<p>DNS Hosts</p>
<p>Port</p>	<p>Port Setting Error Disabled Link Aggregation Group Port Setting LACP EEE Jumbo Frame Port Security Protected Port Storm Control</p>
<p>POE Setting</p>	<p>POE Port Setting POE Port Timer Setting Note: 1. Only Available in PoE/PoE+ Switches. 2. Intelligent PoE/PoE+ Scheduler is special feature of COMMANDO E3000 Series Switches.</p>
<p>VLAN</p>	<p>VLAN Create VLAN VLAN Configuration</p>

	Membership Port Setting Voice VLAN Property Voice OUI Protocol VLAN Protocol Group Group Binding MAC VLAN MAC Group Group Binding Surveillance VLAN Property Surveillance OUI GVRP Property Membership Statistics
MAC Address Table	Dynamic Address Static Address Filtering Address Port Security Address
Spanning Tree	Property Port Setting MST Instance MST Port Setting Statistics
Discovery	LLDP Property Port Setting MED Network Policy MED Port Setting Packet View

	Local Information Neighbor Statistics
DHCP	Property IP Pool Setting VLAN IF Address Group Setting Client List Client Static Binding Table
Multicast	General Property Group Address Router Port Forward All Throttling Filtering Profile Filtering Binding IGMP Snooping Property Querier Statistics MLD Snooping Property Statistics MVR Property Port Setting Group Address
Routing	IPv4 Management and Interfaces IPv4 Interface IPv4 Routes ARP IPv6 Management and Interfaces IPv6 Interface

	<p>IPv6 Addresses IPv6 Routes IPv6 Neighbors RIP Routes Management RIP Routes Setting OSPF Routes Management OSPF Routes Setting</p>
<p>Security</p>	<p>RADIUS TACACS+ AAA Method List Login Authentication Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account Sessions DoS Property Port Setting Dynamic ARP Inspection Property Statistics DHCP Snooping Property Statistics Option82 Property Option82 Circuit ID IP Source Guard Port Setting IMPV Binding Save Database</p>

ACL	MAC ACL MAC ACE IPv4 ACL IPv4 ACE IPv6 ACL IPv6 ACE ACL Binding
QOS	General Property Queue Scheduling CoS Mapping DSCP Mapping IP Precedence Mapping Rate Limit Ingress / Egress Port Egress Queue
Diagnostics	Logging Property Remote Server Mirroring Ping Traceroute Copper Test Fiber Module UDLD Property Neighbor
Management	User Account Management Access Management VLAN Management Service Management ACL Management ACE

Firmware

Upgrade

Active Image

Configuration

Upgrade

Save Configuration

SNMP

View

Group

Community

User

Engine ID

Trap Event

Notification

RMON

Statistics

History

Event

Alarm

Restore Factory Default

1.3 Save, Logout, Reboot, Debug Buttons

1.3.1 Save

By clicking Save button will copy running-config to startup-config to save the current running configuration to the startup configuration file in Switch Memory. This means that if power failure or device OFF/ON configuration will not be lost and remained as per saved configuration.

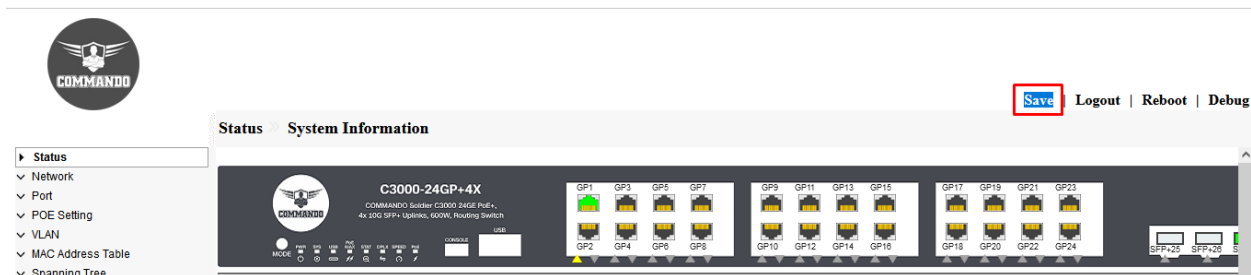


Fig 1.3.1 Save button

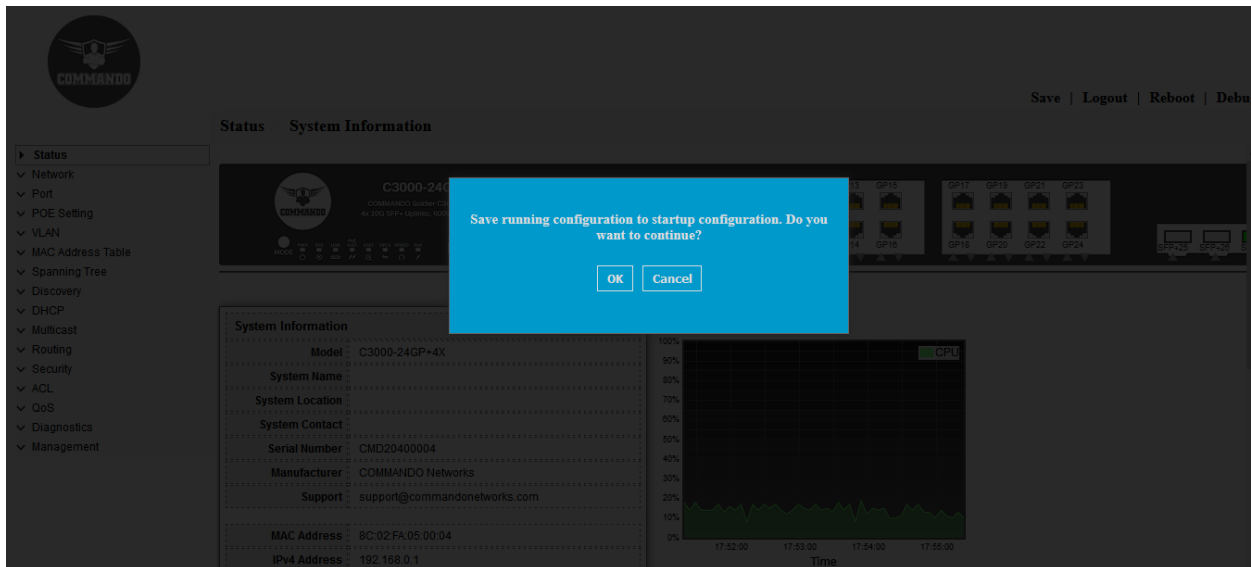


Fig 1.3.2 Applying Save button

1.3.2 Logout

Logging out means to end access to a COMMANDO Switch on a Web GUI. Logging out informs the COMMANDO Switch that the current user wishes to end the login session.



Fig 1.3.3 Logout button on WEBGUI

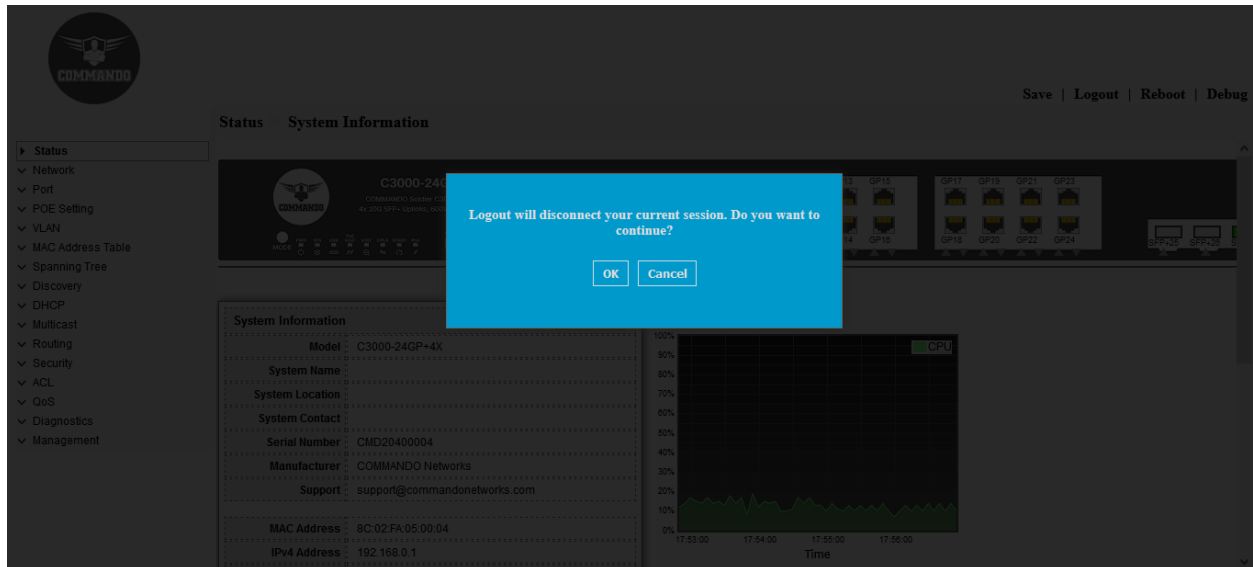


Fig 1.3.4 Applying Logout button on Web GUI

1.3.3 Reboot

Reboot means boot again. COMMANDO Switch is force by this command to power OFF and immediately Power-On. This command forcefully restarting the Switch again.

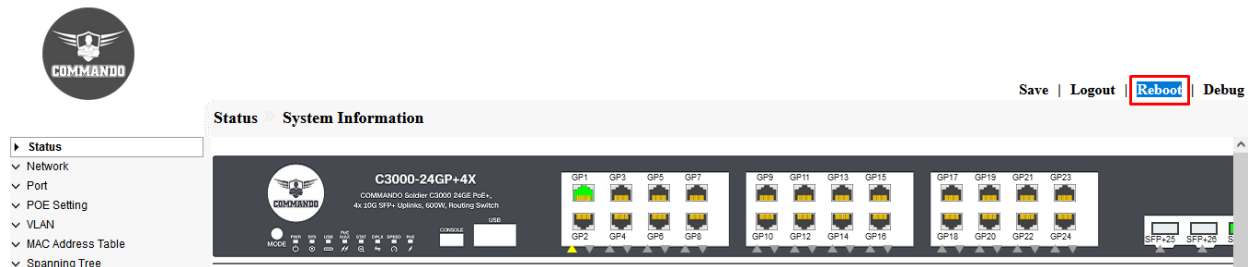


Fig 1.3.5 Reboot button on Web GUI

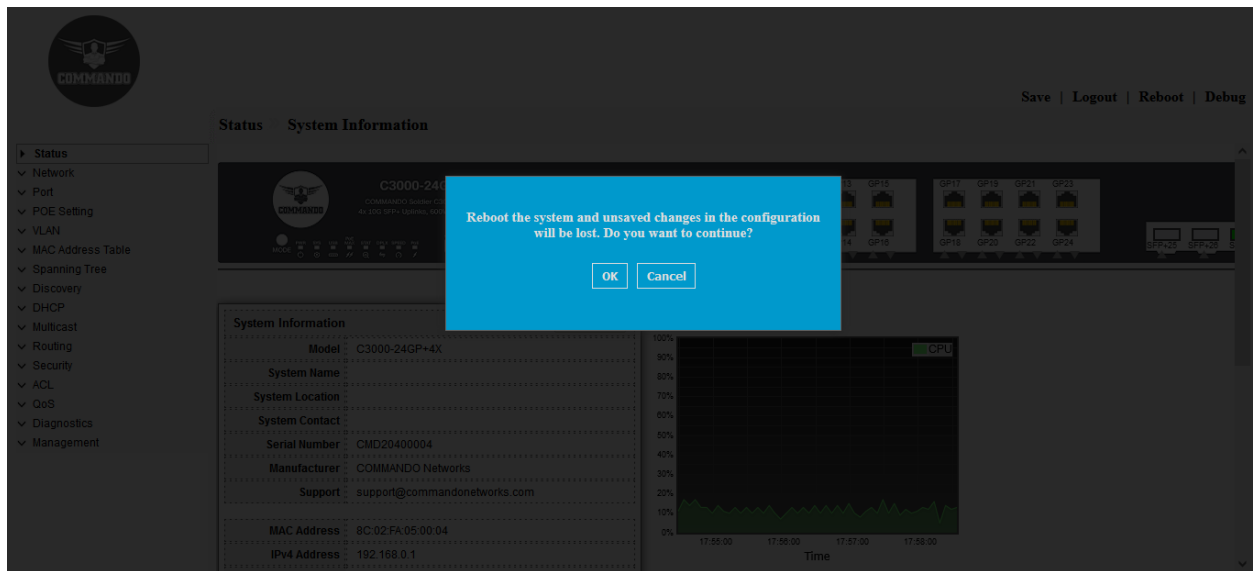


Fig 1.3.6 Applying Reboot button on Web GUI

1.3.4 Debug

Debug is used to find and resolve bugs or defects. Debugging is the process of troubleshooting for detecting and removing of existing and potential issue in network.

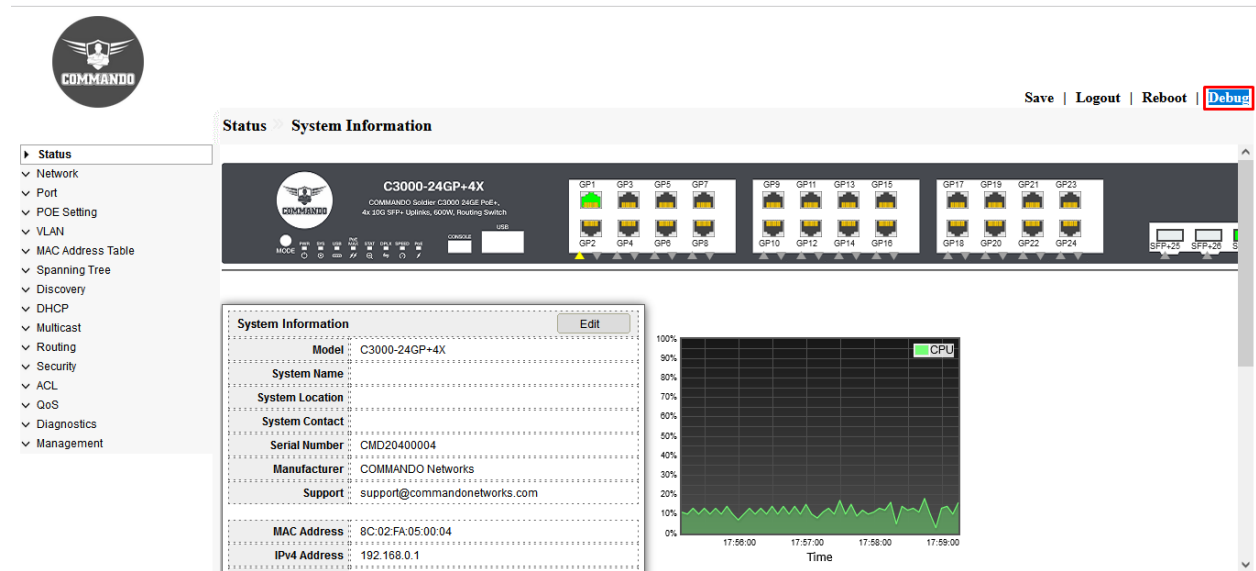


Fig 1.3.6 Debug message button on Web GUI

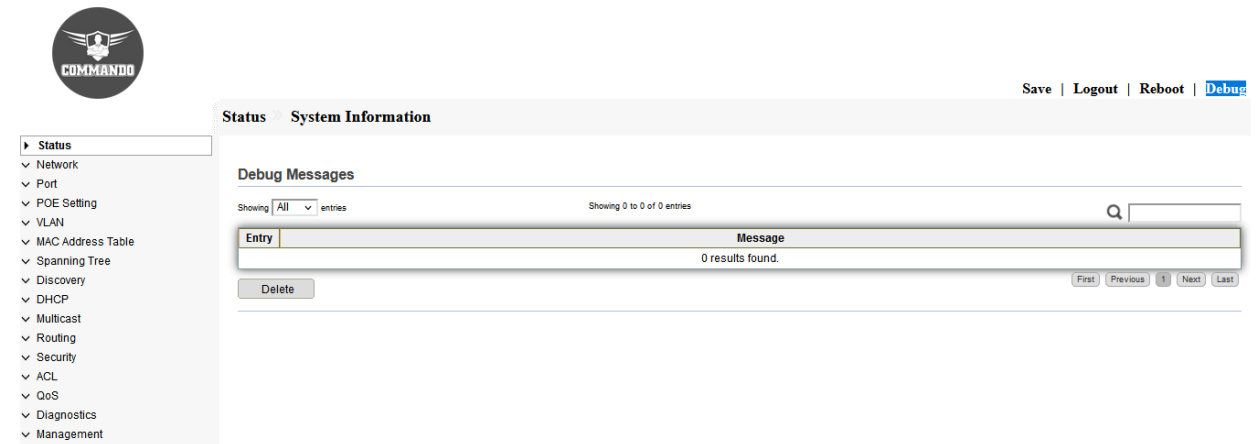


Fig 1.3.7 View Debug message on Web GUI

Chapter 2 COMMANDO E3000 SoldierOS WEB Status

Group Header: Status

After clicking **Status** down arrow keys four corresponding web pages tabs are opened.

System Information: This section describes how to view system information and configure various options on the device. This web page shows the Exact running status of device along with LED Indication like Power, System, connection and activity for all ports, UP/Down status of all ports as well as configuration for devices such as System Information, Model, System Name, System Location, System Contact, Serial Number, MAC Address, IPv4 Address, IPv6 Address, System OID, System Uptime, Current Time, Loader Version, Loader Date, Firmware Version, Firmware Date. This page also gives enabled status device management lines like Telnet, SSH, HTTP, HTTPS, SNMP.

System Time: System time options for configuring the system time, time zone, and Daylight Savings Time (DST).

Logging Message: You can enable or disable logging on the Log Settings page and select whether to aggregate log messages.

Port: You can view port statistics and reset the port counters.

Link Aggregation: Enable/disable the Link Aggregation Control (LAG) protocol and configure the potential member ports to the desired LAGs by using the LAG Management page. By default, all LAGs are empty.

MAC Address Table: There are two types of MAC addresses—static and dynamic. Depending on their type, MAC addresses are either stored in the Static Address table or in the Dynamic Address table, along with VLAN and port information. Static addresses are configured by the user, and therefore, they do not expire. These pages describe how to add MAC addresses to the system. It covers Configuring Static MAC Addresses, Managing Dynamic MAC Addresses.

2.1 System Information

This is the main display page of E3000 SoldierOS. This web page shows the Exact running status of device along with LED Indication like Power, System, connection and activity for all ports, UP/Down status of all ports as well as configuration for devices such as System Information, Model, System Name, System Location, System Contact, Serial Number, MAC Address, IPv4 Address, IPv6 Address, System OID, System Uptime, Current Time, Loader Version, Loader Date, Firmware Version, Firmware Date. This page also gives enabled status device management lines like Telnet, SSH, HTTP, HTTPS, SNMP.

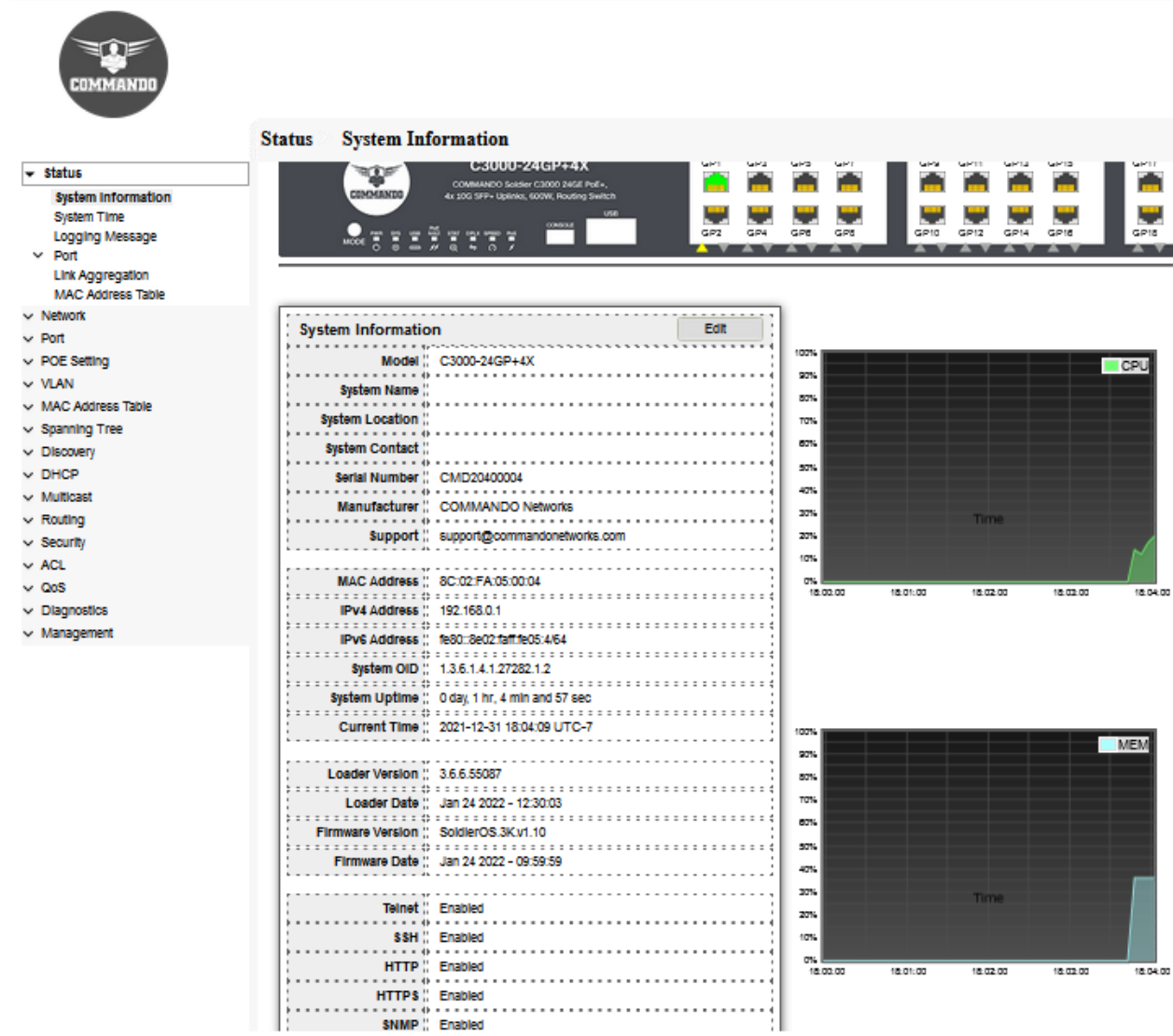


Fig 2.1 System information Web page

2.1.1 Changing the System Name, Location and Contact

Following are the steps to change the Default System Name, Location and Contact.

Status>>System Information>>Edit button

The screenshot displays the COMMANDO network switch management interface. On the left is a navigation menu with the following items: Status (expanded), System Information, System Time, Logging Message, Port (expanded), Link Aggregation, MAC Address Table, Network, VLAN, POE Setting, Spanning Tree, Discovery, DHCP, and Multicast. The main content area is titled "Status > System Information". It features a top status bar with the COMMANDO logo, model number "C3000-24GP+4X", and device details: "COMMANDO Soldier C3000 24GE PoE+, 4x 10G SFP+ Uplinks, 600W, Routing Switch". Below this are physical ports (CONSOLE, USB) and network ports (GP1-GP4). The "System Information" section is a table with the following fields: Model (C3000-24GP+4X), System Name, System Location, and System Contact. An "Edit" button is highlighted with a red box in the top right corner of this section.

System Information	
Model	C3000-24GP+4X
System Name	
System Location	
System Contact	

Fig 2.1.1 Changing the System Name, System Location and System Contact

After clicking **Status>>System Information>>Edit button**, Modify the System Name, System Location and System Contact as per users' requirements.



- ▼ Status
 - System Information**
 - System Time
 - Logging Message
 - ▼ Port
 - Link Aggregation
 - MAC Address Table
 - ▼ Network
 - ▼ Port
 - ▼ POE Setting
 - ▼ VLAN
 - ▼ MAC Address Table
 - ▼ Spanning Tree
 - ▼ Discovery
 - ▼ DHCP
 - ▼ Multicast
 - ▼ Routing
 - ▼ Security
 - ▼ ACL
 - ▼ QoS
 - ▼ Diagnostics
 - ▼ Management

Status > System Information

Edit System Information

System Name	<input type="text" value="C3000"/>
System Location	<input type="text" value="US"/>
System Contact	<input type="text" value="commahdonetworks.c"/>

Apply Close

Fig 2.1.2 Changing System Name, System Location and System Contact

After changing System Name, System Location and System Contact click on **Apply** button. Then you can see the changed System Name, System Location and System Contact.



Status > System Information

- ▼ Status
 - System Information**
 - System Time
 - Logging Message
- ▼ Port
 - Link Aggregation
 - MAC Address Table
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast



System Information		Edit
Model	C3000-24GP+4X	
System Name	C3000	
System Location	US	
System Contact	commandonetworks.com	

Fig 2.1.3 Viewing Changed System Name, System Location and System Contact

2.2 System Time

Synchronized system clock is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events occur. Without synchronized clocks, accurately correlating log files between devices when tracking security breaches or network usage is impossible. Synchronized time also reduces confusion in shared file systems, as it is important for the modification times to be consistent, regardless of the machine on which the file systems reside. For these reasons, it is important that the time configured on all the devices on the network is accurate.

System time can be set manually by the user, dynamically from an SNTP server, or synchronized from the PC running the Web GUI. If an SNTP server is chosen, the manual time settings are overwritten when communications with the server are established. As part of the boot process, the device always configures the time, time zone, and DST. These parameters are obtained from the PC running the Web GUI, SNTP, values set manually, or if all else fails, from the factory defaults.

The following methods are available for setting the system time on the Switches

Manual—You must manually set the time.

From PC—Time can be received from the PC by using browser information.

This method of setting time from PC works with both HTTP and HTTPS connections.

SNTP—Time can be received from SNTP time servers. SNTP ensures accurate network time synchronization of the device up to the millisecond by using an SNTP server for the clock source.

This page allow user to set time source, static time, time zone and daylight-saving settings. Time zone and daylight saving takes effect both static time or time from SNTP server.

To display System Time page, click **Status>> System Time**



- ▼ Status
 - System Information
 - System Time**
 - Logging Message
- ▼ Port
 - Link Aggregation
 - MAC Address Table
- ▼ Network
 - Port
 - POE Setting
 - VLAN
 - MAC Address Table
 - Spanning Tree
 - Discovery
 - DHCP
 - Multicast
 - Routing
 - Security
 - ACL
 - QoS
 - Diagnostics
 - Management

Status System Time

Source	<input type="radio"/> SNTP
	<input type="radio"/> From Computer
	<input checked="" type="radio"/> Manual Time
Time Zone	UTC-7:00
SNTP	
Address Type	<input checked="" type="radio"/> Hostname
	<input type="radio"/> IPv4
Server Address	
Server Port	123 (1 - 65535, default 123)
Manual Time	
Date	2019-12-31 YYYY-MM-DD
Time	17:34:20 HH:MM:SS
Daylight Saving Time	
Type	<input checked="" type="radio"/> None
	<input type="radio"/> Recurring
	<input type="radio"/> Non-recurring
	<input type="radio"/> USA
	<input type="radio"/> European
Offset	60 Min (1 - 1440, default 60)
Recurring	From: Day Sun Week First Month Jan Time
	To: Day Sun Week First Month Jan Time
Non-recurring	From: YYYY-MM-DD HH:MM
	To: YYYY-MM-DD HH:MM
Operational Status	
Current Time	2019-12-31 17:34:20 UTC-7

Apply

Fig 2.2.1 Default System Time configuration page

Time Zone and Daylight Savings Time (DST)

A time zone is one of the areas into which the world is divided where the time is calculated as being a particular number of hours behind or ahead of GM. The main purpose of Daylight-Saving Time (called "Summertime" in many places in the world) is to make better use of daylight. We change our clocks during the summer months to move an hour of daylight from the morning to the evening.



- ▼ Status
 - System Information
 - System Time**
 - Logging Message
 - ▼ Port
 - Link Aggregation
 - MAC Address Table
 - ▼ Network
 - ▼ Port
 - ▼ POE Setting
 - ▼ VLAN
 - ▼ MAC Address Table
 - ▼ Spanning Tree
 - ▼ Discovery
 - ▼ DHCP
 - ▼ Multicast
 - ▼ Routing
 - ▼ Security
 - ▼ ACL
 - ▼ QoS
 - ▼ Diagnostics
 - ▼ Management

Status > System Time

Source	<input type="radio"/> SNTP <input type="radio"/> From Computer <input checked="" type="radio"/> Manual Time
Time Zone	UTC -7:00 UTC -2:00 UTC -1:00 UTC UTC +1:00 UTC +2:00 UTC +3:00 UTC +3:30 UTC +4:00 UTC +4:30 UTC +5:00 UTC +5:30 UTC +5:45 UTC +6:00 UTC +6:30 UTC +7:00 UTC +8:00 UTC +9:00 UTC +9:30 UTC +10:00 UTC +11:00
SNTP	
Address Type	
Server Address	
Server Port	(1 - 65535, default 123)
Manual Time	
Date	YYYY-MM-DD
Time	HH:MM:SS
Daylight Saving Time	
Type	<input type="radio"/> Recurring <input type="radio"/> Non-recurring <input type="radio"/> USA <input type="radio"/> Europe

Fig 2.4.2 Timezone configuration page



Status > **System Time**

Time HH:MM:SS

Daylight Saving Time

Type
 None
 Recurring
 Non-recurring
 USA
 European

Offset Min (1 - 1440, default 60)

Recurring
From: Day Week Month Time
To: Day Week Month Time

Non-recurring
From: YYYY-MM-DD HH:MM
To: YYYY-MM-DD HH:MM

Operational Status
Current Time 2019-12-31 17:34:20 UTC-7

Fig 2.4.3 Daylight saving time configuration page

From Computer

This is the best way to configure the time setting in switch. E3000 Series Switches will take and sync with logging PC time automatically. This is a recommended setting to have proper time setting in switch. Just select proper time zone as per country or requirement.

To configure and view this recommended setting click on **Status>> System Time** and use source From Computer.



- ▼ Status
 - System Information
 - System Time**
 - Logging Message
- ▼ Port
 - Link Aggregation
 - MAC Address Table
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security

Status >> System Time

Source	<input type="radio"/> SNTP
	<input checked="" type="radio"/> From Computer
	<input type="radio"/> Manual Time
Time Zone	UTC-7:00
SNTP	
Address Type	<input checked="" type="radio"/> Hostname
	<input type="radio"/> IPv4
Server Address	
Server Port	123 (1 - 65535, default 123)
Manual Time	
Date	2021-02-18 YYYY-MM-DD
Time	06:27:00 HH:MM:SS

Fig 2.4.4 Time configuration from connected computer page



- ▼ Status
 - System Information
 - System Time
 - Logging Message
 - ▼ Port
 - Link Aggregation
 - MAC Address Table
 - ▼ Network
 - Port
 - POE Setting
 - VLAN
 - MAC Address Table
 - Spanning Tree
 - Discovery
 - DHCP
 - Multicast
 - Routing
 - Security
 - ACL
 - QoS
 - Diagnostics
 - Management

Status **System Time**

Source	<input type="radio"/> SNTP <input checked="" type="radio"/> From Computer <input type="radio"/> Manual Time
Time Zone	UTC -7:00
SNTP	
Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4
Server Address	
Server Port	123 (1 - 65535, default 123)
Manual Time	
Date	2021-02-18 YYYY-MM-DD
Time	06:28:32 HH:MM:SS
Daylight Saving Time	
Type	<input checked="" type="radio"/> None <input type="radio"/> Recurring <input type="radio"/> Non-recurring <input type="radio"/> USA <input type="radio"/> European
Offset	60 Min (1 - 1440, default 60)
Recurring	From: Day Sun Week First Month Jan Time
	To: Day Sun Week First Month Jan Time
Non-recurring	From: YYYY-MM-DD HH:MM
	To: YYYY-MM-DD HH:MM
Operational Status	
Current Time	2021-02-18 06:28:32 UTC-7

Apply

Fig 2.4.5 Time configuration from connected computer page

SNTP

The simple network time protocol (SNTP) is a time synchronization protocol of the TCP/IP protocol family. It is based on the connectionless user datagram protocol (UDP) and can be used on all supporting devices to synchronize system time in IP networks (IPv4 and IPv6). Time can be received from SNTP time servers. SNTP ensures accurate network time synchronization of the device up to the millisecond by using an SNTP server for the clock source. You can also set local or public time server IP or Hostname if time server is locally available.



- Status
 - System Information
 - System Time**
 - Logging Message
- Port
 - Link Aggregation
 - MAC Address Table
- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
 - ACL
 - QoS
- Diagnostics
- Management

Status System Time

Source	<input checked="" type="radio"/> SNTP <input type="radio"/> From Computer <input type="radio"/> Manual Time
Time Zone	UTC -7:00
SNTP	
Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4
Server Address	time1.google.com
Server Port	123 (1 - 65535, default 123)
Manual Time	
Date	2021-02-18 YYYY-MM-DD
Time	08:28:32 HH:MM:SS
Daylight Saving Time	
Type	<input checked="" type="radio"/> None <input type="radio"/> Recurring <input type="radio"/> Non-recurring <input type="radio"/> USA <input type="radio"/> European
Offset	60 Min (1 - 1440, default 60)
Recurring	From: Day Sun Week First Month Jan Time
	To: Day Sun Week First Month Jan Time
Non-recurring	From: YYYY-MM-DD HH-MM
	To: YYYY-MM-DD HH-MM
Operational Status	
Current Time	2021-02-18 08:28:32 UTC-7

Apply

Fig 2.4.6 SNTP Configuration page

After changing Time, you can verify the changed time from system information page.



Status > System Information

- ▼ Status
 - System Information**
 - System Time
 - Logging Message
- ▼ Port
 - Link Aggregation
 - MAC Address Table
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

System Information		Edit
Model	C3000-24GP+4X	
System Name	C3000	
System Location	US	
System Contact	commandonetworks.com	
Serial Number	CMD20400004	
Manufacturer	COMMANDO Networks	
Support	support@commandonetworks.com	
MAC Address	8C:02:FA:05:00:04	
IPv4 Address	192.168.0.1	
IPv6 Address	fe80::8e02:faff:fe05:4/64	
System OID	1.3.6.1.4.1.27282.1.2	
System Uptime	0 day, 1 hr, 11 min and 39 sec	
Current Time	2022-02-21 21:06:44 UTC-7	
Loader Version	3.6.6.55087	
Loader Date	Jan 24 2022 - 12:30:03	

Fig 2.4.5 System Information page displaying current time.

2.3 Logging Message

This page shows the log messages Logging Message Table of RAM by System Log feature, which enables the device to generate multiple independent logs. Each log is a set of messages describing system events. System Log feature, which enables the device to generate multiple independent logs. Each log is a set of messages describing system events. By default, notification Log message sent to the console interface. Log written into a cyclical list of logged events in the RAM and erased when the device reboots. Log written to a cyclical log-file saved to the Flash memory and persists across reboots. To view the logging messages stored on the RAM, click **Status >> Logging Message** and use Viewing option RAM

Note: By default, RAM option will be selected.

COMMANDO

Save | Logout | Reboot | Debug

Status Logging Message

Logging Message Table

Viewing RAM

Showing All entries Showing 1 to 1 of 1 entries

Log ID	Time	Severity	Description
1	Feb 18 2021 06:34:09	info	LOGGING-0-START: Logging is started

Clear Refresh

First Previous 1 Next Last

Fig 2.3.1 Logging Message Table of RAM

To view the logging messages stored on the Flash, click **Status >> Logging Message** and use Viewing option Flash.

COMMANDO

Save | Logout | Reboot | Debug

Status Logging Message

Logging Message Table

Viewing Flash

Showing All entries Showing 0 to 0 of 0 entries

Log ID	Time	Severity	Description
0 results found.			

Clear Refresh

First Previous 1 Next Last

Fig 2.3.2 Logging Message Table of Flash

The number of entries to be shown for logging message table are shown

COMMANDO

Save | Logout | Reboot | Debug

Status **Logging Message**

Logging Message Table

Viewing **RAM**

Showing **All** entries Showing 1 to 27 of 27 entries

Log#	Time	Severity	Description
10	1 2021 17:42:22	notice	AAA-0-CONNECT: New http connection for user admin, source 192.168.0.22 ACCEPTED, aggregated (1)
30	1 2021 17:42:22	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.0.22 ACCEPTED
50	1 2021 17:41:03	notice	AAA-5-DISCONNECT: http connection for user (null), source 192.168.0.22 TERMINATED
100	1 2021 17:40:57	notice	AAA-5-DISCONNECT: telnet connection for user , source async TERMINATED
5	Dec 31 2021 17:36:01	info	SYSTEM-5-SSH_START: SSH service is started
6	Dec 31 2021 17:36:01	info	SYSTEM-6-TELNET_START: TELNET service is started
7	Dec 31 2021 17:32:49	notice	AAA-6-CONNECT: New http connection for user admin, source 192.168.0.22 ACCEPTED
8	Dec 31 2021 17:27:12	notice	AAA-5-DISCONNECT: telnet connection for user , source async TERMINATED
9	Dec 31 2021 17:23:42	info	SYSTEM-5-WEB_TIMEOUT: GUI session timeout: user admin, source 192.168.0.22
10	Dec 31 2021 17:23:42	notice	AAA-6-DISCONNECT: http connection for user admin, source 192.168.0.22 TERMINATED
11	Dec 31 2021 17:11:12	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.0.22 ACCEPTED
12	Dec 31 2021 17:01:07	notice	PORT-5-LINK_DOWN: Interface VLAN2 link down, aggregated (2)
13	Dec 31 2021 17:01:07	notice	PORT-5-LINK_DOWN: Interface GigabitEthernet1 link down, aggregated (2)
14	Dec 31 2021 17:00:09	notice	PORT-5-LINK_UP: Interface VLAN2 link up, aggregated (3)
15	Dec 31 2021 17:00:09	info	PORT-5-SPEED_DUPLEX: Interface GigabitEthernet1 link speed 100M duplex full, aggregated (3)

Fig 2.3.3 Logging Message Table of Entries selection

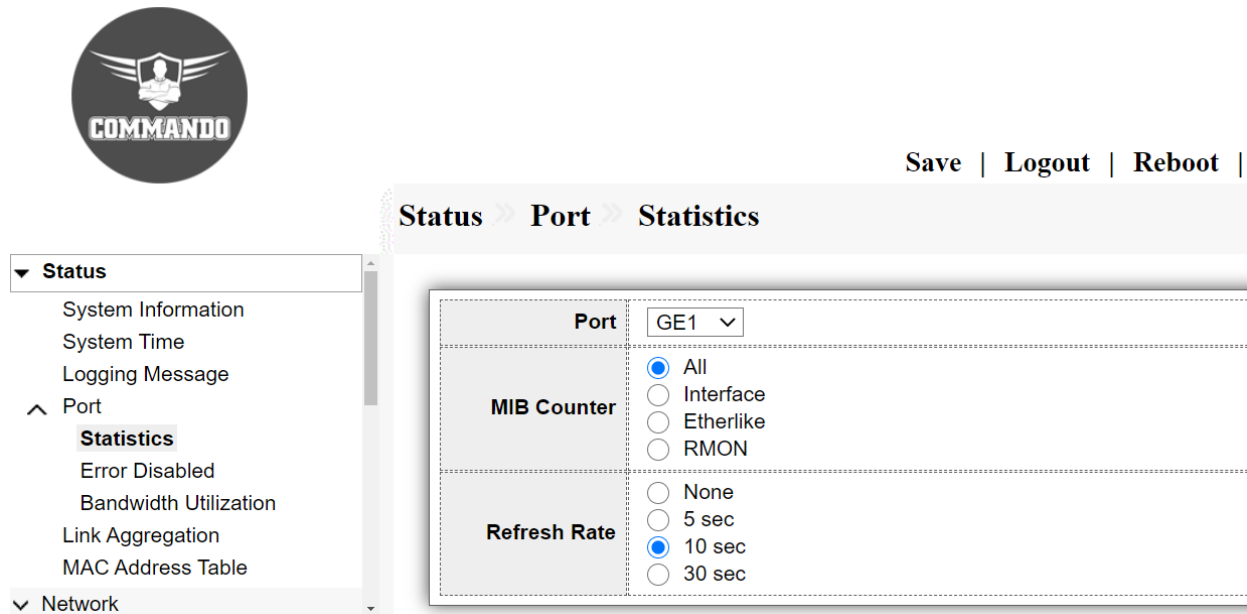
2.4 Port

A management information base (MIB) is a database used for managing the entities in a communication network. Most often associated with the Simple Network Management Protocol (SNMP), the term is also used more generically in contexts such as in OSI/ISO Network management model.

2.4.1 Port Statistics

This page shows Port statistics like MIB Counter & Refresh rate for each port. By default, Port Gigabit Ethernet 1 is selected, and refresh rate is 10 seconds. The Port configuration page displays port summary and status information. To view particular port status, click **Status >> Port >> Statistics** and select Port.

Note: Default selection is GE1



COMMANDO

Save | Logout | Reboot |

Status >> Port >> Statistics

Port	GE1
MIB Counter	<input checked="" type="radio"/> All <input type="radio"/> Interface <input type="radio"/> Etherlike <input type="radio"/> RMON
Refresh Rate	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 30 sec

Fig 2.4.1 Port selection for MIB Counter Statistics



- ▼ Status
 - System Information
 - System Time
 - Logging Message
 - ▲ Port
 - Statistics**
 - Error Disabled
 - Bandwidth Utilization
 - Link Aggregation
 - MAC Address Table
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Status > Port > Statistics

Port: GE1

MIB Counter: All, Interface, Etherlike, RMON

Refresh Rate: None, 5 sec, 10 sec, 30 sec

Clear

Interface	
ifInOctets	919566
ifInUcastPkts	5581
ifInNUcastPkts	432
ifInDiscards	0
ifOutOctets	2499383
ifOutUcastPkts	6161
ifOutNUcastPkts	1173
ifOutDiscards	0
ifInMulticastPkts	387
ifInBroadcastPkts	45
ifOutMulticastPkts	1019
ifOutBroadcastPkts	154

Fig 2.4.2 Gigabit Ethernet 5 port selection for MIB Counter Statistics

The other common type of MIB used for polling statistics is a MIB counter. Interface MIB used to measure traffic on a network interface. The MIB will show you a running total number of the octets (bytes) of traffic that have went in/out of the interface.



Status » Port » Statistics

▼ Status	RMON	
System Information	etherStatsDropEvents	0
System Time	etherStatsOctets	1079063
Logging Message	etherStatsPkts	7083
^ Port	etherStatsBroadcastPkts	45
Statistics	etherStatsMulticastPkts	460
Error Disabled	etherStatsCRCAlignErrors	0
Bandwidth Utilization	etherStatsUnderSizePkts	0
Link Aggregation	etherStatsOverSizePkts	0
MAC Address Table	etherStatsFragments	0
▼ Network	etherStatsJabbers	0
▼ Port	etherStatsCollisions	0
▼ POE Setting	etherStatsPkts64Octets	4357
▼ VLAN	etherStatsPkts65to127Octets	1384
▼ MAC Address Table	etherStatsPkts128to255Octets	120
▼ Spanning Tree	etherStatsPkts256to511Octets	68
▼ Discovery	etherStatsPkts512to1023Octets	1138
▼ DHCP	etherStatsPkts1024to1518Octets	16
▼ Multicast		
▼ Routing		
▼ Security		
▼ ACL		
▼ QoS		
▼ Diagnostics		
▼ Management		

Fig 2.4.3 RMON MIB Counter Statistics

2.4.2 Port Error Disabled

The ErrDisable feature is implemented to handle special situations where the switch detected excessive or late collisions on a port, port duplex misconfiguration, EtherChannel misconfiguration, Bridge Protocol Data Unit (BPDU) port-guard violation, UniDirectional Link Detection (UDLD), and other (miscellaneous) causes.

The error-disable function allows the switch to shut down/ Protect /Restrict a port when it encounters physical, driver or configuration problems. A port being error-disabled is not by itself a cause for alarm, but a symptom of a problem that must be resolved. To display the Error Disabled web page, click **Status >> Port >> Error Disabled**.



Status >> Port >> Error Disabled

Error Disabled Table

<input type="checkbox"/>	Port	Reason	Time Left (sec)
<input type="checkbox"/>	GE1	---	---
<input type="checkbox"/>	GE2	---	---
<input type="checkbox"/>	GE3	---	---
<input type="checkbox"/>	GE4	---	---
<input type="checkbox"/>	GE5	---	---
<input type="checkbox"/>	GE6	---	---
<input type="checkbox"/>	GE7	---	---
<input type="checkbox"/>	GE8	---	---
<input type="checkbox"/>	GE9	---	---
<input type="checkbox"/>	GE10	---	---
<input type="checkbox"/>	GE11	---	---

Navigation menu:

- ▼ Status
 - System Information
 - System Time
 - Logging Message
 - ▲ Port
 - Statistics
 - Error Disabled**
 - Bandwidth Utilization
 - Link Aggregation
 - MAC Address Table
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP

Fig 2.4.4 Default Port Error disabled Table

Recovering form Error disabled state

To recover a port that is in an ErrDisable state, manual intervention is required, and the administrator must access the switch and configure the specific port with 'shutdown' followed by the 'no shutdown' command in CLI. This command sequence will enable the port again, however, if the problem persists expect to find the port in ErrDisable state again soon. In Web GUI can easily recover from error disable by selecting port and pressing recovery button.

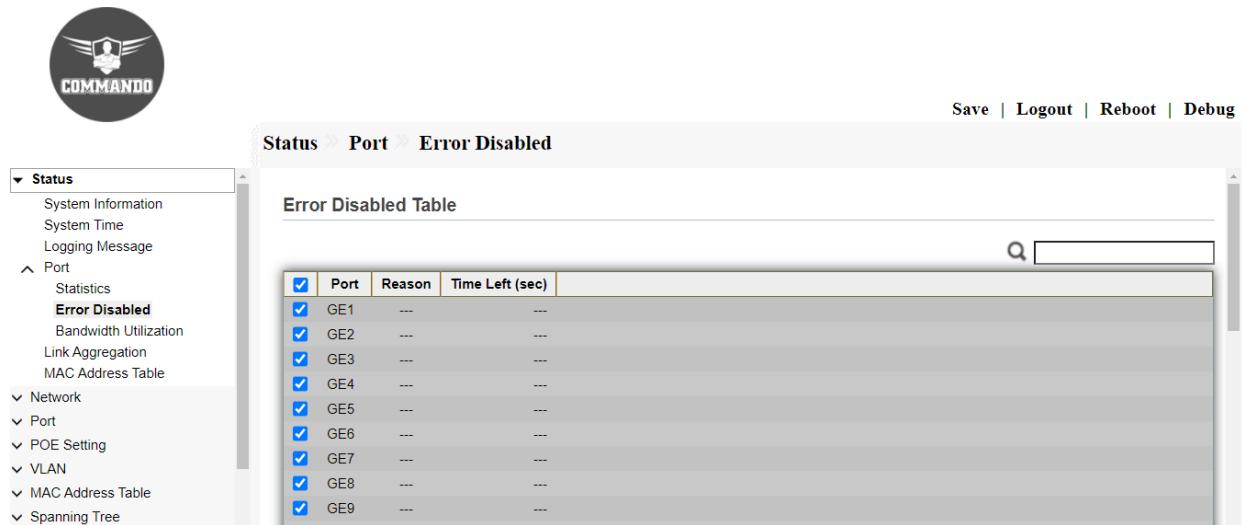


Fig 2.4.5 Recovering form error disabled state.

2.4.3 Port Bandwidth Utilization

Bandwidth utilization for each port can be seen by this page and for the switch fabric itself. Easiest way to look at all ports, this shows how much bandwidth for each switch port interfaces are using. In other words, it helps you monitor bandwidth. This page allow user to look bandwidth utilization in real time. This page will refresh automatically by default in 5 second. To display Bandwidth Utilization web page, click **Status >> Port >> Bandwidth Utilization**.

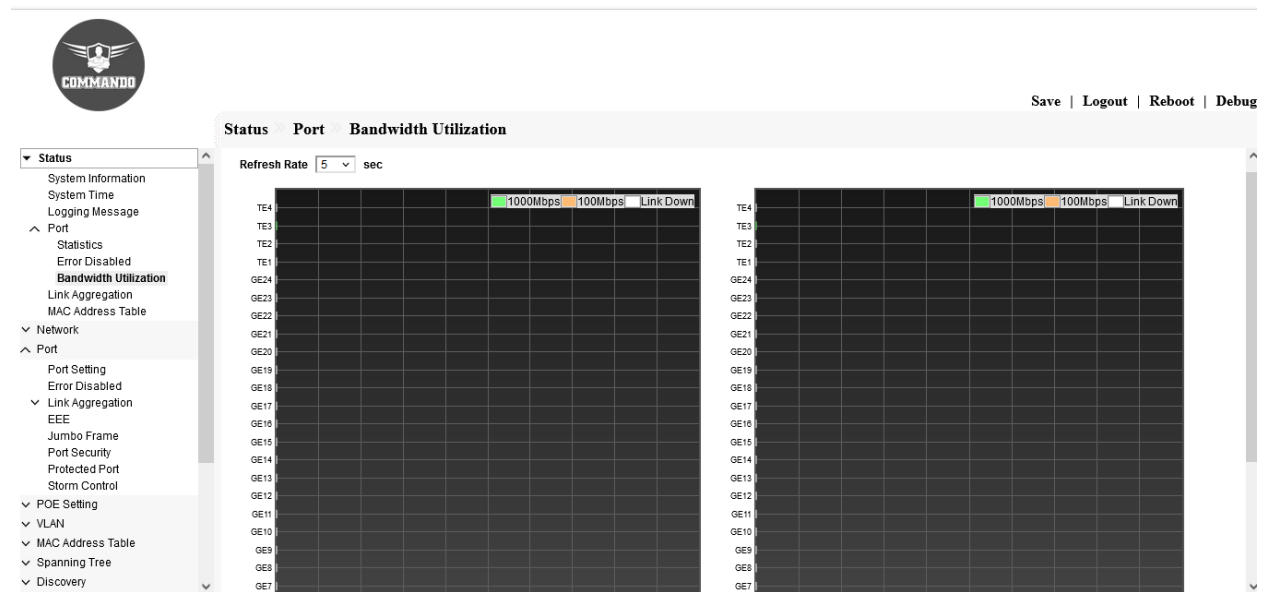


Fig 2.4.6 Bandwidth utilization and refresh rate

2.5 Link Aggregation

Link aggregation is a way of bundling a bunch of individual Ethernet/ Fast Ethernet/ Gigabit Ethernet links together, so they act like a single logical link. The official IEEE standard for link aggregation used to be called 802.3ad.

Link aggregation groups (LAGs) allow you to combine multiple Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and load sharing. Specify LAG membership before you enable the LAG. The switch supports up to eight LAGs. To display the Link Aggregation web page, click **Status >> Link Aggregation**.



Status >> Link Aggregation

Link Aggregation Table

LAG	Name	Type	Link Status	Active Member	Inactive Member
LAG 1		--	--		
LAG 2		--	--		
LAG 3		--	--		
LAG 4		--	--		
LAG 5		--	--		
LAG 6		--	--		
LAG 7		--	--		
LAG 8		--	--		

Status

- System Information
- System Time
- Logging Message
- Port
 - Statistics
 - Error Disabled
 - Bandwidth Utilization
 - Link Aggregation**
 - MAC Address Table
- Network
- Port
 - Port Setting
 - Error Disabled
 - Link Aggregation
 - EEE

Fig 2.5.1 Default Link Aggregation table information.

Link Aggregation Table

LAG	Name	Type	Link Status	Active Member	Inactive Member
LAG 1	LAG-1	Static	Up	GE25,GE27	
LAG 2		---	---		
LAG 3		---	---		
LAG 4		---	---		
LAG 5		---	---		
LAG 6		---	---		
LAG 7		---	---		
LAG 8		---	---		

Fig 2.5.2 Link Aggregation table information.

2.6 Mac Address Table

A MAC address table, sometimes called a Content Addressable Memory (CAM) table, is used on Ethernet switches to determine where to forward traffic on a LAN.

There are two types of MAC addresses—static and dynamic. Depending on their type, MAC addresses are either stored in the Static Address table or in the dynamic address table, along with VLAN and port information. Static addresses are configured by the user, and therefore, they do not expire. To display the MAC Address Table web page, click **Status >> MAC Address Table**.

The screenshot shows the COMMANDO web interface. On the left is a navigation menu with options like Status, Network, Port, POE Setting, VLAN, and MAC Address Table. The MAC Address Table section is expanded, showing sub-options: Dynamic Address, Static Address, Filtering Address, and Port Security Address. The main content area is titled 'MAC Address Table > Dynamic Address'. It features an 'Aging Time' input field set to 300, with a note 'Sec (10 - 630, default 300)' and an 'Apply' button. Below this is a 'Dynamic Address Table' section with a search bar and a table. The table has columns for 'VLAN', 'MAC Address', and 'Port'. One entry is visible: VLAN 1, MAC Address B8:2A:72:A6:FC:1C, Port GE2. At the bottom of the table are 'Refresh' and 'Add Static Address' buttons, and pagination controls showing 'Showing 1 to 1 of 1 entries'.

Fig 2.6.1 Mac Address Table information

The screenshot shows the COMMANDO web interface. On the left is a navigation menu with options like Status, Network, Port, POE Setting, VLAN, and MAC Address Table. The MAC Address Table section is expanded, showing sub-options: Dynamic Address, Static Address, Filtering Address, and Port Security Address. The main content area is titled 'MAC Address Table > Static Address'. It features a 'Static Address Table' section with a search bar and a table. The table has columns for 'VLAN', 'MAC Address', and 'Port'. The table is empty, with the text '0 results found.' below it. At the bottom of the table are 'Add', 'Edit', and 'Delete' buttons, and pagination controls showing 'Showing 0 to 0 of 0 entries'.

Fig 2.6.2 Default Static Mac Address Table information

Chapter 3 Network

DNS: The Domain Name System (DNS) translates domain names into IP addresses for the purpose of locating and addressing hosts. As a DNS client, the Switch resolves domain names to IP addresses using one or more configured DNS servers.

Hosts: DNS Hosts, also known as host record in your domain's that makes the connection between your domain name and its matching IP address.

3.1 DNS

The Domain Name System (DNS) translates domain names into IP addresses for the purpose of locating and addressing hosts. As a DNS client, the device resolves domain names to IP addresses using one or more configured DNS servers.

To configure and view Domain Name System (DNS), click **Network >> DNS**

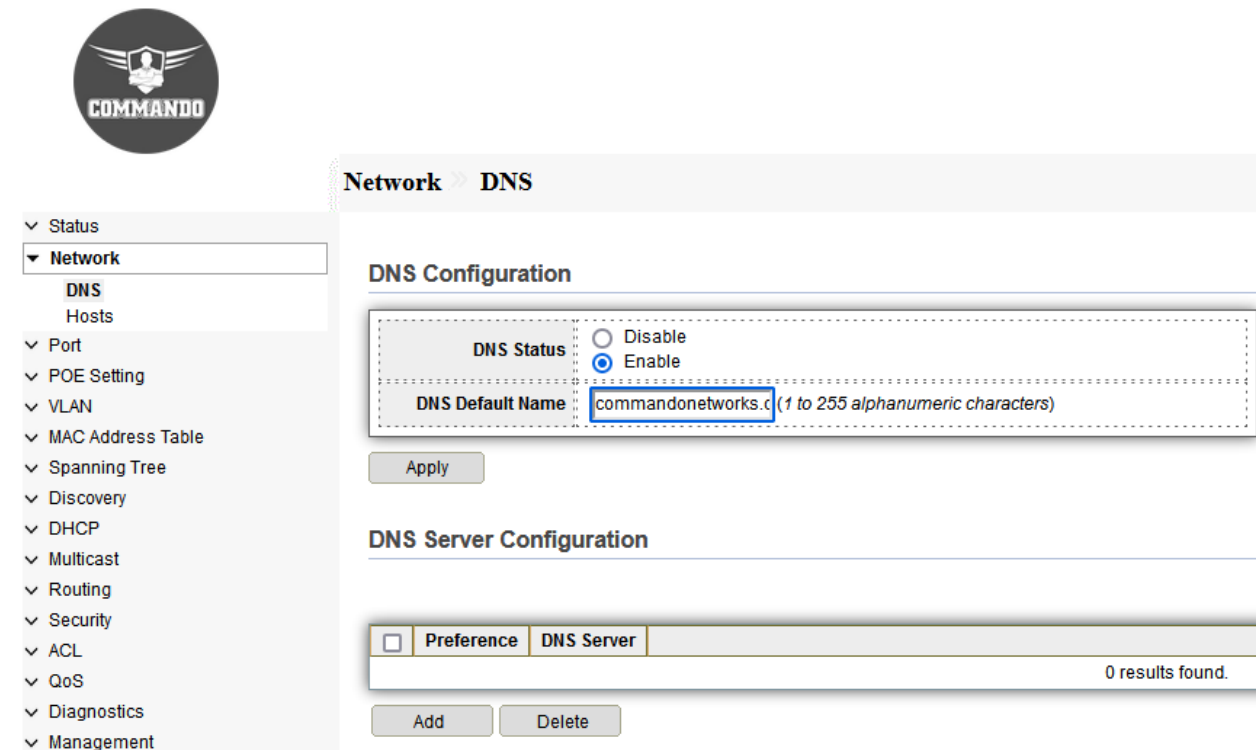


Fig 3.1.1 DNS configuration page



Network > DNS

▼ Status
▼ Network
 DNS
 Hosts
▼ Port
▼ POE Setting
▼ VLAN
▼ MAC Address Table
▼ Spanning Tree
▼ Discovery
▼ DHCP
▼ Multicast
▼ Routing
▼ Security
▼ ACL
▼ QoS
▼ Diagnostics
▼ Management

Add DNS Server

IPv4/IPv6 Address: 192.168.0.3

Apply Close

Fig 3.1.2 Add DNS Server page



Network > DNS

▼ Status
▼ Network
 DNS
 Hosts
▼ Port
▼ POE Setting
▼ VLAN
▼ MAC Address Table
▼ Spanning Tree
▼ Discovery
▼ DHCP
▼ Multicast
▼ Routing
▼ Security
▼ ACL
▼ QoS
▼ Diagnostics
▼ Management

DNS Configuration

DNS Status: Disable Enable

DNS Default Name: commandonetworks.c (1 to 255 alphanumeric characters)

Apply

DNS Server Configuration

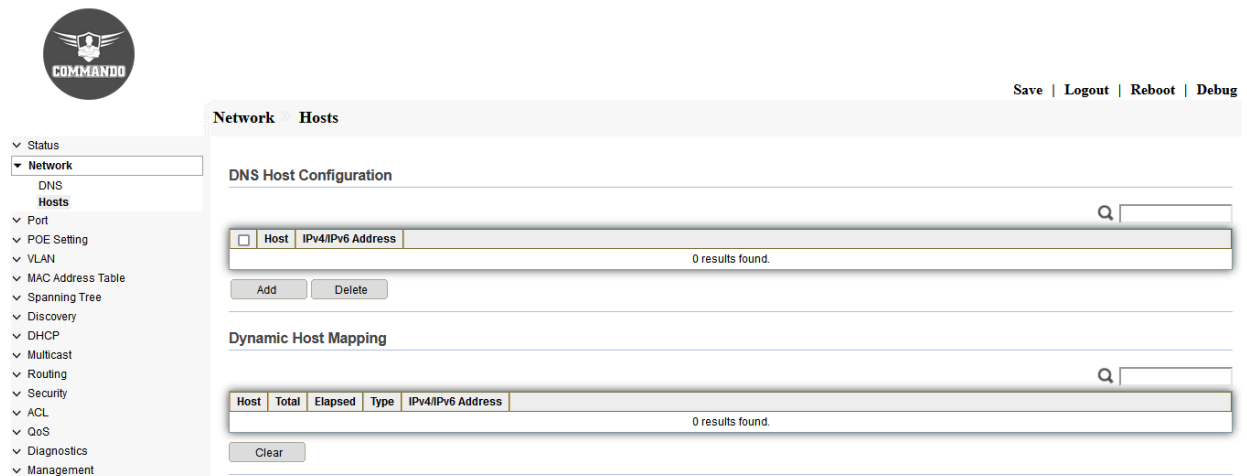
<input type="checkbox"/>	Preference	DNS Server
<input type="checkbox"/>	1	192.168.0.3

Add Delete

Fig 3.1.3 DNS Server configuration page

3.2 Hosts

The Domain Name System, more popular as DNS, is responsible for associating domain names, the user-friendly names of websites, with their corresponding real system names - IP addresses. These IP addresses are vital for bringing the website online and in the DNS system are known as A records. This page shows information about DNS Host Configuration. To configure and view Domain Name System (DNS) Host configuration, click **Network >>Hosts**



The screenshot displays the COMMANDO network management interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The main content area is titled 'Network > Hosts' and contains two sections: 'DNS Host Configuration' and 'Dynamic Host Mapping'. Each section has a search bar and a table with 0 results found. The 'DNS Host Configuration' table has columns for Host and IPv4/IPv6 Address. The 'Dynamic Host Mapping' table has columns for Host, Total, Elapsed, Type, and IPv4/IPv6 Address. At the top right of the interface are links for Save, Logout, Reboot, and Debug.

Fig 3.2.1 DNS Host blank configuration page



- ▼ Status
- ▼ Network
 - DNS
 - Hosts**
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Network > **Hosts**

Add Host

Host	<input type="text" value="commandonetworks.com"/> (1 to 255 alphanumeric characters)
IPv4/IPv6 Address	<input type="text" value="192.168.0.3"/>

Fig 3.2.2 Add DNS Host and IP address configuration page



- ▼ Status
- ▼ Network
 - DNS
 - Hosts**
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Save | Logout | Reboot | Debug

Network **Hosts**

DNS Host Configuration

<input type="checkbox"/>	Host	IPv4/IPv6 Address
<input type="checkbox"/>	commandonetworks.com	192.168.0.3

Dynamic Host Mapping

Host	Total	Elapsed	Type	IPv4/IPv6 Address
0 results found.				

Fig 3.2.3 DNS Host configuration page

Chapter 4 Port

Port Setting: You can view the summary or detailed information on the switch ports using this page. To see the summary information on all ports on the switch. Port setting allows to configure all ports description, status, speed, duplex, flow control.

Error Disabled: This page enables automatically reactivating a port that has been shutdown / restrict /protect because of an error condition.

Link Aggregation: Link Aggregation Control Protocol (LACP) is part of the IEEE specification (802.3az) that enables you to bundle several physical ports together to form a single logical channel (LAG). LAGs multiply the bandwidth, increase port flexibility, and provide link redundancy between two devices.

Group: Select the LAG number. Traffic load balancing over the active member ports of a LAG is managed by MAC Addresses, IP and MAC Addresses.

Port Setting: You can view the summary or detailed information of LAG ports using this page.

LACP: Select to enable LACP on the selected LAG. Traffic load balancing over the active member ports of a LAG is managed by MAC Addresses, IP and MAC Addresses.

EEE: This page enables the IEEE 802.3az Energy Efficient Ethernet (EEE) function, cable length power saving, and link-up and link-down power saving.

Jumbo Frame: A jumbo frame is an Ethernet frame with a payload greater than the standard maximum transmission unit (MTU) of 1,500 bytes. Jumbo frames are used on local area networks that support at least 1 Gbps and can be as large as 10,000 bytes.

Port Security: Network security can be increased by limiting access on a port to users with specific MAC addresses. The MAC addresses can be either dynamically learned or statically configured. Port security monitors received and learned packets. Ports are limited to users with specific MAC addresses.

Protected Port: Protected Ports provide Layer 2 isolation between interfaces.

Storm Control: Storm protection enables you to limit the number of frames entering the Switch and you can select the types of frames that are counted towards this limit.

Mirroring: Port mirroring is used on a network device to send a copy of network packets seen on one switch port, multiple other ports, or on to network monitoring connection on another port on the switch.

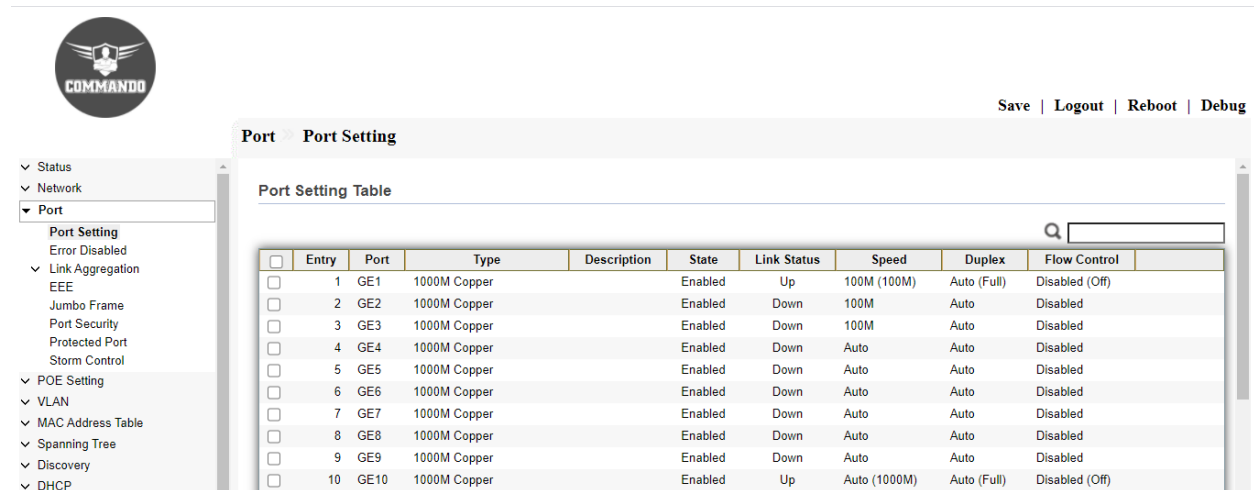
4.1 Port Setting

This page shows Port statistics like Port State, Link Status, speed & Flow control for each port. Port setting allows multiple ports Description, status, speed, duplex, flow control selection pages.

The switch comes with default port settings that should allow you to connect to the Ethernet Ports without any necessary configuration. Should there be a need to change the name of the ports, Port State, negotiation settings or flow control settings, you can do this in the Port settings as shown below:

Select Port number, Click on Edit, Enter the Port description, Select/Deselect Port State to Enable or Disable it. Select the Port speed Auto to Manually from 10M/100M/1000M. This page shows port current status and allow user to edit port configurations. Select port entry and click “Edit” button to edit port configurations.

To display Port Setting web page, click **Port >> Port Setting**



The screenshot shows a web interface for a network switch. On the left is a navigation menu with categories like Status, Network, and Port. The 'Port' category is expanded to show 'Port Setting'. The main area displays a 'Port Setting Table' with 10 rows of port configurations. Each row includes a checkbox, an entry number, port name (GE1-GE10), type (1000M Copper), description, state (Enabled), link status (Up/Down), speed, duplex (Auto/Full), and flow control (Disabled/Off). At the top right of the table area are buttons for 'Save', 'Logout', 'Reboot', and 'Debug'. A search bar is also present above the table.

<input type="checkbox"/>	Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input type="checkbox"/>	1	GE1	1000M Copper		Enabled	Up	100M (100M)	Auto (Full)	Disabled (Off)
<input type="checkbox"/>	2	GE2	1000M Copper		Enabled	Down	100M	Auto	Disabled
<input type="checkbox"/>	3	GE3	1000M Copper		Enabled	Down	100M	Auto	Disabled
<input type="checkbox"/>	4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	10	GE10	1000M Copper		Enabled	Up	Auto (1000M)	Auto (Full)	Disabled (Off)

Fig 4.1.1 Port setting table page



Save | Logout | Reboot |

Port > Port Setting

Port Setting Table

<input checked="" type="checkbox"/>	Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input checked="" type="checkbox"/>	1	GE1	1000M Copper		Enabled	Up	100M (100M)	Auto (Full)	Disabled (Off)
<input checked="" type="checkbox"/>	2	GE2	1000M Copper		Enabled	Down	100M	Auto	Disabled
<input checked="" type="checkbox"/>	3	GE3	1000M Copper		Enabled	Down	100M	Auto	Disabled
<input checked="" type="checkbox"/>	4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	10	GE10	1000M Copper		Enabled	Up	Auto (1000M)	Auto (Full)	Disabled (Off)
<input checked="" type="checkbox"/>	11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	13	GE13	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	14	GE14	1000M Copper		Enabled	Down	Auto	Auto	Disabled
<input checked="" type="checkbox"/>	15	GE15	1000M Copper		Enabled	Down	Auto	Auto	Disabled

Fig 4.1.2 Port setting multiple ports selection page.



Port > Port Setting

Edit Port Setting

Port	GE1-GE28
Description	COMMANDO
State	<input checked="" type="checkbox"/> Enable
Speed	<input checked="" type="radio"/> Auto <input type="radio"/> 10M <input type="radio"/> Auto - 10M <input type="radio"/> 100M <input type="radio"/> Auto - 100M <input type="radio"/> 1000M <input type="radio"/> Auto - 1000M <input type="radio"/> 10G <input type="radio"/> Auto - 10M/100M
Duplex	<input checked="" type="radio"/> Auto <input type="radio"/> Full <input type="radio"/> Half
Flow Control	<input checked="" type="radio"/> Auto <input type="radio"/> Enable <input type="radio"/> Disable

Apply Close

Fig 4.1.3 Port setting multiple ports Description, status, speed, duplex, flow control selection page.

4.2 Error Disabled

When a port is in error-disabled state, it will shut down and no traffic is sent or received on that port. Automatic Recovery Interval to enable the error recovery mechanism for the port security err-disable state by default is 300 seconds.

BPDU Guard: It enable the error recovery mechanism from BPDU guard error-disable state.

UDLD: It enable error recovery mechanism for the UDLD shutdown state.

Self Loop: If by mistake the ports on switches are connected by cables and self-loop is formed then recovery mechanism for the self-loop shutdown state.

Broadcast flood: A "Flood" is an uncontrolled broadcast, usually caused by a fault, such as when there is a loop in the physical network then recovery mechanism for the broadcast flood hanging state.

Unknown Multicast flood: Unknown multicast traffic is flooded to all Layer 2 ports then recovery mechanism for the Unknown Multicast flood hanging state.

ACL: It enable. error recovery mechanism for the ACL deny error-disable state.

Port Security: It enable the error recovery mechanism for the port security err-disable state.

DHCP Rate Limit: By default, DHCP rate limit is disabled. The maximum rate of sending DHCP messages to the DHCP server can be enabled. Excess packets in a specified period are discarded.

ARP Rate limit: The ARP packet rate limit feature allows you to limit the rate of ARP packets delivered to the switch. An ARP attack detection-enabled device will send all received ARP packets to the Switch for inspection. Processing excessive ARP packets will make the Switch malfunction or even crash. This feature can prevent ARP packets rate.

To configure and view Port Error disabled, click **Port >> Error Disabled**



- ∨ Status
- ∨ Network
- ∨ Port
 - Port Setting
 - Error Disabled**
 - ∨ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ QoS

Port > Error Disabled

Recovery Interval	<input type="text" value="300"/>	Sec (30 - 86400)
BPDU Guard	<input type="checkbox"/>	Enable
UDLD	<input type="checkbox"/>	Enable
Self Loop	<input type="checkbox"/>	Enable
Broadcast Flood	<input type="checkbox"/>	Enable
Unknown Multicast Flood	<input type="checkbox"/>	Enable
Unicast Flood	<input type="checkbox"/>	Enable
ACL	<input type="checkbox"/>	Enable
Port Security	<input type="checkbox"/>	Enable
DHCP Rate Limit	<input type="checkbox"/>	Enable
ARP Rate Limit	<input type="checkbox"/>	Enable

Apply

Fig 4.2.1 Error disabled selection page.



- ∨ Status
- ∨ Network
- ∨ Port
 - Port Setting
 - Error Disabled**
 - ∨ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ QoS

Port > Error Disabled

Recovery Interval	<input type="text" value="300"/>	Sec (30 - 86400)
BPDU Guard	<input checked="" type="checkbox"/>	Enable
UDLD	<input checked="" type="checkbox"/>	Enable
Self Loop	<input checked="" type="checkbox"/>	Enable
Broadcast Flood	<input type="checkbox"/>	Enable
Unknown Multicast Flood	<input type="checkbox"/>	Enable
Unicast Flood	<input type="checkbox"/>	Enable
ACL	<input checked="" type="checkbox"/>	Enable
Port Security	<input type="checkbox"/>	Enable
DHCP Rate Limit	<input type="checkbox"/>	Enable
ARP Rate Limit	<input type="checkbox"/>	Enable

Fig 4.2.2 Enabling various parameters in Error disabled selection page.

4.3 Link Aggregation

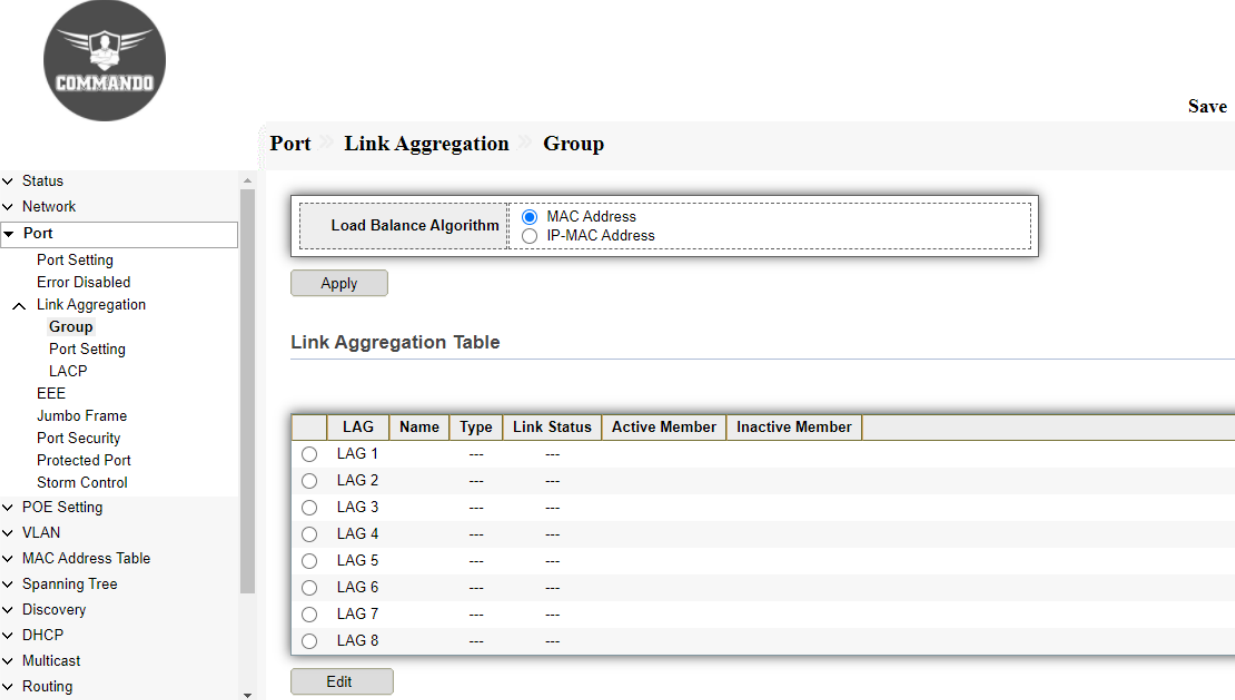
Link aggregation groups (LAGs) allow you to combine multiple Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and load sharing. Specify LAG membership before you enable the LAG. The switch supports up to Eight static LAGs.

This page shows Link Aggregation configuration.

4.3.1 Group

Link aggregation group function allows you to aggregate multiple physical ports into one logic port to increase bandwidth. This switch supports up to 8 groups Link Aggregation & up to 8 ports as one group. This page is to configure link aggregation group load balance algorithm and select group member.

To view the Group menu, Click **Port >> Link Aggregation >> Group**.



The screenshot shows the COMMANDO web interface for configuring Link Aggregation groups. On the left is a navigation menu with categories like Status, Network, Port, Link Aggregation, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, and Routing. The 'Link Aggregation' section is expanded to show 'Group'. The main content area has a breadcrumb trail: **Port > Link Aggregation > Group**. In the top right corner, there is a **Save** button. Below the breadcrumb, there is a 'Load Balance Algorithm' section with two radio button options: **MAC Address** (selected) and **IP-MAC Address**. An **Apply** button is located below these options. Below that is the 'Link Aggregation Table' section, which contains a table with 8 rows representing LAG 1 through LAG 8. Each row has a radio button in the first column, followed by columns for LAG, Name, Type, Link Status, Active Member, and Inactive Member. All Name, Type, and Link Status fields are currently empty (---). An **Edit** button is located at the bottom of the table.

	LAG	Name	Type	Link Status	Active Member	Inactive Member
<input type="radio"/>	LAG 1	---	---	---		
<input type="radio"/>	LAG 2	---	---	---		
<input type="radio"/>	LAG 3	---	---	---		
<input type="radio"/>	LAG 4	---	---	---		
<input type="radio"/>	LAG 5	---	---	---		
<input type="radio"/>	LAG 6	---	---	---		
<input type="radio"/>	LAG 7	---	---	---		
<input type="radio"/>	LAG 8	---	---	---		

Fig 4.3.1 Link Aggregation group selection page.



Save | Log

Port > Link Aggregation > Group

Load Balance Algorithm MAC Address IP-MAC Address

Apply

Link Aggregation Table

LAG	Name	Type	Link Status	Active Member	Inactive Member
<input checked="" type="radio"/>	LAG 1	---	---		
<input type="radio"/>	LAG 2	---	---		
<input type="radio"/>	LAG 3	---	---		
<input type="radio"/>	LAG 4	---	---		
<input type="radio"/>	LAG 5	---	---		
<input type="radio"/>	LAG 6	---	---		
<input type="radio"/>	LAG 7	---	---		
<input type="radio"/>	LAG 8	---	---		

Edit

Fig 4.3.2 Link Aggregation LAG selection for editing page.



Port > Link Aggregation > Group

Edit Link Aggregation Group

LAG 1

Name

Type Static LACP

Member

Available Port	Selected Port
GE3	GE1
GE4	GE2
GE5	
GE6	
GE7	
GE8	
GE9	
GE10	

Apply Close

Fig 4.3.3 Link Aggregation Edit LAG page.



Port > Link Aggregation > Group

Load Balance Algorithm: MAC Address, IP-MAC Address

Apply

Link Aggregation Table

	LAG	Name	Type	Link Status	Active Member	Inactive Member
<input type="radio"/>	LAG 1	COMMANDO	Static	Up	GE1	GE2
<input type="radio"/>	LAG 2	---	---	---	---	---
<input type="radio"/>	LAG 3	---	---	---	---	---
<input type="radio"/>	LAG 4	---	---	---	---	---
<input type="radio"/>	LAG 5	---	---	---	---	---
<input type="radio"/>	LAG 6	---	---	---	---	---
<input type="radio"/>	LAG 7	---	---	---	---	---
<input type="radio"/>	LAG 8	---	---	---	---	---

Edit

Fig 4.3.4 Link Aggregation Table page.



Port > Link Aggregation > Group

Edit Link Aggregation Group

LAG: 2

Name: COMMANDOLACP

Type: Static, LACP

Member:

Available Port	Selected Port
GE11	GE3
GE12	GE4
GE13	GE6
GE14	GE5
GE15	GE7
GE16	GE8
GE17	GE9
GE18	GE10

Apply Close

Fig 4.3.5 LACP Edit LAG page.



Port > Link Aggregation > Group

Load Balance Algorithm MAC Address IP-MAC Address

Apply

Link Aggregation Table

	LAG	Name	Type	Link Status	Active Member	Inactive Member
<input type="radio"/>	LAG 1	COMMANDO	Static	Up	GE1	GE2
<input type="radio"/>	LAG 2	COMMANDOLACP	LACP	Down		GE3-GE10
<input type="radio"/>	LAG 3		---	---		
<input type="radio"/>	LAG 4		---	---		
<input type="radio"/>	LAG 5		---	---		
<input type="radio"/>	LAG 6		---	---		
<input type="radio"/>	LAG 7		---	---		
<input type="radio"/>	LAG 8		---	---		

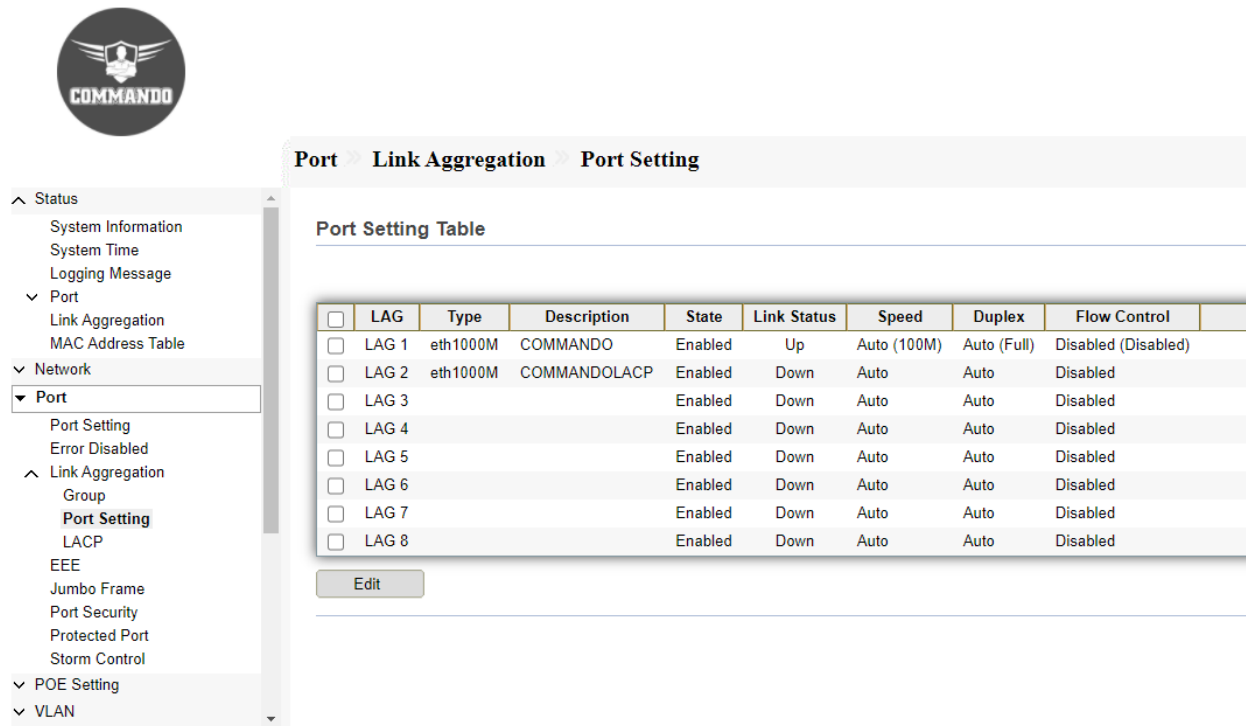
Edit

Fig 4.3.6 Link Aggregation group configuration page

4.3.2 Port Setting

This page shows Port Setting Table of LAG like Type, Description, State, Link Status, Speed, Duplex & Flow control. This page shows LAG port current status and allow user to edit LAG port configurations. Select LAG entry and click Edit button to edit LAG port configurations.

To display LAG Port Setting web page, click **Port >> Link Aggregation >> Port Setting**.



The screenshot displays the COMMANDO network management interface. On the left is a navigation menu with categories like Status, Network, and Link Aggregation. The 'Port Setting' option under 'Link Aggregation' is selected. The main content area shows the 'Port Setting Table' with a table of LAG configurations and an 'Edit' button below it.

<input type="checkbox"/>	LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input type="checkbox"/>	LAG 1	eth1000M	COMMANDO	Enabled	Up	Auto (100M)	Auto (Full)	Disabled (Disabled)
<input type="checkbox"/>	LAG 2	eth1000M	COMMANDOLACP	Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 3			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 4			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 5			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 6			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 7			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 8			Enabled	Down	Auto	Auto	Disabled

Fig 4.3.7 Link Aggregation port setting table page



- ^ Status
 - System Information
 - System Time
 - Logging Message
- ^ Port
 - Link Aggregation
 - MAC Address Table
- ^ Network
 - Port
 - Port Setting
 - Error Disabled
- ^ Link Aggregation
 - Group
 - Port Setting
 - LACP
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
- ^ POE Setting
- ^ VLAN

Port > Link Aggregation > Port Setting

Port Setting Table

<input type="checkbox"/>	LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input checked="" type="checkbox"/>	LAG 1	eth1000M	COMMANDOLAG	Enabled	Up	Auto (100M)	Auto (Full)	Auto (Disabled)
<input checked="" type="checkbox"/>	LAG 2	eth1000M	COMMANDOLAG	Enabled	Down	Auto	Auto	Auto
<input type="checkbox"/>	LAG 3			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 4			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 5			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 6			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 7			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 8			Enabled	Down	Auto	Auto	Disabled

Edit

Fig 4.3.8 Link Aggregation selecting port page



- ^ Status
 - System Information
 - System Time
 - Logging Message
- ^ Port
 - Link Aggregation
 - MAC Address Table
- ^ Network
 - Port
 - Port Setting
 - Error Disabled
- ^ Link Aggregation
 - Group
 - Port Setting
 - LACP
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
- ^ POE Setting
- ^ VLAN

Port > Link Aggregation > Port Setting

Edit Port Setting

Port	LAG1-LAG2	
Description	COMMANDOLAG	
State	<input checked="" type="checkbox"/> Enable	
Speed	<input checked="" type="radio"/> Auto	<input type="radio"/> 10M
	<input type="radio"/> Auto - 10M	<input type="radio"/> 100M
	<input type="radio"/> Auto - 100M	<input type="radio"/> 1000M
	<input type="radio"/> Auto - 1000M	<input type="radio"/> 10G
	<input type="radio"/> Auto - 10M/100M	
Flow Control	<input checked="" type="radio"/> Auto	
	<input type="radio"/> Enable	
	<input type="radio"/> Disable	

Apply Close

Fig 4.3.9 Link Aggregation port setting LAG1-LAG2 and flow control page



Port > Link Aggregation > Port Setting

Port Setting Table

<input type="checkbox"/>	LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input type="checkbox"/>	LAG 1	eth1000M	COMMANDOLAG	Enabled	Up	Auto (100M)	Auto (Full)	Auto (Disabled)
<input type="checkbox"/>	LAG 2	eth1000M	COMMANDOLAG	Enabled	Down	Auto	Auto	Auto
<input type="checkbox"/>	LAG 3			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 4			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 5			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 6			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 7			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 8			Enabled	Down	Auto	Auto	Disabled

Edit

Fig 4.3.10 Link Aggregation port setting table for LAG1-LAG2 page

4.3.3 LACP

Link Aggregation Control Protocol (LACP) is part of the IEEE specification (802.3az) that enables you to bundle several physical ports together to form a single logical channel (LAG). The Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LAGs multiply the bandwidth, increase port flexibility, and provide link redundancy between two devices.

Two types of LAGs are supported:

Static LAG: A LAG is static if the LACP is disabled on it. The group of ports

assigned to a static LAG are always active members.

Dynamic LAG: In Dynamic LAG LACP is enabled on it. The group of ports assigned to dynamic LAG determines which ports are active member ports. The non-active ports are standby ports ready to replace any failing active member ports.

Load Balancing Traffic forwarded to a LAG is load-balanced across the active member ports, thus achieving an effective bandwidth close to the aggregate bandwidth of all the active member ports of the LAG.

Traffic load balancing over the active member ports of a LAG is managed by a hash-based distribution function that distributes Unicast and Multicast traffic based on Layer 2 or Layer 3 packet header information.

The device supports two modes of load balancing:

MAC Addresses: Based on the Destination and Source MAC addresses of all packets.
IP and MAC Addresses: Based on the Destination and Source IP addresses for IP packets, and Destination and Source MAC addresses for non-IP packets.

Timeout: The Timeout controls the period between BPDU transmissions. Long will transmit LACP packets each second, while Short will wait for 30 seconds before sending a LACP packet.

Port Priority: It controls the priority of the ports. If the LACP partner wants to form a larger group than is supported by this device, then this parameter will control which ports will be active & which ports will in backup role. Lower the number means greater the priority. By default, system priority for LACP is 32768.

LAG is treated by the system as a single logical port. In particular, the LAG has port attributes like a regular port, such as state and speed. The device supports 8 LAGs with up to 8 ports in a LAG group. Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Switches connected by multiple links that require high-speed redundant links. This page allow user to configure LACP global and port configurations. Select ports and click Edit button to edit port configuration. To display the LACP Setting page , click **Port >> Link Aggregation >> LACP**.

The screenshot shows the COMMANDO network management interface. On the left is a navigation menu with categories like Status, Network, Port, Link Aggregation, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, and Multicast. The 'Port' section is expanded to show 'LACP' as the selected option. The main content area is titled 'Port > Link Aggregation > LACP'. At the top, there is a 'System Priority' field with a value of '32768' and a note '(1 - 65535, default 32768)'. Below this is an 'Apply' button. The 'LACP Port Setting Table' is displayed below, containing a table with columns for 'Entry', 'Port', 'Port Priority', and 'Timeout'. The table lists 9 entries, each with a checkbox, an entry number, a port name (GE1-GE9), a port priority of 1, and a timeout of 'Long'.

<input type="checkbox"/>	Entry	Port	Port Priority	Timeout
<input type="checkbox"/>	1	GE1	1	Long
<input type="checkbox"/>	2	GE2	1	Long
<input type="checkbox"/>	3	GE3	1	Long
<input type="checkbox"/>	4	GE4	1	Long
<input type="checkbox"/>	5	GE5	1	Long
<input type="checkbox"/>	6	GE6	1	Long
<input type="checkbox"/>	7	GE7	1	Long
<input type="checkbox"/>	8	GE8	1	Long
<input type="checkbox"/>	9	GE9	1	Long

Fig 4.3.6 Link Aggregation LACP Port Setting Table page



- ▼ Status
- ▼ Network
- ▼ Port
- Port Setting
- Error Disabled
- ^ Link Aggregation
- Group
- Port Setting
- LACP**
- EEE
- Jumbo Frame
- Port Security
- Protected Port
- Storm Control
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Port >> Link Aggregation >> LACP

<input checked="" type="checkbox"/>	Entry	Port	Port Priority	Timeout
<input checked="" type="checkbox"/>	1	GE1	1	Long
<input checked="" type="checkbox"/>	2	GE2	1	Long
<input checked="" type="checkbox"/>	3	GE3	1	Long
<input checked="" type="checkbox"/>	4	GE4	1	Long
<input checked="" type="checkbox"/>	5	GE5	1	Long
<input checked="" type="checkbox"/>	6	GE6	1	Long
<input checked="" type="checkbox"/>	7	GE7	1	Long
<input checked="" type="checkbox"/>	8	GE8	1	Long
<input checked="" type="checkbox"/>	9	GE9	1	Long
<input checked="" type="checkbox"/>	10	GE10	1	Long
<input checked="" type="checkbox"/>	11	GE11	1	Long
<input checked="" type="checkbox"/>	12	GE12	1	Long
<input checked="" type="checkbox"/>	13	GE13	1	Long
<input checked="" type="checkbox"/>	14	GE14	1	Long
<input checked="" type="checkbox"/>	15	GE15	1	Long
<input checked="" type="checkbox"/>	16	GE16	1	Long
<input checked="" type="checkbox"/>	17	GE17	1	Long
<input checked="" type="checkbox"/>	18	GE18	1	Long
<input checked="" type="checkbox"/>	19	GE19	1	Long
<input checked="" type="checkbox"/>	20	GE20	1	Long
<input checked="" type="checkbox"/>	21	GE21	1	Long
<input checked="" type="checkbox"/>	22	GE22	1	Long
<input checked="" type="checkbox"/>	23	GE23	1	Long
<input checked="" type="checkbox"/>	24	GE24	1	Long
<input checked="" type="checkbox"/>	25	GE25	1	Long
<input checked="" type="checkbox"/>	26	GE26	1	Long
<input checked="" type="checkbox"/>	27	GE27	1	Long
<input checked="" type="checkbox"/>	28	GE28	1	Long

Edit

Fig 4.3.7 Link Aggregation LACP Port Setting port selection page

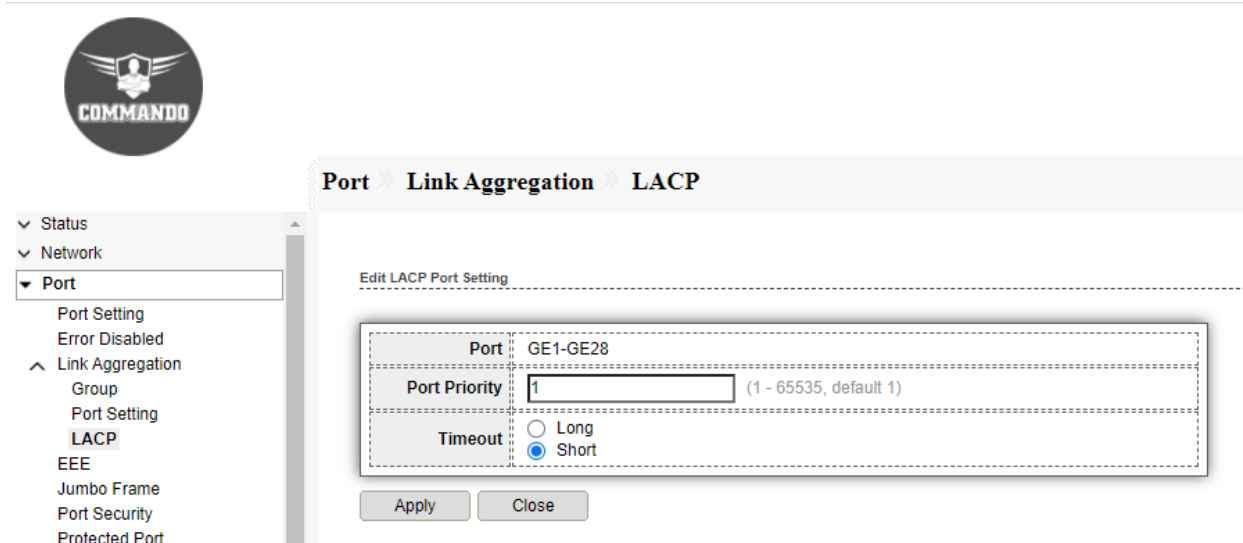


Fig 4.3.8 Edit LACP Port Setting page

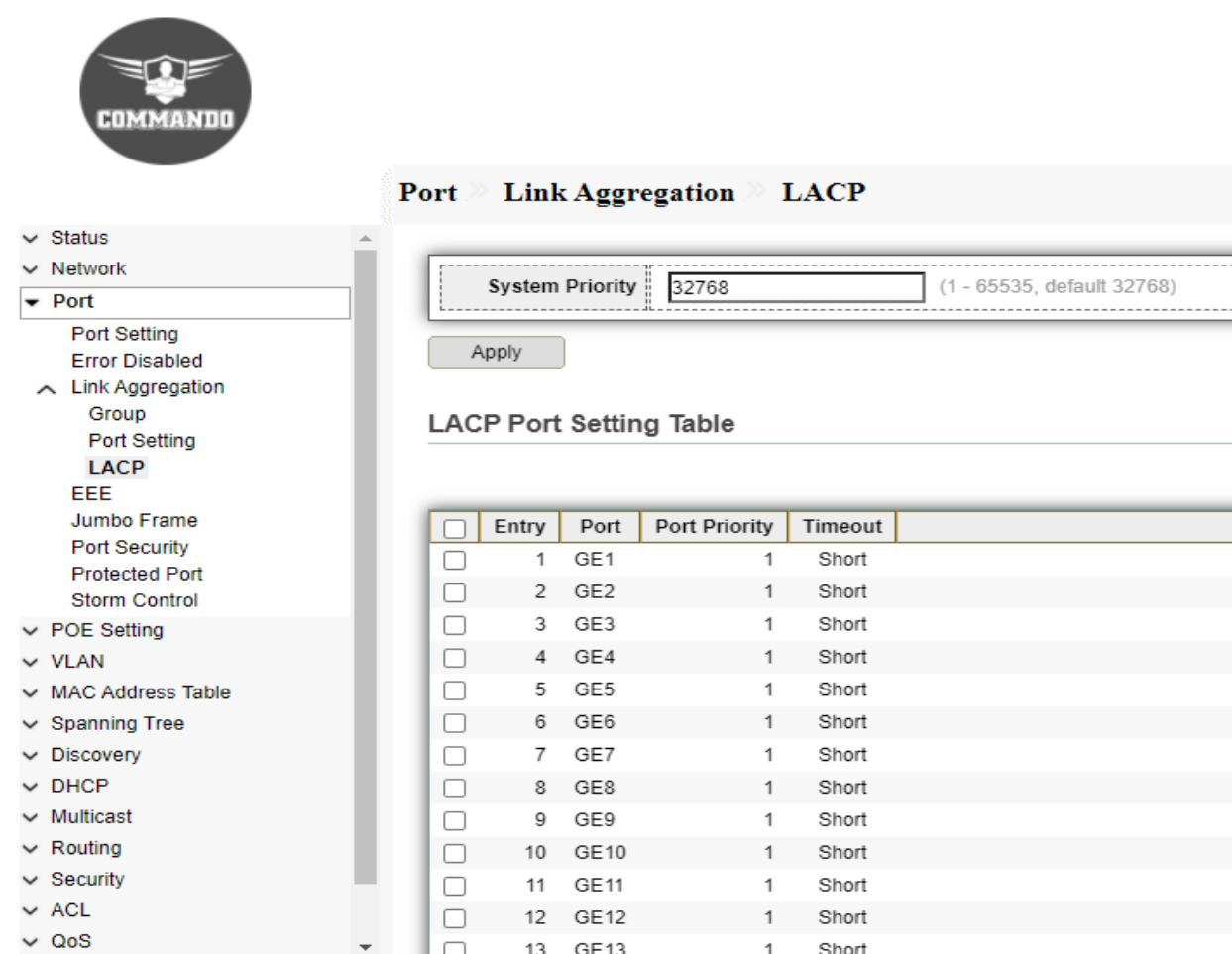


Fig 4.3.9 LACP Port Setting Table page

4.4 EEE

IEEE 802.3az EEE is designed to save power when there is no traffic on the link. IEEE 802.3az Energy Efficient Ethernet (EEE) function, cable length power saving, and link-up and link-down power saving. It Combines the Energy Efficient Ethernet (EEE) 802.3 MAC sublayer with the 10/100/1000BASE-TX physical layers to support operation in Low Power and save power during periods of low link utilization. Short Cable Power Saving dynamically detects and adjusts power that is required for the detected cable length. Link-Down Power Saving reduces the power consumption considerably when the network cable is disconnected. When the network cable is reconnected, the switch detects an incoming signal and restores normal power. This page shows Port setting for EEE, i.e. (Energy Efficient Ethernet) is a technology that reduces switch power consumption during periods of low network traffic. By default, EEE is disabled on E3000 Series Switch and after enabling EEE on Switch it required 50sec time required for EEE activation. This page allow user to configure Energy Efficient Ethernet settings. To configure the EEE, click **Port >> EEE**.



Port >> EEE

- √ Status
- √ Network
- ▼ Port
 - Port Setting
 - Error Disabled
 - √ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
- √ POE Setting
- √ VLAN
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- √ Multicast
- √ Routing
- √ Security
- √ ACL
- √ QoS
- √ Diagnostics
- √ Management

EEE Setting Table

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Disabled
<input type="checkbox"/>	2	GE2	Disabled
<input type="checkbox"/>	3	GE3	Disabled
<input type="checkbox"/>	4	GE4	Disabled
<input type="checkbox"/>	5	GE5	Disabled
<input type="checkbox"/>	6	GE6	Disabled
<input type="checkbox"/>	7	GE7	Disabled
<input type="checkbox"/>	8	GE8	Disabled
<input type="checkbox"/>	9	GE9	Disabled
<input type="checkbox"/>	10	GE10	Disabled
<input type="checkbox"/>	11	GE11	Disabled
<input type="checkbox"/>	12	GE12	Disabled
<input type="checkbox"/>	13	GE13	Disabled
<input type="checkbox"/>	14	GE14	Disabled
<input type="checkbox"/>	15	GE15	Disabled
<input type="checkbox"/>	16	GE16	Disabled

Fig 4.4.1 Port EEE Setting Table port selection page



Port >> EEE

- ▼ Status
- ▼ Network
 - ▼ Port
 - Port Setting
 - Error Disabled
 - ▼ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
 - ▼ POE Setting
 - ▼ VLAN
 - ▼ MAC Address Table
 - ▼ Spanning Tree
 - ▼ Discovery
 - ▼ DHCP
 - ▼ Multicast
 - ▼ Routing
 - ▼ Security
 - ▼ ACL
 - ▼ QoS
 - ▼ Diagnostics
 - ▼ Management

<input checked="" type="checkbox"/>	10	GE10	Disabled
<input checked="" type="checkbox"/>	11	GE11	Disabled
<input checked="" type="checkbox"/>	12	GE12	Disabled
<input checked="" type="checkbox"/>	13	GE13	Disabled
<input checked="" type="checkbox"/>	14	GE14	Disabled
<input checked="" type="checkbox"/>	15	GE15	Disabled
<input checked="" type="checkbox"/>	16	GE16	Disabled
<input checked="" type="checkbox"/>	17	GE17	Disabled
<input checked="" type="checkbox"/>	18	GE18	Disabled
<input checked="" type="checkbox"/>	19	GE19	Disabled
<input checked="" type="checkbox"/>	20	GE20	Disabled
<input checked="" type="checkbox"/>	21	GE21	Disabled
<input checked="" type="checkbox"/>	22	GE22	Disabled
<input checked="" type="checkbox"/>	23	GE23	Disabled
<input checked="" type="checkbox"/>	24	GE24	Disabled
<input checked="" type="checkbox"/>	25	TE1	Disabled
<input checked="" type="checkbox"/>	26	TE2	Disabled
<input checked="" type="checkbox"/>	27	TE3	Disabled
<input checked="" type="checkbox"/>	28	TE4	Disabled

Edit

Fig 4.4.2 Port EEE Setting Table all ports selection page



- ▼ Status
- ▼ Network
- ▼ Port
 - Port Setting
 - Error Disabled
 - ▼ Link Aggregation
 - EEE**
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control

Port >> EEE

Edit EEE Setting

Port	GE1-GE24,TE1-TE4
State	<input checked="" type="checkbox"/> Enable

Apply Close

Fig 4.4.3 Port EEE Setting port application page



Port >> EEE

- √ Status
- √ Network
- ▼ Port
 - Port Setting
 - Error Disabled
 - √ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
- √ POE Setting
- √ VLAN
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- √ Multicast
- √ Routing
- √ Security
- √ ACL
- √ QoS
- √ Diagnostics
- √ Management

EEE Setting Table

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Enabled
<input type="checkbox"/>	2	GE2	Enabled
<input type="checkbox"/>	3	GE3	Enabled
<input type="checkbox"/>	4	GE4	Enabled
<input type="checkbox"/>	5	GE5	Enabled
<input type="checkbox"/>	6	GE6	Enabled
<input type="checkbox"/>	7	GE7	Enabled
<input type="checkbox"/>	8	GE8	Enabled
<input type="checkbox"/>	9	GE9	Enabled
<input type="checkbox"/>	10	GE10	Enabled
<input type="checkbox"/>	11	GE11	Enabled
<input type="checkbox"/>	12	GE12	Enabled
<input type="checkbox"/>	13	GE13	Enabled
<input type="checkbox"/>	14	GE14	Enabled
<input type="checkbox"/>	15	GE15	Enabled
<input type="checkbox"/>	16	GE16	Enabled

Fig 4.4.4 Port EEE Setting Table after Enabled Port page

4.5 Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size of 1518 bytes, which includes the Layer 2 header and Frame Check Sequence (FCS). In other words, jumbo frames refer to Ethernet packets of up to 10000 bytes in size. This page shows the maximum transmission unit (MTU) size of packet that the switch can receive/transmit. User can change the MTU configuration in this page. By default, Jumbo frames are disabled. This page allow user to configure switch jumbo frame size . To Configure Jumbo Frame, click **Port >> Jumbo Frame**.

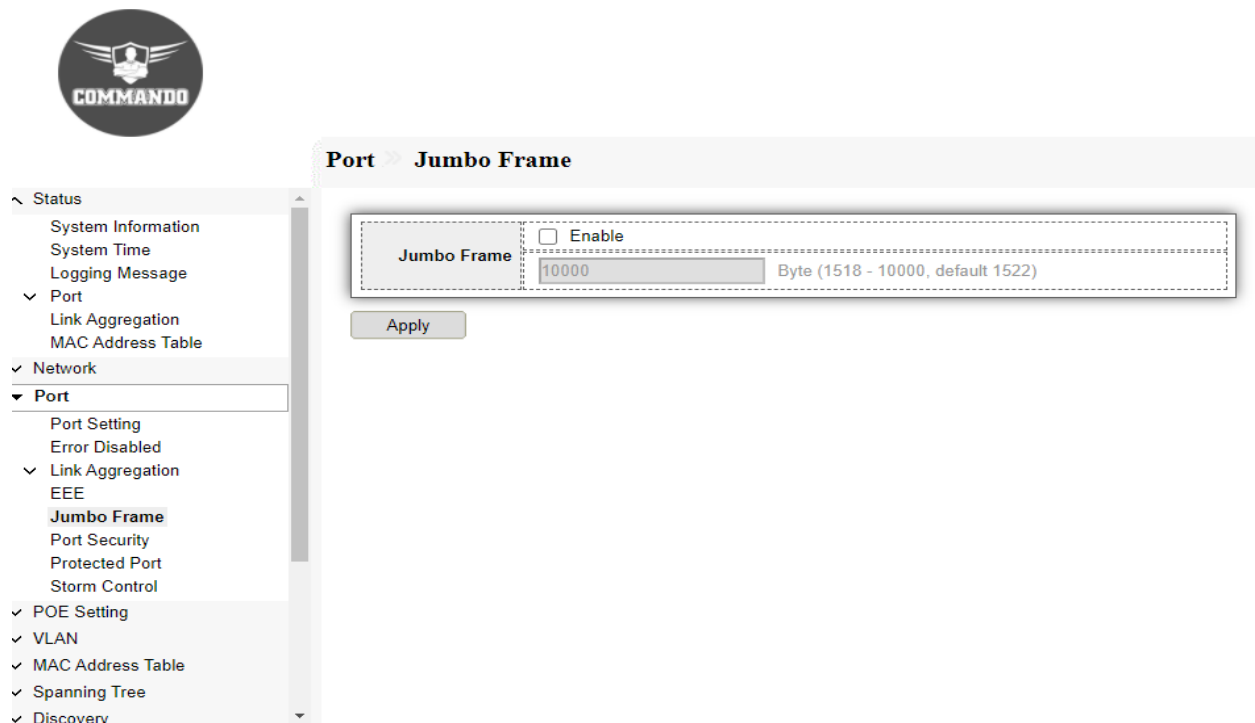


Fig 4.5.1 Jumbo frame enable page



Port > Jumbo Frame

Enable

Jumbo Frame Byte (1518 - 10000, default 1522)

Apply

- ^ Status
 - System Information
 - System Time
 - Logging Message
 - ^ Port
 - Link Aggregation
 - MAC Address Table
 - ^ Network
 - Port
 - Port Setting
 - Error Disabled
 - ^ Link Aggregation
 - EEE
 - Jumbo Frame**
 - Port Security
 - Protected Port
 - Storm Control
 - POE Setting
 - VLAN
 - MAC Address Table
 - Spanning Tree
 - Discovery

Fig 4.5.2 Jumbo Frame Enable for 9216 bytes page

4.6 Port Security

Port security monitors received and learned packets. Access to locked ports is limited to users with specific MAC addresses. Violation Action is when a device with an unauthorized MAC address attempts to use the port, the port will be administratively disabled and must be manually re-enabled.

Protect: Drops packets with unknown source MAC addresses until secure MAC addresses is learned.

Restrict: A port security violation restricts packet after Security Violation. This result into increase in counter and causes an SNMP Notification to be generated.

Shutdown: Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is rebooted.

Sticky: You can Enable/Disable MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn MAC address when the switch restarts.

This page allow user to configure port security settings for each interface. When port security is enabled on interface, Violation action will be performed per limitation. To Configure Port Security, click **Port>> Port Security**



- ^ Status
 - System Information
 - System Time
 - Logging Message
- ✓ Port
 - Link Aggregation
 - MAC Address Table
- ✓ Network
 - ▼ Port
 - Port Setting
 - Error Disabled
 - ✓ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security**
 - Protected Port
 - Storm Control
 - ✓ POE Setting
 - ✓ VLAN
 - ✓ MAC Address Table
 - ✓ Spanning Tree
 - ✓ Discovery

Port > Port Security

State Enable

Rate Limit Packet / Sec (1 - 600, default 100)

Apply

Port Security Table

<input type="checkbox"/>	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
<input type="checkbox"/>	1	GE1	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	2	GE2	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	3	GE3	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	4	GE4	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	5	GE5	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	6	GE6	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	7	GE7	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	8	GE8	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	9	GE9	Disabled	1	0	0	0	Protect	Disabled

Fig 4.6.1 Default Port Security Table page



- ^ Status
 - System Information
 - System Time
 - Logging Message
- ✓ Port
 - Link Aggregation
 - MAC Address Table
- ✓ Network
 - ▼ Port
 - Port Setting
 - Error Disabled
 - ✓ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security**
 - Protected Port
 - Storm Control
 - ✓ POE Setting
 - ✓ VLAN
 - ✓ MAC Address Table
 - ✓ Spanning Tree
 - ✓ Discovery

Save

Port > Port Security

State Enable

Rate Limit Packet / Sec (1 - 600, default 100)

Apply

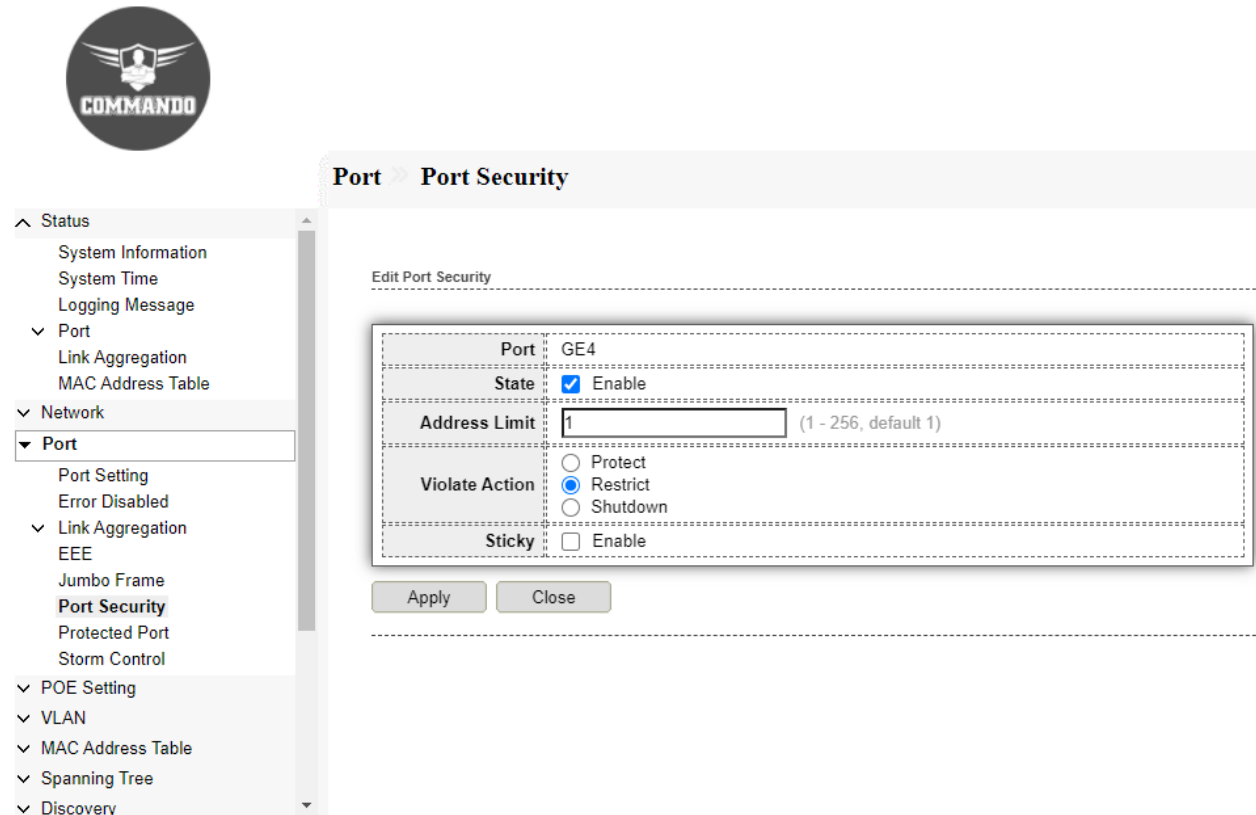
Port Security Table

<input type="checkbox"/>	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
<input type="checkbox"/>	1	GE1	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	2	GE2	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	3	GE3	Disabled	1	0	0	0	Protect	Disabled
<input checked="" type="checkbox"/>	4	GE4	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	5	GE5	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	6	GE6	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	7	GE7	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	8	GE8	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	9	GE9	Disabled	1	0	0	0	Protect	Disabled

Fig 4.6.2 Selecting Port Security GE4 page

Port Security Configuration:

Click on “Port Security” from menu, then Select Port number from Table click on “Edit”. Then Select/Deselect “State” to enable/Disable, Select the Violate Action “Protect or Restrict or Shutdown”, Select\Deselect “Sticky” option & Click on “Apply”.



The screenshot displays the COMMANDO network management interface. On the left is a navigation menu with the following structure:

- ^ Status
 - System Information
 - System Time
 - Logging Message
- ^ Port
 - Link Aggregation
 - MAC Address Table
- ^ Network
 - ▼ Port
 - Port Setting
 - Error Disabled
 - ^ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security**
 - Protected Port
 - Storm Control
- ^ POE Setting
- ^ VLAN
- ^ MAC Address Table
- ^ Spanning Tree
- ^ Discovery

The main content area is titled "Port > Port Security" and contains a form titled "Edit Port Security". The form fields are as follows:

Port	GE4
State	<input checked="" type="checkbox"/> Enable
Address Limit	<input type="text" value="1"/> (1 - 256, default 1)
Violate Action	<input type="radio"/> Protect <input checked="" type="radio"/> Restrict <input type="radio"/> Shutdown
Sticky	<input type="checkbox"/> Enable

At the bottom of the form are two buttons: "Apply" and "Close".

Fig 4.6.3 Edit Port security for GE4 interface page



- ^ Status
 - System Information
 - System Time
 - Logging Message
- ^ Port
 - Link Aggregation
 - MAC Address Table
- ^ Network
 - Port
 - Port Setting
 - Error Disabled
- ^ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
- ^ POE Setting
- ^ VLAN
- ^ MAC Address Table
- ^ Spanning Tree

Port > Port Security

Rate Limit Packet / Sec (1 - 600, default 100)

Apply

Port Security Table

<input type="checkbox"/>	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
<input type="checkbox"/>	1	GE1	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	2	GE2	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	3	GE3	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	4	GE4	Enabled	1	0	0	0	Restrict	Disabled
<input type="checkbox"/>	5	GE5	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	6	GE6	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	7	GE7	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	8	GE8	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	9	GE9	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	10	GE10	Disabled	1	0	0	0	Protect	Disabled

Fig 4.6.4 Port security for GE4 port interface page

4.7 Protected Port

Protected Ports provide Layer 2 isolation between interfaces ports and LAGs that share the same VLAN. Packets received from protected ports can be forwarded only to unprotected egress ports. Port protection is not subject to VLAN membership. Devices connected to protected ports are not allowed to communicate with each other, even if they are members of the same VLAN.

This shows Protected Port function to make port to be protected. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port. To Configure Protected Port, click **Security >> Protected Port**.



Port » Protected Port

- ^ Status
 - System Information
 - System Time
 - Logging Message
 - ✓ Port
 - Link Aggregation
 - MAC Address Table
 - ✓ Network
 - ▼ Port
 - Port Setting
 - Error Disabled
 - ✓ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port**
 - Storm Control
 - ✓ POE Setting
 - ✓ VLAN
 - ✓ MAC Address Table
 - ✓ Spanning Tree
 - ✓ Discovery

Protected Port Table

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Unprotected
<input type="checkbox"/>	2	GE2	Unprotected
<input type="checkbox"/>	3	GE3	Unprotected
<input type="checkbox"/>	4	GE4	Unprotected
<input type="checkbox"/>	5	GE5	Unprotected
<input type="checkbox"/>	6	GE6	Unprotected
<input type="checkbox"/>	7	GE7	Unprotected
<input type="checkbox"/>	8	GE8	Unprotected
<input type="checkbox"/>	9	GE9	Unprotected
<input type="checkbox"/>	10	GE10	Unprotected
<input type="checkbox"/>	11	GE11	Unprotected
<input type="checkbox"/>	12	GE12	Unprotected
<input type="checkbox"/>	13	GE13	Unprotected
<input type="checkbox"/>	14	GE14	Unprotected

Fig 4.7.1 Protected Port Table page



Port » Protected Port

- ^ Status
 - System Information
 - System Time
 - Logging Message
 - ✓ Port
 - Link Aggregation
 - MAC Address Table
 - ✓ Network
 - ▼ Port
 - Port Setting
 - Error Disabled
 - ✓ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port**
 - Storm Control
 - ✓ POE Setting
 - ✓ VLAN
 - ✓ MAC Address Table
 - ✓ Spanning Tree
 - ✓ Discovery

Protected Port Table

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Unprotected
<input type="checkbox"/>	2	GE2	Unprotected
<input type="checkbox"/>	3	GE3	Unprotected
<input type="checkbox"/>	4	GE4	Unprotected
<input type="checkbox"/>	5	GE5	Unprotected
<input checked="" type="checkbox"/>	6	GE6	Unprotected
<input type="checkbox"/>	7	GE7	Unprotected
<input type="checkbox"/>	8	GE8	Unprotected
<input type="checkbox"/>	9	GE9	Unprotected
<input type="checkbox"/>	10	GE10	Unprotected
<input type="checkbox"/>	11	GE11	Unprotected
<input type="checkbox"/>	12	GE12	Unprotected
<input type="checkbox"/>	13	GE13	Unprotected
<input type="checkbox"/>	14	GE14	Unprotected

Fig 4.7.2 Selection of GE6 port for Protected page



Port > Protected Port

^ Status

- System Information
- System Time
- Logging Message
- Port
 - Link Aggregation
 - MAC Address Table
- Network
 - Port
 - Port Setting
 - Error Disabled
 - Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port**
 - Storm Control
 - POE Setting
 - VLAN
 - MAC Address Table
 - Spanning Tree
 - Discovery

Edit Protected Port

Port	GE6
State	<input checked="" type="checkbox"/> Protected

Apply Close

Fig 4.7.3 Enable GE6 port for Protected Port configuration page



Port >> Protected Port

Protected Port Table

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Unprotected
<input type="checkbox"/>	2	GE2	Unprotected
<input type="checkbox"/>	3	GE3	Unprotected
<input type="checkbox"/>	4	GE4	Unprotected
<input type="checkbox"/>	5	GE5	Unprotected
<input type="checkbox"/>	6	GE6	Protected
<input type="checkbox"/>	7	GE7	Unprotected
<input type="checkbox"/>	8	GE8	Unprotected
<input type="checkbox"/>	9	GE9	Unprotected
<input type="checkbox"/>	10	GE10	Unprotected
<input type="checkbox"/>	11	GE11	Unprotected
<input type="checkbox"/>	12	GE12	Unprotected
<input type="checkbox"/>	13	GE13	Unprotected
<input type="checkbox"/>	14	GE14	Unprotected

Navigation Menu:

- ^ Status
 - System Information
 - System Time
 - Logging Message
- ∨ Port
 - Link Aggregation
 - MAC Address Table
- ∨ Network
 - Port**
 - Port Setting
 - Error Disabled
 - ∨ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port**
 - Storm Control
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery

Fig 4.7.4 Protected Port Table after enabling GE1 page

4.8 Storm Control

When Broadcast, Multicast, or Unknown Unicast frames are received, they are duplicated, and a copy is sent to all possible egress ports. This means that in practice they are sent to all ports belonging to the relevant VLAN. In this way, one ingress frame is turned into many, creating the potential for a traffic storm.

Storm protection enables you to limit the number of frames entering the device and to define the types of frames that are counted towards this limit. By default, storm control is disabled. Broadcast storm control is a feature in which the switch intentionally ceases to forward all broadcast traffic if the bandwidth consumed by incoming broadcast frames exceeds a designated threshold.

If a particular type of ingress traffic (unicast, broadcast and multicast) is more than the rising threshold configured on a switch, the interface goes to blocked state for that particular traffic. Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. To configure Storm Control global setting, click **Security >> Storm Control**.

The screenshot shows the COMMANDO network management interface. On the left is a sidebar menu with categories like Status, Network, and Port. The 'Port' section is expanded, showing 'Storm Control' as the selected option. The main content area is titled 'Port Storm Control' and contains a configuration form with two sections: 'Mode' and 'IFG'. The 'Mode' section has radio buttons for 'Packet / Sec' and 'Kbits / Sec', with 'Kbits / Sec' selected. The 'IFG' section has radio buttons for 'Exclude' and 'Include', with 'Exclude' selected. Below the form is an 'Apply' button. Underneath is a 'Port Setting Table' with a table of port configurations.

	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
<input type="checkbox"/>	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Fig 4.8.1 Default Storm control port setting table page



- ^ Status
 - System Information
 - System Time
 - Logging Message
- ^ Port
 - Link Aggregation
 - MAC Address Table
- ^ Network
 - ^ Port
 - Port Setting
 - Error Disabled
 - Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control**
- ^ POE Setting
- ^ VLAN
- ^ MAC Address Table
- ^ Spanning Tree
- ^ Discovery

Port Storm Control

Mode: Packet / Sec
 Kbits / Sec

IFG: Exclude
 Include

Apply

Port Setting Table

Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action	
			State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)		
<input checked="" type="checkbox"/>	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input checked="" type="checkbox"/>	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input checked="" type="checkbox"/>	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input checked="" type="checkbox"/>	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input checked="" type="checkbox"/>	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input checked="" type="checkbox"/>	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input checked="" type="checkbox"/>	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Fig 4.8.2 Storm control Selecting port setting page



- ^ Status
 - System Information
 - System Time
 - Logging Message
- ^ Port
 - Link Aggregation
 - MAC Address Table
- ^ Network
 - ^ Port
 - Port Setting
 - Error Disabled
 - Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control**
- ^ POE Setting
- ^ VLAN
- ^ MAC Address Table
- ^ Spanning Tree
- ^ Discovery

Port Storm Control

Edit Port Setting

Port: GE1-GE28

State: Enable

Broadcast: Enable
1000 Kbps (16 - 1000000, default 10000)

Unknown Multicast: Enable
100 Kbps (16 - 1000000, default 10000)

Unknown Unicast: Enable
10000 Kbps (16 - 1000000, default 10000)

Action: Drop
 Shutdown

Apply Close

Fig 4.8.3 Storm control Edit port setting page



- ^ Status
 - System Information
 - System Time
 - Logging Message
- ^ Port
 - Link Aggregation
 - MAC Address Table
- ^ Network
 - ^ Port**
 - Port Setting
 - Error Disabled
 - ^ Link Aggregation
 - EEE
 - Jumbo Frame
 - Port Security
 - Protected Port
 - Storm Control
 - ^ POE Setting
 - ^ VLAN
 - ^ MAC Address Table
 - ^ Spanning Tree
 - ^ Discovery
 - ^ DHCP
 - ^ Multicast
 - ^ Routing
 - ^ Security
 - ^ ACL
 - ^ QoS
 - ^ Diagnostics
 - ^ Management

Port Storm Control

Mode	<input type="radio"/> Packet / Sec
	<input checked="" type="radio"/> Kbits / Sec
IFG	<input checked="" type="radio"/> Exclude
	<input type="radio"/> Include

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
<input type="checkbox"/>	1	GE1	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	2	GE2	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	3	GE3	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	4	GE4	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	5	GE5	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	6	GE6	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	7	GE7	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	8	GE8	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	9	GE9	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	10	GE10	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	11	GE11	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	12	GE12	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	13	GE13	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	14	GE14	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop
<input type="checkbox"/>	15	GE15	Enabled	Enabled	1008	Disabled	100	Disabled	10000	Drop

Fig 4.8.4 Storm control port setting selection page

Chapter 5 VLAN

VLAN: A VLAN is simply an administratively defined subset of switch ports that are in the same broadcast domain.

Create VLAN: You can create a VLANs. Each VLAN must be configured with a unique VID (VLAN ID) with a value from 2 to 4094.

VLAN Configuration: VLAN configuration lets you assign ports on the switch to a VLAN with an ID number in the range of 1-4094. By default, all ports are members of VLAN 1.

Membership: After you create a new VLAN ID, use the VLAN membership option to add ports to the VLAN.

Port Setting: For setting ports for mode like Hybrid, Access, Trunk, Tunnel and PVID (1-4094).

Voice VLAN: The voice VLAN feature can help ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high.

Property: You can select one VLAN as the voice VLAN, select the Class of Service (CoS) for voice traffic, and enable or disable the voice VLAN for specific ports that carry traffic from IP phones.

Voice OUI: Automatic assignment of traffic to Voice VLAN is done using the Organizationally Unique Identifier (OUI) MAC Address. The first three bytes in a MAC address contain the manufacturer ID (Organizationally Unique Identifiers - OUI) and the last three bytes contain a unique station ID.

Protocol VLAN: A protocol based VLAN processes traffic based on protocol. You can use a protocol based VLAN to define filtering criteria for untagged packets. If you do not change the port configuration or configure a protocol based VLAN, the switch assigns untagged packets to VLAN 1.

Protocol Group: Groups of protocols can be defined and then bound to a port. After the protocol group is bound to a port, every packet originating from a protocol in the group is assigned the VLAN that is configured in the Protocol-Based Groups page.

Group Binding: To add group binding for available ports after selection to particular VLAN for a specific group ID.

MAC VLAN: You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified using a source MAC address and the appropriate VLAN ID. The MAC to VLAN configurations are shared across all ports of the device

MAC Group: When a frame is received from a VLAN that is configured to forward, based on MAC group addresses

Group Binding--> Group Id can map the MAC addresses.

Surveillance VLAN: Surveillance VLAN function ensures the quality of real-time video for monitoring and control without compromising the transmission of conventional network data. This is a special feature of E3000 series Switches.

Property -->VLAN configuration for CCTV is very important to protect the IP cameras against unauthorized access and to separate the security camera system from other computers and devices that are connected to the IP network.

Surveillance OUI: IP surveillance cameras of multiple manufacture having different OUI. You can add a specific manufacturer with the OUI. Surveillance cameras will transmit their data on a Surveillance VLAN.

GVRP: The GVRP page displays information regarding GARP VLAN Registration Protocol (GVRP) frames that were sent or received from a port. GVRP is a standards-based Layer 2 network protocol, for automatic configuration of VLAN information on switches.

Property--> GARP VLAN Registration Protocol (GVRP) is required for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP helps VLAN-aware bridges to automatically learn VLANs to bridge ports mapping. Individual configuration of each switch and VLAN membership registration is not required.

Membership--> GVRP-compliant switches use GARP to register and de-register attribute values, such as VLAN IDs, with each other.

Statistics--> This page shows information for VLAN Configuration like VLAN creation, to assign VLAN Membership, assign per port VLAN configurations.

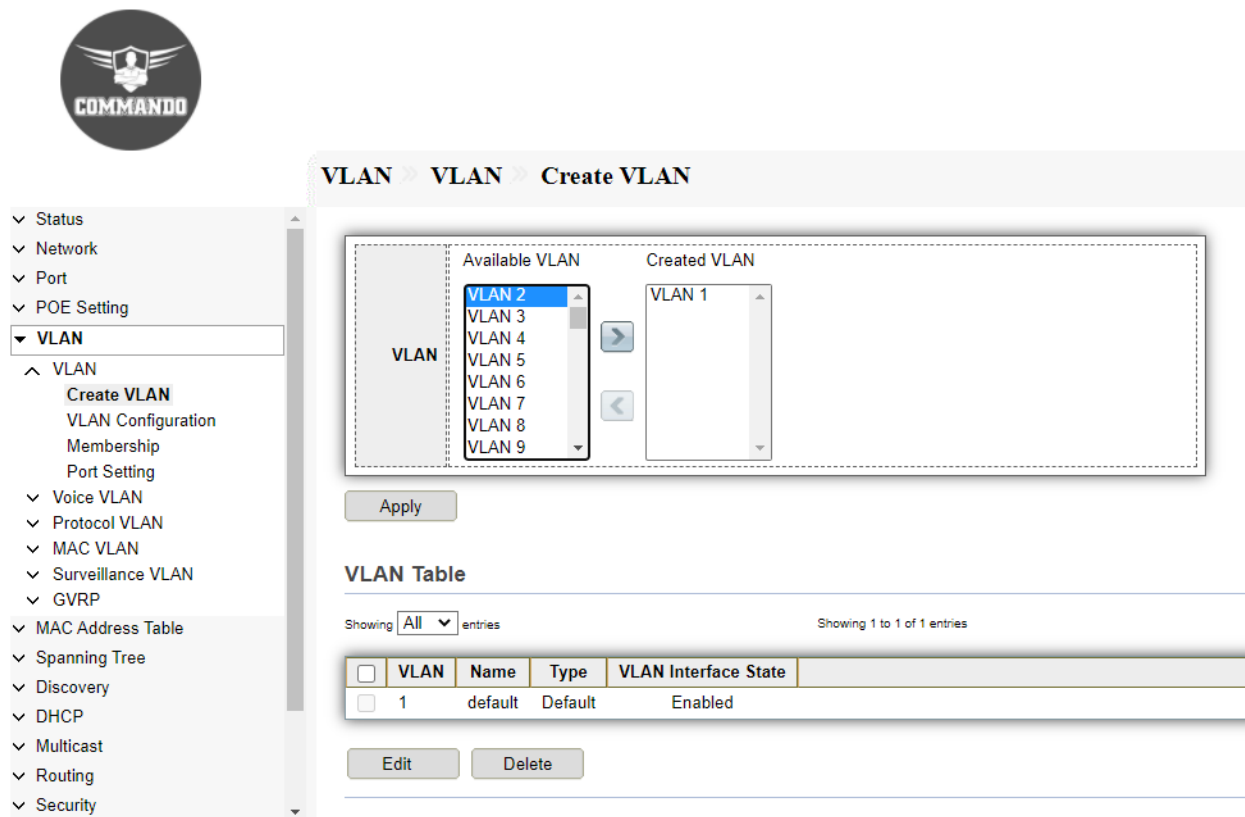
5.1 VLAN

VLAN (Virtual Local Area Network) logically divide one LAN (Local Area Network) into a plurality of subsets, and each subset will form their own broadcast area network. In short, VLAN is a communication technology that logically divide one physical LAN into multiple broadcast area network (multiple VLAN). Hosts within a VLAN can communicate directly but VLAN groups can not directly communicate with each other. So, it will limit the broadcast packets within a VLAN since it cannot directly access between VLAN groups, thus it improves network security.

5.1.1 Create VLAN

This page allows user to add or delete VLAN ID entries. Each VLAN entry has a unique name, user can edit VLAN name in edit page.

To Create VLAN, click **VLAN >> VLAN >> Create VLAN**



COMMANDO

VLAN > VLAN > Create VLAN

Available VLAN

- VLAN 2
- VLAN 3
- VLAN 4
- VLAN 5
- VLAN 6
- VLAN 7
- VLAN 8
- VLAN 9

Created VLAN

- VLAN 1

Apply

VLAN Table

Showing All entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	VLAN	Name	Type	VLAN Interface State
<input type="checkbox"/>	1	default	Default	Enabled

Edit Delete

Fig 5.1.1 Create VLAN Default Page

VLAN Creation:

- Click on “Create VLAN” from menu, select the “Available VLAN” from the list, then Press “>” button & select required VLAN click on “Apply”.
- To change default name of VLAN, Select the VLAN ID & click on “Edit “from VLAN Table, Enter the Name for VLAN & Click on “Apply”.



The screenshot shows the "VLAN > VLAN > Create VLAN" configuration page. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, Voice VLAN, Protocol VLAN, MAC VLAN, Surveillance VLAN, GVRP, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, and Security. The "VLAN" section is expanded, showing "Create VLAN" as the active option.

The main content area is titled "VLAN > VLAN > Create VLAN" and contains two lists of VLANs:

- Available VLAN:** VLAN 4, VLAN 5, VLAN 6, VLAN 7, VLAN 8, VLAN 9, VLAN 11, VLAN 12.
- Created VLAN:** VLAN 1, VLAN 2, VLAN 3, VLAN 10.

Navigation arrows between the lists and an "Apply" button are visible.

Below the lists is the "VLAN Table" section, which shows a table of existing VLANs. The table has columns for "VLAN", "Name", "Type", and "VLAN Interface State".

<input type="checkbox"/>	VLAN	Name	Type	VLAN Interface State
<input type="checkbox"/>	1	default	Default	Enabled
<input type="checkbox"/>	2	VLAN0002	Static	Disabled
<input type="checkbox"/>	3	VLAN0003	Static	Disabled
<input type="checkbox"/>	10	VLAN0010	Static	Disabled

Fig 5.1.2 VLAN Page after VLAN creation



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN**
 - VLAN Configuration
 - Membership
 - Port Setting
 - ▼ Voice VLAN
 - ▼ Protocol VLAN
 - ▼ MAC VLAN
 - ▼ Surveillance VLAN
 - ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security

VLAN > VLAN > Create VLAN

VLAN

VLAN 5
VLAN 6
VLAN 7
VLAN 8
VLAN 9
VLAN 11
VLAN 12

VLAN 2
VLAN 3
VLAN 10

Apply

VLAN Table

Showing All entries Showing 1 to 4 of 4 entries

<input type="checkbox"/>	VLAN	Name	Type	VLAN Interface State
<input type="checkbox"/>	1	default	Default	Enabled
<input checked="" type="checkbox"/>	2	VLAN0002	Static	Disabled
<input type="checkbox"/>	3	VLAN0003	Static	Disabled
<input type="checkbox"/>	10	VLAN0010	Static	Disabled

Edit Delete

Fig 5.1.3 VLAN Default name after VLAN creation



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN**
 - VLAN Configuration
 - Membership
 - Port Setting
 - ▼ Voice VLAN
 - ▼ Protocol VLAN
 - ▼ MAC VLAN
 - ▼ Surveillance VLAN
 - ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security

VLAN > VLAN > Create VLAN

Edit VLAN Name

Name

Apply Close

Fig 5.1.4 Edit VLAN name after VLAN creation



- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN**
 - VLAN Configuration
 - Membership
 - Port Setting
 - ✓ Voice VLAN
 - ✓ Protocol VLAN
 - ✓ MAC VLAN
 - ✓ Surveillance VLAN
 - ✓ GVRP
 - ✓ MAC Address Table
 - ✓ Spanning Tree
 - ✓ Discovery
 - ✓ DHCP
 - ✓ Multicast
 - ✓ Routing
 - ✓ Security

VLAN > VLAN > Create VLAN

VLAN

VLAN 5
VLAN 6
VLAN 7
VLAN 8
VLAN 9
VLAN 11
VLAN 12

VLAN 2
VLAN 3
VLAN 10

Apply

VLAN Table

Showing All entries Showing 1 to 4 of 4 entries

<input type="checkbox"/>	VLAN	Name	Type	VLAN Interface State
<input type="checkbox"/>	1	default	Default	Enabled
<input type="checkbox"/>	2	COMMANDO	Static	Disabled
<input type="checkbox"/>	3	VLAN0003	Static	Disabled
<input type="checkbox"/>	10	VLAN0010	Static	Disabled

Edit Delete

Fig 5.1.5 VLAN Table after VLAN name change page

5.1.2 VLAN Configuration

This page allow user to configure the membership for each port of selected VLAN.

For VLAN Configuration, click **VLAN >> VLAN Configuration**. Click on “Create VLAN” from menu, Select “VLAN” name from Drop down & Select “Untagged” option on the Ports which required to add to the VLAN, then Click on “Apply”.



VLAN > VLAN > VLAN Configuration

VLAN Configuration Table

VLAN: **default** (dropdown menu showing: default, COMMANDO, VLAN0003, VLAN0010)

Entry	Port	Mode	Excluded	Tagged	Membership	PVID	Forbidden
1	GE1	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	GE2	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	GE3	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	GE4	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	GE5	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	GE6	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	GE7	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	GE8	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9	GE9	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10	GE10	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11	GE11	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12	GE12	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
13	GE13	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
14	GE14	Trunk	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Fig 5.1.6 VLAN configuration table page



- √ Status
- √ Network
- √ Port
- √ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN
 - VLAN Configuration**
 - Membership
 - Port Setting
 - √ Voice VLAN
 - √ Protocol VLAN
 - √ MAC VLAN
 - √ Surveillance VLAN
 - √ GVRP
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- √ Multicast
- √ Routing
- √ Security

VLAN » VLAN » VLAN Configuration

VLAN Configuration Table

VLAN

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
2	GE2	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
3	GE3	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
4	GE4	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
5	GE5	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
6	GE6	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
7	GE7	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
8	GE8	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
9	GE9	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
10	GE10	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
11	GE11	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
12	GE12	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
13	GE13	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
14	GE14	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>

Fig 5.1.7 VLAN Selection tap on VLAN configuration table page



VLAN » VLAN » VLAN Configuration

- √ Status
- √ Network
- √ Port
- √ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN
 - VLAN Configuration**
 - Membership
 - Port Setting
 - √ Voice VLAN
 - √ Protocol VLAN
 - √ MAC VLAN
 - √ Surveillance VLAN
 - √ GVRP
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- √ Multicast
- √ Routing
- √ Security

VLAN Configuration Table

VLAN

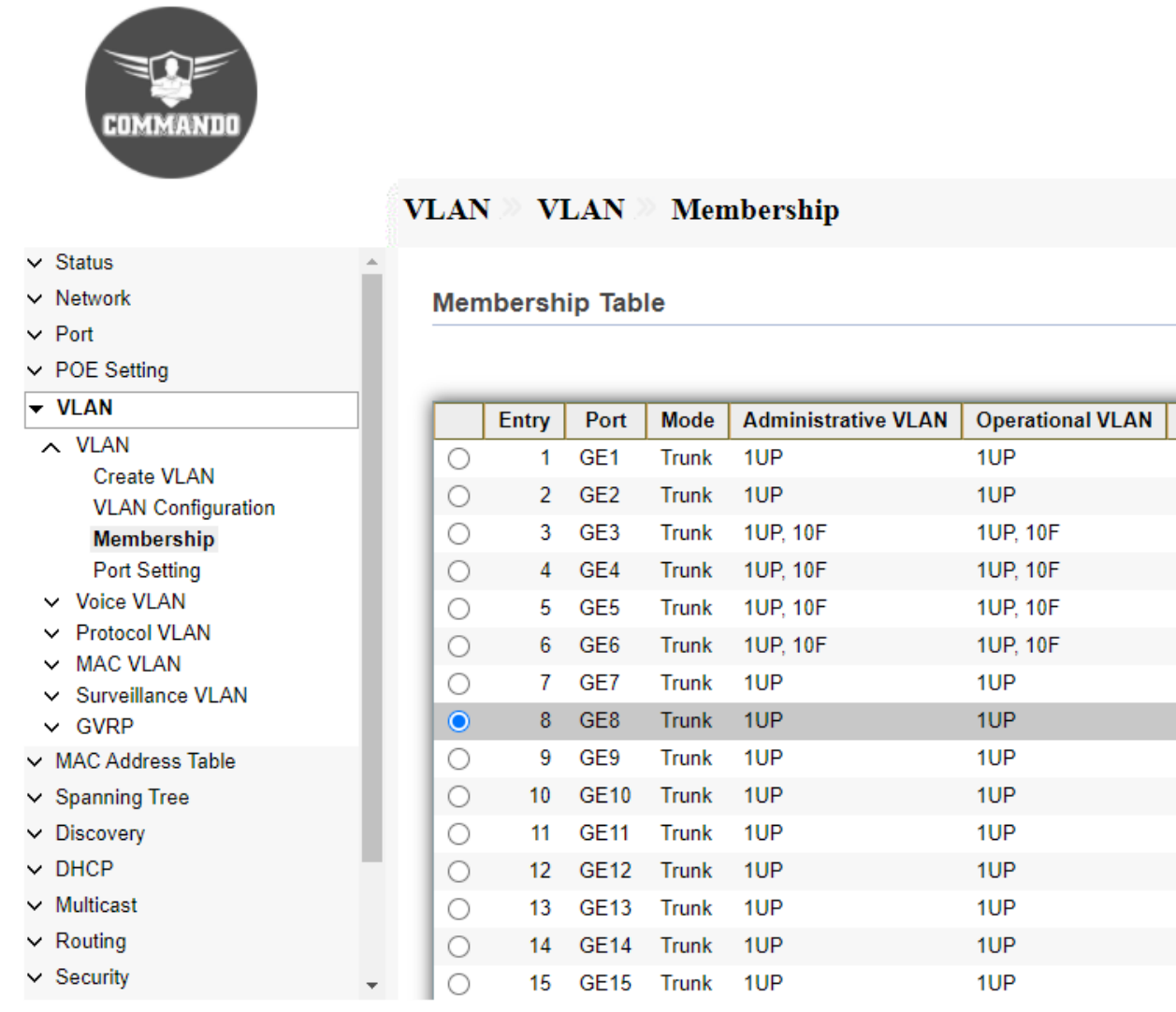
Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
2	GE2	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
3	GE3	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	GE4	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	GE5	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	GE6	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7	GE7	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
8	GE8	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
9	GE9	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
10	GE10	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
11	GE11	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
12	GE12	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
13	GE13	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
14	GE14	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>

Fig 5.1.8 VLAN configuration for Ports selection page

5.1.3 Membership

This page allow user to view membership information for each port and edit membership for specified interface.

For VLAN Membership page, click **VLAN >> Membership**



COMMANDO

VLAN >> VLAN >> Membership

Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
<input type="radio"/>	1	GE1	Trunk	1UP	1UP
<input type="radio"/>	2	GE2	Trunk	1UP	1UP
<input type="radio"/>	3	GE3	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	4	GE4	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	5	GE5	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	6	GE6	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	7	GE7	Trunk	1UP	1UP
<input checked="" type="radio"/>	8	GE8	Trunk	1UP	1UP
<input type="radio"/>	9	GE9	Trunk	1UP	1UP
<input type="radio"/>	10	GE10	Trunk	1UP	1UP
<input type="radio"/>	11	GE11	Trunk	1UP	1UP
<input type="radio"/>	12	GE12	Trunk	1UP	1UP
<input type="radio"/>	13	GE13	Trunk	1UP	1UP
<input type="radio"/>	14	GE14	Trunk	1UP	1UP
<input type="radio"/>	15	GE15	Trunk	1UP	1UP

Fig 5.1.9 VLAN Membership table age



VLAN » VLAN » Membership

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN
 - VLAN Configuration
 - Membership**
 - Port Setting
 - ✓ Voice VLAN
 - ✓ Protocol VLAN
 - ✓ MAC VLAN
 - ✓ Surveillance VLAN
 - ✓ GVRP
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security

Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
<input type="radio"/>	1	GE1	Trunk	1UP	1UP
<input type="radio"/>	2	GE2	Trunk	1UP	1UP
<input type="radio"/>	3	GE3	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	4	GE4	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	5	GE5	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	6	GE6	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	7	GE7	Trunk	1UP	1UP
<input checked="" type="radio"/>	8	GE8	Trunk	1UP	1UP
<input type="radio"/>	9	GE9	Trunk	1UP	1UP
<input type="radio"/>	10	GE10	Trunk	1UP	1UP
<input type="radio"/>	11	GE11	Trunk	1UP	1UP
<input type="radio"/>	12	GE12	Trunk	1UP	1UP
<input type="radio"/>	13	GE13	Trunk	1UP	1UP
<input type="radio"/>	14	GE14	Trunk	1UP	1UP
<input type="radio"/>	15	GE15	Trunk	1UP	1UP

Fig 5.1.10 VLAN membership to be changed for selected port GE8 page



- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN
 - VLAN Configuration
 - Membership**
 - Port Setting
 - ✓ Voice VLAN
 - ✓ Protocol VLAN
 - ✓ MAC VLAN
 - ✓ Surveillance VLAN
 - ✓ GVRP
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security

VLAN > VLAN > Membership

Edit Port Setting

Port	GE8	
Mode	Trunk	
Membership	2	1UP
	10	3T

Forbidden
 Excluded
 Tagged
 Untagged
 PVID

Apply Close

Fig 5.1.11 Edit VLAN membership for selected port GE8 page



VLAN > VLAN > Membership

- ∨ Status
- ∨ Network
- ∨ Port
- ∨ POE Setting
- ∨ **VLAN**
 - ∧ VLAN
 - Create VLAN
 - VLAN Configuration
 - Membership**
 - Port Setting
 - ∨ Voice VLAN
 - ∨ Protocol VLAN
 - ∨ MAC VLAN
 - ∨ Surveillance VLAN
 - ∨ GVRP
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security


	Entry	Port	Mode	Administrative VLAN	Operational VLAN
<input type="radio"/>	1	GE1	Trunk	1UP	1UP
<input type="radio"/>	2	GE2	Trunk	1UP	1UP
<input type="radio"/>	3	GE3	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	4	GE4	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	5	GE5	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	6	GE6	Trunk	1UP, 10F	1UP, 10F
<input type="radio"/>	7	GE7	Trunk	1UP	1UP
<input type="radio"/>	8	GE8	Trunk	1UP, 3T	1UP, 3T
<input type="radio"/>	9	GE9	Trunk	1UP	1UP
<input type="radio"/>	10	GE10	Trunk	1UP	1UP
<input type="radio"/>	11	GE11	Trunk	1UP	1UP
<input type="radio"/>	12	GE12	Trunk	1UP	1UP
<input type="radio"/>	13	GE13	Trunk	1UP	1UP
<input type="radio"/>	14	GE14	Trunk	1UP	1UP
<input type="radio"/>	15	GE15	Trunk	1UP	1UP
<input type="radio"/>	16	GE16	Trunk	1UP	1UP
<input type="radio"/>	17	GE17	Trunk	1UP	1UP
<input type="radio"/>	18	GE18	Trunk	1UP	1UP
<input type="radio"/>	19	GE19	Trunk	1UP	1UP

Fig 5.1.12 VLAN 3 membership for Port GE8 table page

5.1.4 Port Setting

This page allow user to configure ports VLAN settings. The attributes depend on different VLAN port mode.

For Port Setting page, click **VLAN >> Port Setting**



VLAN > VLAN > Port Setting

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
<input type="checkbox"/>	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	10	GE10	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	11	GE11	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	12	GE12	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	13	GE13	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	14	GE14	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	15	GE15	Trunk	1	All	Enabled	Disabled	0x8100

Fig 5.1.13 VLAN port setting table page



VLAN >> VLAN >> Port Setting

- √ Status
- √ Network
- √ Port
- √ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN
 - VLAN Configuration
 - Membership
 - Port Setting**
 - √ Voice VLAN
 - √ Protocol VLAN
 - √ MAC VLAN
 - √ Surveillance VLAN
 - √ GVRP
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- √ Multicast
- √ Routing
- √ Security

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
<input type="checkbox"/>	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
<input checked="" type="checkbox"/>	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
<input checked="" type="checkbox"/>	3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
<input checked="" type="checkbox"/>	4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
<input checked="" type="checkbox"/>	5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	10	GE10	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	11	GE11	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	12	GE12	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	13	GE13	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	14	GE14	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	15	GE15	Trunk	1	All	Enabled	Disabled	0x8100

Fig 5.1.14 VLAN port setting for selected port page



VLAN > VLAN > Port Setting

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN
 - VLAN Configuration
 - Membership
 - Port Setting**
 - ▼ Voice VLAN
 - ▼ Protocol VLAN
 - ▼ MAC VLAN
 - ▼ Surveillance VLAN
 - ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security

Edit Port Setting

Port	GE2-GE5
Mode	<input type="radio"/> Hybrid <input checked="" type="radio"/> Access <input type="radio"/> Trunk <input type="radio"/> Tunnel
PVID	<input type="text" value="3"/> (1 - 4094)
Accept Frame Type	<input checked="" type="radio"/> All <input type="radio"/> Tag Only <input type="radio"/> Untag Only
Ingress Filtering	<input checked="" type="checkbox"/> Enable
Uplink	<input type="checkbox"/> Enable
TPID	<input type="text" value="0x8100"/>

Apply Close

Fig 5.1.15 Edit port setting for selected ports page



- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ▼ **VLAN**
 - ^ VLAN
 - Create VLAN
 - VLAN Configuration
 - Membership
 - Port Setting**
 - ✓ Voice VLAN
 - ✓ Protocol VLAN
 - ✓ MAC VLAN
 - ✓ Surveillance VLAN
 - ✓ GVRP
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security

VLAN > VLAN > Port Setting

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
<input type="checkbox"/>	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	2	GE2	Access	3	Untag Only	Enabled	Disabled	0x8100
<input type="checkbox"/>	3	GE3	Access	3	Untag Only	Enabled	Disabled	0x8100
<input type="checkbox"/>	4	GE4	Access	3	Untag Only	Enabled	Disabled	0x8100
<input type="checkbox"/>	5	GE5	Access	3	Untag Only	Enabled	Disabled	0x8100
<input type="checkbox"/>	6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	10	GE10	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	11	GE11	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	12	GE12	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	13	GE13	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	14	GE14	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	15	GE15	Trunk	1	All	Enabled	Disabled	0x8100

Fig 5.1.16 After Editing port setting for selected ports page

5.2 Voice VLAN

In a LAN, voice devices, such as IP phones, VoIP endpoints, and voice systems are placed into the same VLAN. This VLAN is referred as the voice VLAN. Voice VLAN allows you to easily prioritize IP voice traffic through the switch. This page shows the configuration to enable the functional Voice VLAN on the device.

Voice VLAN can propagate the CoS/802.1p and DSCP settings by using LLDP MED Network policies. The LLDP-MED is set by default to respond with the Voice QoS setting if an appliance sends LLDP-MED packets. MED-supported devices must send their voice traffic with the same CoS/802.1p and DSCP values, as received with the LLDP-MED response.

You can disable the automatic update between Voice VLAN and LLDP-MED and use his own network policies. Working with the OUI mode, the device can additionally configure the mapping and remarking (CoS/802.1p) of the voice traffic based on the OUI. By default, all interfaces are CoS/802.1p trusted. The device applies the quality of service based on the CoS/802.1p value found in the voice stream. In Auto Voice VLAN, you can override the value of the voice streams using advanced QoS. For Telephony OUI voice streams, you can override the quality of service and optionally remark the 802.1p of the voice streams by specifying the desired CoS/802.1p values and using the remarking option under Telephony OUI.

5.2.1 Property

Voice VLAN Configuration:

Click on “Voice VLAN”, then “Property” from menu, Select/Deselect “State” to Enable/Disable, then select “VLAN” name from dropdown, Select “CoS/802.1p Remarking” & Click on “Apply”.

Configuration object and description:

CoS/802.1p: Select a CoS/802.1p value that to be used by LLDP-MED as a voice network policy. This page allow user to configure global and per interface settings of voice VLAN. For Voice VLAN Property, click **VLAN>> Voice VLAN>> Property**.



- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ▼ **VLAN**
- ▼ VLAN
- ▲ Voice VLAN
 - Property**
 - Voice OUI
- ▼ Protocol VLAN
- ▼ MAC VLAN
- ▼ Surveillance VLAN
- ▼ GVRP
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS

VLAN > Voice VLAN > Property

State	<input type="checkbox"/> Enable
VLAN	None
CoS / 802.1p Remarking	<input type="checkbox"/> Enable 6
Aging Time	1440 <small>Min (30 - 65536, default 1440)</small>

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Disabled	Auto	Voice Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Voice Packet
<input type="checkbox"/>	3	GE3	Disabled	Auto	Voice Packet
<input type="checkbox"/>	4	GE4	Disabled	Auto	Voice Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Voice Packet
<input type="checkbox"/>	6	GF6	Disabled	Auto	Voice Packet

Fig 5.2.1 Default Voice VLAN state setting table page



- √ Status
- √ Network
- √ Port
- √ POE Setting
- ▼ **VLAN**
- √ VLAN
- ^ Voice VLAN
- Property**
- Voice OUI
- √ Protocol VLAN
- √ MAC VLAN
- √ Surveillance VLAN
- √ GVRP
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- √ Multicast
- √ Routing
- √ Security
- √ ACL
- √ QoS

VLAN >> Voice VLAN >> Property

State	<input checked="" type="checkbox"/> Enable
VLAN	VLAN0003
CoS / 802.1p Remarking	<input checked="" type="checkbox"/> Enable 4
Aging Time	10000 Min (30 - 65536, default 1440)

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Disabled	Auto	Voice Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Voice Packet
<input type="checkbox"/>	3	GE3	Disabled	Auto	Voice Packet
<input type="checkbox"/>	4	GE4	Disabled	Auto	Voice Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Voice Packet
<input type="checkbox"/>	6	GF6	Disabled	Auto	Voice Packet

Fig 5.2.2 Change Voice VLAN setting CoS/802.1p Remarking page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
- ▼ VLAN
- ▲ Voice VLAN
 - Property
 - Voice OUI
- ▼ Protocol VLAN
- ▼ MAC VLAN
- ▼ Surveillance VLAN
- ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS

VLAN >> Voice VLAN >> Property

State	<input checked="" type="checkbox"/> Enable
VLAN	VLAN0003
CoS / 802.1p Remarking	<input checked="" type="checkbox"/> Enable 4
Aging Time	10000 Min (30 - 65536, default 1440)

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Disabled	Auto	Voice Packet
<input checked="" type="checkbox"/>	2	GE2	Disabled	Auto	Voice Packet
<input checked="" type="checkbox"/>	3	GE3	Disabled	Auto	Voice Packet
<input checked="" type="checkbox"/>	4	GE4	Disabled	Auto	Voice Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Voice Packet
<input type="checkbox"/>	6	GF6	Disabled	Auto	Voice Packet

Fig 5.2.3 Voice VLAN setting CoS/802.1p Remarking page



VLAN > Voice VLAN > Property

▼ Status
▼ Network
▼ Port
▼ POE Setting
▼ **VLAN**
 ▼ VLAN
 ▲ Voice VLAN
 Property
 Voice OUI
 ▼ Protocol VLAN
 ▼ MAC VLAN
 ▼ Surveillance VLAN
 ▼ GVRP
▼ MAC Address Table
▼ Spanning Tree
▼ Discovery
▼ DHCP
▼ Multicast
▼ Routing
▼ Security
▼ ACL
▼ QoS

Edit Port Setting

Port	GE2-GE4
State	<input checked="" type="checkbox"/> Enable
Mode	<input type="radio"/> Auto <input checked="" type="radio"/> Manual
QoS Policy	<input checked="" type="radio"/> Voice Packet <input type="radio"/> All

Apply Close

Fig 5.2.4 Voice VLAN Edit port setting page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
 - ▼ VLAN
 - ▲ Voice VLAN
 - Property**
 - Voice OUI
 - ▼ Protocol VLAN
 - ▼ MAC VLAN
 - ▼ Surveillance VLAN
 - ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS

VLAN » Voice VLAN » Property

State	<input checked="" type="checkbox"/> Enable
VLAN	VLAN0003
CoS / 802.1p Remarking	<input checked="" type="checkbox"/> Enable 4
Aging Time	10000 Min (30 - 65536, default 1440)

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Disabled	Auto	Voice Packet
<input type="checkbox"/>	2	GE2	Enabled	Manual	Voice Packet
<input type="checkbox"/>	3	GE3	Enabled	Manual	Voice Packet
<input type="checkbox"/>	4	GE4	Enabled	Manual	Voice Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Voice Packet
<input type="checkbox"/>	6	GE6	Disabled	Auto	Voice Packet

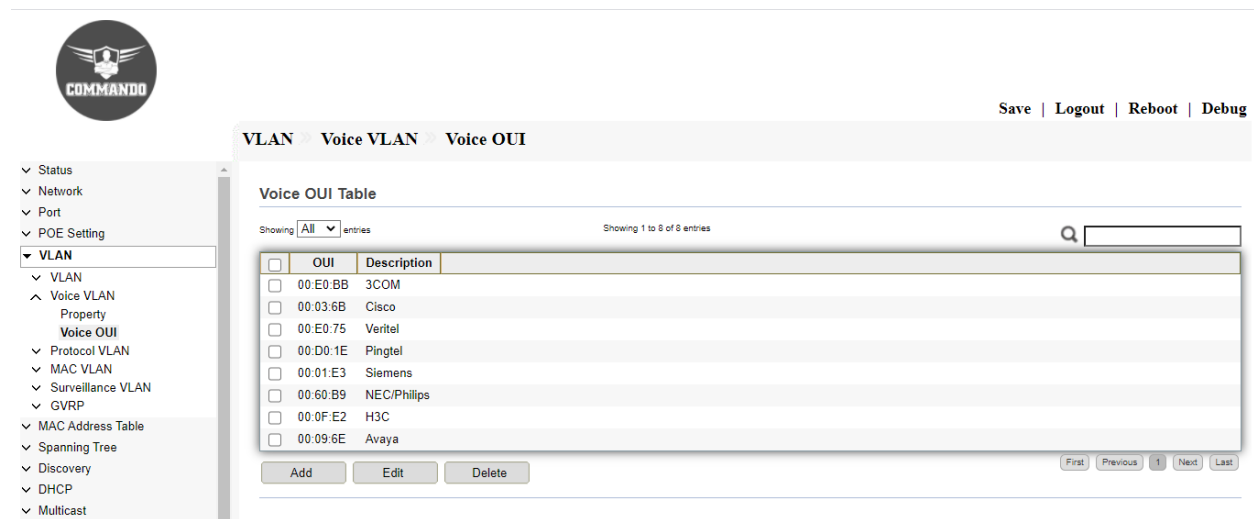
Fig 5.2.5 Voice VLAN Port setting table page

5.2.2 Voice OUI

Voice OUIs are assigned by the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority. Since the number of IP phone manufacturers is limited and well-known, the known OUI values cause the relevant frames, and the port on which they are seen, to be automatically assigned to a Voice VLAN. Organizationally Unique Identifiers (OUI) are the first three bytes of a MAC Address, while the last three bytes contain a unique station ID. You can add a specific manufacturer with the OUI. Once the OUI is added, all traffic received on voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN. Unlike the telephony OUI mode that detects voice devices based on telephony OUI, Auto Voice VLAN mode depends on auto smart port to dynamically add the ports to the voice VLAN.

This page allow user to add, edit or delete OUI MAC addresses. Default has 8 predefined OUI MAC address. This page shows the configuration to enable the functional OUI Voice VLAN on the interfaces.

For Voice OUI, click **VLAN >> Voice VLAN >> Voice OUI**.



The screenshot shows a web-based configuration interface for a network device. On the left is a navigation menu with a 'COMMANDO' logo at the top. The menu items include: Status, Network, Port, POE Setting, VLAN (selected), Voice VLAN, Property, Voice OUI (selected), Protocol VLAN, MAC VLAN, Surveillance VLAN, GVRP, MAC Address Table, Spanning Tree, Discovery, DHCP, and Multicast. The main content area is titled 'Voice OUI Table' and has tabs for 'VLAN', 'Voice VLAN', and 'Voice OUI'. At the top right of the main area are links for 'Save', 'Logout', 'Reboot', and 'Debug'. Below the tabs, there is a search bar and a dropdown menu set to 'All' entries, with a note 'Showing 1 to 8 of 8 entries'. The table contains the following data:

<input type="checkbox"/>	OUI	Description
<input type="checkbox"/>	00:E0:BB	3COM
<input type="checkbox"/>	00:03:6B	Cisco
<input type="checkbox"/>	00:E0:75	Veritel
<input type="checkbox"/>	00:D0:1E	Pingtel
<input type="checkbox"/>	00:01:E3	Siemens
<input type="checkbox"/>	00:60:B9	NEC/Philips
<input type="checkbox"/>	00:0F:E2	H3C
<input type="checkbox"/>	00:09:6E	Avaya

At the bottom of the table are buttons for 'Add', 'Edit', and 'Delete'. On the far right, there are navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'.

Fig 5.2.6 Voice VLAN Voice OUI Table page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
- ▼ VLAN
- ▲ Voice VLAN
 - Property
 - Voice OUI**
- ▼ Protocol VLAN
- ▼ MAC VLAN
- ▼ Surveillance VLAN
- ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP

VLAN > Voice VLAN > Voice OUI

Voice OUI Table

Showing entries Showing 1 to 8 of 8 entries

<input type="checkbox"/>	OUI	Description
<input type="checkbox"/>	00:E0:BB	3COM
<input checked="" type="checkbox"/>	00:03:6B	Cisco
<input type="checkbox"/>	00:E0:75	Veritel
<input type="checkbox"/>	00:D0:1E	Pingtel
<input type="checkbox"/>	00:01:E3	Siemens
<input type="checkbox"/>	00:60:B9	NEC/Philips
<input type="checkbox"/>	00:0F:E2	H3C
<input type="checkbox"/>	00:09:6E	Avaya

Fig 5.2.7 Selecting Voice VLAN Voice OUI page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
- ▼ VLAN
- ▲ Voice VLAN
 - Property
 - Voice OUI**
- ▼ Protocol VLAN
- ▼ MAC VLAN
- ▼ Surveillance VLAN
- ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree

Save |

VLAN > Voice VLAN > Voice OUI

Add Voice OUI

OUI	<input type="text" value="1a"/> : <input type="text" value="2b"/> : <input type="text" value="3c"/>
Description	<input type="text" value="CiscolPPhone"/>

Fig 5.2.8 Voice VLAN Add Voice OUI page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
- ▼ VLAN
- ^ Voice VLAN
 - Property
 - Voice OUI**
- ▼ Protocol VLAN
- ▼ MAC VLAN
- ▼ Surveillance VLAN
- ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast

VLAN > Voice VLAN > Voice OUI

Voice OUI Table

Showing entries

Showing 1 to 9 of 9 entries

<input type="checkbox"/>	OUI	Description
<input type="checkbox"/>	00:E0:BB	3COM
<input type="checkbox"/>	00:03:6B	Cisco
<input type="checkbox"/>	00:E0:75	Veritel
<input type="checkbox"/>	00:D0:1E	Pingtel
<input type="checkbox"/>	00:01:E3	Siemens
<input type="checkbox"/>	00:60:B9	NEC/Philips
<input type="checkbox"/>	00:0F:E2	H3C
<input type="checkbox"/>	00:09:6E	Avaya
<input type="checkbox"/>	1A:2B:3C	CiscoIPPhone

Fig 5.2.9 Voice VLAN Voice OUI Table page

5.3 Protocol VLAN

A protocol based VLAN processes traffic based on protocol. You can use a protocol based VLAN to define filtering criteria for untagged packets. The protocol VLAN defines the protocol profile, which comprises the frame encapsulation and protocol type. One port can be configured with several protocol profiles. When the protocol VLAN is enabled on the port, the protocol profile is configured on the port.

5.3.1 Protocol Group

It shows the configuration to add protocol VLAN group with specified prototype and value. This page allow user to add or edit groups settings of protocol VLAN. For Protocol Group, click **VLAN >> Protocol VLAN >> Protocol Group**.

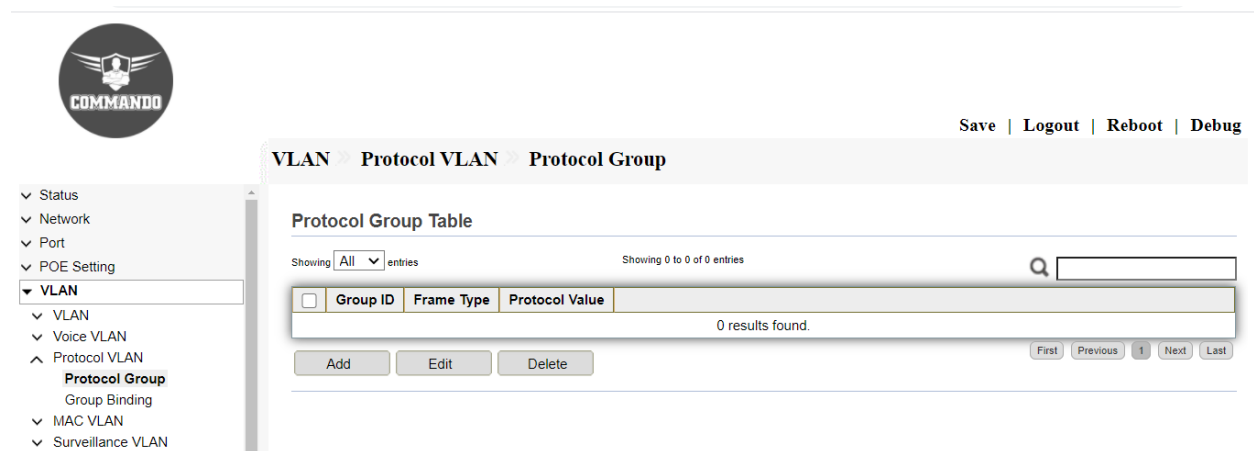


Fig 5.3.1 Default Protocol VLAN Protocol Group Table page

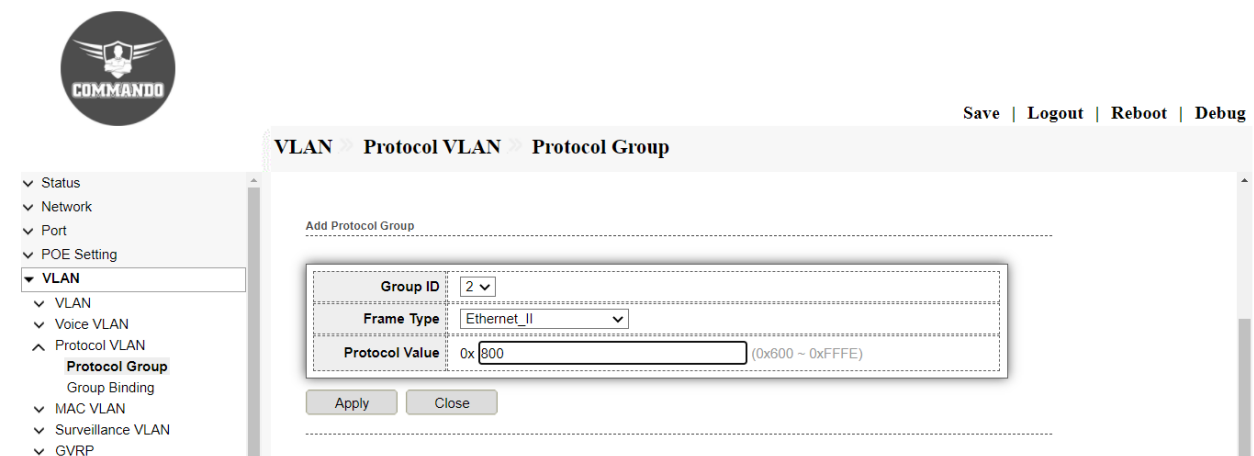


Fig 5.3.2 Add Protocol group page



Save | Logout | Reboot | Debug

VLAN > Protocol VLAN > Protocol Group

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ▼ VLAN
- ✓ VLAN
- ✓ Voice VLAN
- ^ Protocol VLAN
 - Protocol Group**
 - Group Binding
- ✓ MAC VLAN
- ✓ Surveillance VLAN

Protocol Group Table

Showing All entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Group ID	Frame Type	Protocol Value
<input type="checkbox"/>	2	Ethernet_II	0x0800

Add Edit Delete

First Previous 1 Next Last

Fig 5.3.3 Protocol group table page

5.3.2 Group Binding

This page allow user to bind protocol VLAN group to each port with VLAN ID. For Group Binding, click **VLAN>> Protocol VLAN >> Group Binding**.

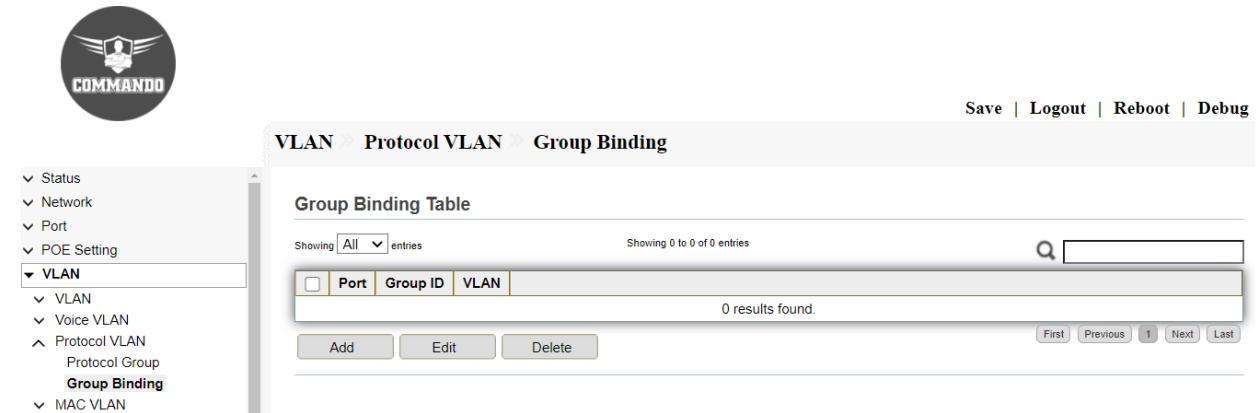


Fig 5.3.5 Default Group Binding Table page

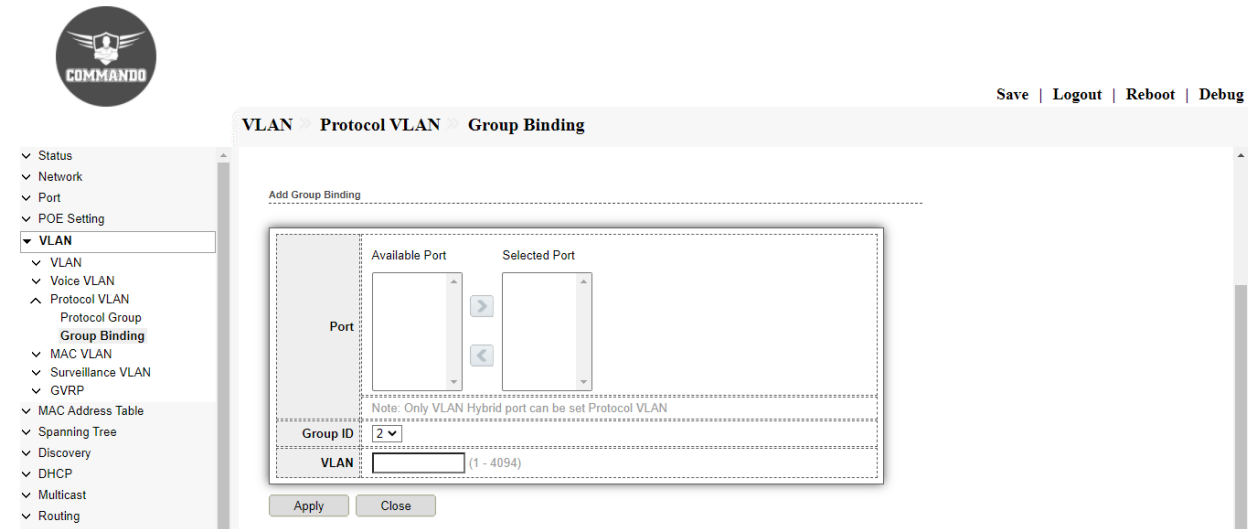


Fig 5.3.6 Add Group Binding page



VLAN > Protocol VLAN > Group Binding

▼ Status
▼ Network
▼ Port
▼ POE Setting
▼ VLAN
▼ VLAN
▼ Voice VLAN
^ Protocol VLAN
 Protocol Group
 Group Binding
▼ MAC VLAN
▼ Surveillance VLAN
▼ GVRP
▼ MAC Address Table
▼ Spanning Tree
▼ Discovery
▼ DHCP
▼ Multicast
▼ Routing

Add Group Binding

Available Port Selected Port

Port

Group ID: 2

VLAN: (1 - 4094)

Apply Close

[Note: Only VLAN Hybrid port can be set Protocol VLAN](#)

Fig 5.3.7 Group Binding for hybrid port page

5.4 MAC VLAN

The MAC-based VLAN classification enables packets to be classified according to their source MAC address. MAC-based VLAN is to divide VLAN ID to the packet according to the source MAC address of the untag packet received by the port.

5.4.1 MAC Group

This page allow user to add or edit groups settings of MAC VLAN.

For MAC page , click **VLAN >> MAC VLAN >> MAC Group**.

The screenshot shows the Commando network management interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, and VLAN. The 'VLAN' category is expanded to show 'MAC VLAN' and 'MAC Group'. The main content area displays the 'MAC Group Table' page. At the top right, there are links for 'Save | Logout | Reboot | Debug'. Below the breadcrumb trail, the page title is 'MAC Group Table'. It shows 'Showing All entries' and 'Showing 0 to 0 of 0 entries'. A search bar is present. The table has columns for 'Group ID', 'MAC Address', and 'Mask', and it is currently empty with '0 results found.' Below the table are 'Add', 'Edit', and 'Delete' buttons. At the bottom right of the table area are pagination controls: 'First', 'Previous', '1', 'Next', and 'Last'.

Fig 5.4.1 Default MAC Group Table page

Click on “MAC Group” from menu, Click on “Add”, then select “Group ID”, “MAC Address” and “Mask” value and Click on “Apply”.



Save | Logout | Reboot | Debug

VLAN > MAC VLAN > MAC Group

Add MAC Group

Group ID	100	(1 - 2147483647)
MAC Address	1a:2d:3c:4f:5d:6a	(A:B:C:D:E:F)
Mask	24	(0 - 48)

Apply Close

Fig 5.4.2 Add MAC Group ID page



Save | Logout | Reboot | Debug

VLAN > MAC VLAN > MAC Group

MAC Group Table

Showing All entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Group ID	MAC Address	Mask
<input type="checkbox"/>	100	1A:2D:3C:4F:5D:6A	24

Add Edit Delete

First Previous 1 Next Last

Fig 5.4.3 Mac Group table page

5.4.2 Group Binding

This page creates MAC-based VLAN groups and map them to a specific interface (Ports/LAG).

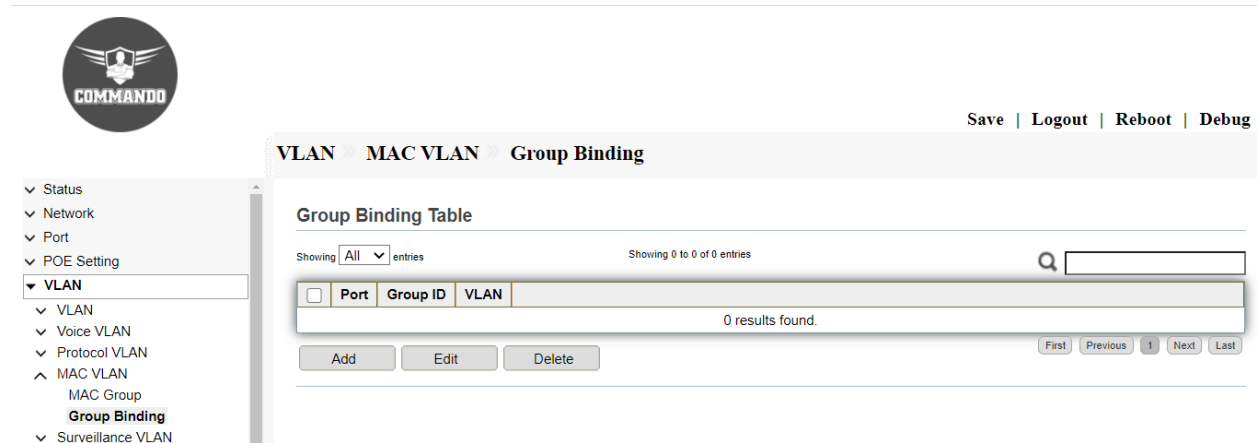


Fig 5.4.4 Blank Group binding table page

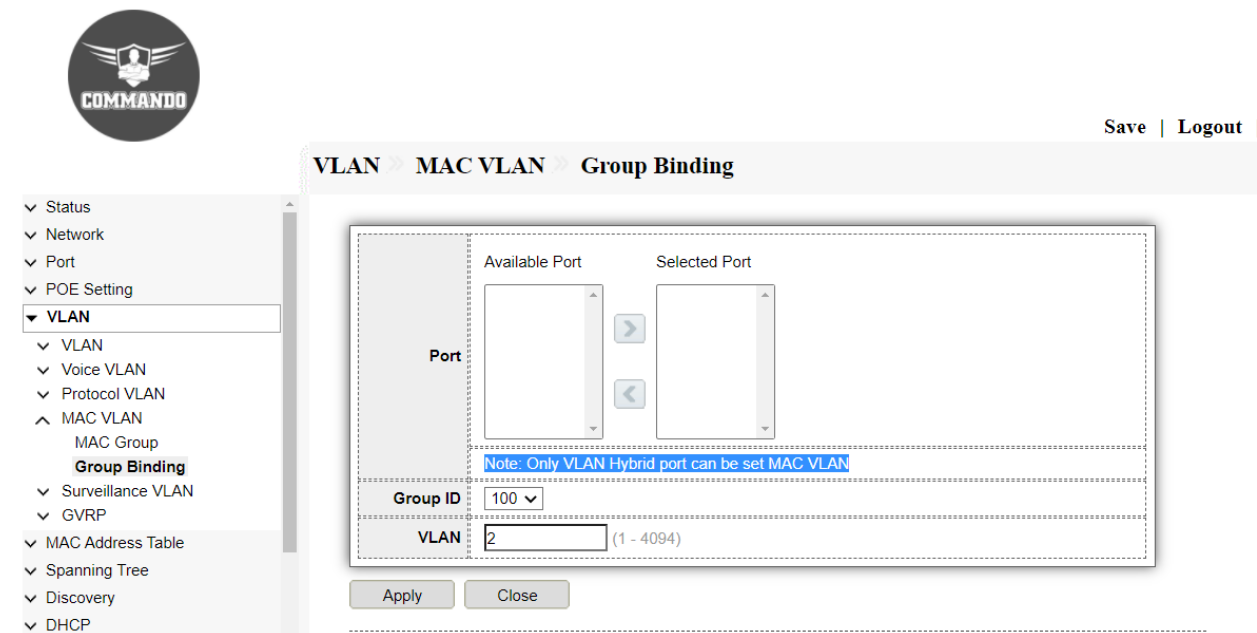


Fig 5.4.5 Blank Group binding for hybrid ports page

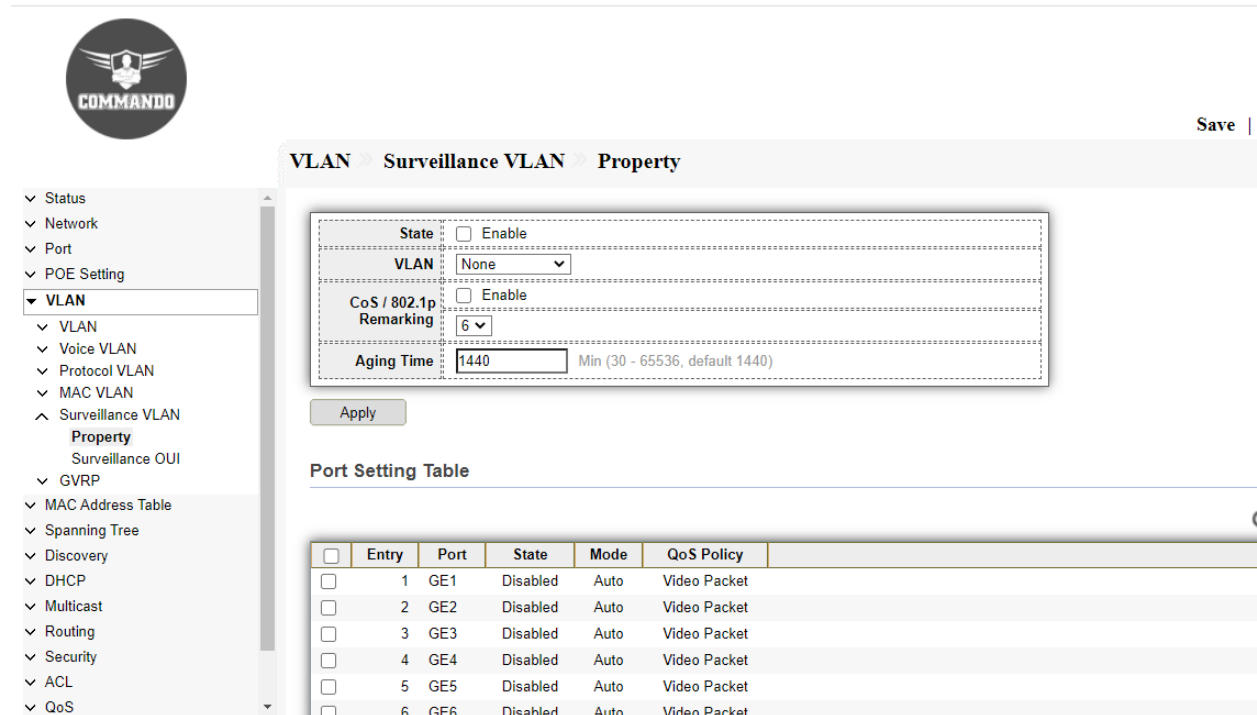
5.5 Surveillance VLAN

Surveillance VLAN is a feature that allows you to automatically place the video traffic from IP cameras to a surveillance VLAN to enhance the IP surveillance service. With a higher priority and individual VLAN, the quality and the security of surveillance traffic are guaranteed. VLAN configuration for CCTV or Surveillance cameras are very important to protect the IP cameras against unauthorized access and to separate the security camera system from other computers and devices that are connected to the IP network. E3000 series switches supports Surveillance VLAN feature. The surveillance devices can be put in Surveillance VLAN which segmenting their traffic from the rest of the network. This ensures security of the data, but also gives the traffic a higher priority through the switch, reducing the chances of the video freezing or being delayed on live streams. This page shows configuration to enable the functional Surveillance VLAN on the device. By default, Surveillance VLAN are disabled and by default setting of CoS / 802.1p remarking of 6.

To configure and view Surveillance VLAN, click **VLAN>>Surveillance VLAN**.

5.5.1 Property

To configure Surveillance VLAN property and view surveillance VLAN port setting, click **VLAN>>Surveillance VLAN>>Property**.



The screenshot shows the 'VLAN > Surveillance VLAN > Property' configuration page. The left sidebar contains a navigation tree with 'VLAN' expanded to 'Surveillance VLAN > Property'. The main configuration area includes the following fields:

- State:** Enable
- VLAN:** None (dropdown)
- CoS / 802.1p Remarking:** Enable, 6 (dropdown)
- Aging Time:** 1440 (text input), Min (30 - 65536, default 1440)

An 'Apply' button is located below the configuration fields. Below the configuration area is the 'Port Setting Table' with the following data:

Entry	Port	State	Mode	QoS Policy
1	GE1	Disabled	Auto	Video Packet
2	GE2	Disabled	Auto	Video Packet
3	GE3	Disabled	Auto	Video Packet
4	GE4	Disabled	Auto	Video Packet
5	GE5	Disabled	Auto	Video Packet
6	GE6	Disabled	Auto	Video Packet

Fig 5.5.1 Surveillance VLAN Property page

Surveillance VLAN Configuration:

Click on “Surveillance VLAN”, then “Property” from menu, Select/Deselect “State” to Enable/Disable, then select “VLAN” name from dropdown, Select “CoS/802.1p Remarking” & Click on “Apply”.

Configuration object and description:

CoS/802.1p: Select a CoS/802.1p value that to be used by LLDP-MED as a voice network policy.



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
- ▼ VLAN
- ▼ Voice VLAN
- ▼ Protocol VLAN
- ▼ MAC VLAN
- ^ Surveillance VLAN
- Property**
- Surveillance OUI
- ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

VLAN > Surveillance VLAN > Property

State	<input checked="" type="checkbox"/> Enable
VLAN	COMMANDO
CoS / 802.1p Remarking	<input checked="" type="checkbox"/> Enable 6
Aging Time	1440 Min (30 - 65536, default 1440)

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Disabled	Auto	Video Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Video Packet
<input type="checkbox"/>	3	GE3	Disabled	Auto	Video Packet
<input type="checkbox"/>	4	GE4	Disabled	Auto	Video Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Video Packet
<input type="checkbox"/>	6	GE6	Disabled	Auto	Video Packet
<input type="checkbox"/>	7	GE7	Disabled	Auto	Video Packet
<input checked="" type="checkbox"/>	8	GE8	Disabled	Auto	Video Packet

Fig 5.5.2 Surveillance VLAN port setting page for selected GE4 port



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
- ▼ VLAN
- ▼ Voice VLAN
- ▼ Protocol VLAN
- ▼ MAC VLAN
- ^ Surveillance VLAN
- Property**
- Surveillance OUI
- ▼ GVRP
- ▼ MAC Address Table

Save

VLAN > Surveillance VLAN > Property

Edit Port Setting

Port	GE8
State	<input checked="" type="checkbox"/> Enable
Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
QoS Policy	<input checked="" type="radio"/> Video Packet <input type="radio"/> All

Apply

Close

Fig 5.5.3 Surveillance VLAN Edit port setting for GE8 port page



VLAN » Surveillance VLAN » Property

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
 - ▼ VLAN
 - ▼ Voice VLAN
 - ▼ Protocol VLAN
 - ▼ MAC VLAN
 - ▲ Surveillance VLAN
 - Property**
 - Surveillance OUI
 - ▼ GVRP
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

State	<input checked="" type="checkbox"/> Enable
VLAN	COMMANDO
CoS / 802.1p Remarking	<input checked="" type="checkbox"/> Enable 6
Aging Time	1440 Min (30 - 65536, default 1440)

Apply

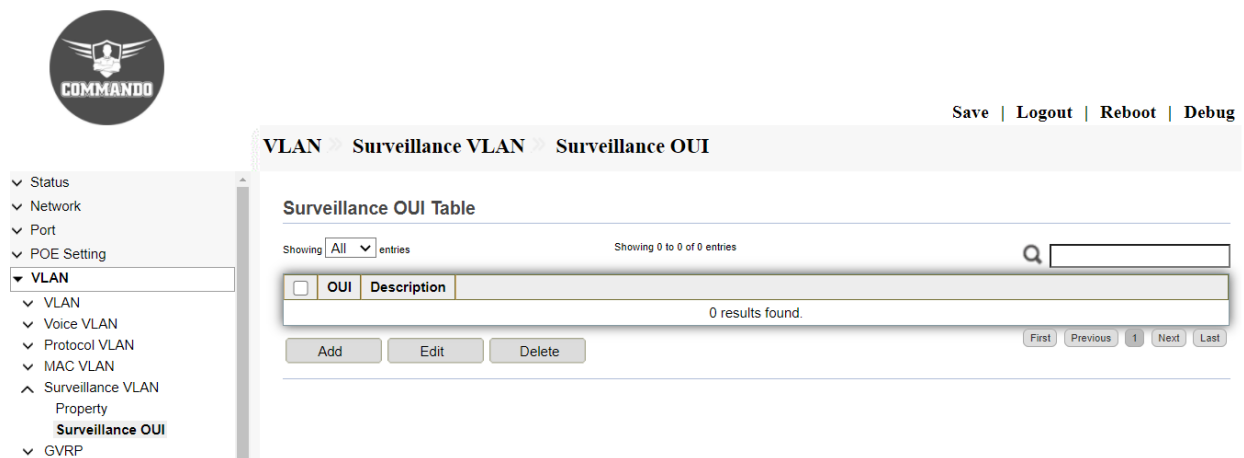
Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Disabled	Auto	Video Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Video Packet
<input type="checkbox"/>	3	GE3	Disabled	Auto	Video Packet
<input type="checkbox"/>	4	GE4	Disabled	Auto	Video Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Video Packet
<input type="checkbox"/>	6	GE6	Disabled	Auto	Video Packet
<input type="checkbox"/>	7	GE7	Disabled	Auto	Video Packet
<input type="checkbox"/>	8	GE8	Enabled	Auto	Video Packet

Fig 5.5.4 Surveillance VLAN Port setting table GE8 port enabled for Video packet

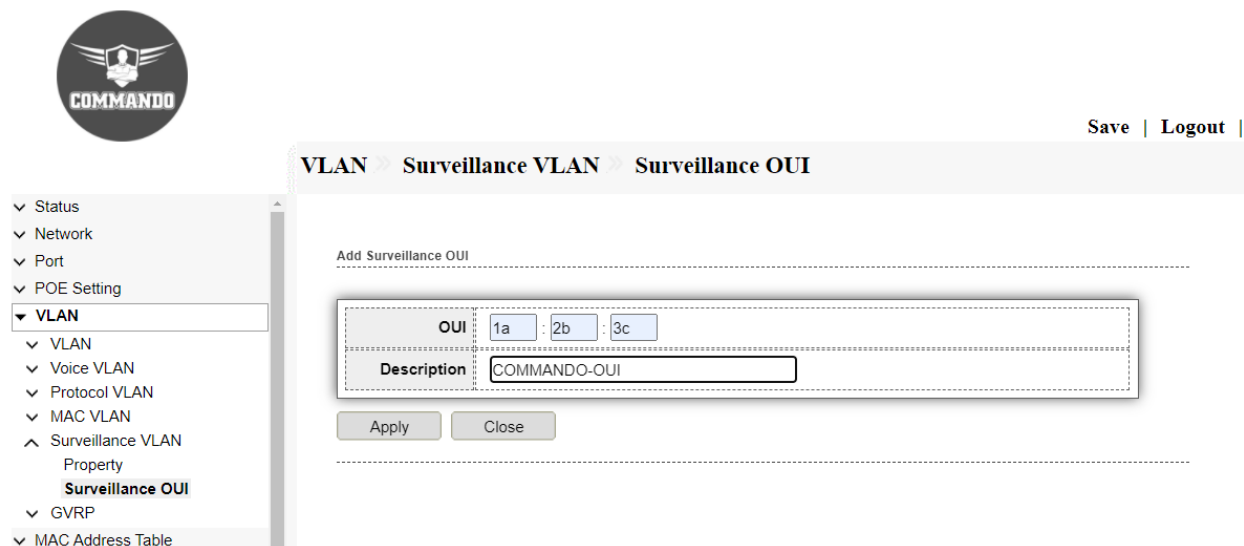
5.5.2 Surveillance OUI

The first six digits of a MAC are called the OUI, and each manufacturer is assigned one or more unique identifiers. For example, these are the OUIs of some common camera manufacturers. Analog cameras (whether SD or HD), by definition of being analog, do not have or need IP addresses since they have no network interface. However, analog cameras are generally connected to recorders or encoders that do have network interfaces and therefore use IP addresses. To configure and view Surveillance OUI, click **VLAN>>Surveillance VLAN>>Surveillance OUI**.



The screenshot shows the COMMANDO web interface. On the left is a navigation menu with a tree structure: Status, Network, Port, POE Setting, VLAN (expanded), Voice VLAN, Protocol VLAN, MAC VLAN, Surveillance VLAN (expanded), Property, Surveillance OUI (highlighted), and GVRP. The main content area is titled "VLAN > Surveillance VLAN > Surveillance OUI" and includes links for "Save | Logout | Reboot | Debug". Below the breadcrumb is a "Surveillance OUI Table" section. It features a search bar, a table with columns "OUI" and "Description", and a message "Showing 0 to 0 of 0 entries" and "0 results found.". Below the table are "Add", "Edit", and "Delete" buttons, and pagination controls: "First | Previous | 1 | Next | Last".

Fig 5.5.5 Surveillance OUI Table page



The screenshot shows the COMMANDO web interface for adding a new Surveillance OUI. The navigation menu on the left is similar to the previous screenshot, with "Surveillance OUI" highlighted. The main content area is titled "VLAN > Surveillance VLAN > Surveillance OUI" and includes links for "Save | Logout |". Below the breadcrumb is a form titled "Add Surveillance OUI". The form has two fields: "OUI" with three input boxes containing "1a", "2b", and "3c", and "Description" with a text box containing "COMMANDO-OUI". Below the form are "Apply" and "Close" buttons.

Fig 5.5.6 Add Surveillance OUI page



Save | Logout | Reboot | Debug

VLAN > Surveillance VLAN > Surveillance OUI

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ VLAN
- ▼ Voice VLAN
- ▼ Protocol VLAN
- ▼ MAC VLAN
- ▲ Surveillance VLAN
 - Property
 - Surveillance OUI**
- ▼ GVRP

Surveillance OUI Table

Showing All entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	OUI	Description
<input type="checkbox"/>	1A:2B:3C	COMMANDO-OUI

Add Edit Delete

First Previous 1 Next Last

Fig 5.5.7 Surveillance OUI Table page

5.6 GVRP

The GVRP is an IEEE 802.1Q-compliant method for facilitating automatic (dynamic) VLAN membership configuration. GVRP-enabled switches can exchange VLAN configuration information with other GVRP-enabled switches. Policy rules or other network management methods can determine who is admitted to a VLAN. Adjacent VLAN-aware devices can exchange VLAN information with each other by using the Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network. Since GVRP requires support for tagging, the port must be configured in Trunk mode. GVRP—VLAN was dynamically created through Generic VLAN Registration Protocol (GVRP). VLANs on a device can be created statically or dynamically, based on the GVRP information exchanged by devices. A VLAN can be static or dynamic (from GVRP). GVRP must be activated globally as well as on each port. When it is activated, it transmits and receives GARP Packet Data Units (GPDUs). VLANs that are defined but not active are not propagated. To propagate the VLAN, it must be up on at least one port. By default, GVRP is disabled globally and on ports. This page shows GVRP configuration. Disable GVRP will clear all learned dynamic VLAN entry and do not learn dynamic VLAN anymore.

To configure and view Generic VLAN Registration Protocol (GVRP), click **VLAN>>GVRP**.

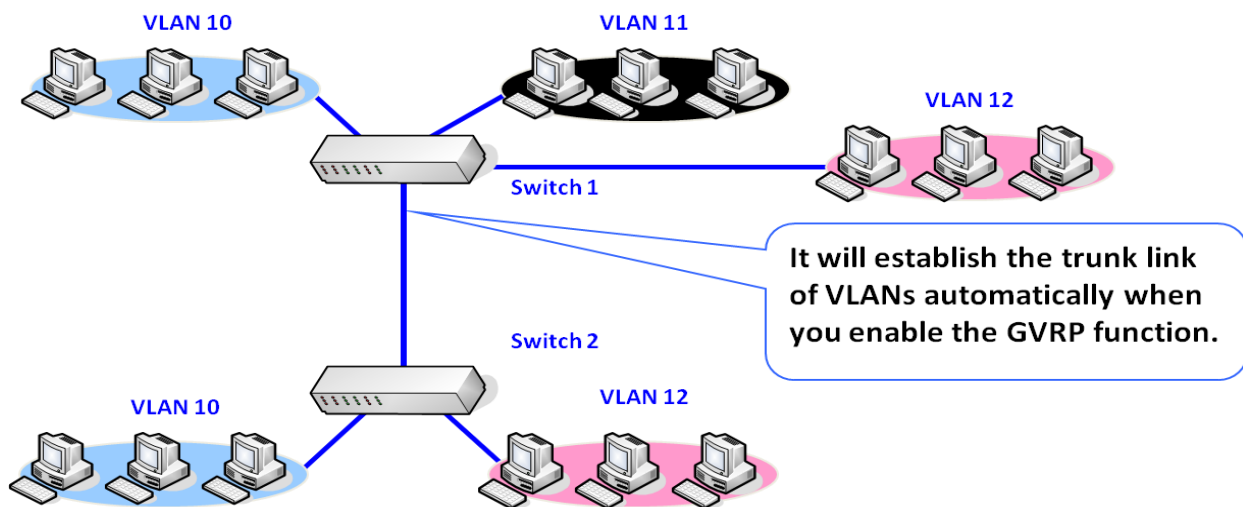


Fig 5.6.1 GVRP Function.

5.6.1 Property

By default, GVRP is disabled in COMMANDO E3000 Series Switches. To Enable, configure GVRP Property and view GVRP Port setting, click **VLAN>>GVRP>>Property**.

The screenshot shows the COMMANDO web interface for configuring GVRP properties. The breadcrumb navigation is **VLAN > GVRP > Property**. The **State** is set to **Enable**. The **Operational Timeout** section contains three rows: **Join** with a value of 20 (range cs (2 - 16375, default 20)), **Leave** with a value of 60 (range cs (45 - 32760, default 60)), and **Leave All** with a value of 1000 (range cs (65 - 32765, default 1000)). Below this is an **Apply** button. The **Port Setting Table** has a search bar and a table with the following data:

<input type="checkbox"/>	Entry	Port	State	VLAN Creation	Registration
<input type="checkbox"/>	1	GE1	Disabled	Enabled	Normal
<input type="checkbox"/>	2	GE2	Disabled	Enabled	Normal

Fig 5.6.1 Default GVRP Property page

The screenshot shows the COMMANDO web interface for configuring GVRP properties. The breadcrumb navigation is **VLAN > GVRP > Property**. The **State** is set to **Enable**. The **Operational Timeout** section contains three rows: **Join** with a value of 20 (range cs (2 - 16375, default 20)), **Leave** with a value of 60 (range cs (45 - 32760, default 60)), and **Leave All** with a value of 1000 (range cs (65 - 32765, default 1000)). Below this is an **Apply** button. The **Port Setting Table** has a search bar and a table with the following data:

<input type="checkbox"/>	Entry	Port	State	VLAN Creation	Registration
<input type="checkbox"/>	1	GE1	Disabled	Enabled	Normal
<input checked="" type="checkbox"/>	2	GE2	Disabled	Enabled	Normal
<input checked="" type="checkbox"/>	3	GE3	Disabled	Enabled	Normal
<input type="checkbox"/>	4	GE4	Disabled	Enabled	Normal

Fig 5.6.2 GVRP Property Port setting table selecting GE2 and GE3 ports page

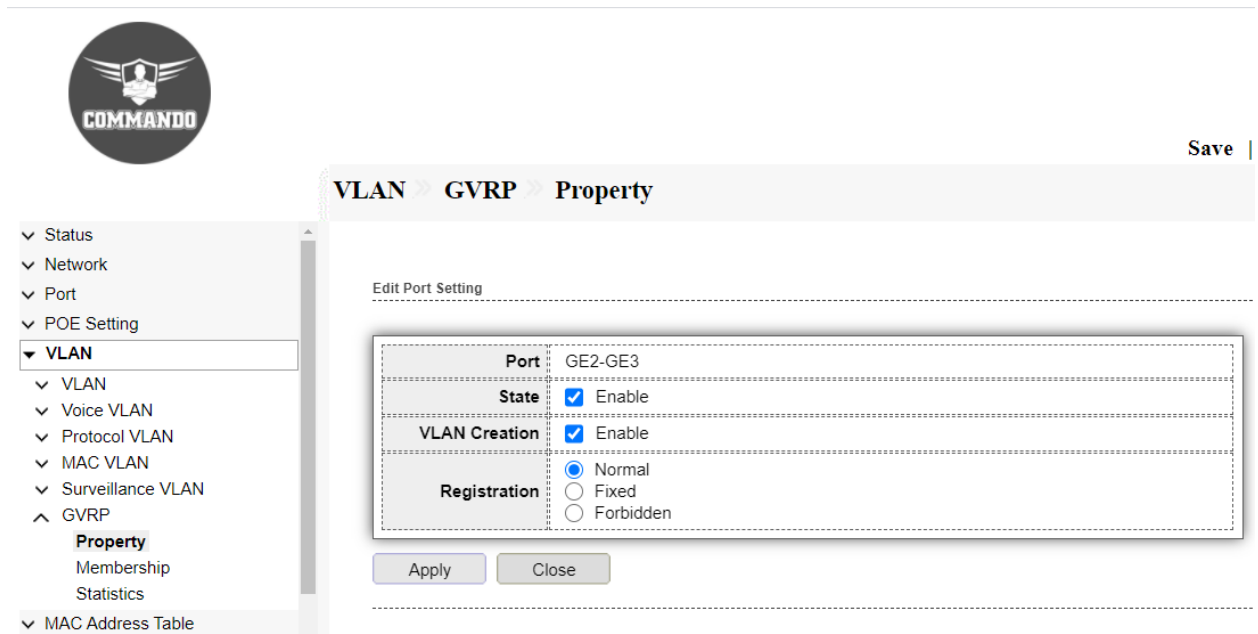


Fig 5.6.3 GVRP Property Edit Port setting for GE2 and GE3 ports page

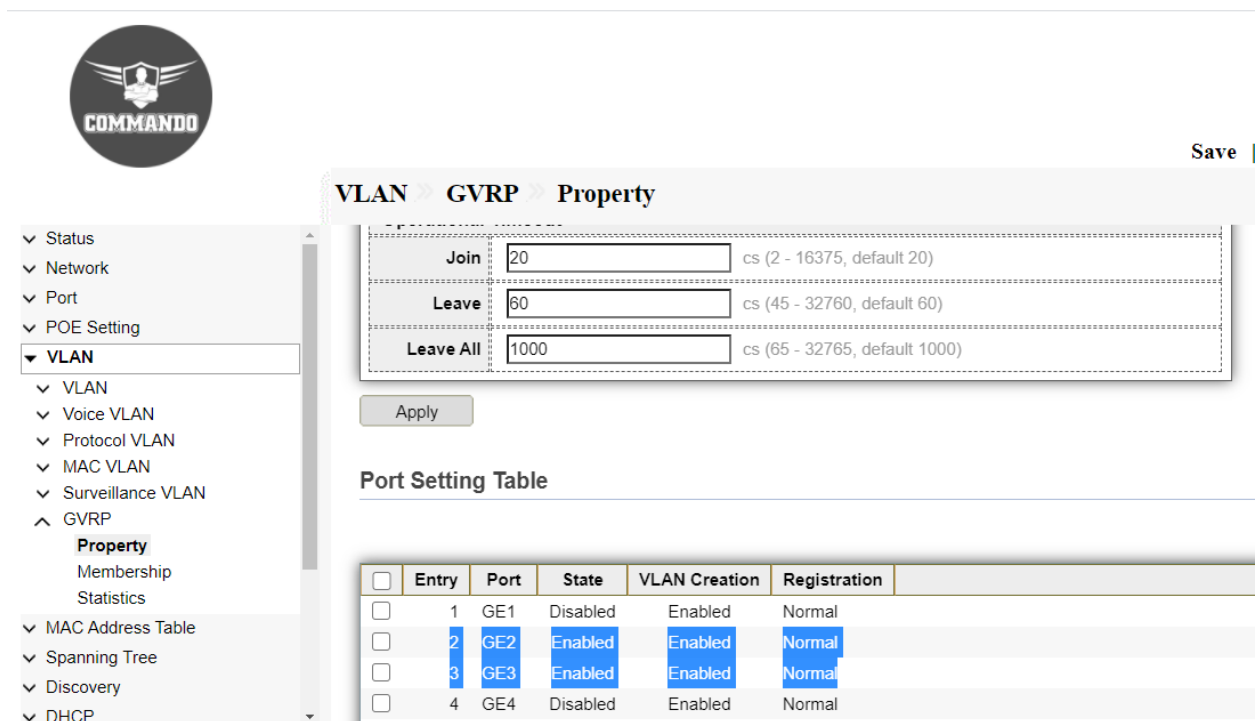
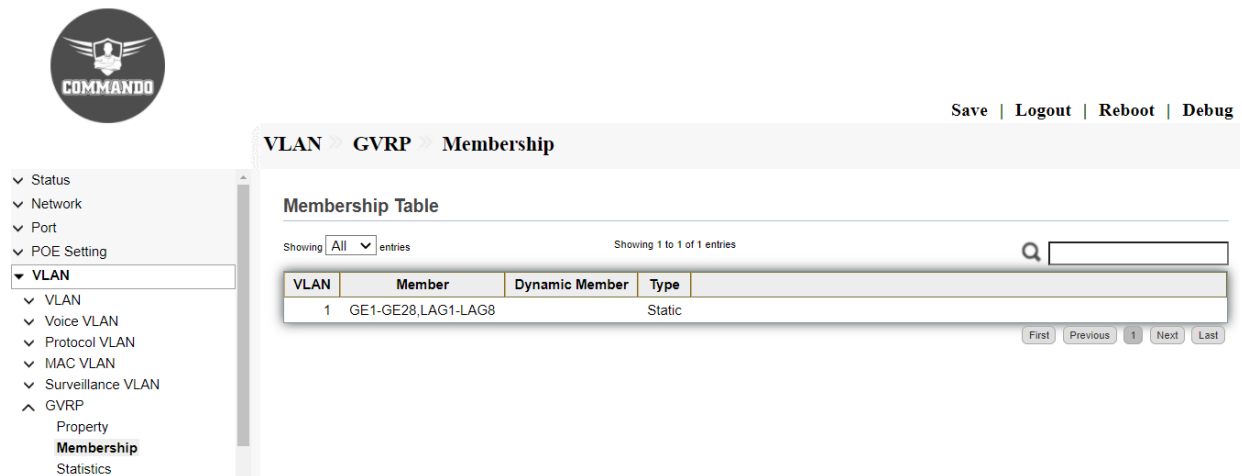


Fig 5.6.4 GVRP Property Port setting table after enabled GE2 and GE3 ports page

5.6.2 Membership

GARP VLAN Registration Protocol (GVRP) is required for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP propagates VLAN membership throughout a network. GVRP allows end stations and switches to issue and revoke declarations relating to VLAN. GVRP provides dynamic registration of VLAN membership; therefore, members can be added or removed from a VLAN at any time.

To view GVRP Membership, click **VLAN>>GVRP>>Membership**.



The screenshot shows the COMMANDO web interface. On the left is a navigation tree with 'Membership' selected under 'GVRP'. The main area is titled 'VLAN > GVRP > Membership' and contains a 'Membership Table'. The table has columns: VLAN, Member, Dynamic Member, and Type. It shows one entry: VLAN 1, Member GE1-GE28,LAG1-LAG8, Dynamic Member, and Type Static. There are also search and navigation controls.

VLAN	Member	Dynamic Member	Type
1	GE1-GE28,LAG1-LAG8		Static

Fig 5.6.5 GVRP Membership Default page

5.6.3 Statistics

The GVRP statistics include those GARP packets sent or received that are exchanging VLAN information by using GVRP. To view GVRP statistics, click **VLAN>>GVRP>>statistics**.



Save

VLAN > GVRP > Statistics

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
 - ▼ VLAN
 - ▼ Voice VLAN
 - ▼ Protocol VLAN
 - ▼ MAC VLAN
 - ▼ Surveillance VLAN
 - ▲ GVRP
 - Property
 - Membership
 - Statistics**
 - ▼ MAC Address Table
 - ▼ Spanning Tree
 - ▼ Discovery
 - ▼ DHCP

Port: GE1

Statistics: All, Receive, Transmit, Error

Refresh Rate: None, 5 sec, 10 sec, 30 sec

Clear

Receive	
Join empty	0
Empty	0
Leave Empty	0

Fig 5.6.7 Default GVRP statistics page



Save

VLAN > GVRP > Statistics

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ **VLAN**
 - ▼ VLAN
 - ▼ Voice VLAN
 - ▼ Protocol VLAN
 - ▼ MAC VLAN
 - ▼ Surveillance VLAN
 - ▲ GVRP
 - Property
 - Membership
 - Statistics**
 - ▼ MAC Address Table
 - ▼ Spanning Tree
 - ▼ Discovery
 - ▼ DHCP

Port: GE1

Statistics: All, Receive, Transmit, Error

Refresh Rate: None, 5 sec, 10 sec, 30 sec

Clear

Receive	
Join empty	
Empty	
Leave Empty	

Fig 5.6.8 GVRP statistics for particular port page

Chapter 6 MAC Address Table

Dynamic Address: In E3000 series switch, the data link layer device, maintains a MAC address table to forward frames to the destination port. The MAC address table entry on the switch is created either statically or dynamically. The Dynamic Address Table contains all of the MAC addresses that are obtained from the incoming traffic to the switch.

Static Address: Static MAC addresses are entered manually into the MAC address table.

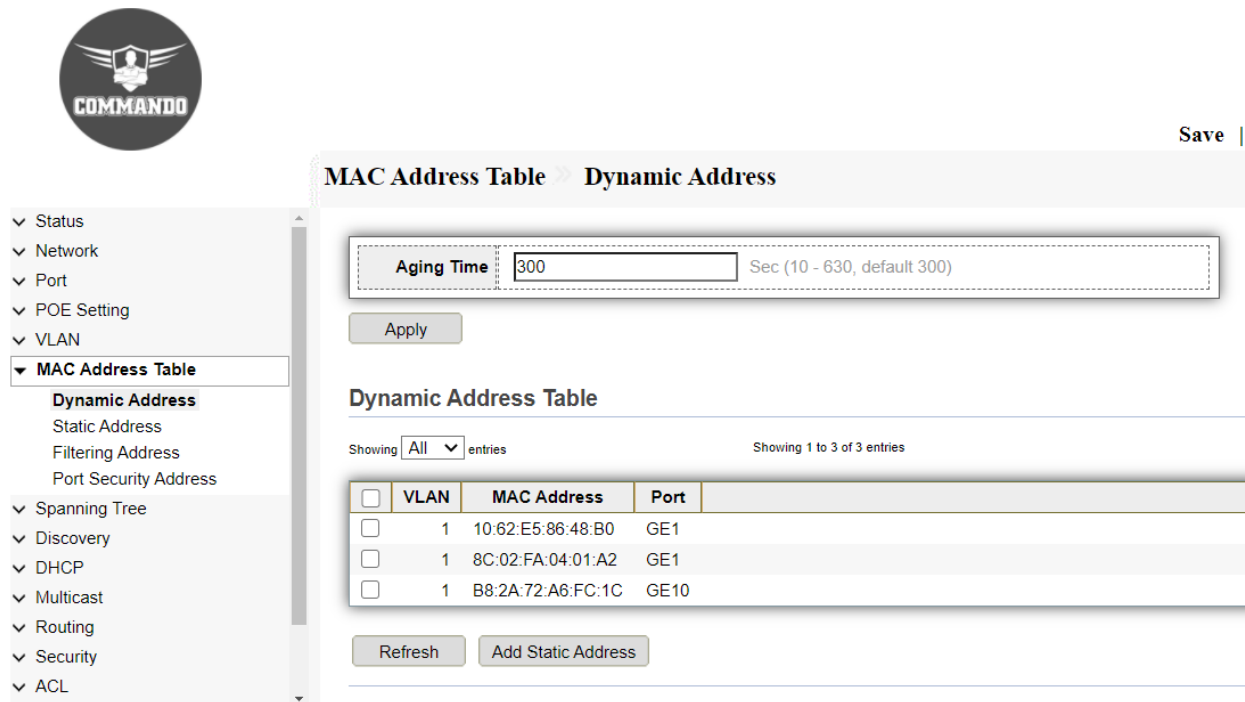
Filtering Address: MAC address filtering allows you to define a list of devices and only allow those devices on your LAN network.

Port Security Address: By using port security, a network administrator can associate specific MAC addresses with the interface.

6.1 Dynamic Address

Dynamic MAC addresses are entered into the table when the switch receives a frame whose source address is not listed in the MAC address table. The switch builds the table dynamically by referencing the source address of frames it receives.

This page shows details to add & clear the dynamic (learned) MAC, static entries from the MAC address table, the specific interface, or the specific VLAN. To view Dynamic Address, click **MAC Address Table >> Dynamic Address**.



The screenshot displays the COMMANDO network management interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, and ACL. The 'MAC Address Table' section is expanded, showing 'Dynamic Address' as the active sub-section. The main content area is titled 'MAC Address Table > Dynamic Address' and includes a 'Save' button in the top right. Below the title, there is a form for 'Aging Time' set to 300 seconds, with a note 'Sec (10 - 630, default 300)' and an 'Apply' button. Underneath is the 'Dynamic Address Table' section, which shows 'Showing All entries' and 'Showing 1 to 3 of 3 entries'. A table lists three entries with columns for checkboxes, VLAN, MAC Address, and Port. At the bottom of the table are 'Refresh' and 'Add Static Address' buttons.

<input type="checkbox"/>	VLAN	MAC Address	Port
<input type="checkbox"/>	1	10:62:E5:86:48:B0	GE1
<input type="checkbox"/>	1	8C:02:FA:04:01:A2	GE1
<input type="checkbox"/>	1	B8:2A:72:A6:FC:1C	GE10

Fig 6.1.1 Dynamic MAC address table page



Save |

MAC Address Table > Dynamic Address

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ▼ **MAC Address Table**
 - Dynamic Address**
 - Static Address
 - Filtering Address
 - Port Security Address
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL

Aging Time Sec (10 - 630, default 300)

Apply

Dynamic Address Table

Showing entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	VLAN	MAC Address	Port
<input type="checkbox"/>	1	B8:2A:72:A6:FC:1C	GE10

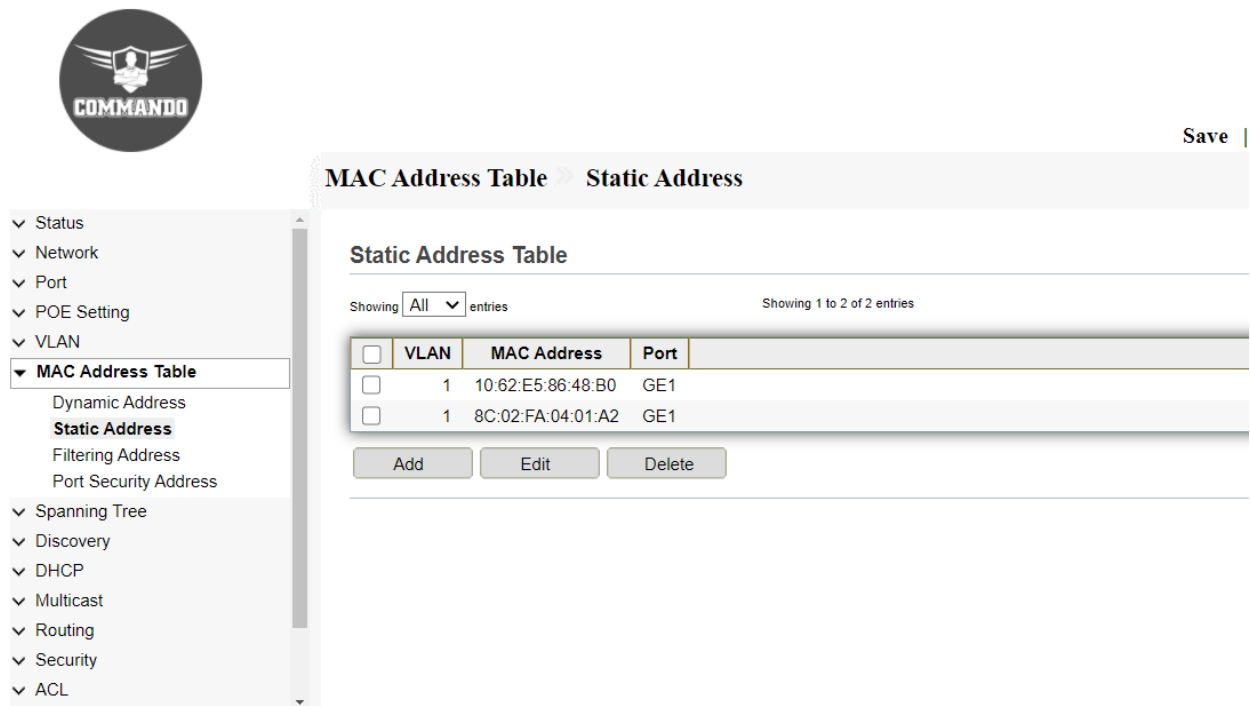
Refresh

Add Static Address

Fig 6.1.2 Add Static address from Dynamic MAC address table page

6.2 Static Address

Static MAC addresses are created manually. E3000 series switch cannot distinguish packets from authorized and unauthorized users when it learns source MAC addresses of packets to maintain the MAC address table. Therefore, if an unauthorized user uses the MAC address of an attacker as the source MAC address of attack packets and connects to another interface of the switch, the switch will learn an incorrect MAC address entry. As a result, packets destined for the authorized user are forwarded to the unauthorized user. To improve security, you can create static MAC address entries to bind MAC addresses of authorized users to specified interfaces. This prevents unauthorized users from intercepting data of authorized users. A static MAC address entry will not be aged out. After being created, a static MAC address entry will not be lost after a system restart if configuration is saved and can only be deleted manually. The VLAN bound to a static MAC address entry must already exist and be assigned to the interface bound to the entry. The MAC address in a static MAC address entry must be a unicast MAC address, and cannot be a multicast or broadcast MAC address. To configure and view the Static Address, click **MAC Address Table >> Static Address**.



The screenshot shows the Commando network management interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, and ACL. The 'MAC Address Table' section is expanded, showing sub-items: Dynamic Address, Static Address, Filtering Address, and Port Security Address. The 'Static Address' sub-item is selected. The main content area displays the 'Static Address Table' configuration page. At the top right of the main area is a 'Save' button. Below the title 'Static Address Table', there is a dropdown menu set to 'All' and the text 'Showing 1 to 2 of 2 entries'. A table with two columns, 'VLAN' and 'MAC Address', and two rows of data is shown. Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

<input type="checkbox"/>	VLAN	MAC Address	Port
<input type="checkbox"/>	1	10:62:E5:86:48:B0	GE1
<input type="checkbox"/>	1	8C:02:FA:04:01:A2	GE1

Fig 6.2.1 Default Static MAC address table default page

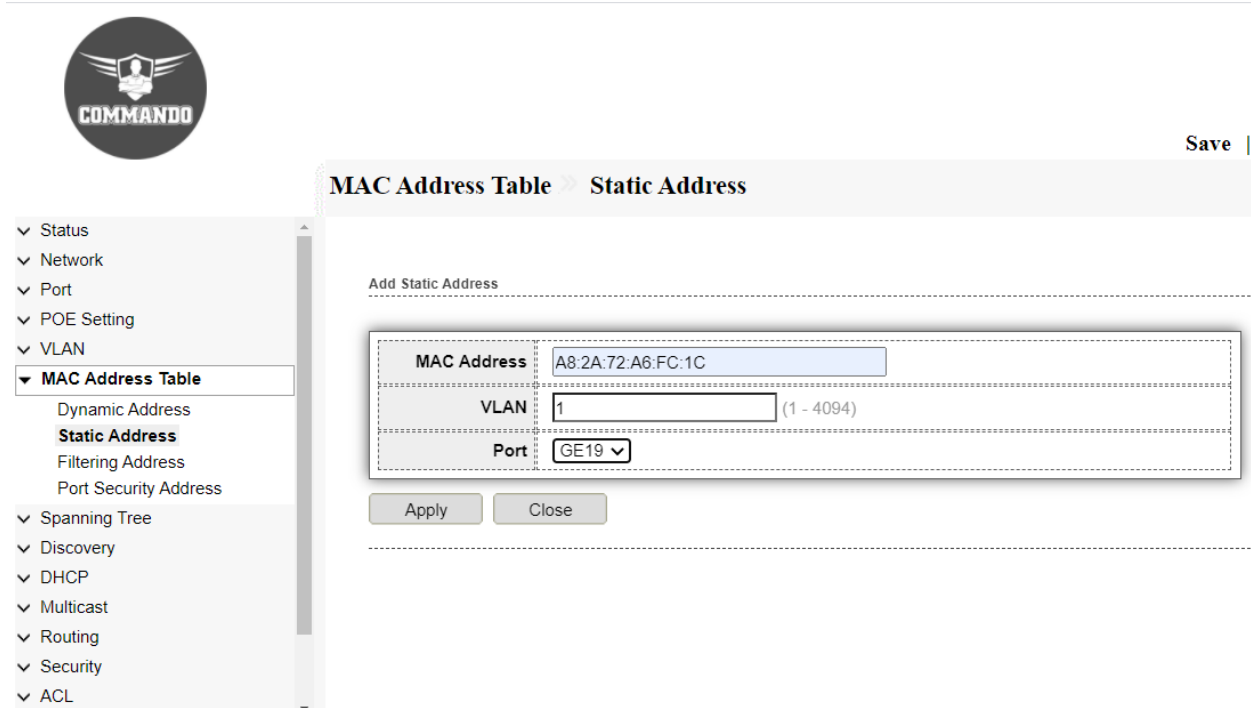


Fig 6.2.2 Add Static MAC address to specified VLAN and port page

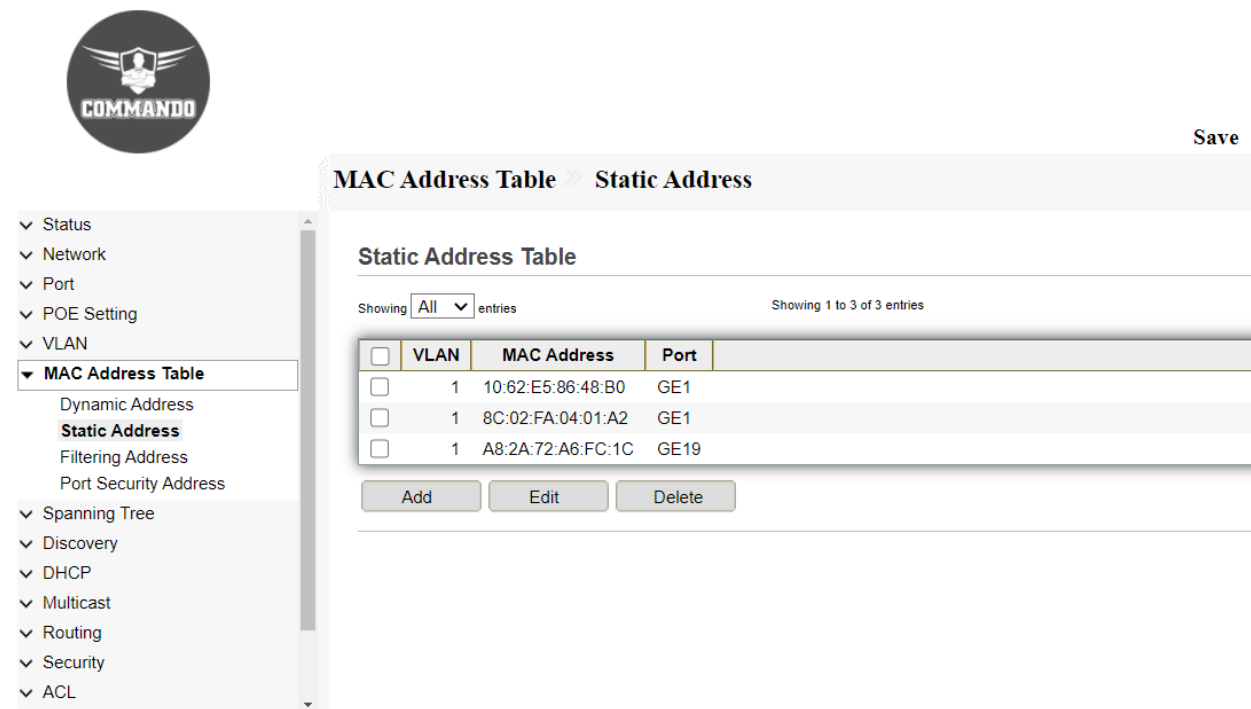


Fig 6.2.3 Static MAC address table After adding MAC address page

6.3 Filtering Address

MAC address filtering allows you to define a list of devices and only allow those devices on your LAN. MAC address filtering to prevent unauthorized network access. By MAC address filtering, you can allow only permitted devices to access the network. To configure and view the Filtering Address , click **MAC Address Table >> Filtering Address**.

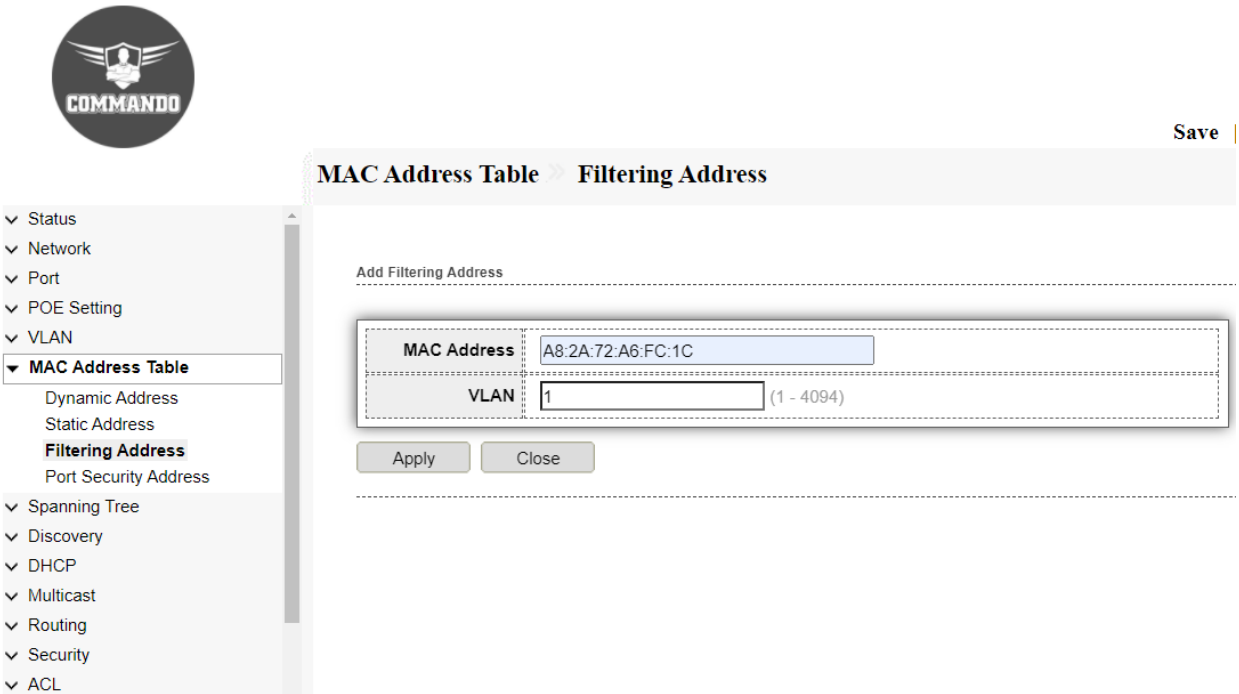


Fig 6.3.1 Filtering address table default page



Save |

MAC Address Table > Filtering Address

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ▼ **MAC Address Table**
 - Dynamic Address
 - Static Address
 - Filtering Address**
 - Port Security Address
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL

Add Filtering Address

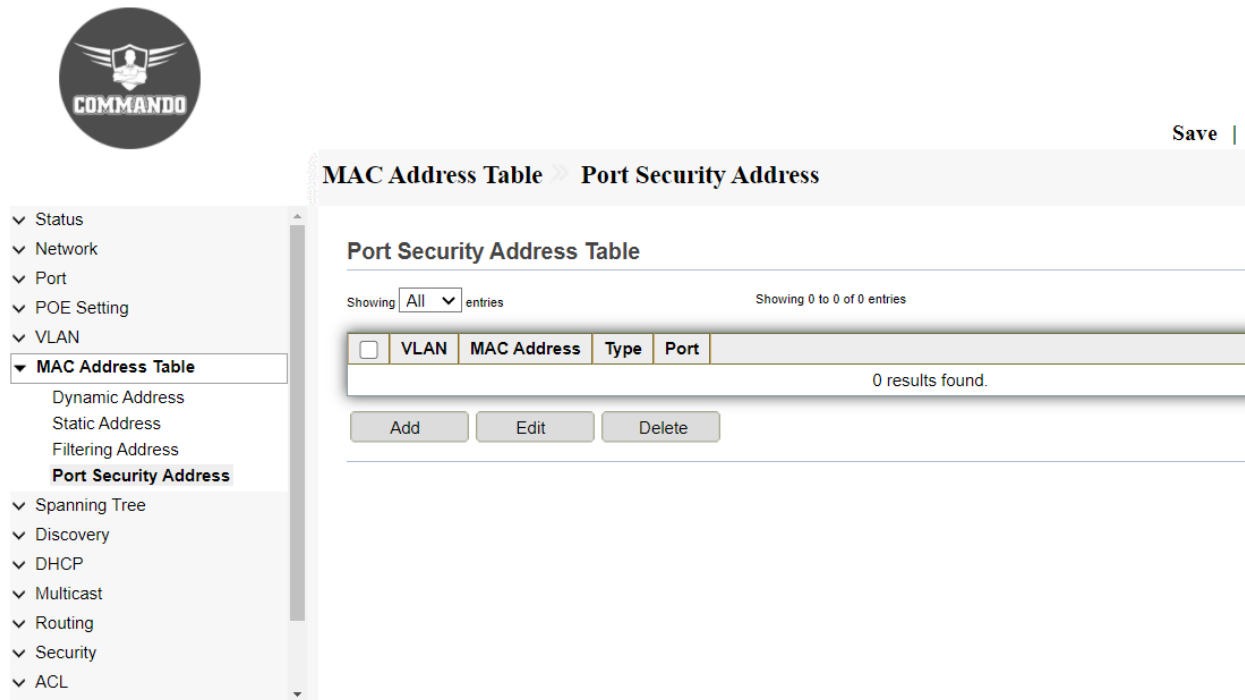
MAC Address	<input type="text" value="A8:2A:72:A6:FC:1C"/>
VLAN	<input type="text" value="1"/> (1 - 4094)

Fig 6.3.2 Add Filtering MAC address to Specified VLAN page

6.4 Port Security Address

Network security can be increased by limiting access on a port to users with specific MAC addresses. The MAC addresses can be either dynamically learned or statically configured.

Port security is a layer two traffic control feature by using port security, user can limit the number of MAC address on a port. You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed. By using port security, a network administrator can associate specific MAC addresses with the interface, which can prevent an attacker to connect his device. To configure and view the Port Security Address, click **MAC Address Table >> Port Security Address**.



The screenshot displays the COMMANDO network management interface. On the left is a navigation menu with a tree structure. The main content area shows the 'Port Security Address' configuration page. At the top right of the main area is a 'Save' button. Below the breadcrumb 'MAC Address Table > Port Security Address', the title 'Port Security Address Table' is displayed. Below the title, there is a 'Showing' dropdown menu set to 'All' and the text 'Showing 0 to 0 of 0 entries'. A table with columns 'VLAN', 'MAC Address', 'Type', and 'Port' is shown, with a message '0 results found.' below it. At the bottom of the table area are three buttons: 'Add', 'Edit', and 'Delete'. The navigation menu on the left includes the following items: Status, Network, Port, POE Setting, VLAN, MAC Address Table (expanded), Dynamic Address, Static Address, Filtering Address, Port Security Address (highlighted), Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, and ACL.

Fig 6.4.1 Port Security address table default page



Save |

MAC Address Table > Port Security Address

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ▼ **MAC Address Table**
 - Dynamic Address
 - Static Address
 - Filtering Address
 - Port Security Address**
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL

Add Port Security Address

MAC Address	<input type="text" value="A8:2A:72:A6:FC:1C"/>
VLAN	<input type="text" value="1"/> (1 - 4094)
Port	<input type="text" value="GE5"/>

Fig 6.4.2 Add Port Security MAC address page

Chapter 7 Spanning Tree

Property: STP protects a Layer 2 Broadcast domain from Broadcast storms by selectively setting links to standby mode to prevent loops. In standby mode, these links temporarily stop transferring user data. After the topology changes so that the data transfer is made possible, the links are automatically re-activated.

Port Setting: By default, IEEE costs used to assign default path

costs to the STP ports. The default path cost assigned to an interface varies

according to the selected method. Short range 1 through 65,535 for port path costs.

Long the range 1 through 200,000,000 for port path costs.

MST Instance: Multiple Spanning Tree Protocol (MSTP) is used to separate the STP port state between various domains (on different VLANs).

MST Port Setting: The global MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree instance.

Statistics: This option displays the STP port statistics counters in the switch.

Spanning tree protects a Layer 2 Broadcast domain from Broadcast storms by selectively setting links to standby mode to prevent loops. In standby mode, these links temporarily stop transferring user data. After the topology changes so that the data transfer is made possible, the links are automatically re-activated. STP/RSTP/MSTP to learn the topology of network and application on switch default Spanning tree setting in E3000 series switches is RSTP.

7.1 Property

Ethernet networks are susceptible to broadcast storms if loops are introduced by links. However, an Ethernet network needs to include loops because they provide redundant paths in case of a link failure. Spanning-tree protocols address both issues because they provide link redundancy while simultaneously preventing undesirable loops.

Spanning-tree protocols intelligently avoid loops in a network by creating a loop free tree topology (spanning tree) of the entire LAN network with only one available path between the tree root and a leaf. All other paths are forced into a standby or disable or redundant state. The tree root is a switch within the network elected by the STA (spanning-tree algorithm) to use when computing the best path between bridges throughout the network and the root bridge. Frames travel through the network to their destination- a leaf. A tree branch is a network segment, or link, between bridges. Switches that forward frames through an STP spanning tree are called designated bridges.

Spanning Tree Operation modes:

STP: The Spanning Tree Protocol (STP) is responsible for identifying links in the network and shutting down the redundant ones, preventing possible network loops. In order to do so, all switches in the network exchange BPDU messages between them to agree upon the root bridge. The Spanning Tree Protocol (STP) is a network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include backup links providing fault tolerance if an active link fails. Provides a single path between any two end stations, avoiding and eliminating loops.

Rapid STP (RSTP): Rapid Spanning Tree Protocol (RSTP) as 802.1w. RSTP provides significantly faster recovery in response to network changes or failures, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP. Detects network topology to provide faster convergence of the spanning tree.

Multiple STP (MSTP): IEEE 802.1s MSTP (Multiple Spanning Tree Protocol) makes it possible for VLAN switching devices to use multiple Spanning Trees, allowing traffic belonging to different VLANs to flow over potentially different paths within the LAN. It builds upon the advancements of RSTP with its decreased time for network re-spans.

It detects Layer 2 loops and attempts to mitigate them by preventing the involved port from transmitting traffic. Since loops exist on a per-Layer 2-domain basis, a situation can occur where there is a loop in VLAN A and no loop in VLAN B. If both VLANs are on Port X, and STP wants to mitigate the loop, it stops traffic on the entire port, including VLAN B traffic.

Spanning Tree Property:

BPDU Handling: Select how Bridge Protocol Data Unit (BPDU) packets are managed when STP is disabled on the port or the device. BPDUs are used to transmit spanning tree information.

Filtering: Filters BPDU packets when Spanning Tree is disabled on an interface.

Flooding: Floods BPDU packets when Spanning Tree is disabled on an interface.

Path Cost Default Values: selects the method used to assign default path costs to the STP ports. The default path cost assigned to an interface varies according to the selected method.

Short: Specifies the range 1 through 65,535 for port path costs.

Long: Specifies the range 1 through 200,000,000 for port path costs.

Note: By default, E3000 Series switches use Long port path cost.

Spanning Tree Configuration:

To configure and view the Spanning Tree, click **Spanning Tree >> Property**.

Note: By default, RSTP is enabled on E3000 Series switch.

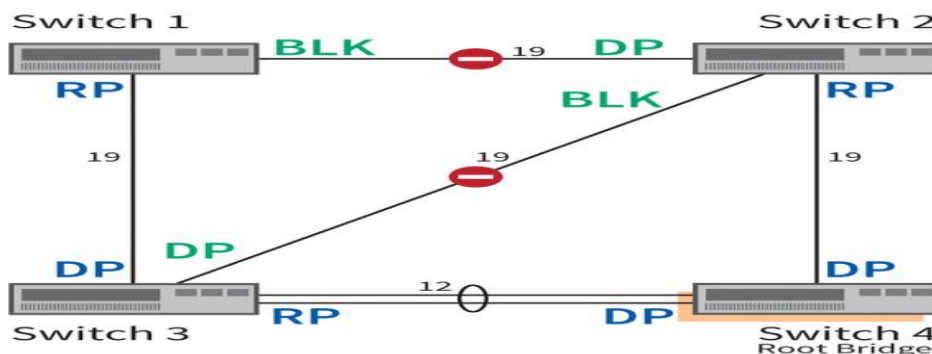


Fig 7.1.1 Spanning Tree enabled network Changed topology .



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance
 - MST Port Setting
 - Statistics
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Spanning Tree Property

State	<input type="checkbox"/> Enable
Operation Mode	<input type="radio"/> STP <input checked="" type="radio"/> RSTP <input type="radio"/> MSTP
Path Cost	<input checked="" type="radio"/> Long <input type="radio"/> Short
BPDU Handling	<input type="radio"/> Filtering <input checked="" type="radio"/> Flooding
Priority	<input type="text" value="32768"/> (0 - 61440, default 32768)
Hello Time	<input type="text" value="2"/> Sec (1 - 10, default 2)
Max Age	<input type="text" value="20"/> Sec (6 - 40, default 20)
Forward Delay	<input type="text" value="15"/> Sec (4 - 30, default 15)
Tx Hold Count	<input type="text" value="6"/> (1 - 10, default 6)
Region Name	<input type="text" value="8C:02:FA:04:03:59"/>
Revision	<input type="text" value="0"/> (0 - 65535, default 0)
Max Hop	<input type="text" value="20"/> (1 - 40, default 20)
Operational Status	
Bridge Identifier	32768-8C:02:FA:04:03:59
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	N/A
Root Path Cost	0
Topology Change Count	0
Last Topology Change	0D/0H/0M/0S

Apply

Fig 7.1.2 Default Spanning Tree property page

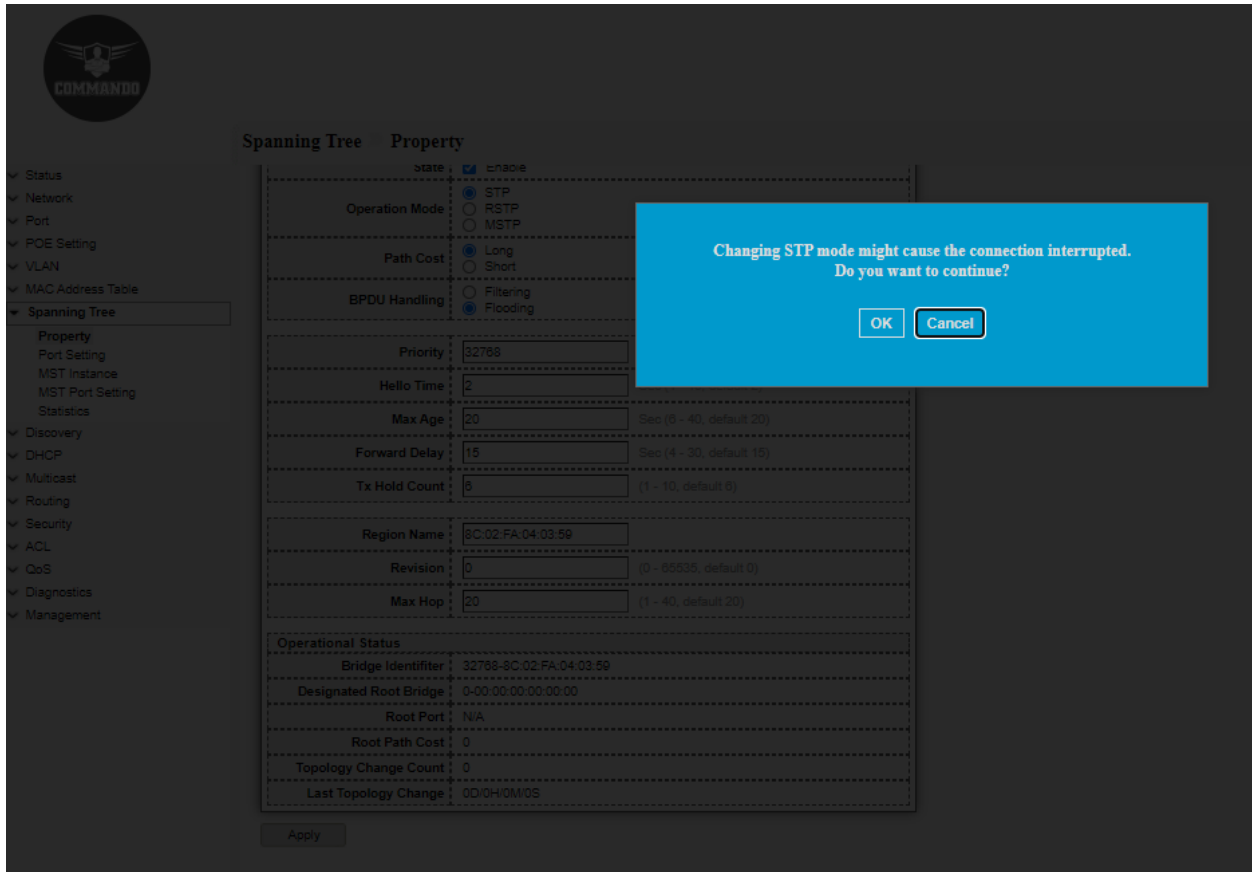


Fig 7.1.3 Change Spanning Tree mode property page



Spanning Tree » Property

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance
 - MST Port Setting
 - Statistics
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

State	<input checked="" type="checkbox"/> Enable
Operation Mode	<input checked="" type="radio"/> STP <input type="radio"/> RSTP <input type="radio"/> MSTP
Path Cost	<input checked="" type="radio"/> Long <input type="radio"/> Short
BPDU Handling	<input type="radio"/> Filtering <input checked="" type="radio"/> Flooding
Priority	<input type="text" value="32768"/> (0 - 61440, default 32768)
Hello Time	<input type="text" value="2"/> Sec (1 - 10, default 2)
Max Age	<input type="text" value="20"/> Sec (6 - 40, default 20)
Forward Delay	<input type="text" value="15"/> Sec (4 - 30, default 15)
Tx Hold Count	<input type="text" value="6"/> (1 - 10, default 6)
Region Name	<input type="text" value="8C:02:FA:04:03:59"/>
Revision	<input type="text" value="0"/> (0 - 65535, default 0)
Max Hop	<input type="text" value="20"/> (1 - 40, default 20)

Fig 7.1.4 Change Spanning Tree mode page

7.2 Port Setting

The STP/RSTP/MSTP Port Settings page enables you to configure STP/RSTP/MSTP on a per-port basis, and to view the information learned by the protocol, such as the designated bridge.

To configure and view the STP port settings, click **Spanning Tree >> Port Setting**.

Spanning Tree Port Setting

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost	
<input type="checkbox"/>	1	GE1	Disabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-8C-02-FA-04-03-59	128-1	20000
<input type="checkbox"/>	2	GE2	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
<input type="checkbox"/>	3	GE3	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
<input type="checkbox"/>	4	GE4	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
<input type="checkbox"/>	5	GE5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
<input type="checkbox"/>	6	GE6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
<input type="checkbox"/>	7	GE7	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
<input type="checkbox"/>	8	GE8	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
<input type="checkbox"/>	9	GE9	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000
<input type="checkbox"/>	10	GE10	Disabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-8C-02-FA-04-03-59	128-10	20000
<input type="checkbox"/>	11	GE11	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000
<input type="checkbox"/>	12	GE12	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000
<input type="checkbox"/>	13	GE13	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
<input type="checkbox"/>	14	GE14	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
<input type="checkbox"/>	15	GE15	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
<input type="checkbox"/>	16	GE16	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000
<input type="checkbox"/>	17	GE17	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000
<input type="checkbox"/>	18	GE18	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000
<input type="checkbox"/>	19	GE19	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000
<input type="checkbox"/>	20	GE20	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000
<input type="checkbox"/>	21	GE21	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-21	20000

Fig 7.2.1 Spanning tree port setting page

Spanning Tree Port Setting

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost	
<input type="checkbox"/>	1	GE1	Disabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-8C-02-FA-04-03-59	128-1	20000
<input checked="" type="checkbox"/>	2	GE2	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
<input checked="" type="checkbox"/>	3	GE3	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
<input checked="" type="checkbox"/>	4	GE4	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
<input type="checkbox"/>	5	GE5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
<input type="checkbox"/>	6	GE6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
<input type="checkbox"/>	7	GE7	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
<input type="checkbox"/>	8	GE8	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
<input type="checkbox"/>	9	GE9	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000
<input type="checkbox"/>	10	GE10	Disabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-8C-02-FA-04-03-59	128-10	20000
<input type="checkbox"/>	11	GE11	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000
<input type="checkbox"/>	12	GE12	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000
<input type="checkbox"/>	13	GE13	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
<input type="checkbox"/>	14	GE14	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
<input type="checkbox"/>	15	GE15	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
<input type="checkbox"/>	16	GE16	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000
<input type="checkbox"/>	17	GE17	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000

Fig 7.2.2 Selecting port for Setting all Spanning Tree Parameters page



Spanning Tree Port Setting

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
 - Property
 - Port Setting
 - MST Instance
 - MST Port Setting
 - Statistics
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Edit Port Setting

Port	GE2-GE4
State	<input checked="" type="checkbox"/> Enable
Path Cost	<input type="text" value="0"/> (0 - 200000000) (0 = Auto)
Priority	<input type="text" value="128"/>
Edge Port	<input checked="" type="checkbox"/> Enable
BPDU Filter	<input type="checkbox"/> Enable
BPDU Guard	<input type="checkbox"/> Enable
Point-to-Point	<input checked="" type="radio"/> Auto <input type="radio"/> Enable <input type="radio"/> Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-2
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

Apply

Close

Fig 7.2.3 Setting ports for Spanning Tree Parameters page



Save | Logout | Reboot | Debug

Spanning Tree Port Setting

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
 - Property
 - Port Setting
 - MST Instance
 - MST Port Setting
 - Statistics
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Desi
<input type="checkbox"/>	1	GE1	Disabled	200000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-8C:02:FA:04:03:59	128-1
<input type="checkbox"/>	2	GE2	Enabled	20000	128	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2
<input type="checkbox"/>	3	GE3	Enabled	20000	128	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3
<input type="checkbox"/>	4	GE4	Enabled	20000	128	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4
<input type="checkbox"/>	5	GE5	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5
<input type="checkbox"/>	6	GE6	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6
<input type="checkbox"/>	7	GE7	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7
<input type="checkbox"/>	8	GE8	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8
<input type="checkbox"/>	9	GE9	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9
<input type="checkbox"/>	10	GE10	Disabled	200000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-8C:02:FA:04:03:59	128-10
<input type="checkbox"/>	11	GE11	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11
<input type="checkbox"/>	12	GE12	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12
<input type="checkbox"/>	13	GE13	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13
<input type="checkbox"/>	14	GE14	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14
<input type="checkbox"/>	15	GE15	Disabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15

Fig 7.2.4 Spanning tree Port setting Table page

7.3 MST Instance

MSTP supports multiple instances on a single physical interface. MSTP is an extension of RSTP that maps multiple independent spanning-tree instances onto one physical topology. Each spanning-tree instance (STI) includes one or more VLANs. Unlike in STP and RSTP configurations, a port might belong to multiple VLANs and be dynamically blocked in one spanning-tree instance but forwarding in another. This behavior significantly improves network resource utilization by load-balancing across the network and maintaining switch CPU loads at moderate levels. MSTP also leverages the fast reconvergence time of RSTP when a network, switch, or port failure occurs within a spanning-tree instance.

MSTP creates a common and internal spanning tree (CIST) to interconnect and manage all MSTP regions and even individual devices that run RSTP or STP, which are recognized as distinct spanning-tree regions by MSTP. The CIST views each MSTP region as a virtual bridge, regardless of the actual number of devices participating in the MSTP region and enables multiple spanning-tree instances (MSTIs) to link to other regions. The CIST is a single topology that connects all switches (STP, RSTP, and MSTP devices) through an active topology, ensuring connectivity between LANs and devices within a bridged network. This functionality provided by MSTP enables you to better utilize network resources while remaining backward-compatible with older network devices. Multiple Spanning Tree Protocol (MSTP) is used to separate the STP port state between various domains (on different VLANs).

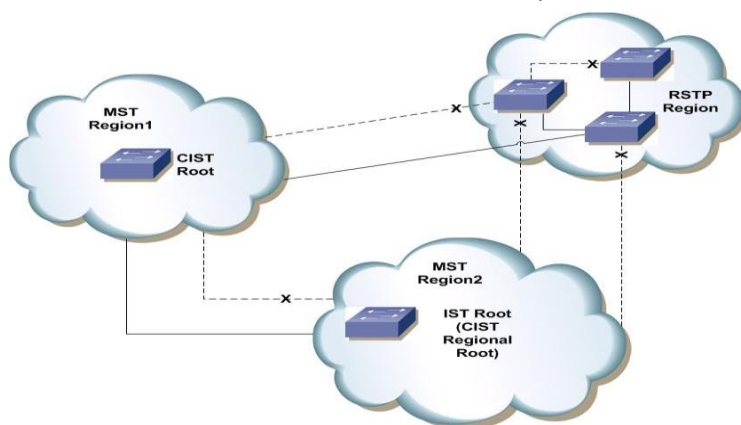


Fig 7.3.1 MST Enabled Network Topology change

To configure and view MST instance setting, click **Spanning Tree >> MST Instance**.



Save | Logout |

Spanning Tree > MST Instance

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance**
 - MST Port Setting
 - Statistics
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

MST Instance Table

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
<input type="radio"/>	0	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	1-4094
<input type="radio"/>	1	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	2	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	3	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	4	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	5	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	6	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	7	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	8	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	9	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	10	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	11	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	12	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	13	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	14	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	15	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	

Edit

Fig 7.3.2 Spanning tree MST instance Table page



Spanning Tree > MST Instance

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance**
 - MST Port Setting
 - Statistics
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Edit MST Instance Setting

MSTI	2
VLAN	Available VLAN: 2, 3, 4, 5, 6, 7, 8, 9 Selected VLAN: 1
Priority	32768 (0 - 61440, default 32768)
Bridge Identifier	32768-8C:02:FA:04:03:59
Designated Root Bridge	32768-8C:02:FA:04:03:59
Root Port	
Root Path Cost	0
Remaining Hop	20

Apply

Close

Fig 7.3.3 Spanning tree MST interface setting page



Spanning Tree > MST Instance

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance**
 - MST Port Setting
 - Statistics
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
<input type="radio"/>	0	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	2-4094
<input type="radio"/>	1	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input checked="" type="radio"/>	2	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	1
<input type="radio"/>	3	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	4	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	5	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	6	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	7	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	8	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	9	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	10	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	11	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	12	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	13	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	14	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	
<input type="radio"/>	15	32768	32768-8C:02:FA:04:03:59	32768-8C:02:FA:04:03:59	N/A	0	20	

Edit

Fig 7.3.4 Spanning tree MST Instance page

7.4 MST Port Setting

The MST Port Settings page enables you to configure MST on a per-port basis, and to view the information learned by the protocol, such as the designated bridge. To configure MST port setting, click **Spanning Tree >> MST Port Setting**.

The screenshot shows the Commando network management interface. The top navigation bar includes the Commando logo, the text "Spanning Tree MST Port Setting", and links for "Save | Logout | Reboot". A left-hand sidebar contains a tree view of configuration categories, with "Spanning Tree" expanded to show "MST Port Setting". The main content area displays the "MST Port Setting Table" for MST Instance 0. The table has 14 columns: Entry, Port, Path Cost, Priority, Port Role, Port State, Mode, Type, Designated Bridge, Designated Port ID, Designated Cost, and Remaining Hop. It lists 16 ports (GE1 to GE16) with their respective configurations. Ports 1, 10, and 11 are designated, while others are disabled. The designated bridge for ports 1 and 10 is 32768-8C:02:FA:04:03:59, and for port 11 it is 0-00:00:00:00:00:00.

Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop	
<input type="checkbox"/>	1	GE1	200000	128	Designated	Forwarding	STP	Boundary	32768-8C:02:FA:04:03:59	128-1	0	20
<input type="checkbox"/>	2	GE2	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-2	0	20
<input type="checkbox"/>	3	GE3	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-3	0	20
<input type="checkbox"/>	4	GE4	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-4	0	20
<input type="checkbox"/>	5	GE5	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-5	0	20
<input type="checkbox"/>	6	GE6	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-6	0	20
<input type="checkbox"/>	7	GE7	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-7	0	20
<input type="checkbox"/>	8	GE8	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-8	0	20
<input type="checkbox"/>	9	GE9	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-9	0	20
<input type="checkbox"/>	10	GE10	200000	128	Designated	Forwarding	STP	Boundary	32768-8C:02:FA:04:03:59	128-10	0	20
<input type="checkbox"/>	11	GE11	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-11	0	20
<input type="checkbox"/>	12	GE12	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-12	0	20
<input type="checkbox"/>	13	GE13	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-13	0	20
<input type="checkbox"/>	14	GE14	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-14	0	20
<input type="checkbox"/>	15	GE15	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-15	0	20
<input type="checkbox"/>	16	GE16	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-16	0	20

Fig 7.4.1 Spanning tree MST port setting table page

This screenshot is similar to the previous one but shows the "MST Instance" dropdown menu open, displaying options 0 through 15. The table content remains the same as in Figure 7.4.1, showing the configuration for MST Instance 0.

Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop	
<input type="checkbox"/>	1	GE1	200000	128	Designated	Forwarding	STP	Boundary	32768-8C:02:FA:04:03:59	128-1	0	20
<input type="checkbox"/>	2	GE2	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-2	0	20
<input type="checkbox"/>	3	GE3	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-3	0	20
<input type="checkbox"/>	4	GE4	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-4	0	20
<input type="checkbox"/>	5	GE5	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-5	0	20
<input type="checkbox"/>	6	GE6	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-6	0	20
<input type="checkbox"/>	7	GE7	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-7	0	20
<input type="checkbox"/>	8	GE8	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-8	0	20
<input type="checkbox"/>	9	GE9	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-9	0	20
<input type="checkbox"/>	10	GE10	200000	128	Designated	Forwarding	STP	Boundary	32768-8C:02:FA:04:03:59	128-10	0	20
<input type="checkbox"/>	11	GE11	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-11	0	20
<input type="checkbox"/>	12	GE12	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-12	0	20
<input type="checkbox"/>	13	GE13	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-13	0	20
<input type="checkbox"/>	14	GE14	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-14	0	20
<input type="checkbox"/>	15	GE15	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-15	0	20
<input type="checkbox"/>	16	GE16	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-16	0	20

Fig 7.4.2 Spanning tree MST Instant selection page



Save | Logout | Reboot

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance
 - MST Port Setting**
 - Statistics
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Spanning Tree > MST Port Setting

MST Port Setting Table

MSTI 0

<input type="checkbox"/>	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
<input type="checkbox"/>	1	GE1	200000	128	Designated	Forwarding	STP	Boundary	32768-8C:02:FA:04:03:59	128-1	0	20
<input type="checkbox"/>	2	GE2	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-2	0	20
<input type="checkbox"/>	3	GE3	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-3	0	20
<input type="checkbox"/>	4	GE4	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-4	0	20
<input type="checkbox"/>	5	GE5	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-5	0	20
<input checked="" type="checkbox"/>	6	GE6	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-6	0	20
<input checked="" type="checkbox"/>	7	GE7	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-7	0	20
<input type="checkbox"/>	8	GE8	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-8	0	20
<input type="checkbox"/>	9	GE9	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-9	0	20
<input type="checkbox"/>	10	GE10	200000	128	Designated	Forwarding	STP	Boundary	32768-8C:02:FA:04:03:59	128-10	0	20
<input type="checkbox"/>	11	GE11	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-11	0	20
<input type="checkbox"/>	12	GE12	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-12	0	20
<input type="checkbox"/>	13	GE13	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-13	0	20
<input type="checkbox"/>	14	GE14	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-14	0	20

Fig 7.4.3 Spanning tree MST port selection page



Spanning Tree > MST Port Setting

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance
 - MST Port Setting**
 - Statistics
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Edit MST Port Setting

MSTI	0
Port	GE6-GE7
Path Cost	<input type="text" value="10"/> (0 - 200000000) (0 = Auto)
Priority	<input type="text" value="64"/>
Port Role	Disabled
Port State	Disabled
Mode	STP
Type	Boundary
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-6
Designated Cost	20000
Remaining Hop	20

Apply Close

Fig 7.4.4 Edit MST port setting for selected port page



Spanning Tree > MST Port Setting

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance
 - MST Port Setting**
 - Statistics
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

MST Port Setting Table

MSTI 0 ▼

Q


<input type="checkbox"/>	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
<input type="checkbox"/>	1	GE1	200000	128	Designated	Forwarding	STP	Boundary	32768-8C:02:FA:04:03:59	128-1	0	20
<input type="checkbox"/>	2	GE2	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-2	0	20
<input type="checkbox"/>	3	GE3	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-3	0	20
<input type="checkbox"/>	4	GE4	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-4	0	20
<input type="checkbox"/>	5	GE5	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-5	0	20
<input type="checkbox"/>	6	GE6	10	64	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	84-6	0	20
<input type="checkbox"/>	7	GE7	10	64	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	84-7	0	20
<input type="checkbox"/>	8	GE8	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-8	0	20
<input type="checkbox"/>	9	GE9	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-9	0	20
<input type="checkbox"/>	10	GE10	200000	128	Designated	Forwarding	STP	Boundary	32768-8C:02:FA:04:03:59	128-10	0	20
<input type="checkbox"/>	11	GE11	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-11	0	20
<input type="checkbox"/>	12	GE12	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-12	0	20
<input type="checkbox"/>	13	GE13	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-13	0	20
<input type="checkbox"/>	14	GE14	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-14	0	20

Fig 7.4.5 MST port setting table page

7.5 Statistics

Display the total number of spanning tree BPDUs transmitted, received, processed, and dropped.

To View and clear Spanning Tree statistics, click **Spanning Tree >> Statistics**.



Spanning Tree >> Statistics

Statistics Table

Refresh Rate sec

<input type="checkbox"/>	Entry	Port	Receive BPDU			Transmit BPDU		
			Config	TCN	MSTP	Config	TCN	MSTP
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0
<input type="checkbox"/>	7	GE7	0	0	0	0	0	0
<input type="checkbox"/>	8	GE8	0	0	0	0	0	0
<input type="checkbox"/>	9	GE9	0	0	0	0	0	0
<input type="checkbox"/>	10	GE10	0	0	0	0	0	0
<input type="checkbox"/>	11	GE11	0	0	0	0	0	0
<input type="checkbox"/>	12	GE12	0	0	0	0	0	0
<input type="checkbox"/>	13	GE13	0	0	0	0	0	0
<input type="checkbox"/>	14	GE14	0	0	0	0	0	0

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance
 - MST Port Setting
 - Statistics**
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Fig 7.5.1 Spanning tree statistics table page



Spanning Tree > Statistics

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ **Spanning Tree**
 - Property
 - Port Setting
 - MST Instance
 - MST Port Setting
 - Statistics**
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

STP Port Statistic

Port	GE1
Refresh Rate	<input checked="" type="radio"/> None <input type="radio"/> 5 sec <input type="radio"/> 10 sec <input type="radio"/> 30 sec
Receive BPDU	
Config	0
TCN	0
MSTP	0
Transmit BPDU	
Config	0
TCN	0
MSTP	0

Refresh

Clear

Close

Fig 7.5.2 Spanning tree Port Statistic page

Chapter 8 Discovery

LLDP: The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network.

Property: Link Layer Discovery Protocol (LLDP) is a layer 2 neighbor discovery protocol that allows devices to advertise device information to their directly connected peers/neighbors. It is best practice to enable LLDP globally to standardize network topology across all devices if you have a multi-vendor network.

Port Setting: Configuring the LLDP Port Settings allows you to activate LLDP and SNMP notification per port and enter the Type-Length Values (TLVs) that are sent in the LLDP Protocol Data Unit (PDU).

MED Network Policy: An LLDP MED network policy is a related set of configuration settings for a specific real-time application such as voice or video. The media endpoint device should send its traffic as specified in the network policy that it receives. Network policies are associated with ports on the LLDP MED Port Settings page.

MED Port Setting: The LLDP MED Port Settings page enables the selection of LLDP-MED Type-Length Values (TLVs) and/or the network policies that are to be included in the outgoing LLDP advertisement for each interface. LLDP TLVs are used to describe individual pieces of information that the protocols transfer.

Packet View: LLDP packet view information displayed.

Local Information: This page displays the local information advertisements (TLVs) that will be transmitted by the LLDP agent.

Neighbor: The LLDP Neighbor Information page contains information that was received from neighboring devices.

Statistics: The LLDP Statistics page displays LLDP statistical information per port.

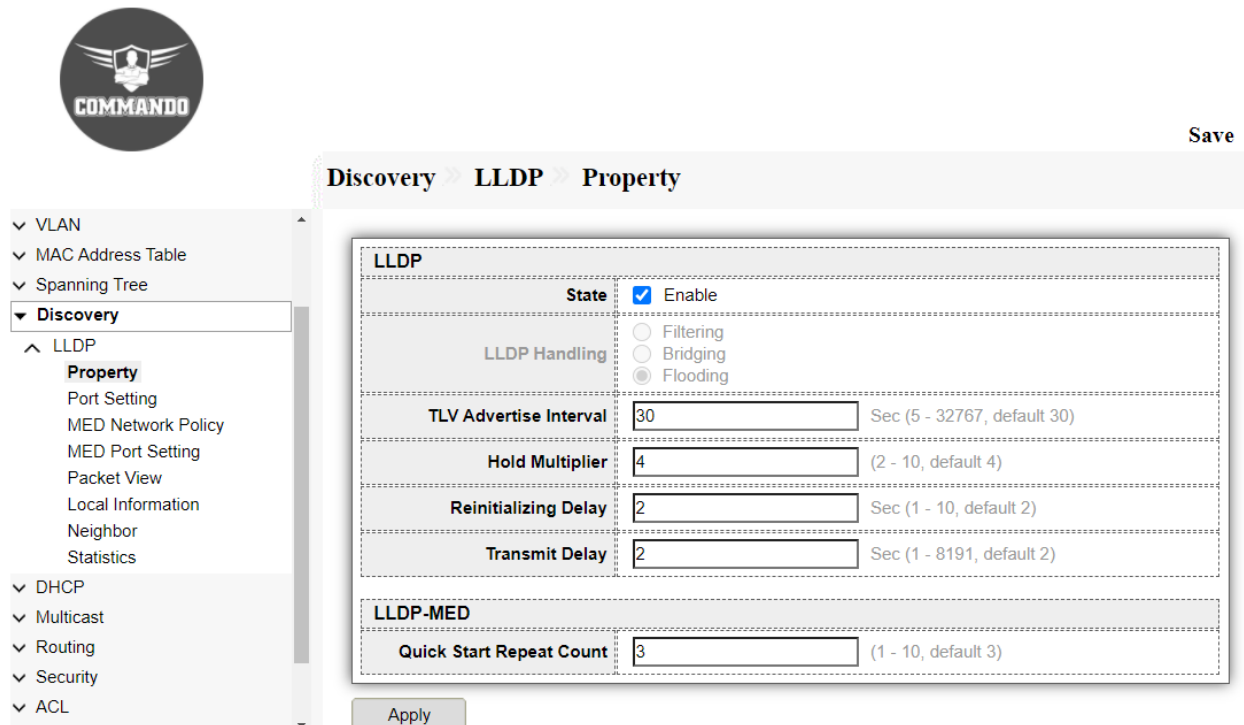
8.1 LLDP

LLDP is a protocol that enables network managers to troubleshoot and enhance network management in multi-vendor environments. LLDP standardizes methods for network devices to advertise themselves to other systems, and to store discovered information.

8.1.1 LLDP Property

The LLDP protocol has an extension called LLDP Media Endpoint Discovery (LLDP-MED), which provides and accepts information from media endpoint devices such as VoIP phones and video phones Property.

To configure LLDP Property, click **Discovery >> LLDP >> Property**.



The screenshot shows the configuration page for LLDP Property. On the left is a navigation tree with a 'COMMANDO' logo at the top. The tree includes categories like VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, and ACL. Under 'Discovery', 'LLDP' is expanded to show 'Property' as the selected option. The main content area is titled 'Discovery >> LLDP >> Property' and contains a 'Save' button in the top right. The configuration is divided into two sections: 'LLDP' and 'LLDP-MED'. The 'LLDP' section includes a 'State' field set to 'Enable', 'LLDP Handling' options (Filtering, Bridging, Flooding) with 'Flooding' selected, and input fields for 'TLV Advertise Interval' (30), 'Hold Multiplier' (4), 'Reinitializing Delay' (2), and 'Transmit Delay' (2). The 'LLDP-MED' section includes a 'Quick Start Repeat Count' field set to 3. An 'Apply' button is located at the bottom of the configuration area.

LLDP	
State	<input checked="" type="checkbox"/> Enable
LLDP Handling	<input type="radio"/> Filtering <input type="radio"/> Bridging <input checked="" type="radio"/> Flooding
TLV Advertise Interval	<input type="text" value="30"/> Sec (5 - 32767, default 30)
Hold Multiplier	<input type="text" value="4"/> (2 - 10, default 4)
Reinitializing Delay	<input type="text" value="2"/> Sec (1 - 10, default 2)
Transmit Delay	<input type="text" value="2"/> Sec (1 - 8191, default 2)


LLDP-MED	
Quick Start Repeat Count	<input type="text" value="3"/> (1 - 10, default 3)

Fig 8.1.1 LLDP property page

8.2 Port Setting

The Port Settings page enables activating LLDP and SNMP notification per port and entering the TLVs that are sent in the LLDP PDU. The LLDP-MED TLVs to be advertised can be selected in the LLDP MED Port Settings page, and the management address TLV of the device may be configured.

To configure LLDP Port Setting, click **Discovery > LLDP > Port Setting**



Discovery > LLDP > Port Setting

- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery**
 - LLDP
 - Property
 - Port Setting**
 - MED Network Policy
 - MED Port Setting
 - Packet View
 - Local Information
 - Neighbor
 - Statistics
 - DHCP
 - Multicast
 - Routing
 - Security
 - ACL
 - QoS
 - Diagnostics
 - Management

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	Selected TLV
<input type="checkbox"/>	1	GE1	Normal	802.1 PVID
<input type="checkbox"/>	2	GE2	Normal	802.1 PVID
<input type="checkbox"/>	3	GE3	Normal	802.1 PVID
<input type="checkbox"/>	4	GE4	Normal	802.1 PVID
<input type="checkbox"/>	5	GE5	Normal	802.1 PVID
<input type="checkbox"/>	6	GE6	Normal	802.1 PVID
<input type="checkbox"/>	7	GE7	Normal	802.1 PVID
<input type="checkbox"/>	8	GE8	Normal	802.1 PVID
<input type="checkbox"/>	9	GE9	Normal	802.1 PVID
<input type="checkbox"/>	10	GE10	Normal	802.1 PVID
<input type="checkbox"/>	11	GE11	Normal	802.1 PVID
<input type="checkbox"/>	12	GE12	Normal	802.1 PVID
<input type="checkbox"/>	13	GE13	Normal	802.1 PVID
<input type="checkbox"/>	14	GE14	Normal	802.1 PVID
<input type="checkbox"/>	15	GE15	Normal	802.1 PVID

Fig 8.2.1 Default LLDP port setting table page



Discovery >> LLDP >> Port Setting

- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ▼ Discovery
 - ^ LLDP
 - Property
 - Port Setting**
 - MED Network Policy
 - MED Port Setting
 - Packet View
 - Local Information
 - Neighbor
 - Statistics
 - ✓ DHCP
 - ✓ Multicast
 - ✓ Routing
 - ✓ Security
 - ✓ ACL
 - ✓ QoS
 - ✓ Diagnostics
 - ✓ Management

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	Selected TLV
<input type="checkbox"/>	1	GE1	Normal	802.1 PVID
<input checked="" type="checkbox"/>	2	GE2	Normal	802.1 PVID
<input checked="" type="checkbox"/>	3	GE3	Normal	802.1 PVID
<input checked="" type="checkbox"/>	4	GE4	Normal	802.1 PVID
<input type="checkbox"/>	5	GE5	Normal	802.1 PVID
<input type="checkbox"/>	6	GE6	Normal	802.1 PVID
<input type="checkbox"/>	7	GE7	Normal	802.1 PVID
<input type="checkbox"/>	8	GE8	Normal	802.1 PVID
<input type="checkbox"/>	9	GE9	Normal	802.1 PVID
<input type="checkbox"/>	10	GE10	Normal	802.1 PVID
<input type="checkbox"/>	11	GE11	Normal	802.1 PVID
<input type="checkbox"/>	12	GE12	Normal	802.1 PVID
<input type="checkbox"/>	13	GE13	Normal	802.1 PVID
<input type="checkbox"/>	14	GE14	Normal	802.1 PVID
<input type="checkbox"/>	15	GE15	Normal	802.1 PVID

Fig 8.2.2 LLDP port setting selection of GE2, GE3 and GE4 page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ **Discovery**
 - ▲ LLDP
 - Property
 - Port Setting**
 - MED Network Policy
 - MED Port Setting
 - Packet View
 - Local Information
 - Neighbor
 - Statistics
 - ▼ DHCP
 - ▼ Multicast
 - ▼ Routing
 - ▼ Security
 - ▼ ACL
 - ▼ QoS
 - ▼ Diagnostics
 - ▼ Management

Discovery >> LLDP >> Port Setting

Edit Port Setting

Port	GE2-GE4	
Mode	<input checked="" type="radio"/> Transmit	
	<input type="radio"/> Receive	
	<input type="radio"/> Normal	
	<input type="radio"/> Disable	
Optional TLV	Available TLV	Selected TLV
	Port Description System Name System Description 802.3 MAC-PHY 802.3 Link Aggregation	802.1 PVID System Capabilities
802.1 VLAN Name	Available VLAN	Selected VLAN
		VLAN 1

Apply Close

Fig 8.2.3 Edit LLDP port setting of GE2, GE3 and GE4 page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ **Discovery**
 - ▲ LLDP
 - Property
 - Port Setting**
 - MED Network Policy
 - MED Port Setting
 - Packet View
 - Local Information
 - Neighbor
 - Statistics
 - ▼ DHCP
 - ▼ Multicast

Save | Logout | Reboot | Debug

Discovery >> LLDP >> Port Setting

Port Setting Table

Entry	Port	Mode	Selected TLV
<input type="checkbox"/>	1 GE1	Normal	802.1 PVID
<input type="checkbox"/>	2 GE2	Normal	System Capabilities , 802.1 PVID , 802.1 VLAN Name
<input type="checkbox"/>	3 GE3	Normal	System Capabilities , 802.1 PVID , 802.1 VLAN Name
<input type="checkbox"/>	4 GE4	Normal	System Capabilities , 802.1 PVID , 802.1 VLAN Name
<input type="checkbox"/>	5 GE5	Normal	802.1 PVID
<input type="checkbox"/>	6 GE6	Normal	802.1 PVID
<input type="checkbox"/>	7 GE7	Normal	802.1 PVID
<input type="checkbox"/>	8 GE8	Normal	802.1 PVID
<input type="checkbox"/>	9 GE9	Normal	802.1 PVID
<input type="checkbox"/>	10 GE10	Normal	802.1 PVID
<input type="checkbox"/>	11 GE11	Normal	802.1 PVID
<input type="checkbox"/>	12 GE12	Normal	802.1 PVID

Fig 8.2.4 LLDP port setting table after Editing page

8.3 MED Network Policy

Enables the advertisement and discovery of network policies for real-time applications such as voice and/or video. LLDP Media Endpoint Discovery (LLDP-MED) is an extension of LLDP that provides the following additional capabilities to support media endpoint devices. Network Policy Number—Select the number of the policy to be created.

To Configure LLDP MED Network Policy, click **Discovery >> LLDP >> MED Network Policy**.



The screenshot displays the COMMANDO network management interface. On the left is a navigation tree with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The 'Discovery' category is expanded, and 'LLDP' is selected, with 'MED Network Policy' highlighted. The main content area shows the breadcrumb 'Discovery >> LLDP >> MED Network Policy' and a table titled 'MED Network Policy Table'. The table has columns for Policy ID, Application, VLAN, VLAN Tag, Priority, and DSCP. It shows 'Showing 0 to 0 of 0 entries' and '0 results found.' Below the table are 'Add', 'Edit', and 'Delete' buttons.

Fig 8.3.1 LLDP MED Network Policy ID page



Save |

Discovery > LLDP > MED Network Policy

Add MED Network Policy

Policy ID	1
Application	Video Conferencing
VLAN	<input type="text"/> Range (0 - 4095)
VLAN Tag	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
Priority	0
DSCP	0

Apply Close

Fig 8.3.2 LLDP Add MED Network Policy page



Save | Logout | Reboot

Discovery > LLDP > MED Network Policy

MED Network Policy Table

Showing All entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP	
<input type="checkbox"/>	1	Video Conferencing	1	Tagged	0	0	

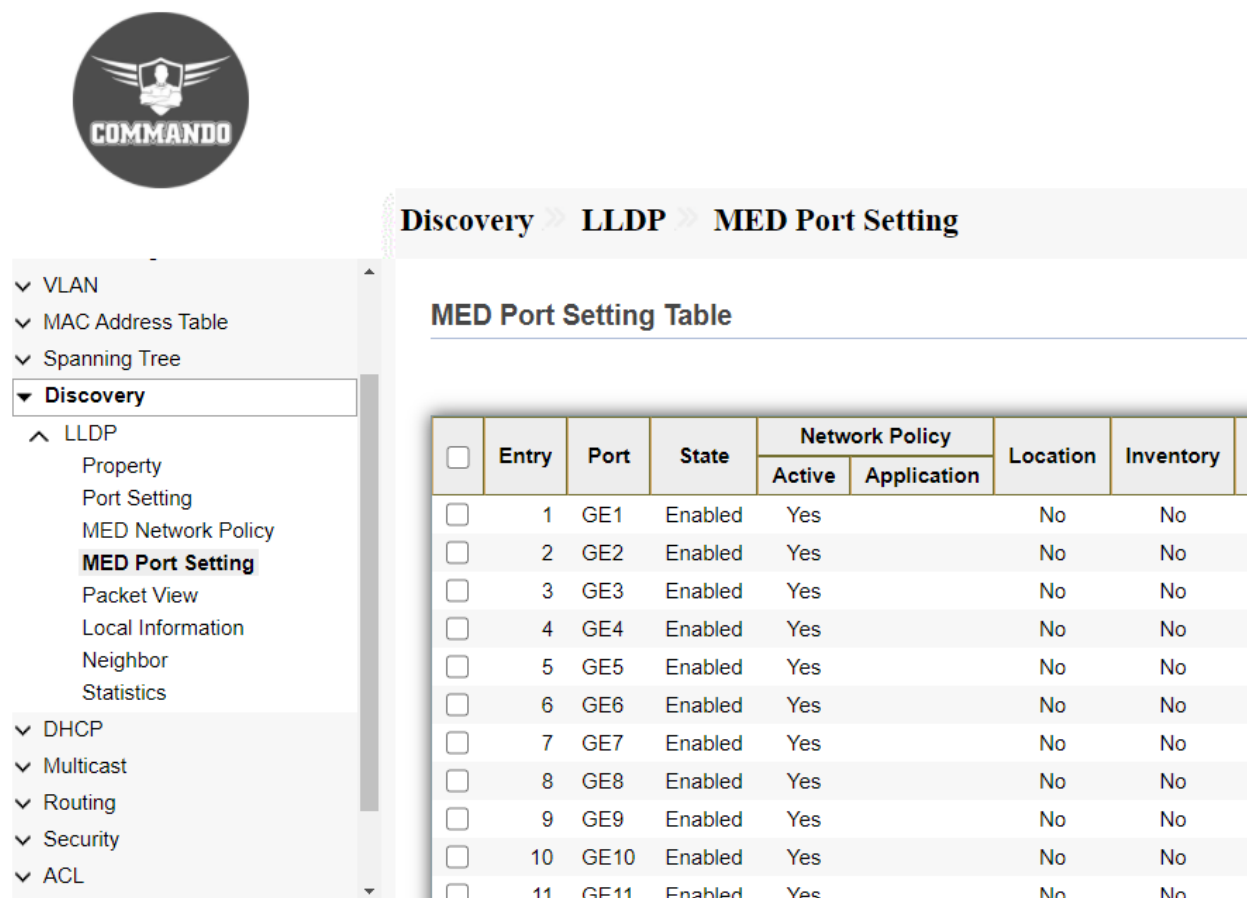
Add Edit Delete

First Previous 1 N

Fig 8.3.3 LLDP MED Network Policy Table after setting for Policy ID 4 page

8.4 MED Port Setting

The LLDP MED Port Settings page enables the selection of the LLDP-MED TLVs and/or the network policies to be included in the outgoing LLDP advertisement for the desired interfaces. The LLDP MED Port Settings page enables the selection of the LLDP-MED TLVs and/or the network policies to be included in the outgoing LLDP advertisement for the desired interfaces. Network policies are configured using the LLDP MED Network Policy page. To Configure LLDP MED Port Setting, click **Discovery >> LLDP >> MED Port Setting**.



Discovery >> LLDP >> MED Port Setting

MED Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Network Policy		Location	Inventory
				Active	Application		
<input type="checkbox"/>	1	GE1	Enabled	Yes		No	No
<input type="checkbox"/>	2	GE2	Enabled	Yes		No	No
<input type="checkbox"/>	3	GE3	Enabled	Yes		No	No
<input type="checkbox"/>	4	GE4	Enabled	Yes		No	No
<input type="checkbox"/>	5	GE5	Enabled	Yes		No	No
<input type="checkbox"/>	6	GE6	Enabled	Yes		No	No
<input type="checkbox"/>	7	GE7	Enabled	Yes		No	No
<input type="checkbox"/>	8	GE8	Enabled	Yes		No	No
<input type="checkbox"/>	9	GE9	Enabled	Yes		No	No
<input type="checkbox"/>	10	GE10	Enabled	Yes		No	No
<input type="checkbox"/>	11	GE11	Enabled	Yes		No	No

Fig 8.4.1 LLDP MED port setting table page



Discovery >> LLDP >> MED Port Setting

- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ **Discovery**
 - ∧ LLDP
 - Property
 - Port Setting
 - MED Network Policy
 - MED Port Setting**
 - Packet View
 - Local Information
 - Neighbor
 - Statistics
 - ∨ DHCP
 - ∨ Multicast
 - ∨ Routing
 - ∨ Security
 - ∨ ACL

MED Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Network Policy		Location	Inventory	
				Active	Application			
<input type="checkbox"/>	1	GE1	Enabled	Yes		No	No	
<input checked="" type="checkbox"/>	2	GE2	Enabled	Yes		No	No	
<input checked="" type="checkbox"/>	3	GE3	Enabled	Yes		No	No	
<input checked="" type="checkbox"/>	4	GE4	Enabled	Yes		No	No	
<input checked="" type="checkbox"/>	5	GE5	Enabled	Yes		No	No	
<input checked="" type="checkbox"/>	6	GE6	Enabled	Yes		No	No	
<input type="checkbox"/>	7	GE7	Enabled	Yes		No	No	
<input type="checkbox"/>	8	GE8	Enabled	Yes		No	No	
<input type="checkbox"/>	9	GE9	Enabled	Yes		No	No	
<input type="checkbox"/>	10	GE10	Enabled	Yes		No	No	
<input type="checkbox"/>	11	GE11	Enabled	Yes		No	No	

Fig 8.4.2 LLDP MED port setting for ports page



Discovery > LLDP > MED Port Setting

- √ Status
- √ Network
- √ Port
- √ POE Setting
- √ VLAN
- √ MAC Address Table
- √ Spanning Tree
- ▼ Discovery
 - ^ LLDP
 - Property
 - Port Setting
 - MED Network Policy
 - MED Port Setting**
 - Packet View
 - Local Information
 - Neighbor
 - Statistics
 - √ DHCP
 - √ Multicast
 - √ Routing
 - √ Security
 - √ ACL
 - √ QoS
 - √ Diagnostics
 - √ Management

Edit MED Port Setting

Port	GE2-GE6	
State	<input checked="" type="checkbox"/> Enable	
Optional TLV	Available TLV	Selected TLV
	Location	Network Policy Inventory
Network policy	Available Policy	Selected Policy
		1 (Video Conferencing)
Location		
Coordinate	<input type="text"/>	(16 pairs of hexadecimal characters)
Civic	<input type="text"/>	(6 - 160 pairs of hexadecimal characters)
ECS ELIN	<input type="text"/>	(10 - 25 pairs of hexadecimal characters)

Apply Close

Fig 8.4.3 Edit LLDP MED port setting for selected ports page



Discovery > LLDP > MED Port Setting

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
 - ^ LLDP
 - Property
 - Port Setting
 - MED Network Policy
 - MED Port Setting**
 - Packet View
 - Local Information
 - Neighbor
 - Statistics
 - ▼ DHCP
 - ▼ Multicast
 - ▼ Routing
 - ▼ Security
 - ▼ ACL
 - ▼ QoS
 - ▼ Diagnostics
 - ▼ Management

MED Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Network Policy		Location	Inventory
				Active	Application		
<input type="checkbox"/>	1	GE1	Enabled	Yes		No	No
<input type="checkbox"/>	2	GE2	Enabled	Yes	Video Conferencing	No	Yes
<input type="checkbox"/>	3	GE3	Enabled	Yes	Video Conferencing	No	Yes
<input type="checkbox"/>	4	GE4	Enabled	Yes	Video Conferencing	No	Yes
<input type="checkbox"/>	5	GE5	Enabled	Yes	Video Conferencing	No	Yes
<input type="checkbox"/>	6	GE6	Enabled	Yes	Video Conferencing	No	Yes
<input type="checkbox"/>	7	GE7	Enabled	Yes		No	No
<input type="checkbox"/>	8	GE8	Enabled	Yes		No	No
<input type="checkbox"/>	9	GE9	Enabled	Yes		No	No
<input type="checkbox"/>	10	GE10	Enabled	Yes		No	No
<input type="checkbox"/>	11	GE11	Enabled	Yes		No	No
<input type="checkbox"/>	12	GE12	Enabled	Yes		No	No
<input type="checkbox"/>	13	GE13	Enabled	Yes		No	No
<input type="checkbox"/>	14	GE14	Enabled	Yes		No	No
<input type="checkbox"/>	15	GE15	Enabled	Yes		No	No
<input type="checkbox"/>	16	GE16	Enabled	Yes		No	No
<input type="checkbox"/>	17	GE17	Enabled	Yes		No	No
<input type="checkbox"/>	18	GE18	Enabled	Yes		No	No

Fig 8.4.4 LLDP MED port setting Table page

8.5 Packet View

LLDP packets are sent every 30 seconds that defines messages, encapsulated in Ethernet frames for the purpose of giving devices a means of announcing basic device information to other devices on the LAN. You can view connecting devices that are sending LLDP packets from this location. It is helpful with initial connectivity or troubleshooting.

To view LLDP Overloading, click **Discovery >> LLDP >> Packet View**.



Discovery >> LLDP >> Packet View

Packet View Table

	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
<input type="radio"/>	1	GE1	38	1450	Not Overloading
<input type="radio"/>	2	GE2	165	1323	Not Overloading
<input type="radio"/>	3	GE3	165	1323	Not Overloading
<input type="radio"/>	4	GE4	165	1323	Not Overloading
<input type="radio"/>	5	GE5	143	1345	Not Overloading
<input type="radio"/>	6	GE6	143	1345	Not Overloading
<input type="radio"/>	7	GE7	38	1450	Not Overloading
<input type="radio"/>	8	GE8	38	1450	Not Overloading
<input type="radio"/>	9	GE9	38	1450	Not Overloading
<input type="radio"/>	10	GE10	39	1449	Not Overloading
<input type="radio"/>	11	GE11	39	1449	Not Overloading
<input type="radio"/>	12	GE12	39	1449	Not Overloading
<input type="radio"/>	13	GE13	39	1449	Not Overloading
<input type="radio"/>	14	GE14	39	1449	Not Overloading
<input type="radio"/>	15	GE15	39	1449	Not Overloading
<input type="radio"/>	16	GE16	39	1449	Not Overloading
<input type="radio"/>	17	GE17	39	1449	Not Overloading
<input type="radio"/>	18	GE18	39	1449	Not Overloading
<input type="radio"/>	19	GE19	39	1449	Not Overloading

Navigation Menu:

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ **Discovery**
 - ▲ LLDP
 - Property
 - Port Setting
 - MED Network Policy
 - MED Port Setting
 - Packet View**
 - Local Information
 - Neighbor
 - Statistics
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Fig 8.5.1 Default LLDP Packet view Table page



Discovery » LLDP » Packet View

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
 - ▲ LLDP
 - Property
 - Port Setting
 - MED Network Policy
 - MED Port Setting
 - Packet View**
 - Local Information
 - Neighbor
 - Statistics
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Packet View Table

	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
<input checked="" type="radio"/>	1	GE1	38	1450	Not Overloading
<input type="radio"/>	2	GE2	165	1323	Not Overloading
<input type="radio"/>	3	GE3	165	1323	Not Overloading
<input type="radio"/>	4	GE4	165	1323	Not Overloading
<input type="radio"/>	5	GE5	143	1345	Not Overloading
<input type="radio"/>	6	GE6	143	1345	Not Overloading
<input type="radio"/>	7	GE7	38	1450	Not Overloading
<input type="radio"/>	8	GE8	38	1450	Not Overloading
<input type="radio"/>	9	GE9	38	1450	Not Overloading
<input type="radio"/>	10	GE10	39	1449	Not Overloading
<input type="radio"/>	11	GE11	39	1449	Not Overloading
<input type="radio"/>	12	GE12	39	1449	Not Overloading
<input type="radio"/>	13	GE13	39	1449	Not Overloading
<input type="radio"/>	14	GE14	39	1449	Not Overloading
<input type="radio"/>	15	GE15	39	1449	Not Overloading
<input type="radio"/>	16	GE16	39	1449	Not Overloading
<input type="radio"/>	17	GE17	39	1449	Not Overloading
<input type="radio"/>	18	GE18	39	1449	Not Overloading

Fig 8.5.2 LLDP Packet view Table selecting GE1 port page



Discovery > LLDP > Packet View

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ▼ Discovery
 - ^ LLDP
 - Property
 - Port Setting
 - MED Network Policy
 - MED Port Setting
 - Packet View**
 - Local Information
 - Neighbor
 - Statistics
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

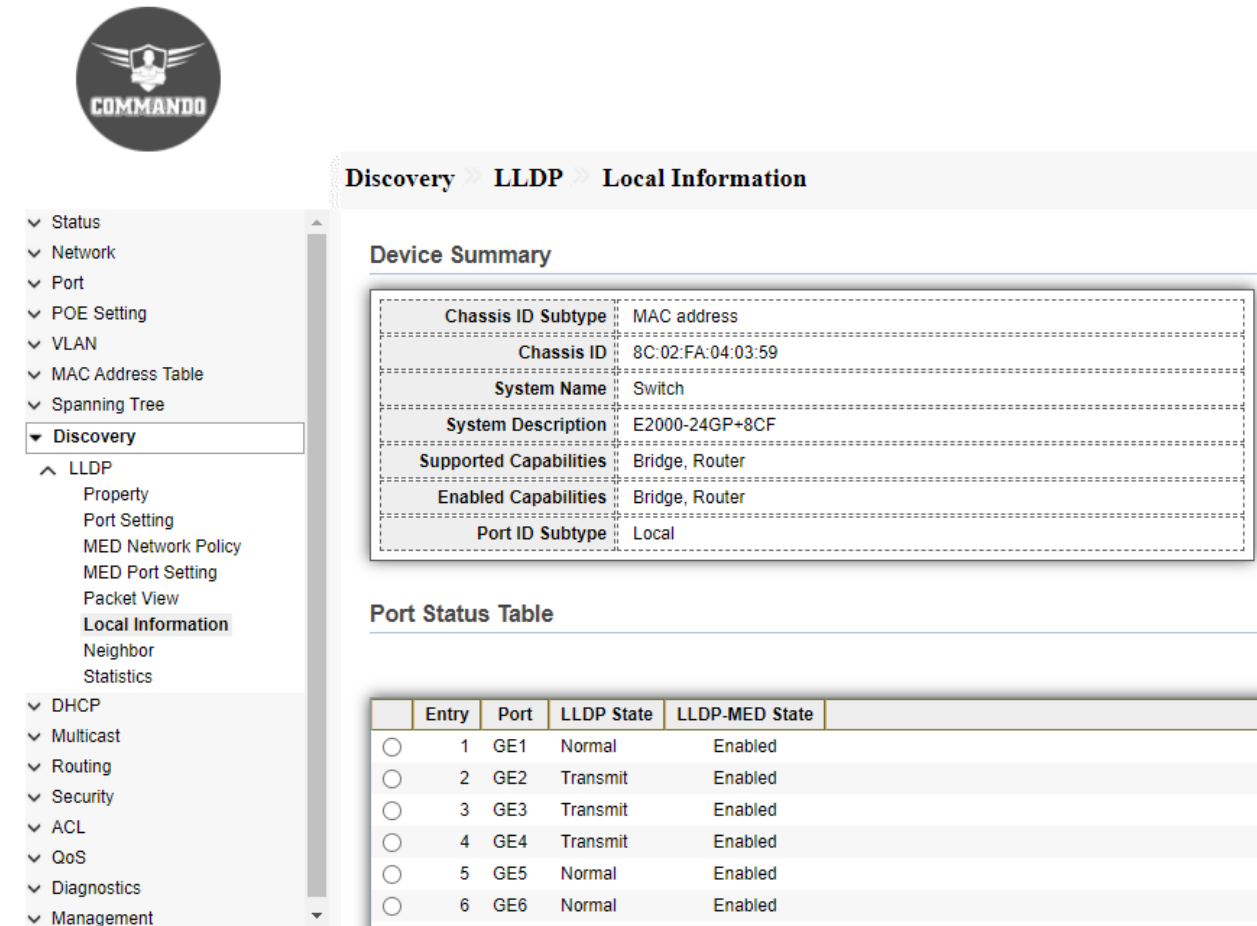
Packet View Detail

Port	GE1
Mandatory TLVs	
Size (Bytes)	21
Operational Status	Transmitted
MED Capabilities	
Size (Bytes)	9
Operational Status	Transmitted
MED Location	
Size (Bytes)	0
Operational Status	Transmitted
MED Network Policy	
Size (Bytes)	0
Operational Status	Transmitted
MED Inventory	
Size (Bytes)	0
Operational Status	Transmitted
MED Extended Power via MDI	

Fig 8.5.3 LLDP Packet view detail for GE1 port page

8.6 Local Information

It displays the information contained in the LLDP TLVs to be sent about the local system. To view and displays LLDP local port status advertised on a port. To View LLDP Local Device, click **Discovery >> LLDP >> Local Information**.



COMMANDO

Discovery > LLDP > Local Information

Device Summary

Chassis ID Subtype	MAC address
Chassis ID	8C:02:FA:04:03:59
System Name	Switch
System Description	E2000-24GP+8CF
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID Subtype	Local

Port Status Table

	Entry	Port	LLDP State	LLDP-MED State
<input type="radio"/>	1	GE1	Normal	Enabled
<input type="radio"/>	2	GE2	Transmit	Enabled
<input type="radio"/>	3	GE3	Transmit	Enabled
<input type="radio"/>	4	GE4	Transmit	Enabled
<input type="radio"/>	5	GE5	Normal	Enabled
<input type="radio"/>	6	GE6	Normal	Enabled

Fig 8.6.1 LLDP Local Information device summary page



Discovery >> LLDP >> Local Information

- ∨ Status
- ∨ Network
- ∨ Port
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ **Discovery**
 - ∧ LLDP
 - Property
 - Port Setting
 - MED Network Policy
 - MED Port Setting
 - Packet View
 - Local Information**
 - Neighbor
 - Statistics
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ QoS
- ∨ Diagnostics
- ∨ Management

Device Summary

Chassis ID Subtype	MAC address
Chassis ID	8C:02:FA:04:03:59
System Name	Switch
System Description	E2000-24GP+8CF
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID Subtype	Local

Port Status Table

	Entry	Port	LLDP State	LLDP-MED State
<input checked="" type="radio"/>	1	GE1	Normal	Enabled
<input type="radio"/>	2	GE2	Transmit	Enabled
<input type="radio"/>	3	GE3	Transmit	Enabled
<input type="radio"/>	4	GE4	Transmit	Enabled
<input type="radio"/>	5	GE5	Normal	Enabled
<input type="radio"/>	6	GE6	Normal	Enabled

Fig 8.6.2 LLDP Local Information Selecting port GE1 page



Discovery > LLDP > Local Information

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
 - ▲ LLDP
 - Property
 - Port Setting
 - MED Network Policy
 - MED Port Setting
 - Packet View
 - Local Information**
 - Neighbor
 - Statistics
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Local Information Detail

Chassis ID Subtype	MAC address
Chassis ID	8C:02:FA:04:03:59
System Name	Switch
System Description	E2000-24GP+8CF
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID	GE1
Port ID Subtype	Local
Port Description	

Management Address Table

Address Subtype	Address	Interface Subtype	Interface Number
0 results found.			

MAC/PHY Detail

Auto-Negotiation Supported	N/A
Auto-Negotiation Enabled	N/A
Auto-Negotiation Advertised Capabilities	N/A
Operational MAU Type	N/A

802.3 Detail

802.3 Maximum Frame Size	N/A
--------------------------	-----

802.3 Link Aggregation

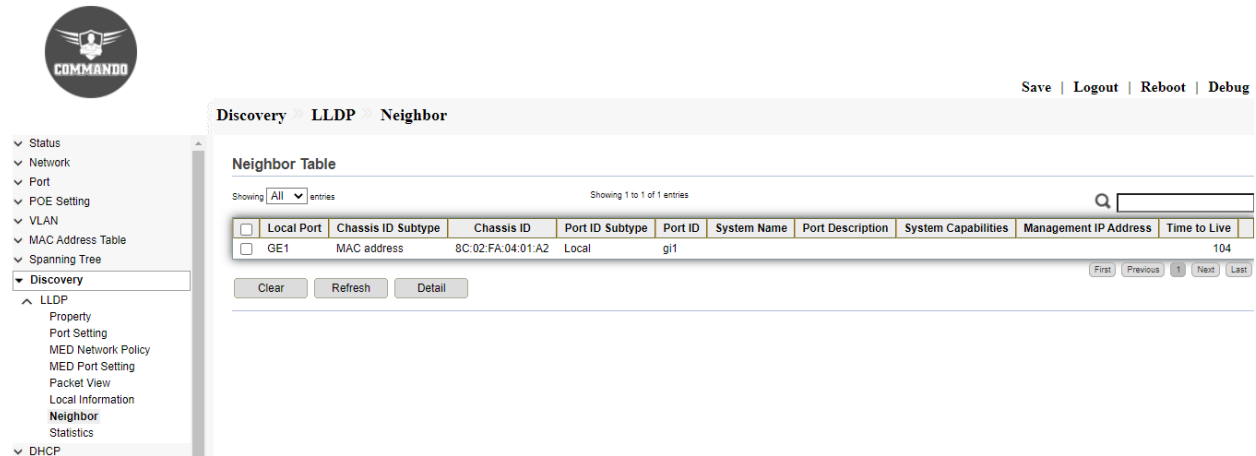
Aggregation Capability	N/A
Aggregation Status	N/A

Fig 8.6.3 LLDP Local Information details for port GE1 page

8.7 Neighbor

The LLDP Neighbors Information page contains information that was received from neighboring devices. The neighbor information table is populated as advertisements from the neighbors arrive on the ports. Use the LLDP Neighbor page to view LLDP neighbors' information.

To view LLDP Remote Device, click **Discovery >> LLDP >> Neighbor**.



The screenshot shows the COMMANDO web interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, LLDP, and DHCP. The 'Discovery' menu is expanded, showing 'LLDP' and 'Neighbor' selected. The main content area displays the 'Neighbor Table' with a search bar and a table of one entry. The table has columns for Local Port, Chassis ID Subtype, Chassis ID, Port ID Subtype, Port ID, System Name, Port Description, System Capabilities, Management IP Address, and Time to Live. The entry shows 'GE1' as the local port, 'MAC address' as the subtype, '8C:02:FA:04:01:A2' as the chassis ID, 'Local' as the port ID subtype, and 'gi1' as the port ID. Below the table are 'Clear', 'Refresh', and 'Detail' buttons. At the top right of the interface are links for 'Save', 'Logout', 'Reboot', and 'Debug'.


<input type="checkbox"/>	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Port Description	System Capabilities	Management IP Address	Time to Live
<input type="checkbox"/>	GE1	MAC address	8C:02:FA:04:01:A2	Local	gi1					104

Fig 8.7.1 LLDP Neighbors table default page

8.8 Statistics

The LLDP Statistics page displays LLDP statistical information per port. The Link Layer Discovery Protocol (LLDP) Statistics page displays summary and per-port information for LLDP frames transmitted and received on the switch.

To view LLDP Statistics status, click **Discovery >> LLDP >> Statistics**.



Discovery > LLDP > Statistics

- ∨ Status
- ∨ Network
- ∨ Port
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ **Discovery**
 - ∧ LLDP
 - Property
 - Port Setting
 - MED Network Policy
 - MED Port Setting
 - Packet View
 - Local Information
 - Neighbor
 - Statistics**
 - ∨ DHCP
 - ∨ Multicast
 - ∨ Routing
 - ∨ Security
 - ∨ ACL

Global Statistics

Insertions	1
Deletions	0
Drops	0
AgeOuts	0

Clear Refresh

Statistics Table

<input type="checkbox"/>	Entry	Port	Transmit Frame		Receive Frame			Receive TLV		Neighbor Timeout
			Total		Total	Discard	Error	Discard	Unrecognized	
<input type="checkbox"/>	1	GE1	234		231	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0		0	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0		0	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0		0	0	0	0	0	0

Fig 8.8.1 LLDP Global statistics page

Chapter 9 DHCP

DHCP (Dynamic Host Configuration Protocol) is widely used to automatically assign IP addresses and other network configuration parameters to network devices, enhancing the utilization of IP address.

DHCP Server

DHCP Server is used to dynamically assign IP addresses, default gateway and other parameters to DHCP clients. DHCP (dynamic host configuration protocol) allows a server to assign an IP address to a computer from a preselected range of numbers configured for a particular network.

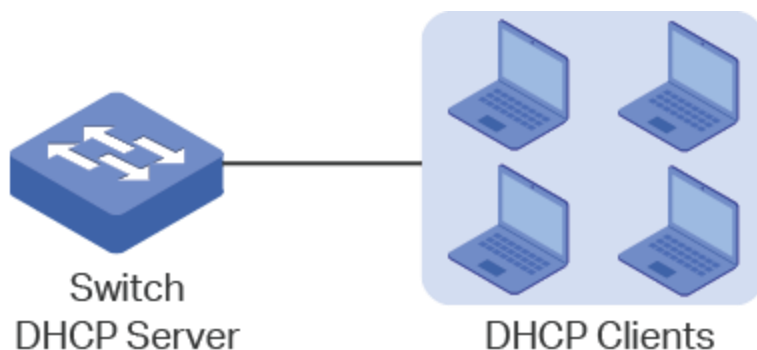


Fig 9.1 DHCP Server and Clients

DHCP Relay

DHCP Relay is used to process and forward DHCP packets between different subnets or VLANs. DHCP clients broadcast DHCP request packets to require for IP addresses. Without this function, clients cannot obtain IP addresses from a DHCP server in the different LAN because the broadcast packets can be transmitted only in the same LAN. DHCP Relay includes three features: Option 82, DHCP Interface Relay and DHCP VLAN Relay.

DHCP Option 82: Option 82 is called the DHCP Relay Agent Information Option.

When enabled, the DHCP relay agent can inform the DHCP server of some specified information of clients by inserting an Option 82 payload to DHCP request packets before forwarding them to the DHCP server, so that the DHCP server can distribute the

IP addresses or other parameters to clients based on the payload. In this way, Option 82 prevents DHCP client requests from untrusted sources. Besides, it allows the DHCP server to assign IP addresses of different address pools to clients in different groups.

Property: Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring IP address, gateways and other IP related things automatically to connected hosts.

IP Pool Setting: You can customize the DHCP pool subnet and address range to provide simultaneous access to a greater number of clients.

VLAN IF Address Group Setting: For Configuring a Layer 3 VLAN interface.

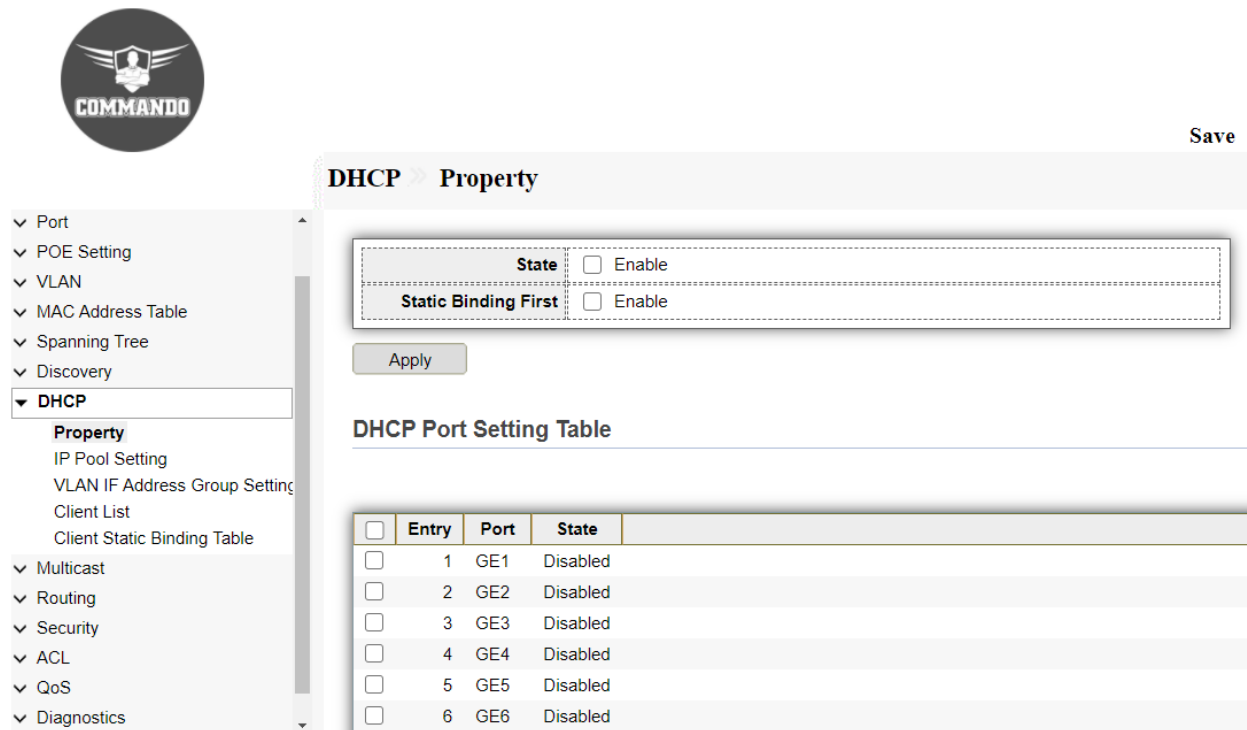
Client List: DHCP server to dynamically choose IP addresses from the IP Pools and assign them permanently to clients. To view clients this page is used.

Client Static Binding Table: Configuring the DHCP Server and the Static-Binding. The following table describes the static binding options. Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol (DHCP) local server.

9.1 Property

DHCP property page allows you to enable DHCP which is by default disabled.

To configure and view DHCP property, click **DHCP >> Property**.



The screenshot shows the COMMANDO web interface. On the left is a navigation menu with categories like Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, and Diagnostics. The DHCP section is expanded, showing sub-items: Property, IP Pool Setting, VLAN IF Address Group Setting, Client List, and Client Static Binding Table. The main content area is titled 'DHCP > Property' and features a 'Save' button in the top right. Below the title is a dashed box containing two settings: 'State' with an unchecked checkbox and 'Static Binding First' with an unchecked checkbox. An 'Apply' button is located below these settings. A section titled 'DHCP Port Setting Table' contains a table with columns for 'Entry', 'Port', and 'State'. The table lists six entries, each with a checkbox in the 'Entry' column and a 'Disabled' state.

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Disabled
<input type="checkbox"/>	2	GE2	Disabled
<input type="checkbox"/>	3	GE3	Disabled
<input type="checkbox"/>	4	GE4	Disabled
<input type="checkbox"/>	5	GE5	Disabled
<input type="checkbox"/>	6	GE6	Disabled

Fig 9.1.1 Default DHCP Property page

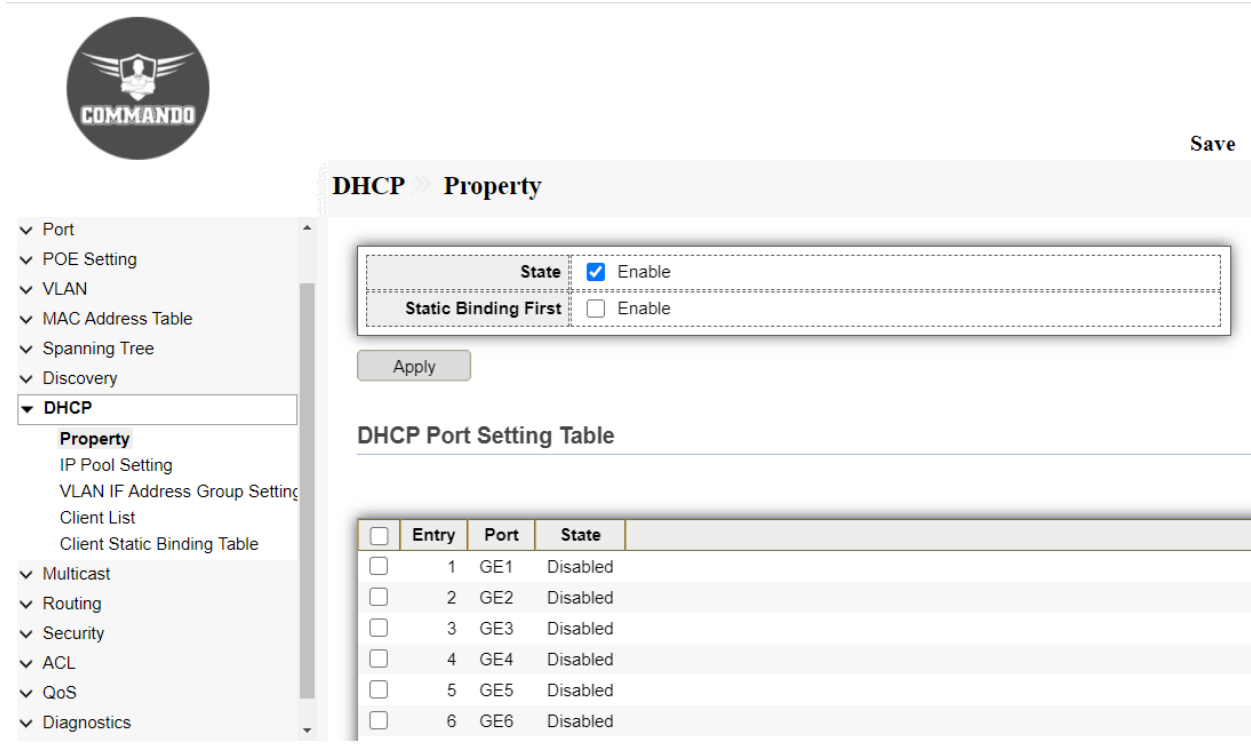


Fig 9.1.2 Enable DHCP Property page

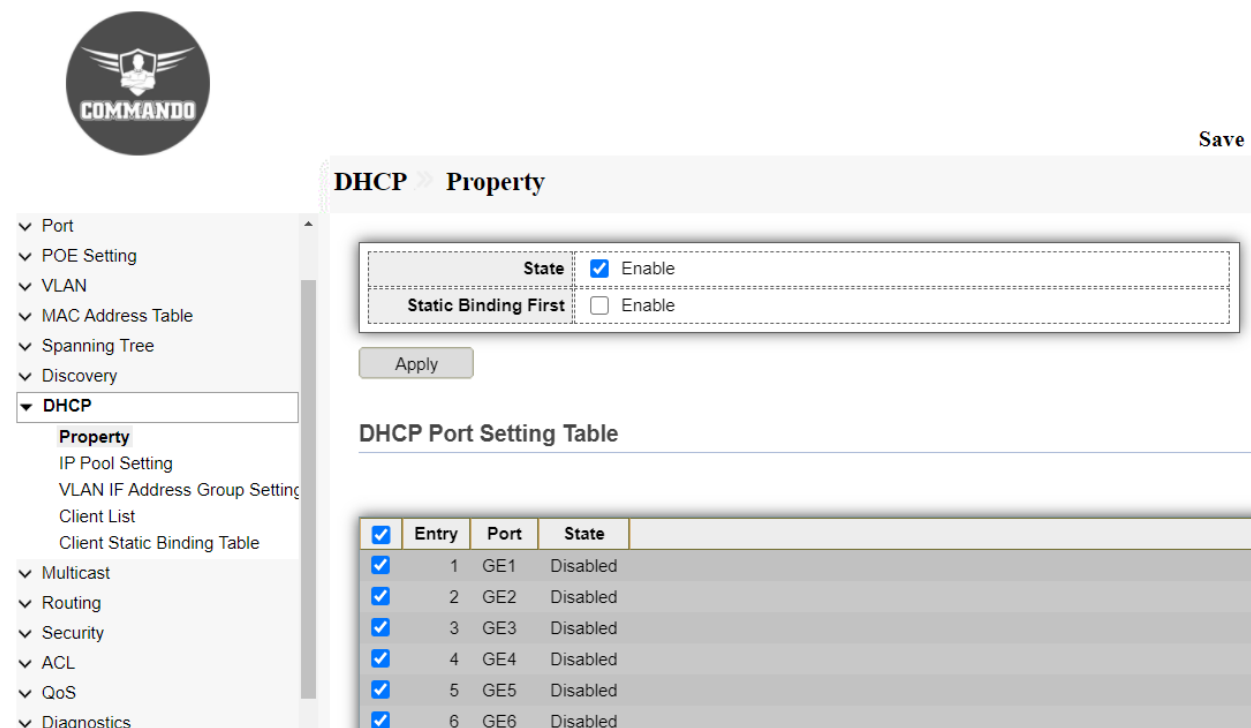


Fig 9.1.3 Selecting ports on DHCP Property page



Save | Logout | Reboot | Debug

DHCP **Property**

Edit Port Setting

Port	GE1-GE28,LAG1-LAG8
State	<input checked="" type="checkbox"/> Enable

Apply Close

Fig 9.1.4 Edit ports setting DHCP Property page



Save

DHCP **Property**

State	<input checked="" type="checkbox"/> Enable
Static Binding First	<input type="checkbox"/> Enable

Apply

DHCP Port Setting Table

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Enabled
<input type="checkbox"/>	2	GE2	Enabled
<input type="checkbox"/>	3	GE3	Enabled
<input type="checkbox"/>	4	GE4	Enabled
<input type="checkbox"/>	5	GE5	Enabled
<input type="checkbox"/>	6	GE6	Enabled

Fig 9.1.5 DHCP port setting table after enabling page

9.2 IP Pool Setting

With IP Pool setting can set Start IP address and End address and gateway of pool along with mask. DNS Primary and secondary server along with DHCP leased time can also be set. By default, lease time is 1day before renewal of IP.

To configure and view IP Pool Setting, click **DHCP >> IP Pool Setting**.

The screenshot displays the COMMANDO web interface for DHCP IP Pool Setting. On the left, a navigation menu is visible with 'DHCP' expanded to show 'IP Pool Setting'. The main content area is titled 'DHCP > IP Pool Setting' and features an 'IP Pool Table'. The table has columns for 'Pool', 'Section', 'Start Address', 'End Address', 'Gateway', 'Mask', 'DNS Primary Server', 'DNS Second Server', and 'Lease time'. The table is currently empty, showing '0 results found.' and navigation buttons for 'Add', 'Edit', 'Delete', 'First', 'Previous', '1', 'Next', and 'Last'. The page also includes a 'COMMANDO' logo and navigation links for 'Save', 'Logout', 'Reboot', and 'Debug'.

Fig 9.2.1 Default DHCP IP Pool setting page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
 - Property
 - IP Pool Setting**
 - VLAN IF Address Group Setting
 - Client List
 - Client Static Binding Table
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

DHCP > IP Pool Setting

IP Pool Table

Pool	<input type="text" value="192.168.10.0"/> (1 to 32 alphanumeric characters)
Gateway	<input type="text" value="192.168.10.1"/>
Mask	<input type="text" value="255.255.255.0"/>
IP Address Section	Section: <input type="text" value="1"/>
	Start Address: <input type="text" value="192.168.10.10"/>
	End Address: <input type="text" value="192.168.10.100"/>
DNS Primary Server	<input type="checkbox"/> Enable <input type="text"/>
DNS Second Server	<input type="checkbox"/> Enable <input type="text"/>
Lease time	<input type="text" value="1"/> Day <input type="text" value="00"/> Hour <input type="text" value="00"/> Minute

Fig 9.2.2 Edit DHCP IP Pool setting page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
 - Property
 - IP Pool Setting**
 - VLAN IF Address Group Setting
 - Client List
 - Client Static Binding Table
- ▼ Multicast
- ▼ Routing

[Save](#) | [Logout](#) | [Reboot](#) | [Debug](#)

DHCP > IP Pool Setting

IP Pool Table

Showing entries

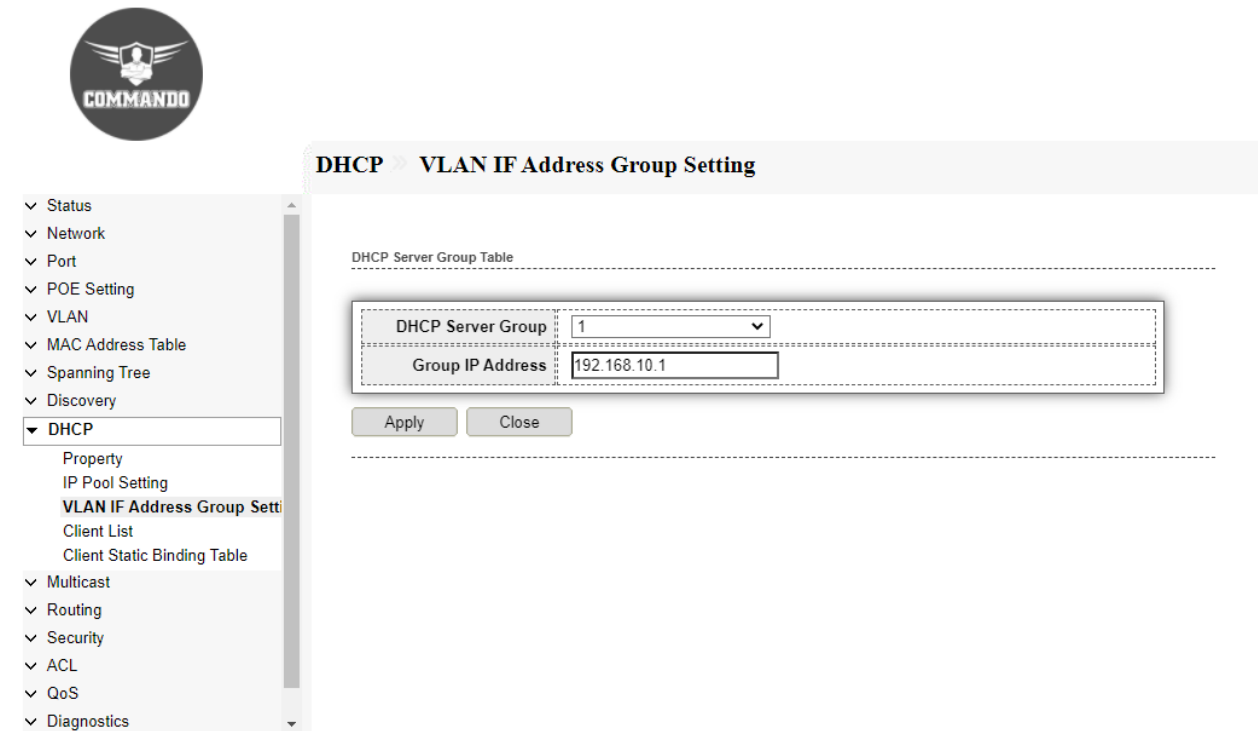
Showing 1 to 1 of 1 entries

	Pool	Section		Gateway	Mask	DNS Primary Server	DNS Second Server	Lease time		
		Section	Start Address							End Address
<input type="checkbox"/>	192.168.10.0	1	192.168.10.10	192.168.10.100	192.168.10.1	255.255.255.0	0.0.0.0	0.0.0.0	1:0:0	

Fig 9.2.3 DHCP IP Pool Table after setting page

9.3 VLAN IF Address Group Setting

VLAN interface can be bind with group IP address. To configure and view VLAN IF Address Group Setting, click **DHCP >> VLAN IF Address Group Setting**.



COMMANDO

DHCP > VLAN IF Address Group Setting

DHCP Server Group Table

DHCP Server Group	1
Group IP Address	192.168.10.1

Apply Close

Fig 9.3.1 DHCP VLAN Interface address pool and Server group table page.



DHCP » VLAN IF Address Group Setting

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ▼ **DHCP**
 - Property
 - IP Pool Setting
 - VLAN IF Address Group Setting**
 - Client List
 - Client Static Binding Table
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics

VLAN Interface Address Pool Table

Interface

DHCP Server Group

Apply

DHCP Server Group Table

	Group ID	Group IP Address	Bind VLAN Interface
<input type="radio"/>	1	192.168.10.1	---

Add

Edit

Delete

Fig 9.3.2 DHCP Binding VLAN Interface to DHCP server group IP address page.



- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ▼ DHCP
 - Property
 - IP Pool Setting
 - VLAN IF Address Group Setting**
 - Client List
 - Client Static Binding Table
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics

DHCP > VLAN IF Address Group Setting

VLAN Interface Address Pool Table

Interface:

DHCP Server Group:

DHCP Server Group Table

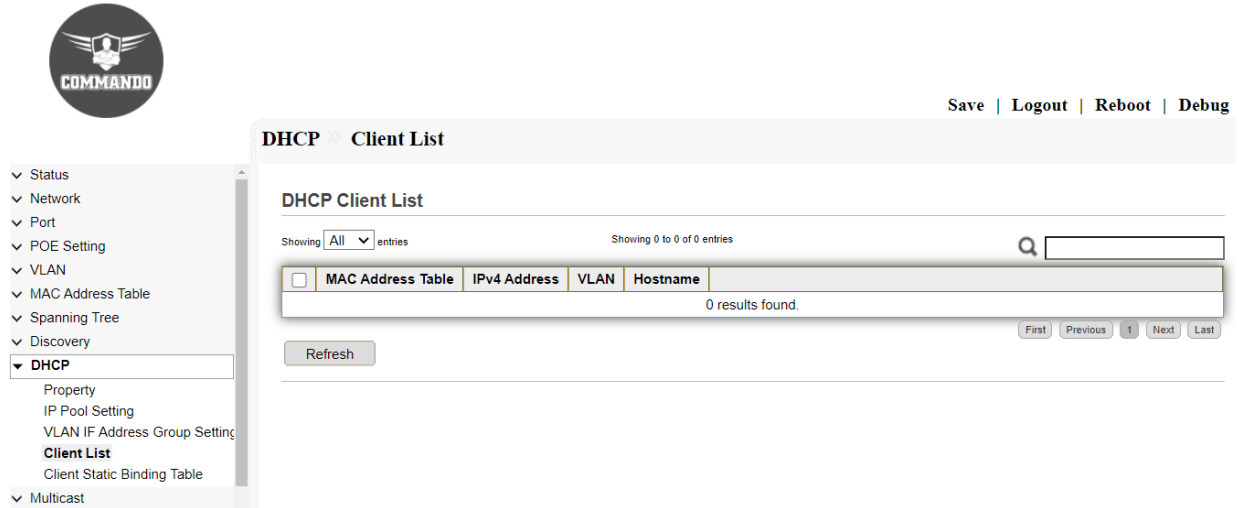
	Group ID	Group IP Address	Bind VLAN Interface
<input type="radio"/>	1	192.168.10.1	vlan 1

Fig 9.3.3 DHCP Binding VLAN Interface to DHCP server group

9.4 Client List

The DHCP Client Table allows you to check the devices that are connected to your network. After creating DHCP server group and binding with VLAN, the members of VLANs are automatically provide IP address. These assigned IP address to client can be seen with DHCP client List.

To view DHCP Client list, click **DHCP >> Client list**.



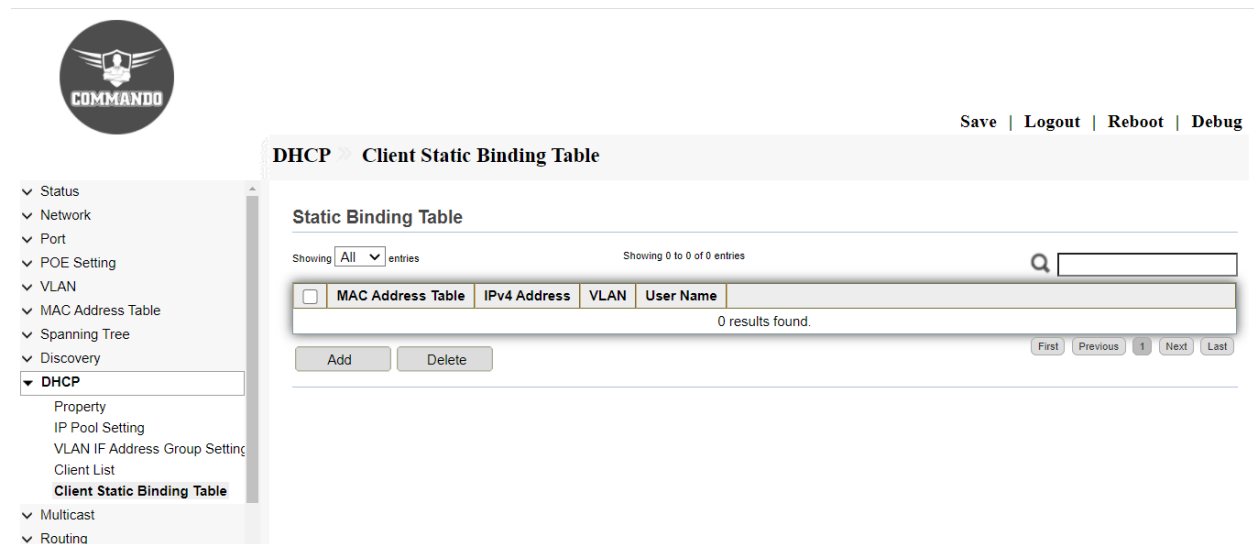
The screenshot shows the COMMANDO network management interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, and Multicast. The DHCP section is expanded, showing sub-items: Property, IP Pool Setting, VLAN IF Address Group Setting, Client List (highlighted), and Client Static Binding Table. The main content area is titled 'DHCP Client List' and includes a search bar, a table with columns for MAC Address Table, IPv4 Address, VLAN, and Hostname, and a 'Refresh' button. The table currently shows '0 results found.' At the top right of the interface are links for 'Save | Logout | Reboot | Debug'.

Fig 9.4.1 DHCP Client list page.

9.5 Client Static Binding Table

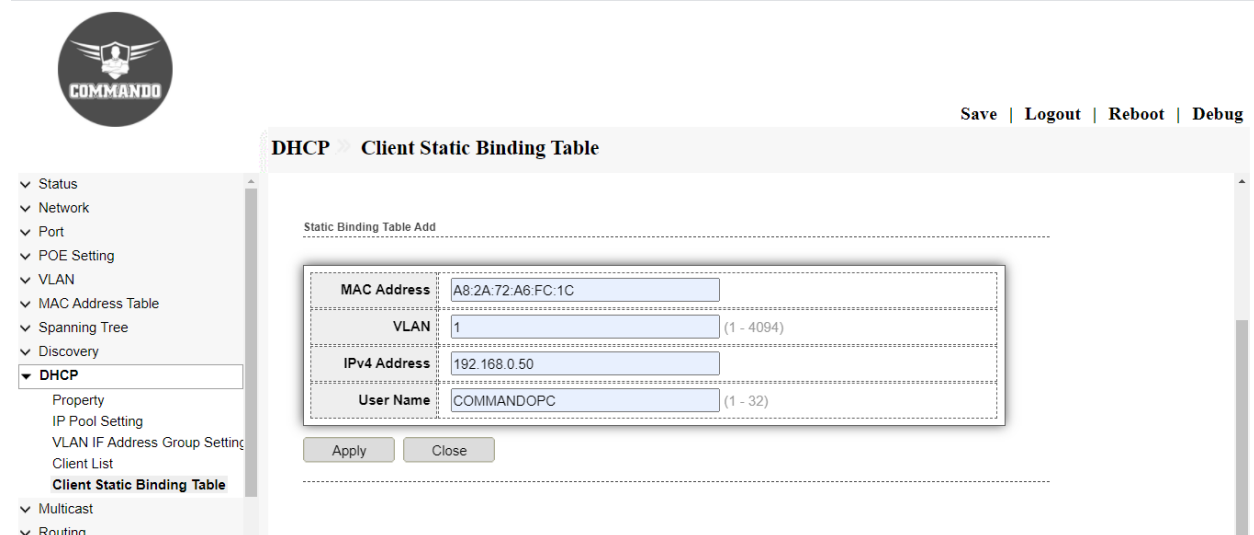
The DHCP static binding feature enables assignment of static IP addresses without creating numerous host pools with manual bindings with MAC addresses. A static binding is a mapping between a fixed IP address and the client's MAC address. Client can be bound with static IP address and by particular name also can be assigned to clients.

To configure and view DHCP Client Static Binding, click **DHCP >> Client Static Binding Table**.



The screenshot shows the Commando web interface for the DHCP Client Static Binding Table. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, and DHCP. The DHCP menu is expanded, showing sub-items like Property, IP Pool Setting, VLAN IF Address Group Setting, Client List, and Client Static Binding Table. The main content area is titled "DHCP Client Static Binding Table" and includes a "Static Binding Table" section. This section has a search bar, a table with columns for MAC Address Table, IPv4 Address, VLAN, and User Name, and a "0 results found" message. Below the table are "Add" and "Delete" buttons and pagination controls (First, Previous, 1, Next, Last). At the top right of the main area are links for "Save", "Logout", "Reboot", and "Debug".

Fig 9.5.1 Default DHCP Client Binding Table page.



The screenshot shows the Commando web interface for the DHCP Client Static Binding Table Add page. The navigation menu is the same as in the previous screenshot. The main content area is titled "DHCP Client Static Binding Table" and includes a "Static Binding Table Add" section. This section contains a form with the following fields: "MAC Address" (A8:2A:72:A6:FC:1C), "VLAN" (1, with a range of 1 - 4094), "IPv4 Address" (192.168.0.50), and "User Name" (COMMANDOPC, with a range of 1 - 32). Below the form are "Apply" and "Close" buttons. At the top right of the main area are links for "Save", "Logout", "Reboot", and "Debug".

Fig 9.5.2 DHCP Client add static binding page.



Save | Logout | Reboot | Debug

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ▼ **DHCP**
 - Property
 - IP Pool Setting
 - VLAN IF Address Group Setting
 - Client List
 - Client Static Binding Table**
- ✓ Multicast

DHCP Client Static Binding Table

Static Binding Table

Showing **All** entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	MAC Address Table	IPv4 Address	VLAN	User Name
<input type="checkbox"/>	A8:2A:72:A6:FC:1C	192.168.0.50	1	COMMANDOPC

1

Fig 9.5.3 DHCP Client Static Binding Table page.

Chapter 10 Multicast

General: Multicast is group communication where data transmission is addressed to a group of devices simultaneously. Multicast can be one-to-many or many-to-many distribution.

Property: Multicast packets are replicated in the network at the point where paths diverge. Multicast includes Internet Group Management Protocol, Protocol Independent Multicast and Multicast VLAN Registration.

Group Address: RFC 2365 provides limited guidelines on how the multicast address space can be divided and used privately by enterprises. The terminology “Administratively Scoped IPv4 multicast space” relates to the group address range of 239.0.0.0 to 239.255.255.255.

Router Port: A Multicast router (Mrouter) port is a port that connects to a Multicast router. The device includes the Multicast router port(s) numbers when it forwards the Multicast streams and IGMP/MLD registration messages.

Forward All: The Multicast Forward All page allows you to choose which interfaces receive multicast streams in which VLANs.

Throttling: This page displays the IGMP throttling configurations for all interfaces on the switch or for a specified interface.

Filtering Profile: A Multicast filter profile permits or denies a range of Multicast groups to be learned when the join group.

Filtering Binding: Multicast filtering to receive only messages to multicast addresses assigned to its own host at the link layer level. The filter is set when the host joins a multicast group.

IGMP Snooping: IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic to control delivery of IP multicast.

Property: Internet Group Management Protocol (IGMP) snooping allows the switch to forward multicast traffic intelligently. you can block even more multicast traffic and reduce your risk of a denial of service (DoS) attack, you can choose to block multicast traffic from unknown addresses.

Querier: The IGMP/MLD Snooping Querier is used to support a Layer 2 Multicast domain of snooping switches in the absence of a Multicast router.

Statistics: This page shows summary of IGMP statistics: Membership Query—Number of membership queries sent and received. Group Leave—Number of groups leave messages sent or received. Mtrace Response—Number of Mtrace response messages sent or received.

MLD Snooping: Multicast Listener Discovery (MLD) snooping constrains the flooding of IPv6 multicast traffic on VLANs.

Property: MLD snooping runs on a Layer 2 device as an IPv6 multicast constraining mechanism to improve multicast forwarding efficiency. It creates Layer 2 multicast forwarding entries from MLD messages that are exchanged.

Statistics: Display information about MLD snooping statistics.

MVR: Multicast VLAN Registration (MVR) is designed for distribution of multicast traffic on a dedicated multicast VLAN across segregated access networks, while allowing subscribers who are on different VLANs to join and leave the multicast groups carried in the Multicast VLAN. Multicast VLAN registration (MVR) enables more efficient distribution of IPTV multicast streams across an Ethernet ring-based Layer 2 network.

Property: When you configure MVR, you create a multicast VLAN (MVLAN) that becomes the only VLAN over which IPTV multicast traffic flows throughout the Layer 2 network. Devices with MVR enabled selectively forward IPTV multicast traffic from interfaces on the MVLAN (source interfaces) to hosts that are connected to interfaces that are not part of the MVLAN that you designate as MVR receiver ports.

Port Setting: MVR Port Setting, Port configuration, status, statistics, mirroring, security. MVR Function can provide different VLAN users to receive MVR Mode VLAN.

Group Address: MVR is not enabled by default on devices that support MVR. You explicitly configure an MVLAN and assign a range of multicast group addresses to it. That VLAN carries MVLAN traffic for the configured multicast groups. You then configure other VLANs to be MVR receiver VLANs that receive multicast streams from the MVLAN.

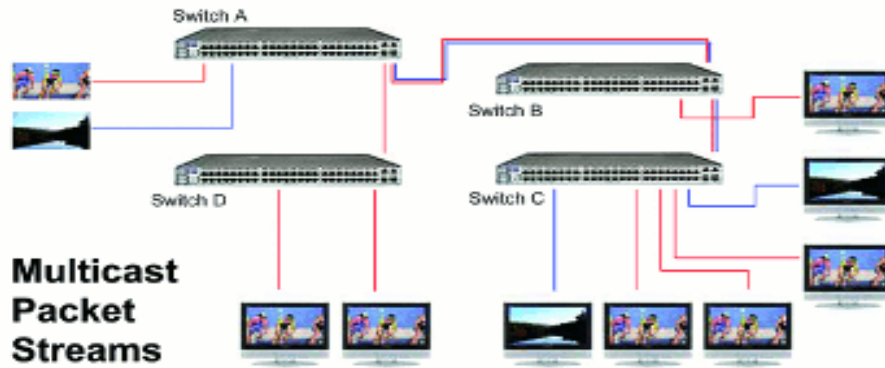


Fig 10.1.1 Multicast Packet Streams page

10.1 General

In computer networking, multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution.

10.1.1 Property

The Properties page enables you to configure the Bridge Multicast filtering status. By default, all Multicast frames are flooded to all ports of the VLAN. To selectively forward only to relevant ports and filter (drop) the Multicast on the rest of the ports, enable Bridge Multicast filtering status in the Properties page. If filtering is enabled, Multicast frames are forwarded to a subset of the ports in the relevant VLAN as defined in the Multicast Forwarding Data Base. Multicast filtering is enforced on all traffic. By default, such traffic is flooded to all relevant ports, but you can limit forwarding to a smaller subset. To view and configure multicast general property, click **Multicast >> General >> Property**.

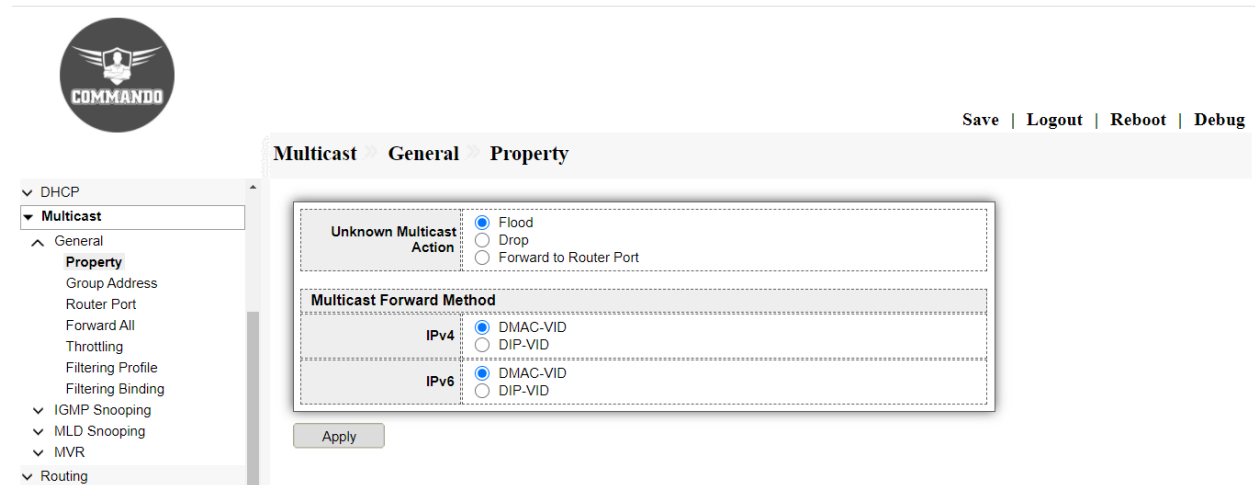
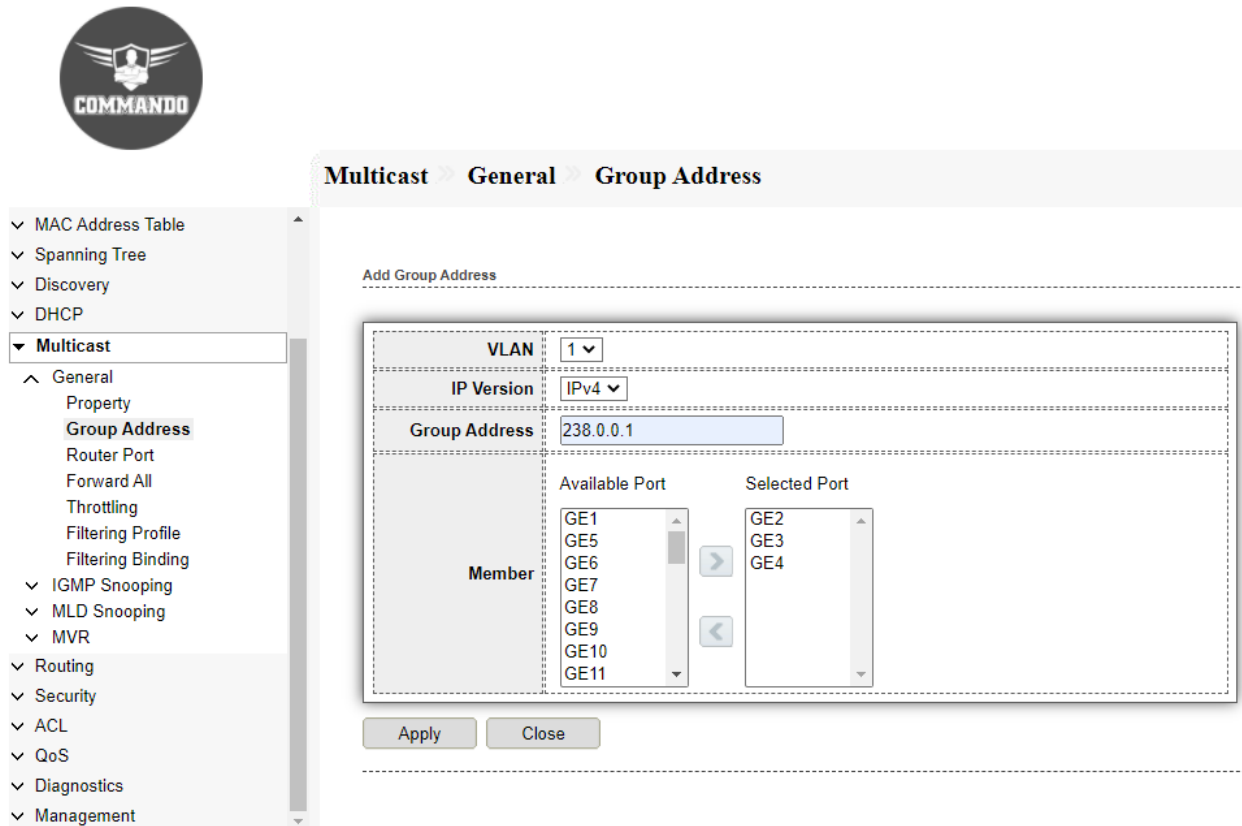


Fig 10.1.1 Multicast general property page

10.1.2 Group Address

IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It is the IP-specific form of multicast and is used for streaming media and other network applications. Full range of multicast addresses is from 224.0.0.0 to 239.255.255.255. Since multicast addresses represent a group of IP devices. This page allow user to browse all multicast groups that dynamic learned or statically added.

To view and configure Multicast General Group, click **Multicast >> General >> Group Address**.



The screenshot displays the COMMANDO network management interface. On the left is a navigation tree with the following items: MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast (expanded), General, Property, Group Address (highlighted), Router Port, Forward All, Throttling, Filtering Profile, Filtering Binding, IGMP Snooping, MLD Snooping, MVR, Routing, Security, ACL, QoS, Diagnostics, and Management. The main content area is titled "Multicast > General > Group Address" and contains a configuration form for "Add Group Address".

The configuration form includes the following fields and sections:

- VLAN:** A dropdown menu set to "1".
- IP Version:** A dropdown menu set to "IPv4".
- Group Address:** A text input field containing "238.0.0.1".
- Member:** A section with two columns: "Available Port" and "Selected Port".
 - Available Port:** A list box containing GE1, GE5, GE6, GE7, GE8, GE9, GE10, and GE11.
 - Selected Port:** A list box containing GE2, GE3, and GE4.
 - Navigation arrows (right and left) are positioned between the two list boxes.

At the bottom of the form are two buttons: "Apply" and "Close".

Fig 10.1.2 Multicast default group address table page



Multicast >> **General** >> **Group Address**

Group Address Table

IP Version

Showing entries Showing 1 to 1 of 1 entries

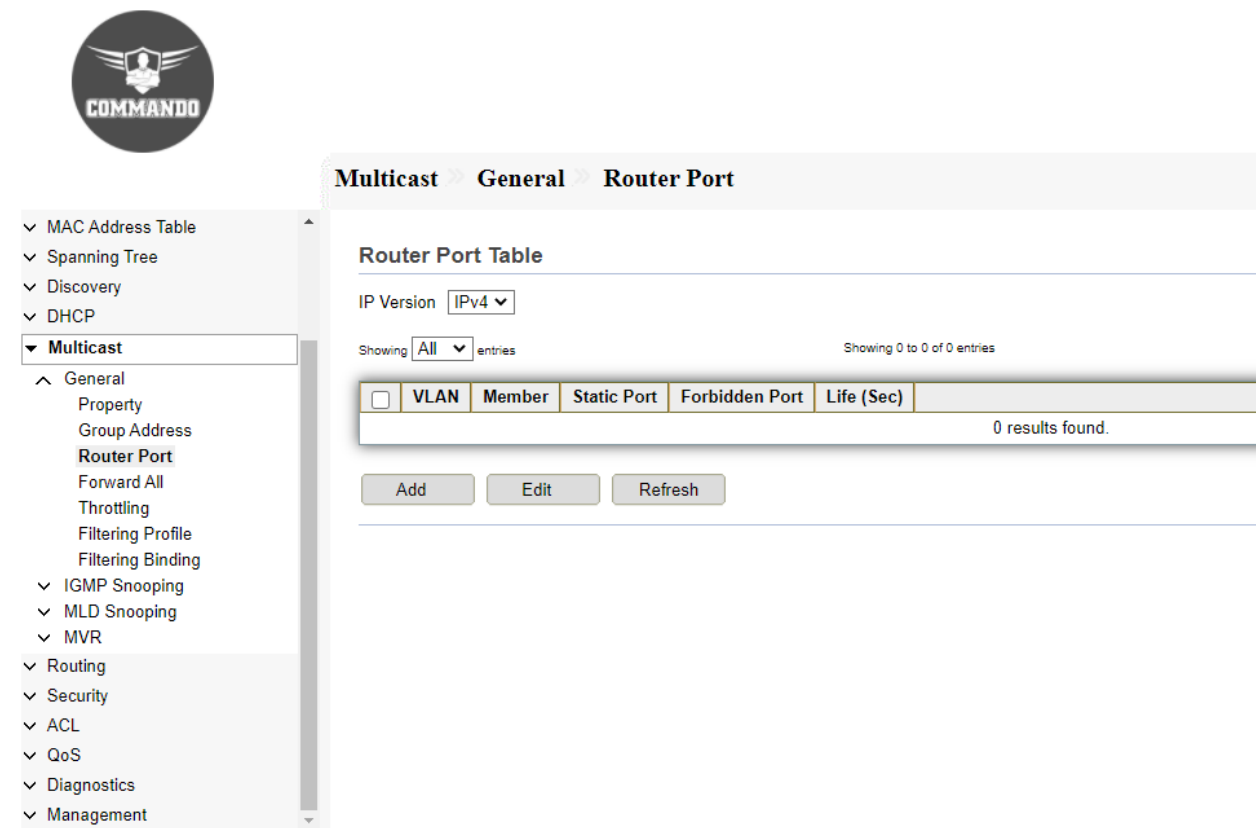
<input type="checkbox"/>	VLAN	Group Address	Member	Type	Life (Sec)	
<input type="checkbox"/>	1	238.0.0.1	GE2-GE5	Static		

Fig 10.1.3 Multicast group address table page

10.1.3 Router Port

A Multicast router (Mrouter) port is a port that connects to a Multicast router. The device includes the Multicast router port(s) numbers when it forwards the Multicast streams and IGMP/MLD registration messages. Router port is a port on snooping switch that is connecting to the IGMP querier. This page allow user to browse all router port information. The static and forbidden router port can set by user.

To configure and view multicast router port table web page, click **Multicast >> General >> Router Port**.



The screenshot shows a web interface for configuring Multicast Router Ports. On the left is a navigation menu with a 'COMMANDO' logo at the top. The menu items include: MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast (expanded), General (expanded), Property, Group Address, Router Port (highlighted), Forward All, Throttling, Filtering Profile, Filtering Binding, IGMP Snooping, MLD Snooping, MVR, Routing, Security, ACL, QoS, Diagnostics, and Management. The main content area is titled 'Multicast > General > Router Port' and contains a 'Router Port Table' section. This section includes an 'IP Version' dropdown set to 'IPv4', a 'Showing All entries' indicator, and a table with columns: , VLAN, Member, Static Port, Forbidden Port, Life (Sec), and a summary row showing '0 results found.'. Below the table are 'Add', 'Edit', and 'Refresh' buttons.

Fig 10.1.5 Multicast default router port table page



Multicast > General > Router Port

- ∨ Status
- ∨ Network
- ∨ Port
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ **Multicast**
 - ∧ General
 - Property
 - Group Address
 - Router Port**
 - Forward All
 - Throttling
 - Filtering Profile
 - Filtering Binding
 - ∨ IGMP Snooping
 - ∨ MLD Snooping
 - ∨ MVR
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ QoS
- ∨ Diagnostics
- ∨ Management

Add Router Port

VLAN	Available VLAN	>	<	Selected VLAN
	<div style="border: 1px solid gray; height: 40px;"></div>			<div style="border: 1px solid gray; height: 40px; text-align: center;">1</div>
IP Version IPv4 ▾				
Type <input checked="" type="radio"/> Static <input type="radio"/> Forbidden				
Port	Available Port	>	<	Selected Port
	<div style="border: 1px solid gray; padding: 2px;">GE1 GE3 GE4 GE5 GE6 GE7 GE8 GE9</div>			<div style="border: 1px solid gray; padding: 2px; text-align: center;">GE2</div>

Apply Close

Fig 10.1.6 Multicast router port selection page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ **Multicast**
 - ^ General
 - Property
 - Group Address
 - Router Port**
 - Forward All
 - Throttling
 - Filtering Profile
 - Filtering Binding
 - ▼ IGMP Snooping
 - ▼ MLD Snooping
 - ▼ MVR
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Multicast ▸ General ▸ Router Port

Router Port Table

IP Version

Showing entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	VLAN	Member	Static Port	Forbidden Port	Life (Sec)
<input type="checkbox"/>	1	GE2	GE2		

Fig 10.1.7 Multicast router port table by selecting GE5 and GE7 port page

10.1.4 Forward All

The Multicast Forward All page allows you to choose which interfaces receive multicast streams in which VLANs.

To view and configure multicast Forward All web page, click **Multicast >> General >> Forward All**.

The screenshot shows the COMMANDO web interface. On the left is a navigation tree with categories: DHCP, Multicast (expanded), General, Forward All (expanded), Throttling, Filtering Profile, Filtering Binding, IGMP Snooping, MLD Snooping, MVR, Routing, and Security. The main content area is titled 'Multicast > General > Forward All' and includes a 'Save | Logout | Reboot | Debug' menu. Below the breadcrumb is the 'Forward All Table' section. It features an 'IP Version' dropdown set to 'IPv4', a 'Showing All entries' indicator, and a search box. A table with columns 'VLAN', 'Static Port', and 'Forbidden Port' is displayed, showing '0 results found.' Below the table are 'Add', 'Edit', and 'Delete' buttons, and a pagination control with 'First', 'Previous', '1', 'Next', and 'Last' buttons.

Fig 10.1.8 Multicast default forward all table page



- √ Status
- √ Network
- √ Port
- √ POE Setting
- √ VLAN
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- ▼ **Multicast**
 - ^ General
 - Property
 - Group Address
 - Router Port
 - Forward All**
 - Throttling
 - Filtering Profile
 - Filtering Binding
 - √ IGMP Snooping
 - √ MLD Snooping
 - √ MVR
- √ Routing
- √ Security
- √ ACL
- √ QoS
- √ Diagnostics
- √ Management

Multicast > **General** > **Forward All**

Add Forward All

VLAN	Available VLAN	Selected VLAN
	<input type="text"/>	<input type="text" value="1"/>
IP Version	IPv4	
Type	<input checked="" type="radio"/> Static <input type="radio"/> Forbidden	
Port	Available Port	Selected Port
	<input type="text" value="GE1"/> GE3 GE4 GE5 GE6 GE7 GE8 GE9	<input type="text" value="GE2"/>

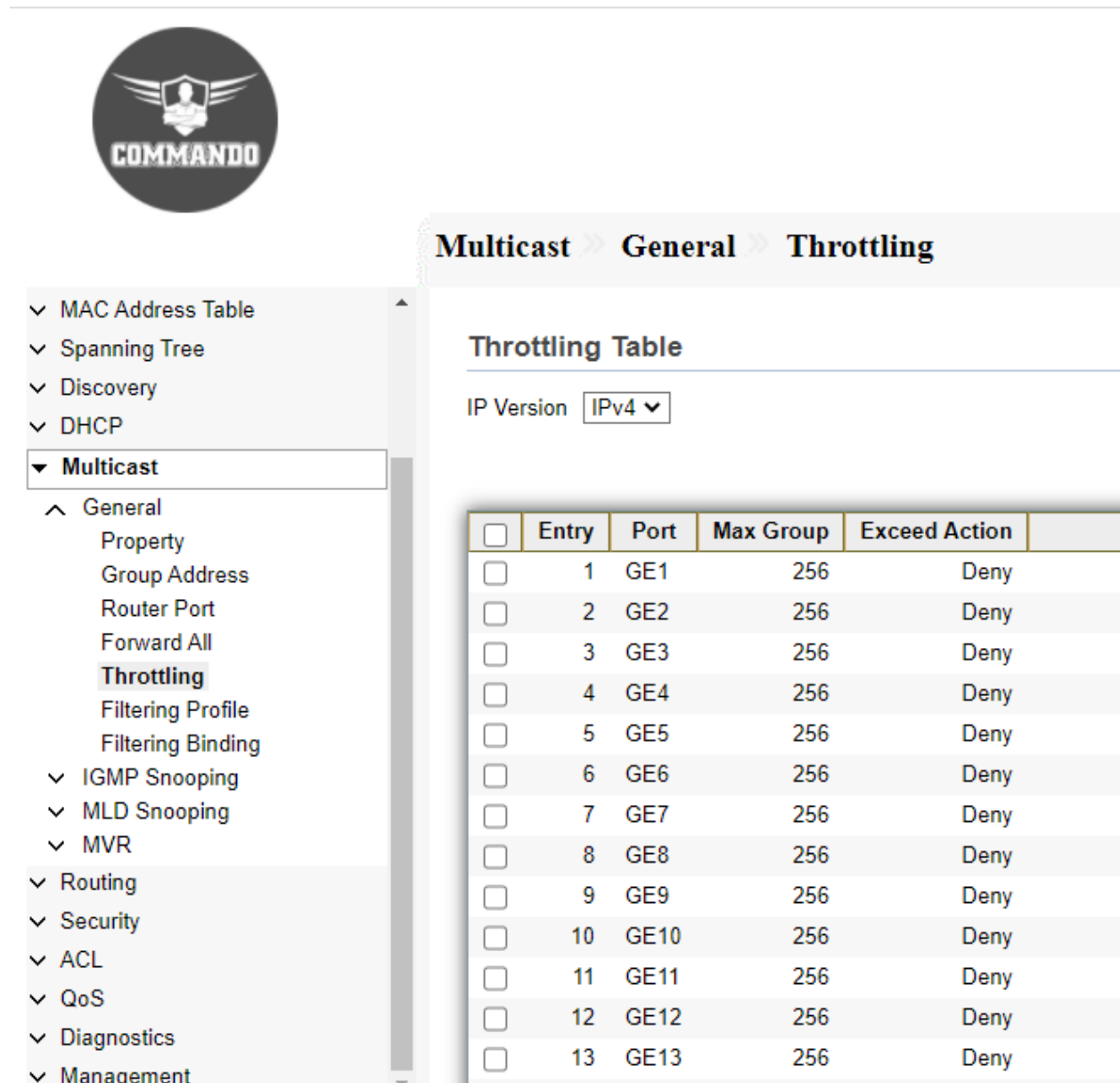
Apply Close

Fig 10.1.9 Multicast default forward all table page

10.1.5 Throttling

With the throttling feature, you can set the maximum number of groups that a Layer 2 interface can join. This page allow user to configure port can learned max group number and if port group number arrived max group number action

To view and configure multicast max-group number and action, click **Multicast >> General >> Throttling**.



The screenshot displays the COMMANDO network management interface. On the left is a navigation menu with the following items: MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast (expanded), General, Property, Group Address, Router Port, Forward All, Throttling (highlighted), Filtering Profile, Filtering Binding, IGMP Snooping, MLD Snooping, MVR, Routing, Security, ACL, QoS, Diagnostics, and Management. The main content area is titled "Multicast >> General >> Throttling" and contains a "Throttling Table" section. Below the title, there is a dropdown menu for "IP Version" set to "IPv4". The table lists 13 entries, each with a checkbox, an entry number, a port name (GE1-GE13), a maximum group number (256), and an exceed action (Deny).

<input type="checkbox"/>	Entry	Port	Max Group	Exceed Action
<input type="checkbox"/>	1	GE1	256	Deny
<input type="checkbox"/>	2	GE2	256	Deny
<input type="checkbox"/>	3	GE3	256	Deny
<input type="checkbox"/>	4	GE4	256	Deny
<input type="checkbox"/>	5	GE5	256	Deny
<input type="checkbox"/>	6	GE6	256	Deny
<input type="checkbox"/>	7	GE7	256	Deny
<input type="checkbox"/>	8	GE8	256	Deny
<input type="checkbox"/>	9	GE9	256	Deny
<input type="checkbox"/>	10	GE10	256	Deny
<input type="checkbox"/>	11	GE11	256	Deny
<input type="checkbox"/>	12	GE12	256	Deny
<input type="checkbox"/>	13	GE13	256	Deny

Fig 10.1.10 Multicast Default throttling table page



Multicast >> General >> Throttling

Throttling Table

IP Version

<input type="checkbox"/>	Entry	Port	Max Group	Exceed Action
<input type="checkbox"/>	1	GE1	256	Deny
<input type="checkbox"/>	2	GE2	256	Deny
<input type="checkbox"/>	3	GE3	256	Deny
<input checked="" type="checkbox"/>	4	GE4	256	Deny
<input checked="" type="checkbox"/>	5	GE5	256	Deny
<input type="checkbox"/>	6	GE6	256	Deny
<input type="checkbox"/>	7	GE7	256	Deny
<input type="checkbox"/>	8	GE8	256	Deny
<input type="checkbox"/>	9	GE9	256	Deny
<input type="checkbox"/>	10	GE10	256	Deny
<input type="checkbox"/>	11	GE11	256	Deny
<input type="checkbox"/>	12	GE12	256	Deny
<input type="checkbox"/>	13	GE13	256	Deny

Navigation menu (left):

- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast**
 - General
 - Property
 - Group Address
 - Router Port
 - Forward All
 - Throttling**
 - Filtering Profile
 - Filtering Binding
 - IGMP Snooping
 - MLD Snooping
 - MVR
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management

Fig 10.1.11 Multicast Selecting port for throttling page



Save |

Multicast » General » Throttling

- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ▼ **Multicast**
 - ^ General
 - Property
 - Group Address
 - Router Port
 - Forward All
 - Throttling**
 - Filtering Profile
 - Filtering Binding
- ✓ IGMP Snooping
- ✓ MLD Snooping
- ✓ MVR

Edit Throttling

Port	GE2-GE3
IP Version	IPv4
Max Group	<input type="text" value="256"/> (0 - 256)
Exceed Action	<input type="radio"/> Deny <input checked="" type="radio"/> Replace

Fig 10.1.12 Edit Multicast throttling page



Multicast >> General >> Throttling

- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ▼ **Multicast**
 - ^ General
 - Property
 - Group Address
 - Router Port
 - Forward All
 - Throttling**
 - Filtering Profile
 - Filtering Binding
 - ✓ IGMP Snooping
 - ✓ MLD Snooping
 - ✓ MVR
- ✓ Routing
- ✓ Security
- ✓ ACL

Throttling Table

IP Version


<input type="checkbox"/>	Entry	Port	Max Group	Exceed Action
<input type="checkbox"/>	1	GE1	256	Deny
<input type="checkbox"/>	2	GE2	256	Replace
<input type="checkbox"/>	3	GE3	256	Replace
<input type="checkbox"/>	4	GE4	256	Deny
<input type="checkbox"/>	5	GE5	256	Deny
<input type="checkbox"/>	6	GE6	256	Deny
<input type="checkbox"/>	7	GE7	256	Deny
<input type="checkbox"/>	8	GE8	256	Deny
<input type="checkbox"/>	9	GE9	256	Deny
<input type="checkbox"/>	10	GE10	256	Deny
<input type="checkbox"/>	-

Fig 10.1.13 Multicast throttling Table page

10.1.6 Filtering Profile

Multicast Filtering allows you to control the set of multicast groups to which a host can belong. You can filter multicast joins on a per-port basis by configuring IP multicast profiles (IGMP profiles or MLD profiles) and associating them with individual switch ports. This page allow user to add, edit or delete profile for IGMP or MLD snooping.

To view and configure Multicast Profile, click **Multicast >> General >> Filtering Profile**.



Multicast > General > Filtering Profile

Filtering Profile Table

IP Version

Showing entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Profile ID	Start Address	End Address	Action	
0 results found.					

- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast**
 - General
 - Property
 - Group Address
 - Router Port
 - Forward All
 - Throttling
 - Filtering Profile**
 - Filtering Binding
 - IGMP Snooping
 - MLD Snooping
 - MVR
- Routing
- Security
- ACL

Fig 10.1.13 Multicast default filtering profile table page



Save |

Multicast > General > Filtering Profile

Add Profile

Profile ID	<input type="text" value="1"/> (1 - 128)
IP Version	<input type="text" value="IPv4"/>
Start Address	<input type="text" value="239.0.0.10"/>
End Address	<input type="text" value="239.0.0.100"/>
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

Fig 10.1.14 Multicast Add filtering profile page



Multicast > General > Filtering Profile

Filtering Profile Table

IP Version

Showing entries Showing 1 to 1 of 1 entries

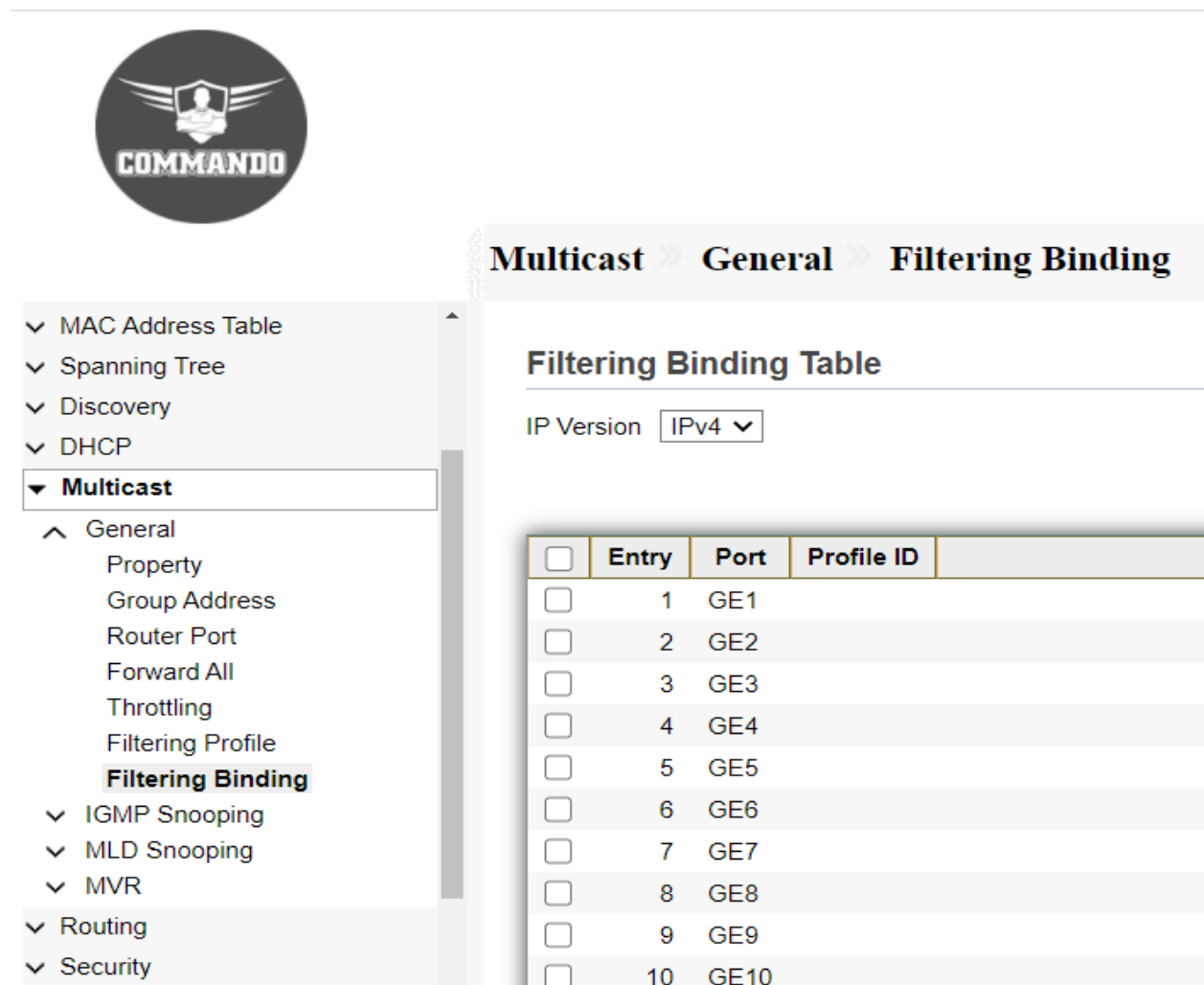
<input type="checkbox"/>	Profile ID	Start Address	End Address	Action
<input type="checkbox"/>	1	239.0.0.10	239.0.0.100	Allow

Fig 10.1.15 Multicast filtering profile table page

10.1.7 Filtering Binding

With the functions for managing multicast groups, the switch can only allow specific member ports to join specific multicast groups or disallow specific member ports to join specific multicast groups. You can achieve this filtering function by creating a profile and binding it to the corresponding member port. You can bind the created IGMP profile or MLD profile to ports and configure the number of multicast groups a port can join and the overflow action. This page allow user to bind/remove profile for each port.

To view and configure Multicast port filter binding profile, click **Multicast >> General >> Filtering Binding**.



The screenshot displays the COMMANDO network management interface. At the top left is the COMMANDO logo. The navigation menu on the left includes: MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast (expanded), General (expanded), Property, Group Address, Router Port, Forward All, Throttling, Filtering Profile, Filtering Binding (highlighted), IGMP Snooping, MLD Snooping, MVR, Routing, and Security. The main content area shows the breadcrumb path: **Multicast >> General >> Filtering Binding**. Below this is the **Filtering Binding Table** with an IP Version dropdown set to IPv4. The table lists 10 entries, each with a checkbox, an Entry number, a Port name, and a Profile ID column.

<input type="checkbox"/>	Entry	Port	Profile ID
<input type="checkbox"/>	1	GE1	
<input type="checkbox"/>	2	GE2	
<input type="checkbox"/>	3	GE3	
<input type="checkbox"/>	4	GE4	
<input type="checkbox"/>	5	GE5	
<input type="checkbox"/>	6	GE6	
<input type="checkbox"/>	7	GE7	
<input type="checkbox"/>	8	GE8	
<input type="checkbox"/>	9	GE9	
<input type="checkbox"/>	10	GE10	

Fig 10.1.16 Multicast default filtering binding table page



- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast**
 - General
 - Property
 - Group Address
 - Router Port
 - Forward All
 - Throttling
 - Filtering Profile
 - Filtering Binding**
 - IGMP Snooping
 - MLD Snooping
 - MVR
- Routing

Multicast >> General >> Filtering Binding

Filtering Binding Table

IP Version

<input type="checkbox"/>	Entry	Port	Profile ID
<input type="checkbox"/>	1	GE1	
<input checked="" type="checkbox"/>	2	GE2	
<input checked="" type="checkbox"/>	3	GE3	
<input type="checkbox"/>	4	GE4	
<input type="checkbox"/>	5	GE5	
<input type="checkbox"/>	6	GE6	
<input type="checkbox"/>	7	GE7	
<input type="checkbox"/>	8	GE8	
<input type="checkbox"/>	9	GE9	

Fig 10.1.17 Multicast filtering Binding Port selection page



- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast**
 - General
 - Property
 - Group Address
 - Router Port
 - Forward All
 - Throttling
 - Filtering Profile
 - Filtering Binding**
 - IGMP Snooping
 - MLD Snooping

Save | Logout |

Multicast >> General >> Filtering Binding

Edit Filtering Binding

Port	GE2-GE3
IP Version	IPv4
Profile ID	<input checked="" type="checkbox"/> Enable
	<input type="text" value="1"/>

Fig 10.1.18 Multicast Edit filtering Binding page

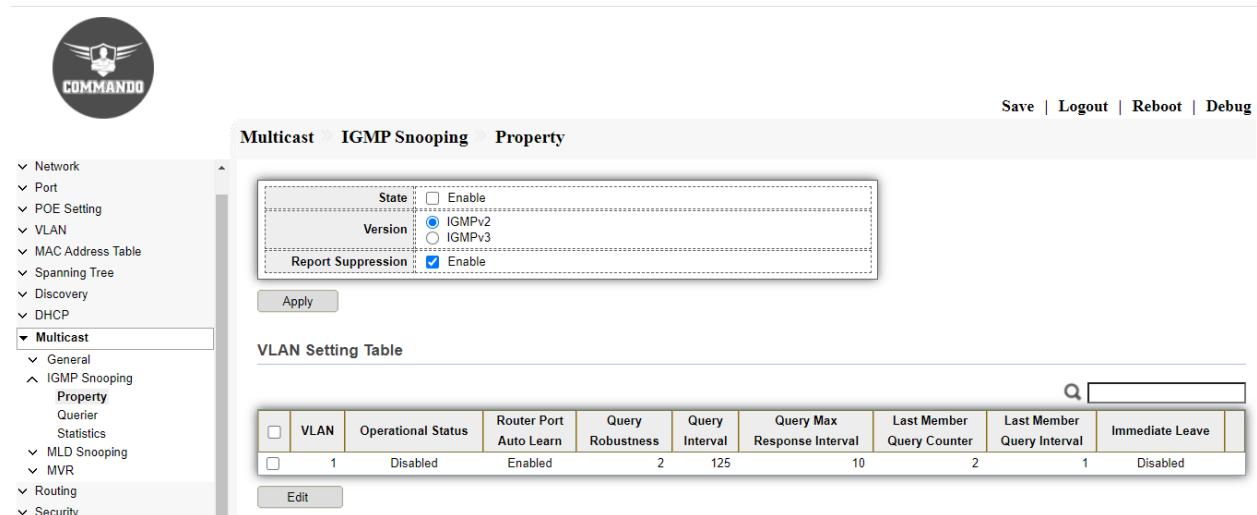
10.2 IGMP Snooping

IGMP Snooping transmits data on demand on data link layer by analyzing IGMP packets between the IGMP querier and the users, to build and maintain Layer 2 multicast forwarding table. This page shows configuration about IGMP Snooping. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast stream.

10.2.1 Property

This page allow user to configure global settings of IGMP snooping and configure specific VLAN settings of IGMP Snooping.

To view and configure IGMP Snooping global setting and VLAN Setting, click **Multicast >> IGMP Snooping >> Property**.



The screenshot displays the COMMANDO network management interface. The breadcrumb trail indicates the current page is **Multicast > IGMP Snooping > Property**. The configuration form includes the following settings:

- State:** Enable
- Version:** IGMPv2, IGMPv3
- Report Suppression:** Enable

An **Apply** button is located below the configuration form.

The **VLAN Setting Table** is shown below the configuration form. It includes a search bar and an **Edit** button. The table contains the following data:

<input type="checkbox"/>	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
<input type="checkbox"/>	1	Disabled	Enabled	2	125	10	2	1	Disabled

Fig 10.2.1 Default IGMP snooping property page



- network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast**
- General
- IGMP Snooping
 - Property**
 - Querier
 - Statistics
- MLD Snooping
- MVR
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management

Multicast **IGMP Snooping** Property

State	<input checked="" type="checkbox"/> Enable
Version	<input checked="" type="radio"/> IGMPv2 <input type="radio"/> IGMPv3
Report Suppression	<input checked="" type="checkbox"/> Enable

Apply

VLAN Setting Table

<input type="checkbox"/>	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
<input type="checkbox"/>	1	Disabled	Enabled	2	125	10	2	1	Disabled

Edit

Fig 10.2.2 IGMP snooping property VLAN setting page



Multicast > IGMP Snooping > Property

- √ Status
- √ Network
- √ Port
- √ POE Setting
- √ VLAN
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- ▼ **Multicast**
- √ General
- ^ IGMP Snooping
- Property**
- Querier
- Statistics
- √ MLD Snooping
- √ MVR
- √ Routing
- √ Security
- √ ACL
- √ QoS
- √ Diagnostics
- √ Management

Edit VLAN Setting

VLAN	1
State	<input type="checkbox"/> Enable
Router Port Auto Learn	<input checked="" type="checkbox"/> Enable
Immediate leave	<input type="checkbox"/> Enable
Query Robustness	<input type="text" value="2"/> (1 - 7, default 2)
Query Interval	<input type="text" value="125"/> Sec (30 - 18000, default 125)
Query Max Response Interval	<input type="text" value="10"/> Sec (5 - 20, default 10)
Last Member Query Counter	<input type="text" value="2"/> (1 - 7, default 2)
Last Member Query Interval	<input type="text" value="1"/> Sec (1 - 25, default 1)
Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

Apply

Close

Fig 10.2.3 IGMP snooping Edit VLAN setting page



Save | Logout |

- √ Status
- √ Network
- √ Port
- √ POE Setting
- √ VLAN
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- √ **Multicast**
 - √ General
 - √ IGMP Snooping
 - √ **Property**
 - √ Querier
 - √ Statistics
 - √ MLD Snooping
 - √ MVR
- √ Routing
- √ Security
- √ ACL
- √ QoS
- √ Diagnostics

Multicast > IGMP Snooping Property

State	<input checked="" type="checkbox"/> Enable
Version	<input checked="" type="radio"/> IGMPv2 <input type="radio"/> IGMPv3
Report Suppression	<input checked="" type="checkbox"/> Enable

Apply

VLAN Setting Table

<input type="checkbox"/>	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
<input type="checkbox"/>	1	Enabled	Enabled	2	125	10	2	1	Enabled

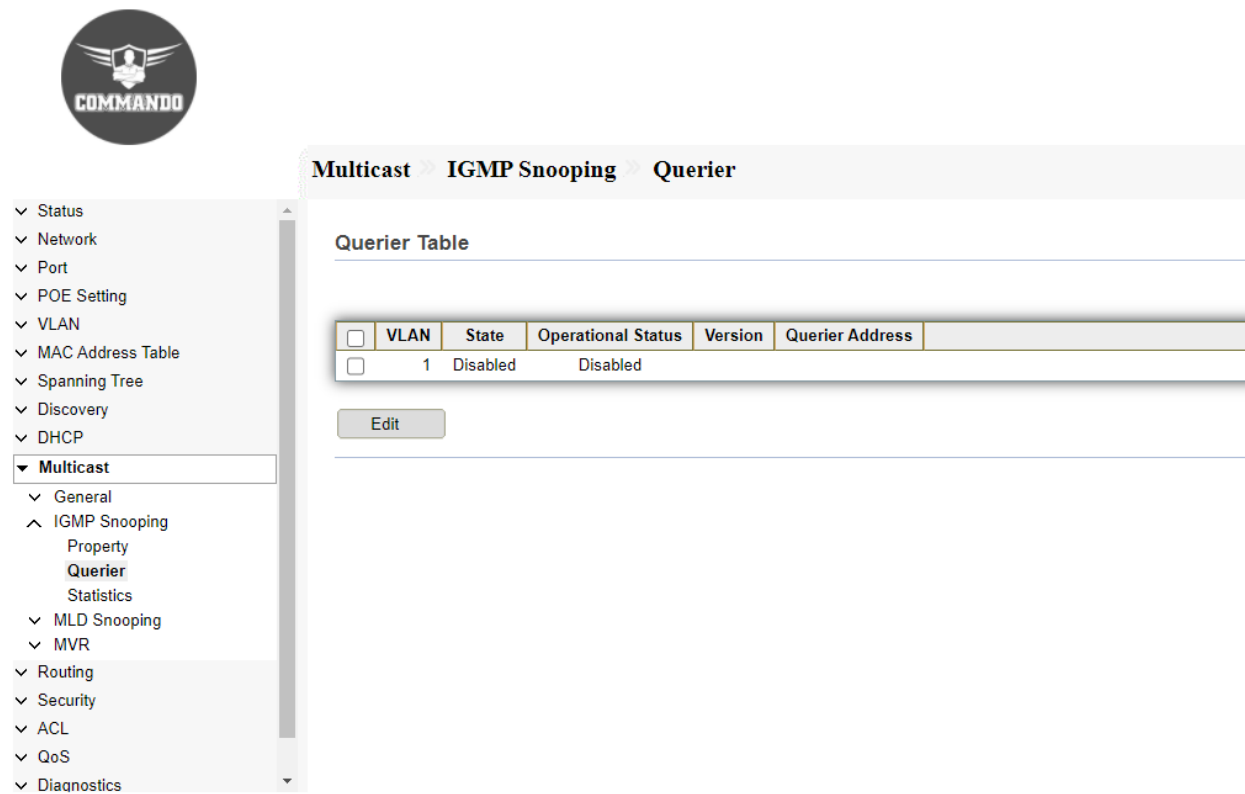
Edit

Fig 10.2.4 IGMP snooping property page

10.2.2 Querier

IGMP Snooping Querier periodically sends a general query on the network to solicit membership information and sends group-specific queries when it receives leave messages from hosts. This page allow user to configure querier settings on specific VLAN of IGMP Snooping.

To view and configure IGMP Snooping Querier Setting web page, click **Multicast >> IGMP Snooping >> Querier**.



The screenshot displays the Commando network management interface. On the left is a navigation sidebar with a tree view. The 'Multicast' section is expanded, showing sub-items: General, IGMP Snooping (with 'Property' and 'Querier' sub-items), MLD Snooping, and MVR. The 'Querier' item is selected. The main content area has a breadcrumb trail: Multicast > IGMP Snooping > Querier. Below the breadcrumb is the title 'Querier Table'. A table with the following structure is shown:

<input type="checkbox"/>	VLAN	State	Operational Status	Version	Querier Address
<input type="checkbox"/>	1	Disabled	Disabled		

Below the table is an 'Edit' button.

Fig 10.2.5 Default IGMP snooping Querier table page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ **Multicast**
- ▼ General
- ▲ IGMP Snooping
 - Property
 - Querier**
 - Statistics
- ▼ MLD Snooping
- ▼ MVR
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics

Multicast > IGMP Snooping > Querier

Edit Querier

VLAN	1
State	<input checked="" type="checkbox"/> Enable
Version	<input checked="" type="radio"/> IGMPv2 <input type="radio"/> IGMPv3

Apply Close

Fig 10.2.6 IGMP snooping Selecting VLAN Querier page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ **Multicast**
- ▼ General
- ▲ IGMP Snooping
 - Property
 - Querier**
 - Statistics
- ▼ MLD Snooping
- ▼ MVR
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics

Multicast > IGMP Snooping > Querier

Querier Table

<input type="checkbox"/>	VLAN	State	Operational Status	Version	Querier Address
<input type="checkbox"/>	1	Enabled	Enabled	IGMPv2	192.168.0.1

Edit

Fig 10.2.7 IGMP snooping Querier page

10.2.3 Statistics

IGMP statistics of receive and transmit packets. IGMP global statistics provides membership reports, membership queries transmitted and received, and unknown messages.

To view IGMP Snooping Statistics, click **Multicast >> IGMP Snooping >> Statistics**.

COMMANDO

Multicast >> IGMP Snooping >> Statistics

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ **Multicast**
 - ▼ General
 - ▲ IGMP Snooping
 - Property
 - Querier
 - Statistics**
 - ▼ MLD Snooping
 - ▼ MVR
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Receive Packet		
Total	:	2
Valid	:	2
InValid	:	0
Other	:	0
Leave	:	0
Report	:	2
General Query	:	0
Special Group Query	:	0
Source-specific Group Query	:	0

Transmit Packet		
Leave	:	0
Report	:	0
General Query	:	2
Special Group Query	:	0
Source-specific Group Query	:	0

Clear Refresh

Fig 10.2.9 IGMP snooping statistics page

10.3 MLD Snooping

Multicast Listener Discovery (MLD) snooping constrains the flooding of IPv6 multicast traffic on VLANs. MLD snooping performs the same function as IGMP snooping with the only difference being that MLD snooping is for IPv6 and IGMP snooping for IPv4 environments. This page shows configuration of ipv6 MLD snooping to enable MLD snooping function. Disable will clear all ipv6 MLD snooping dynamic group and dynamic router port and make the static ipv6 MLD group invalid. No more dynamic group and router port by MLD message will be learned.

The COMMANDO E3000 series switch supports two versions of MLD snooping:

MLDv1 snooping detects MLDv1 control packets and sets up traffic bridging based on IPv6 destination Multicast addresses.

MLDv2 uses control packets to forward traffic based on source IPv6 address and destination IPv6 Multicast address.

10.3.1 Property

This page allow user to configure global settings of MLD snooping and configure specific VLAN settings of MLD Snooping.

To view and configure MLD Snooping global setting, click **Multicast >> MLD Snooping >> Property**.

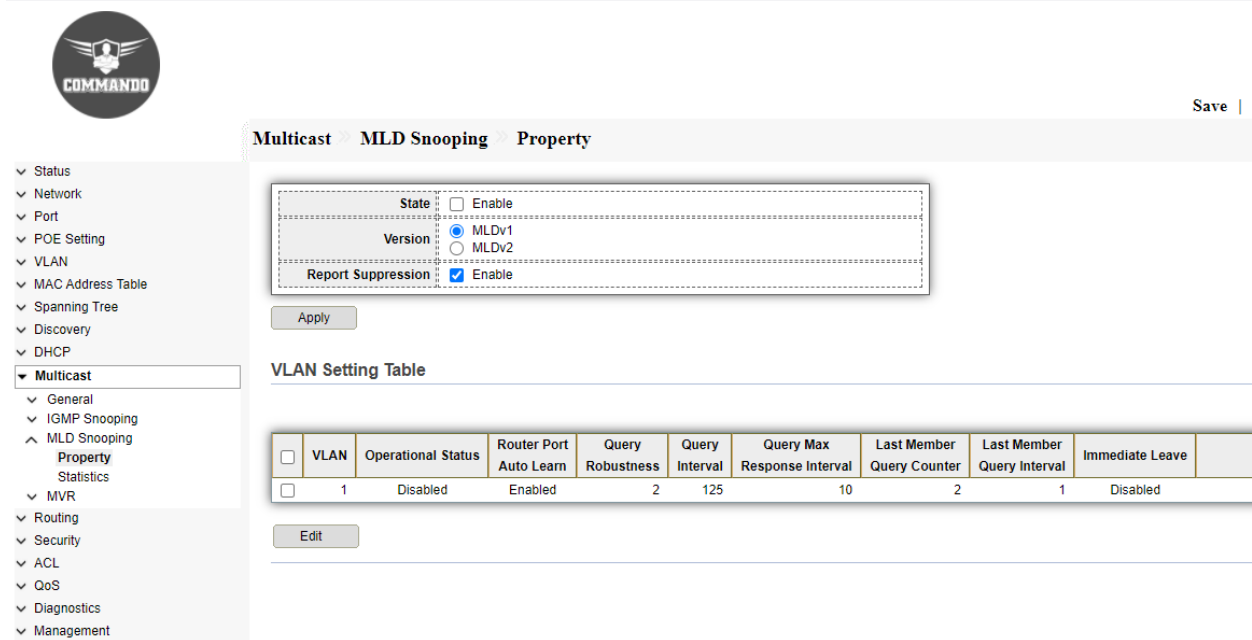


Fig 10.3.1 Multicast MLD Snooping default property page

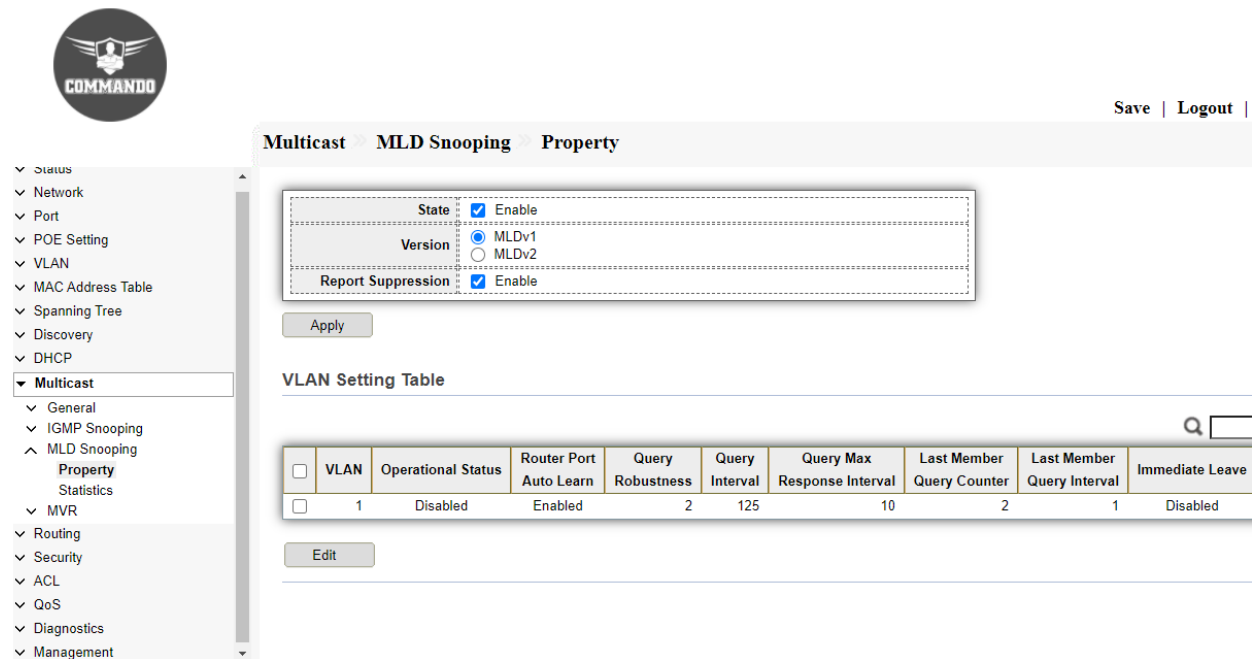


Fig 10.3.2 Enabling MLD Snooping property page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
 - ▼ General
 - ▼ IGMP Snooping
 - ▲ MLD Snooping
 - Property
 - Statistics
 - ▼ MVR
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Multicast MLD Snooping Property

State	<input checked="" type="checkbox"/> Enable
Version	<input checked="" type="radio"/> MLDv1 <input type="radio"/> MLDv2
Report Suppression	<input checked="" type="checkbox"/> Enable

Apply

VLAN Setting Table

<input type="checkbox"/>	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
<input checked="" type="checkbox"/>	1	Disabled	Enabled	2	125	10	2	1	Disabled

Edit

Fig 10.3.3 Selecting VLAN for MLD Snooping property page



Multicast > MLD Snooping > Property

- √ Status
- √ Network
- √ Port
- √ POE Setting
- √ VLAN
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- ▼ **Multicast**
- √ General
- √ IGMP Snooping
- ^ MLD Snooping
- Property**
- Statistics
- √ MVR
- √ Routing
- √ Security
- √ ACL
- √ QoS
- √ Diagnostics
- √ Management

Edit VLAN Setting

VLAN	1
State	<input checked="" type="checkbox"/> Enable
Router Port Auto Learn	<input checked="" type="checkbox"/> Enable
Immediate leave	<input type="checkbox"/> Enable
Query Robustness	<input type="text" value="1"/> (1 - 7, default 2)
Query Interval	<input type="text" value="125"/> Sec (30 - 18000, default 125)
Query Max Response Interval	<input type="text" value="10"/> Sec (5 - 20, default 10)
Last Member Query Counter	<input type="text" value="2"/> (1 - 7, default 2)
Last Member Query Interval	<input type="text" value="1"/> Sec (1 - 25, default 1)
Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

Apply Close

Fig 10.3.4 Edit VLAN Setting for MLD Snooping page



Save | Logout |

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ **Multicast**
- ▼ General
- ▼ IGMP Snooping
- ▲ MLD Snooping
 - Property**
 - Statistics
- ▼ MVR
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Multicast > MLD Snooping > Property

State	<input checked="" type="checkbox"/> Enable
Version	<input type="radio"/> MLDv1 <input checked="" type="radio"/> MLDv2
Report Suppression	<input checked="" type="checkbox"/> Enable

Apply

VLAN Setting Table

<input type="checkbox"/>	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
<input type="checkbox"/>	1	Enabled	Enabled	2	125	10	2	1	Disabled

Edit

Fig 10.3.5 Multicast MLD Snooping property page

10.3.2 Statistics

This page is used to display statistics for the MLD messages, and IPv6 PIM hello messages learned through MLD snooping. We can View the statistics of the various MLD packets that have been received or transmitted.

To view MLD Snooping Statistics, click **Multicast >> MLD Snooping >> Statistics**.

The screenshot shows the COMMANDO network management interface. On the left is a navigation tree with the following items: Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, **Multicast** (expanded), General, IGMP Snooping, MLD Snooping (expanded), Property, **Statistics** (highlighted), MVR, Routing, Security, ACL, QoS, Diagnostics, and Management. The main content area has a breadcrumb trail: **Multicast >> MLD Snooping >> Statistics**. Below the breadcrumb is a table with two sections: 'Receive Packet' and 'Transmit Packet'. Each section contains a list of statistics with their respective values, all of which are 0. At the bottom of the table are two buttons: 'Clear' and 'Refresh'.

Receive Packet	
Total	0
Valid	0
InValid	0
Other	0
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0

Transmit Packet	
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0

Fig 10.3.6 Multicast MLD Snooping statistics page

10.4 MVR

Multicast VLAN Registration (MVR) allows a single multicast VLAN to be shared for multicast member ports in different VLANs in IPv4 network. In IGMP Snooping, if member ports are in different VLANs, a copy of the multicast streams is sent to each VLAN that has member ports. While MVR provides a dedicated multicast VLAN to forward multicast traffic over the Layer 2 network, to avoid duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the multicast VLAN without interfering with their relationships in other VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

10.4.1 Property


Clients can dynamically join or leave the multicast VLAN without interfering with their relationships in other VLANs.

There are two types of MVR modes:

Compatible Mode: In compatible mode, the MVR switch does not forward report or leave messages from the hosts to the IGMP querier. So, the IGMP querier cannot learn the multicast groups membership information from the MVR switch. You must statically configure the IGMP querier to transmit all the required multicast streams to the MVR switch via the multicast VLAN.

Dynamic Mode: In dynamic mode, after receiving report or leave messages from the hosts, the MVR switch will forward them to the IGMP querier via the multicast VLAN (with appropriate translation of the VLAN ID). So, the IGMP querier can learn the multicast groups membership information through the report and leave messages and transmit the multicast streams to the MVR switch via the multicast VLAN according to the multicast forwarding table.

To view and configure multicast MVR property, click **Multicast >> MVR >>Property**.




Save

Multicast > MVR > Property

- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ **Multicast**
 - ▼ General
 - ▼ IGMP Snooping
 - ▼ MLD Snooping
 - ▲ MVR
 - Property**
 - Port Setting
 - Group Address
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

State	<input type="checkbox"/> Enable
VLAN	1
Mode	<input checked="" type="radio"/> Compatible <input type="radio"/> Dynamic
Group Start	0.0.0.0
Group Count	1 (1 - 128)
Query Time	1 Sec (1 - 10)
Operational Group	
Maximum	128
Current	0

Fig 10.4.1 Default MVR Property page



Save

Multicast > MVR > Property

- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ **Multicast**
 - ▼ General
 - ▼ IGMP Snooping
 - ▼ MLD Snooping
 - ▲ MVR
 - Property**
 - Port Setting
 - Group Address
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

State	<input checked="" type="checkbox"/> Enable
VLAN	1
Mode	<input checked="" type="radio"/> Compatible <input type="radio"/> Dynamic
Group Start	239.0.0.1
Group Count	1 (1 - 128)
Query Time	1 Sec (1 - 10)
Operational Group	
Maximum	128
Current	0

Fig 10.4.2 Setting MVR Property page

10.4.2 Port Setting

This page allow user to configure port role and port immediate leave.
To view and configure MVR port role and immediate leave state, click **Multicast >> MVR >> Port Setting**.



Multicast >> MVR >> Port Setting

▼ MAC Address Table
▼ Spanning Tree
▼ Discovery
▼ DHCP
▼ **Multicast**
 ▼ General
 ▼ IGMP Snooping
 ▼ MLD Snooping
 ^ MVR
 Property
 Port Setting
 Group Address
▼ Routing
▼ Security
▼ ACL
▼ QoS
▼ Diagnostics
▼ Management

Port Setting Table

<input type="checkbox"/>	Entry	Port	Role	Immediate Leave
<input type="checkbox"/>	1	GE1	None	Disabled
<input type="checkbox"/>	2	GE2	None	Disabled
<input type="checkbox"/>	3	GE3	None	Disabled
<input type="checkbox"/>	4	GE4	None	Disabled
<input type="checkbox"/>	5	GE5	None	Disabled
<input type="checkbox"/>	6	GE6	None	Disabled
<input type="checkbox"/>	7	GE7	None	Disabled
<input type="checkbox"/>	8	GE8	None	Disabled
<input type="checkbox"/>	9	GE9	None	Disabled
<input type="checkbox"/>	10	GE10	None	Disabled
<input type="checkbox"/>	11	GE11	None	Disabled
<input type="checkbox"/>	12	GE12	None	Disabled

Fig 10.4.3 Multicast MVR Port Setting page



Multicast » MVR » Port Setting

- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ▼ **Multicast**
 - ✓ General
 - ✓ IGMP Snooping
 - ✓ MLD Snooping
 - ^ MVR
 - Property
 - Port Setting**
 - Group Address
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Port Setting Table

<input checked="" type="checkbox"/>	Entry	Port	Role	Immediate Leave
<input checked="" type="checkbox"/>	1	GE1	None	Disabled
<input checked="" type="checkbox"/>	2	GE2	None	Disabled
<input checked="" type="checkbox"/>	3	GE3	None	Disabled
<input checked="" type="checkbox"/>	4	GE4	None	Disabled
<input checked="" type="checkbox"/>	5	GE5	None	Disabled
<input checked="" type="checkbox"/>	6	GE6	None	Disabled
<input checked="" type="checkbox"/>	7	GE7	None	Disabled
<input checked="" type="checkbox"/>	8	GE8	None	Disabled
<input checked="" type="checkbox"/>	9	GE9	None	Disabled
<input checked="" type="checkbox"/>	10	GE10	None	Disabled
<input checked="" type="checkbox"/>	11	GE11	None	Disabled
<input checked="" type="checkbox"/>	12	GE12	None	Disabled

Fig 10.4.4 Multicast MVR Port Selection page



Save | Logout |

Multicast > MVR > Port Setting

- Discovery
- DHCP
- Multicast**
 - General
 - IGMP Snooping
 - MLD Snooping
 - MVR
 - Property
 - Port Setting**
 - Group Address
- Routing
- Security
- ACL

Edit Port Setting

Port	GE1-GE28,LAG1-LAG8
Role	<input type="radio"/> None <input type="radio"/> Receiver <input checked="" type="radio"/> Source
Immediate Leave	<input checked="" type="checkbox"/> Enable

Apply Close

Fig 10.4.5 Multicast MVR Edit port setting page



Multicast > MVR > Port Setting

- ∨ Status
- ∨ Network
- ∨ Port
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ **Multicast**
 - ∨ General
 - ∨ IGMP Snooping
 - ∨ MLD Snooping
 - ∧ MVR
 - Property
 - Port Setting**
 - Group Address
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ QoS
- ∨ Diagnostics
- ∨ Management

Port Setting Table

<input type="checkbox"/>	Entry	Port	Role	Immediate Leave
<input type="checkbox"/>	1	GE1	Source	Enabled
<input type="checkbox"/>	2	GE2	Source	Enabled
<input type="checkbox"/>	3	GE3	Source	Enabled
<input type="checkbox"/>	4	GE4	Source	Enabled
<input type="checkbox"/>	5	GE5	Source	Enabled
<input type="checkbox"/>	6	GE6	Source	Enabled
<input type="checkbox"/>	7	GE7	Source	Enabled
<input type="checkbox"/>	8	GE8	Source	Enabled
<input type="checkbox"/>	9	GE9	Source	Enabled
<input type="checkbox"/>	10	GE10	Source	Enabled
<input type="checkbox"/>	11	GE11	Source	Enabled
<input type="checkbox"/>	12	GE12	Source	Enabled
<input type="checkbox"/>	13	GE13	Source	Enabled
<input type="checkbox"/>	14	GE14	Source	Enabled
<input type="checkbox"/>	15	GE15	Source	Enabled
<input type="checkbox"/>	16	GE16	Source	Enabled

Fig 10.4.6 Multicast MVR Port setting Table page

9.4.3 Group Address

You explicitly configure an MVLAN assign a range of multicast group addresses to it. That VLAN carries MVLAN traffic for the configured multicast groups.

To view and configure Multicast MVR Group Table, click **Multicast >> MVR >> Group Address**.

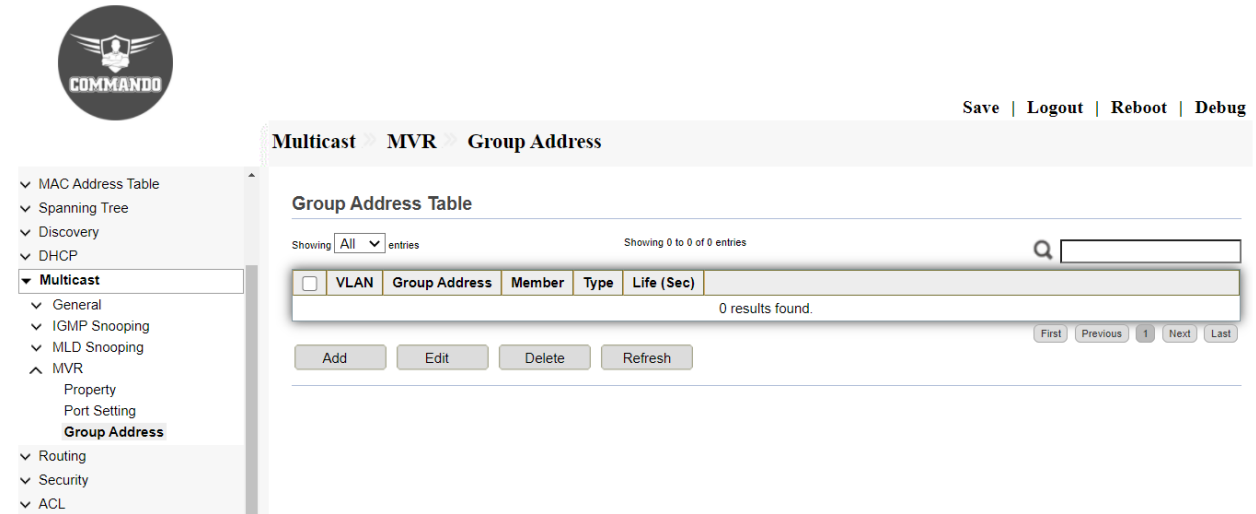


Fig 10.4.7 Multicast MVR default group address Table page

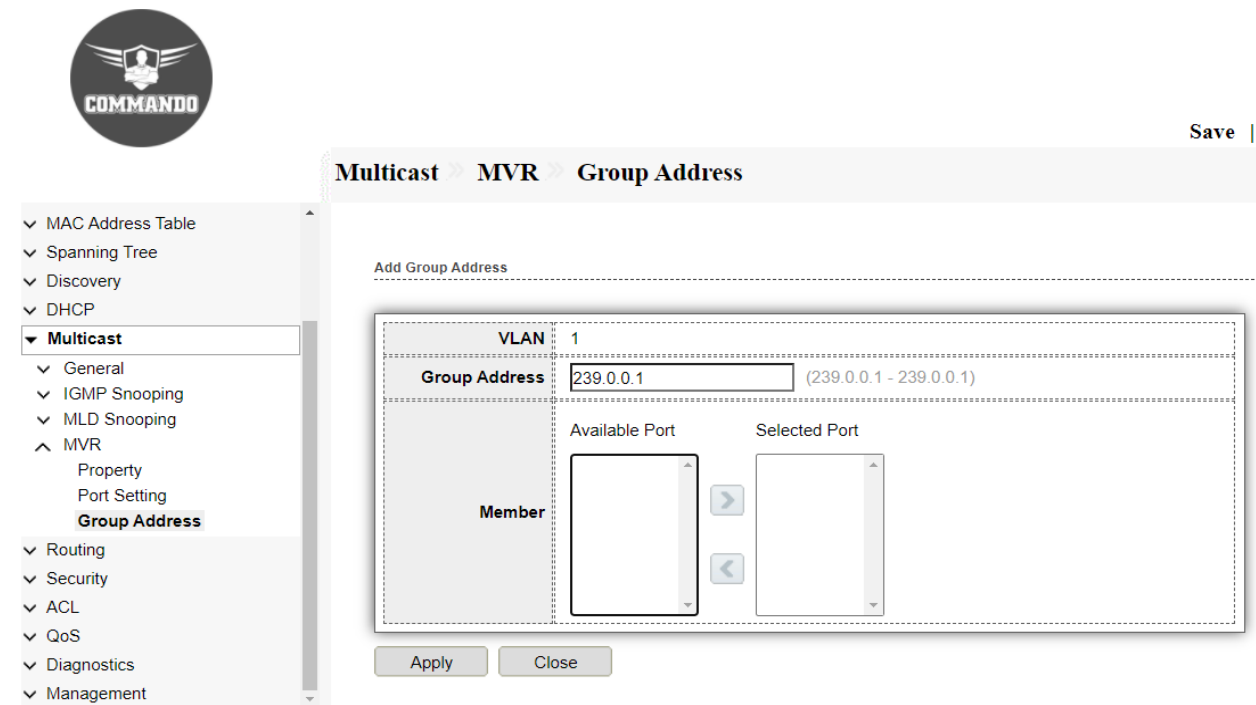


Fig 10.4.8 Multicast MVR Add group address page

Chapter 11 Routing

IPv4 Management and Interfaces: The IP address is configured under a logical interface, known as the management domain or VLAN. Usually, the default VLAN 1 acts like the switch's own NIC for connecting into a LAN to send IP packets.

IPv4 Interface: The IPv4 Interface page is used to configure IP addresses for device management. This IP address can be configured on a VLAN, loopback interface.

IPv4 Routes: IPv4 Routes deliver packets to destination network IPv4 addresses by forwarding them to interfaces of next hop addresses specified by the routing table.

ARP: The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

IPv6 Management and Interfaces: An IPv6 interface can be configured on a port, LAG, VLAN, loopback interface or tunnel.

IPv6 Interface: IPv6 addresses are assigned to interfaces, not nodes.

IPv6 Addresses: IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets, a group sometimes also called a hexet). The groups are separated by colons (:)

IPv6 Routes: IPv6 Routes deliver packets to destination network IPv6 addresses by forwarding them to interfaces of next hop addresses specified by the routing table.

IPv6 Neighbors: This page shows Routing configuration like the interface VLAN configuration to config IP interface on the device. IP address in VLAN interface mode to configure the device's IP address.

RIP Routes Management: RIP Routes deliver packets to destination network by forwarding them on basis of hop count as a routing metric.

RIP Routes Setting: Rip Routing can be enabled along with Network ID and subnet mask can be set.

OSPF Routes Management: OSPF uses the shortest path first (SPF) algorithm to determine routes that should be added to the routing table. OSPF routers maintain a map of the internetwork called the link state database.

OSPF Routes Setting: OSPF Routing can be enable along with Area Id, Network ID and Mask.

11.1 IPv4 Management and Interfaces

To manage the device by using the web-based configuration utility, the IPv4 device management IP address by default is 192.168.0.1 is access IP. You can set VLAN IP address and can create loopback interfaces.

Types of Interfaces in E3000 Switch

Trunk interface:

When a trunk interface connects to a device such as an AP/Switches that can receive and send tagged and untagged frames simultaneously, you need to configure the default VLAN for the trunk interface so that the trunk interface can add the VLAN tag to untagged frames.

Hybrid interface:

When a hybrid interface connects to an AP/hub/host/Switch/server that sends untagged frames to the switch, you need to configure the default VLAN for the hybrid interface so that the hybrid interface can add the VLAN tag to untagged frames. Frames sent by a switch all carry VLAN tags. Sometimes VLAN tags need to be removed from frames sent by a hybrid interface. A trunk interface allows untagged packets from only one VLAN, so the interface must be configured as hybrid.

Tunnel Interface:

A tunnel interface is a doorway to a VPN tunnel. VPN traffic enters and exits a VPN tunnel through a tunnel interface. When you bind a tunnel interface to a VPN tunnel, you can use that tunnel interface to route VPN traffic to a specific destination.

Access Interface:

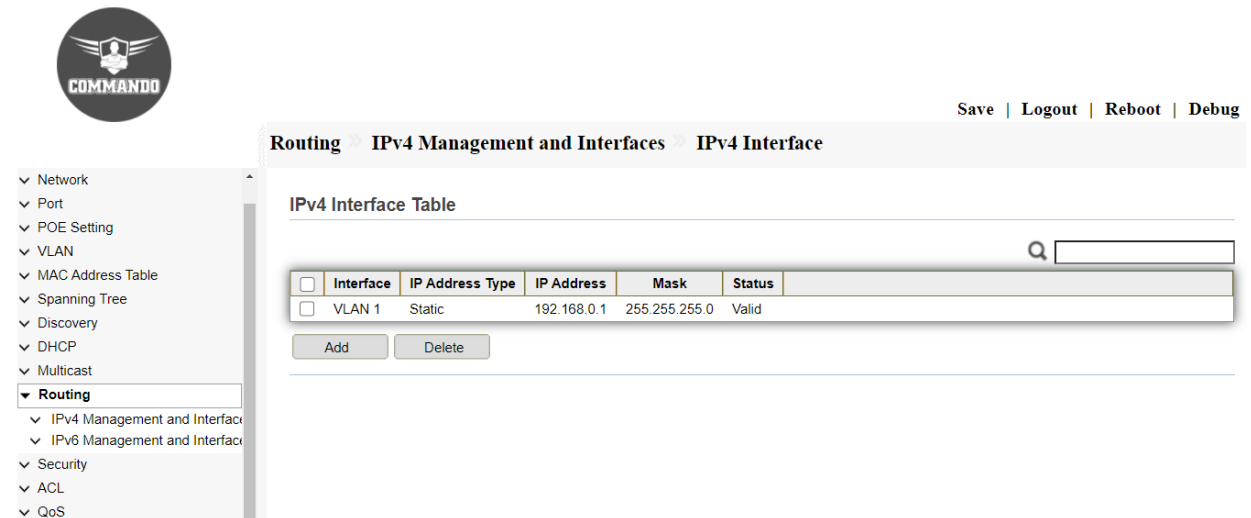
An access interface generally connects to a PC/Host or server that cannot identify VLAN tags or is used when VLANs do not need to be differentiated. Access interfaces can only receive and send untagged frames and can add only a unique VLAN tag to untagged frames.

11.1.1 IPv4 Interface

To manage the device by using the web-based configuration utility, the IPv4 device management IP address by default is 192.168.0.1. The device IP address can be manually configured also.

The IPv4 Interface page is used to configure IP addresses for device management. This IP address can be configured on VLAN, loopback interface.

To configure and view IPV4 interface, click **Routing >> IPv4 Management and Interfaces >> IPv4 Interface**.



The screenshot displays the Commando web-based configuration utility interface. On the left is a navigation menu with categories like Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, and QoS. The 'Routing' section is expanded, showing 'IPv4 Management and Interfaces' and 'IPv6 Management and Interfaces'. The main content area shows the breadcrumb 'Routing > IPv4 Management and Interfaces > IPv4 Interface' and a top bar with 'Save | Logout | Reboot | Debug' options. Below this is the 'IPv4 Interface Table' which includes a search box and a table with one entry: VLAN 1 with a Static IP address of 192.168.0.1 and a mask of 255.255.255.0. Below the table are 'Add' and 'Delete' buttons.

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status
<input type="checkbox"/>	VLAN 1	Static	192.168.0.1	255.255.255.0	Valid

Fig 11.1.1 Default IPv4 interface table page



Save |

Routing > IPv4 Management and Interfaces > IPv4 Interface

- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interface
 - IPv4 Interface**
 - IPv4 Routes
 - ARP
 - IPv6 Management and Interface
- Security

IPv4 Interface Table

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status
<input type="checkbox"/>	VLAN 1	Static	192.168.0.1	255.255.255.0	Valid

Add Delete

Fig 11.1.2 IPv4 interface configuration page



Save |

Routing > IPv4 Management and Interfaces > IPv4 Interface

- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interface
 - IPv4 Interface**
 - IPv4 Routes
 - ARP
 - IPv6 Management and Interface
- Security
- ACL

Add IPv4 Interface

Interface	<input type="radio"/> VLAN	<input checked="" type="radio"/> Loopback
Address Type	<input type="radio"/> Dynamic	<input checked="" type="radio"/> Static
IP Address	<input type="text" value="192.168.10.1"/>	
Mask	<input checked="" type="radio"/> Network Mask	<input type="text" value="255.255.255.0"/>
	<input type="radio"/> Prefix Length	<input type="text" value=""/> (8 - 32)

Apply Close

Fig 11.1.3 Creating IPv4 loopback interface configuration page

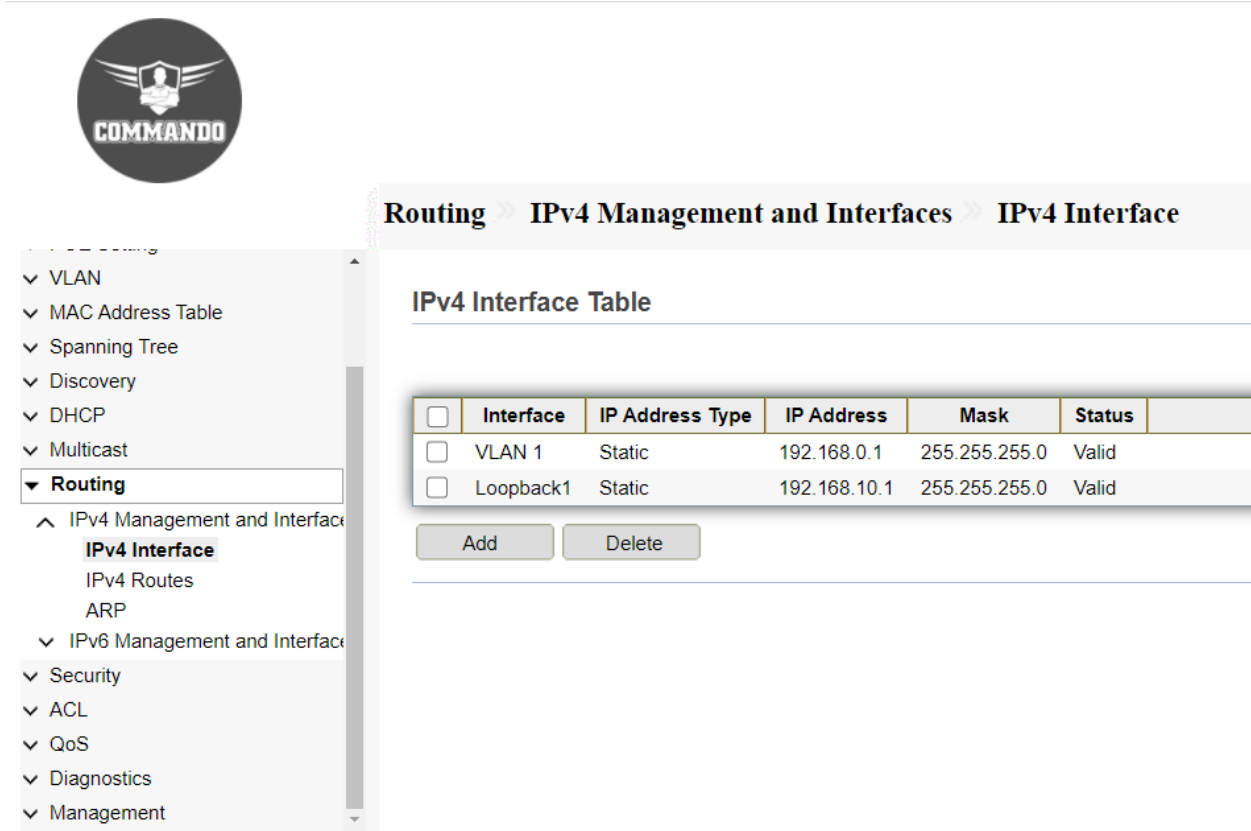


Fig 11.1.4 IPv4 interface table page

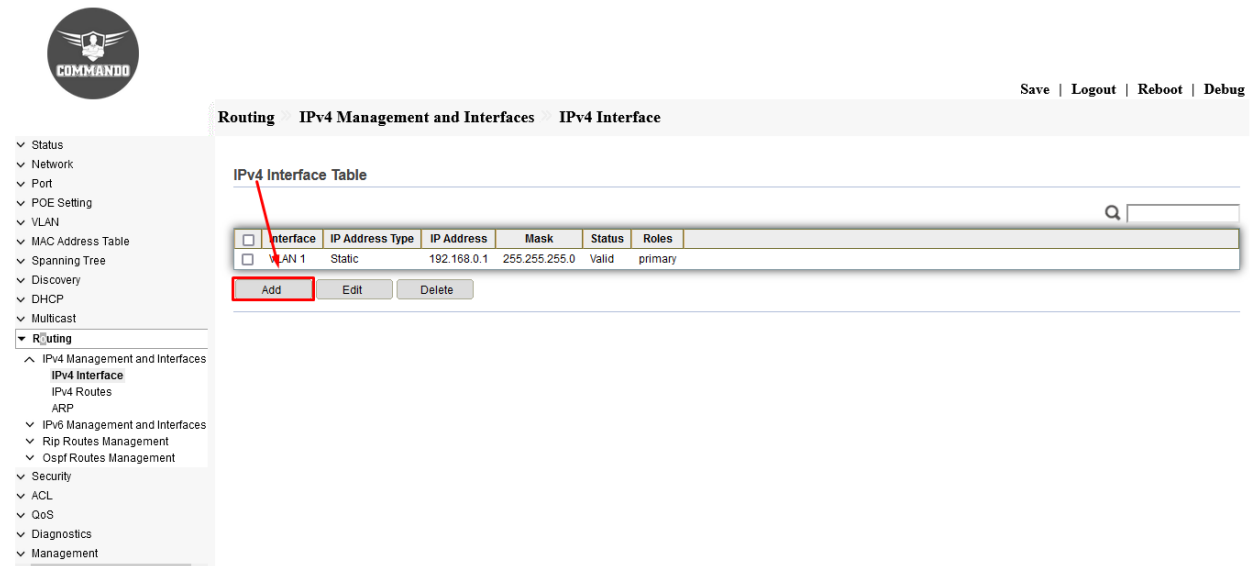


Fig 11.1.5 Add IPv4 interface page



Routing > IPv4 Management and Interfaces > IPv4 Interface

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ▼ **Routing**
 - ^ IPv4 Management and Interfaces
 - IPv4 Interface**
 - IPv4 Routes
 - ARP
 - ✓ IPv6 Management and Interfaces
 - ✓ Rip Routes Management
 - ✓ Ospf Routes Management
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Add IPv4 Interface

Interface	<input checked="" type="radio"/> VLAN <input type="text" value="2"/>
	<input type="radio"/> Loopback
Address Type	<input type="radio"/> Dynamic
	<input checked="" type="radio"/> Static
IP Address	<input type="text" value="192.168.1.2"/>
Mask	<input type="radio"/> Network Mask <input type="text"/>
	<input checked="" type="radio"/> Prefix Length <input type="text" value="24"/> (8 - 30)
Roles	<input checked="" type="radio"/> primary
	<input type="radio"/> sub

Apply Close

Fig 11.1.6 Add IPv4 address for VLAN 2 page



Routing » IPv4 Management and Interfaces » IPv4 Interface

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ▼ **Routing**
 - ^ IPv4 Management and Interfaces
 - IPv4 Interface**
 - IPv4 Routes
 - ARP
 - ✓ IPv6 Management and Interfaces
 - ✓ Rip Routes Management
 - ✓ Ospf Routes Management
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

IPv4 Interface Table

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status	Roles
<input type="checkbox"/>	VLAN 1	Static	192.168.0.1	255.255.255.0	Valid	primary
<input type="checkbox"/>	VLAN 2	Static	192.168.1.2	255.255.255.0	Valid	primary

Add

Edit

Delete

Fig 11.1.7 IPv4 address for VLAN 2 page

11.2.1 IPv4 Routes

Static IPv4 Routes: A static IPv4 route is a pre-determined path that network information must follow to reach a specific host or network.

Destination: To Specify the destination IPv4 address of the packets.

Subnet Mask: To Specify the subnet mask of the destination IPv4 address.

Next Hop: To Specify the IPv4 gateway address to which the packet should be sent next.

Distance: Specify the administrative distance, which is the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv4 routing table. The valid value ranges from 1 to 255 and the default value is 1.

Default IPv4 Routes: The default route is a special type of static route, which specifies a path that the device should use if the destination address is not included in any other routes. Therefore, a default route can solve this problem, if no route to the destination is specified, the device will send the packets to a specific device, that is, the default gateway. Then the default gateway will forward the packets to the destination. A default route consists of three parts mainly Destination, Subnet Mask and Next Hop (Gateway). The destination and subnet mask are both the fixed value 0.0.0.0, which means arbitrary destination IP addresses that are not matched by other route entries.

Routing table: Routing table is used for a Layer 3 device (in this configuration guide, it means the switch) to forward packets to the correct destination. When the switch receives packets of which the source IP address and destination IP address are in different subnets, it will check the routing table, find the correct outgoing interface then forward the packets. The routing table mainly contains two types of routing entries: Dynamic routing entries and Static routing entries.

Dynamic routing entries: Dynamic routing entries are automatically generated by the switch for connected networks. The switch use dynamic routing protocols to automatically calculate the best route to forward packets.

Static routing entries: Static routing entries are manually added non-aging routing entries. In a simple network with a small number of devices, you only need to configure static routes to ensure that the devices from different subnets can communicate with each other. On a complex large-scale network, static routes ensure stable connectivity for important applications because the static routes remain unchanged even when the topology changes.

To reduce costs, generally most enterprises use L2+/L3 switches to connect internal devices and an egress router/L3 Switch to connect to an ISP network for access the ISP network, the Layer 3 switch and egress router need to interwork at Layer 3. Most Layer 3 switches do not support routed interfaces or IP based interfaces or support limited routed interfaces. Generally, a VLAN interface is used as a Layer 3 interface to communicate with other Layer 3 interface of the router/ L3 switch and then static route or a dynamic routing protocol is configured to implement Layer 3 connectivity between the L3 switch and egress router/ other L3 Switch.

Interface based VLAN assignment is the simplest and most effective method which is deployed in E3000 Switch. VLANs are assigned based on interfaces. After an interface is added to a VLAN, the interface can forward packets from the VLAN. Ethernet interfaces are classified into access, trunk, and hybrid interfaces according to the connected interfaces to the Ethernet interfaces and number of VLANs from which untagged frames are permitted to access interface. The E3000 switch processes only tagged frames and an access interface connected to devices only receive and send untagged frames, so the access interface needs to add a VLAN tag to received frames. That is, you must configure the default VLAN for the access interface. After the default VLAN is configured, the access interface joins the VLAN. An access interface needs to process only untagged frames. If a user connects a switching device to a user side interface without permission, the user side interface may receive tagged frames. You can configure the user side interface to discard tagged frames, preventing unauthorized access.

The E3000 Series switch supports IPv4 static routing and IPv6 static routing configuration. To configure and view IPV4 interface, click **Routing >> IPv4 Management and Interfaces >> IPv4 Routes**. This page enables configuring and

viewing IPv4 static routes on the device. When routing traffic, the next hop is decided on according to the longest prefix match. A destination IPv4 address may match multiple routes in the IPv4 Static Route Table.

The screenshot shows the COMMANDO web interface. At the top right, there are links for 'Save | Logout | Reboot | Debug'. The main navigation bar includes 'Routing', 'IPv4 Management and Interfaces', and 'IPv4 Routes'. The left sidebar contains a tree view with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, IPv4 Management and Interfaces, IPv6 Management and Interfaces, and Security. Under 'Routing', 'IPv4 Routes' is selected. The main content area is titled 'IPv4 Routing Table' and features a search bar. Below the search bar is a table with the following data:

<input type="checkbox"/>	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
<input type="checkbox"/>	192.168.0.0	24	Directly Connected				VLAN 1*
<input type="checkbox"/>	192.168.10.0	24	Directly Connected				Loopback1*

Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

Fig 11.2.1 Default IPv4 Routing Table as per created Layer 3 interface page

Static IPv4 Routes Configuration:

Click on “IPv4 Management and Interfaces”, then “IPv4 Routes” from menu, Click on “Add”, then enter “IP Address”, “Mask”, “Next Hop Router IP Address” & “Metric” value and Click on “Apply”.

Configuration object and description:

Next Hop Router IP Address: Enter the next hop IP address or destination link IP address to reach that particular network.



Routing > IPv4 Management and Interfaces > IPv4 Routes

- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interfaces
 - IPv4 Interface
 - IPv4 Routes**
 - ARP
 - IPv6 Management and Interfaces
- Security
 - ACL
 - QoS
- Diagnostics
- Management

Add IPv4 Static Route

IP Address	<input type="text" value="192.168.1.0"/>
Mask	<input checked="" type="radio"/> Network Mask <input type="text" value="255.255.255.0"/>
	<input type="radio"/> Prefix Length <input type="text" value=""/> (0 - 32)
Next Hop Router IP Address	<input type="text" value="192.168.1.1"/>
Metric	<input type="text" value="1"/> (1 - 255, default 1)

Fig 11.2.2 Add IPv4 Static route page

Default IPv4 Routes Configuration:

Keep Network and mask all zero with Next hop IP as preferred and can set metric also.



- Membership
- Port Setting
- Voice VLAN
- Protocol VLAN
- MAC VLAN
- Surveillance VLAN
- GVRP
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interface
 - IPv4 Interface
 - IPv4 Routes**
 - ARP
 - IPv6 Management and Interface
 - Rip Routes Management
 - Rip Routes Setting
 - Ospf Routes Management
 - Ospf Routes Setting
- Security
- ACL

Routing » IPv4 Management and Interfaces » IPv4 Routes

Add IPv4 Static Route

IP Address	<input type="text" value="0.0.0.0"/>
Mask	<input type="radio"/> Network Mask <input type="text"/>
	<input checked="" type="radio"/> Prefix Length <input type="text" value="0"/> (0 - 32)
Next Hop Router IP Address	<input type="text" value="192.168.1.1"/>
Metric	<input type="text" value="1"/> (1 - 255, default 1)

Fig 11.2.3 Add IPv4 Default route page



- Membership
- Port Setting
- Voice VLAN
- Protocol VLAN
- MAC VLAN
- Surveillance VLAN
- GVRP
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interface
 - IPv4 Interface
 - IPv4 Routes**
 - ARP
 - IPv6 Management and Interface
 - Rip Routes Management
 - Rip Routes Setting
 - Ospf Routes Management
 - Ospf Routes Setting
- Security
- ACL

[Save](#) | [Logout](#) | [Reboot](#) | [Debug](#)

Routing » IPv4 Management and Interfaces » IPv4 Routes

IPv4 Routing Table

<input type="checkbox"/>	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
<input checked="" type="checkbox"/>	0.0.0.0	0	Default	192.168.1.1	1	1	VLAN 2*
<input type="checkbox"/>	192.168.0.0	24	Directly Connected				VLAN 1*
<input type="checkbox"/>	192.168.1.0	24	Directly Connected				VLAN 2*
<input type="checkbox"/>	192.168.2.0	24	Ospf	192.168.1.1	11	110	VLAN 2*

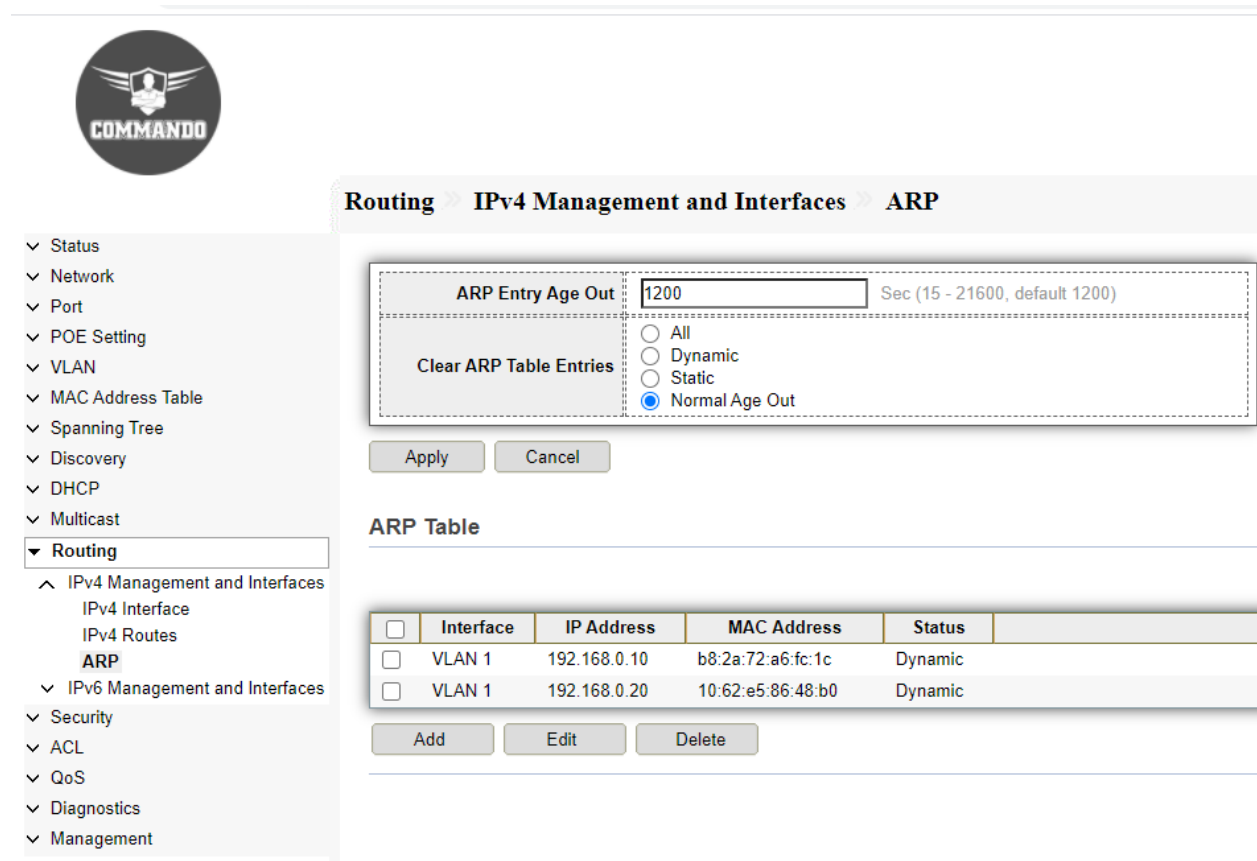
Fig 11.2.4 IPv4 routing table page

11.1.3 ARP

The E3000 Switches maintains an ARP (Address Resolution Protocol) table for all devices connected to it. The ARP table to obtain the MAC address of the device. The ARP table contains both static and dynamic addresses. Static addresses are manually configured and do not age out. The device creates dynamic addresses from the ARP packets it receives.

To view and configure ARP Table, click **Routing >> IPv4 Management and Interfaces >> ARP**.

Dynamic addresses age out after a configured time 20 minutes.



COMMANDO

Routing > IPv4 Management and Interfaces > ARP

ARP Entry Age Out: Sec (15 - 21600, default 1200)

Clear ARP Table Entries:

- All
- Dynamic
- Static
- Normal Age Out

Apply Cancel

ARP Table

<input type="checkbox"/>	Interface	IP Address	MAC Address	Status
<input type="checkbox"/>	VLAN 1	192.168.0.10	b8:2a:72:a6:fc:1c	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.0.20	10:62:e5:86:48:b0	Dynamic

Add Edit Delete

Fig 11.1.4 Default ARP table page



Save |

Routing > IPv4 Management and Interfaces > ARP

- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ▼ **Routing**
 - ^ IPv4 Management and Interface
 - IPv4 Interface
 - IPv4 Routes
 - ARP**
 - ✓ IPv6 Management and Interface
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Add ARP

Interface	VLAN <input type="text" value="1"/>
Note: Only interfaces with an valid IPv4 address are available for selection	
IP Address	<input type="text" value="192.168.0.2"/>
MAC Address	<input type="text" value="1a:2d:3c:4f:5d:6a"/>

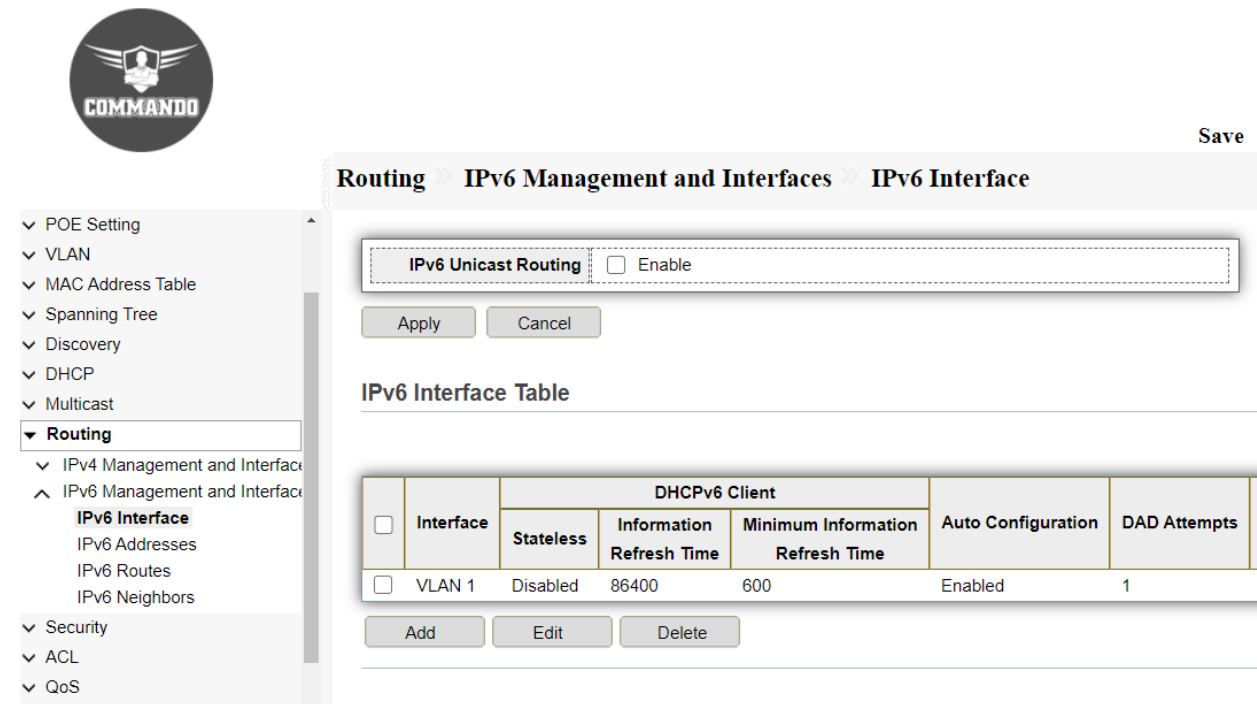
Fig 11.1.5 Add ARP page

11.2 IPv6 Management and Interfaces

Assigning IPv6 addresses to a network device enables the device to communicate with other devices on the network with IPv6 address.

11.2.1 IPv6 Interface

An IPv6 interface can be configured on a VLAN and loopback interface. To configure and view IPV6 interface, click **Routing >> IPv6 Management and Interfaces >> IPv6 Interface**.



The screenshot shows the COMMANDO network management interface. On the left is a navigation menu with categories like POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, and QoS. The 'Routing' category is expanded, showing 'IPv6 Management and Interfaces' and 'IPv6 Interface' selected. The main content area has a breadcrumb trail: 'Routing > IPv6 Management and Interfaces > IPv6 Interface'. At the top right is a 'Save' button. Below the breadcrumb is a configuration box for 'IPv6 Unicast Routing' with an 'Enable' checkbox and 'Apply' and 'Cancel' buttons. Below that is the 'IPv6 Interface Table' section, which contains a table with columns for 'Interface', 'DHCPv6 Client' (subdivided into 'Stateless', 'Information Refresh Time', and 'Minimum Information Refresh Time'), 'Auto Configuration', and 'DAD Attempts'. A single row is shown for 'VLAN 1' with values: Stateless: Disabled, Information Refresh Time: 86400, Minimum Information Refresh Time: 600, Auto Configuration: Enabled, DAD Attempts: 1. Below the table are 'Add', 'Edit', and 'Delete' buttons.

	Interface	DHCPv6 Client			Auto Configuration	DAD Attempts
		Stateless	Information Refresh Time	Minimum Information Refresh Time		
<input type="checkbox"/>	VLAN 1	Disabled	86400	600	Enabled	1

Fig 11.2.1 Default IPv6 interface Table page



Save |

Routing > IPv6 Management and Interfaces > IPv6 Interface

- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interface
 - IPv6 Management and Interface
 - IPv6 Interface**
 - IPv6 Addresses
 - IPv6 Routes
 - IPv6 Neighbors
- Security
- ACL
- QoS

IPv6 Unicast Routing Enable

Apply Cancel

IPv6 Interface Table

	Interface	DHCPv6 Client			Auto Configuration	DAD Attempts
		Stateless	Information Refresh Time	Minimum Information Refresh Time		
<input type="checkbox"/>	VLAN 1	Disabled	86400	600	Enabled	1

Add Edit Delete

Fig 11.2.2 Enable IPv6 Unicast Routing page



Save |

Routing > IPv6 Management and Interfaces > IPv6 Interface

- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interface
 - IPv6 Management and Interface
 - IPv6 Interface**
 - IPv6 Addresses
 - IPv6 Routes
 - IPv6 Neighbors
- Security
- ACL
- QoS

Add IPv6 Interface

Interface VLAN 1 Loopback

Auto Configuration Enable

DAD Attempts (0 - 600, default 1)

DHCPv6 Client

Stateless Enable

Information Refresh Time (86400 - 4294967294, default 86400)

Minimum Information Refresh Time (600 - 4294967294, default 600)

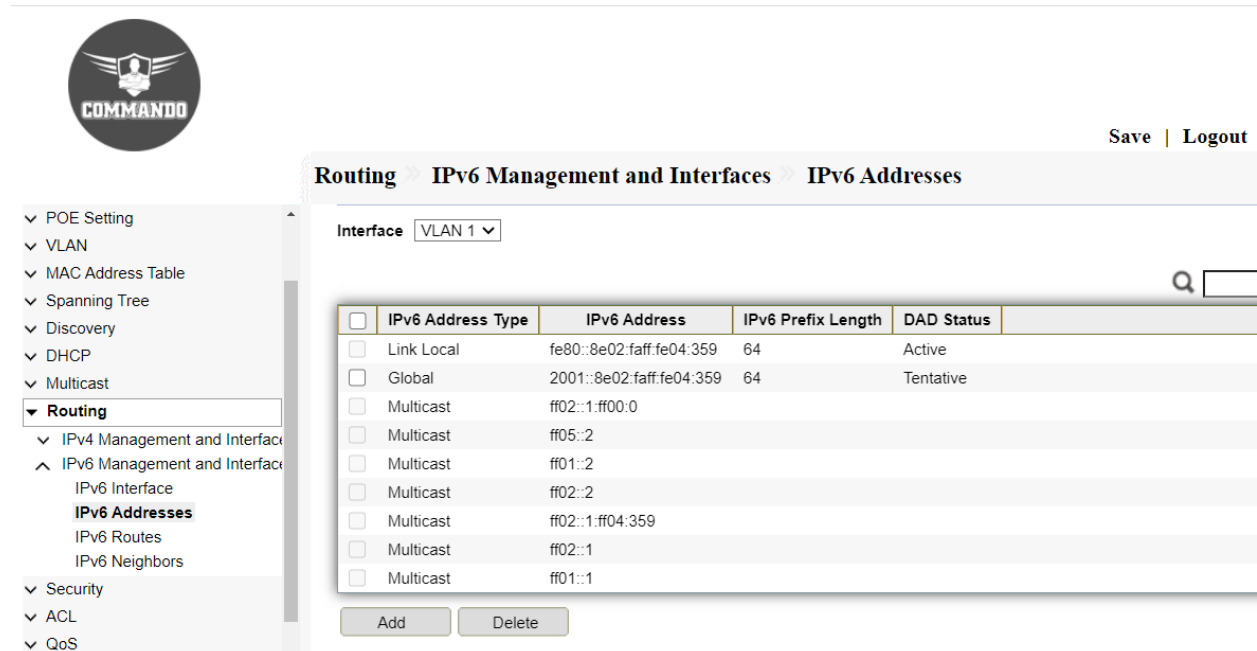
Apply Close

Fig 11.2.3 Add IPv6 interface page

11.2.2 IPv6 Addresses

An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets, a group sometimes also called a hextet). The groups are separated by colons (:). The three types of IPv6 addresses are: unicast, anycast, and multicast addresses.

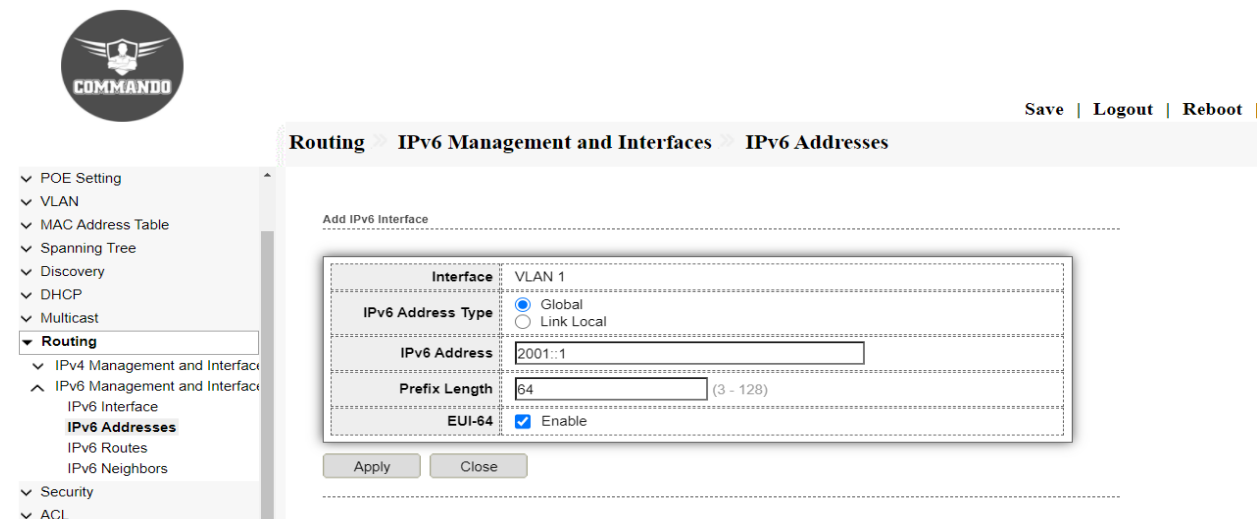
To configure and view IPv6 address, click **Routing >> IPv6 Management and Interfaces >> IPv6 addresses**.



The screenshot shows the COMMANDO web interface. On the left is a navigation menu with categories like POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, and QoS. The 'Routing' section is expanded to show 'IPv6 Management and Interfaces' > 'IPv6 Addresses'. The main content area has a breadcrumb trail: 'Routing > IPv6 Management and Interfaces > IPv6 Addresses'. At the top right are 'Save' and 'Logout' buttons. Below the breadcrumb is a search bar and a table of IPv6 addresses. The table has columns for 'IPv6 Address Type', 'IPv6 Address', 'IPv6 Prefix Length', and 'DAD Status'. The interface also shows 'Interface: VLAN 1' and 'Add' and 'Delete' buttons at the bottom.

<input type="checkbox"/>	IPv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status
<input type="checkbox"/>	Link Local	fe80::8e02:faff:fe04:359	64	Active
<input type="checkbox"/>	Global	2001::8e02:faff:fe04:359	64	Tentative
<input type="checkbox"/>	Multicast	ff02::1:ff00:0		
<input type="checkbox"/>	Multicast	ff05::2		
<input type="checkbox"/>	Multicast	ff01::2		
<input type="checkbox"/>	Multicast	ff02::2		
<input type="checkbox"/>	Multicast	ff02::1:ff04:359		
<input type="checkbox"/>	Multicast	ff02::1		
<input type="checkbox"/>	Multicast	ff01::1		

Fig 11.2.4 IPv6 address table page



The screenshot shows the 'Add IPv6 Interface' configuration page in the COMMANDO web interface. The navigation menu is similar to the previous screenshot. The breadcrumb trail is 'Routing > IPv6 Management and Interfaces > IPv6 Addresses'. At the top right are 'Save', 'Logout', and 'Reboot' buttons. The main content area is titled 'Add IPv6 Interface' and contains a form with the following fields: 'Interface' (VLAN 1), 'IPv6 Address Type' (radio buttons for Global and Link Local, with Global selected), 'IPv6 Address' (text input with value 2001::1), 'Prefix Length' (text input with value 64 and a range indicator '(3 - 128)'), and 'EUI-64' (checkbox checked and labeled 'Enable'). 'Apply' and 'Close' buttons are at the bottom.

Fig 11.2.5 Add IPv6 interface page



Save |

Routing > IPv6 Management and Interfaces > IPv6 Addresses

- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interface
 - IPv6 Management and Interface
 - IPv6 Interface
 - IPv6 Addresses**
 - IPv6 Routes
 - IPv6 Neighbors
- Security
- ACL
- QoS
- Diagnostic

IPv6 Address Table

Interface

<input type="checkbox"/>	IPv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status	
<input type="checkbox"/>	Link Local	fe80::8e02:faff:fe04:359	64	Active	
<input type="checkbox"/>	Multicast	ff02::1:ff00:0			
<input type="checkbox"/>	Multicast	ff05::2			
<input type="checkbox"/>	Multicast	ff01::2			
<input type="checkbox"/>	Multicast	ff02::2			
<input type="checkbox"/>	Multicast	ff02::1:ff04:359			
<input type="checkbox"/>	Multicast	ff02::1			
<input type="checkbox"/>	Multicast	ff01::1			

Fig 11.2.6 IPv6 address table after adding IPv6 address page

11.2.3 IPv6 Routes

This page enables configuring and viewing IPv6 static routes on the device. When routing traffic, the next hop is decided on according to the longest prefix match. A destination IPv6 address may match multiple routes in the IPv6 Static Route Table. To configure and view IPv6 address, click **Routing >> IPv6 Management and Interfaces >> IPv6 Routes**.

The screenshot displays the Commando network management interface. On the left is a navigation tree with categories like Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The 'Routing' section is expanded, showing sub-items for IPv4, IPv6, and IPv6 Neighbors. The main content area is titled 'IPv6 Routing Table' and features a table with columns: Destination IP Prefix, Prefix Length, Route Type, Next Hop Router IP Address, Metric, Administrative Distance, and Outgoing. Below the table, it indicates '0 results found.' and provides 'Add', 'Edit', and 'Delete' buttons. A 'Save' button is located in the top right corner of the interface.

Fig 11.2.8 Default IPv6 routing table page



Routing > IPv6 Management and Interfaces > IPv6 Routes

Add IPv6 Static Route

IPv6 Prefix	<input type="text" value="2001::"/>
IPv6 Prefix Length	<input type="text" value="64"/> (0 - 128)
Next Hop Router IP Address	<input type="text" value="2002::1"/>
Metric	<input type="text" value="1"/> (1 - 255, default 1)

Apply Close

Fig 11.2.9 Add IPv6 static route page

IPv6 Routes Configuration:

Click on “IPv6 Management and Interfaces”, then “IPv6 Routes” from menu.

Click on “Add”, then enter “IP Address”, “Mask”, “Next Hop Router IP Address” & “Metric” value. Click on “Apply”.

Configuration object and description:

Next Hop Router IP Address: Enter the next hop IP address or destination link IP address.

11.2.4 IPv6 Neighbors

The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a IPv6 neighbor, and track neighboring devices.

To configure and view IPV6 address, click **Routing >> IPv6 Management and Interfaces >> IPv6 Neighbors**.

The screenshot shows the Commando network management interface. On the left is a navigation menu with categories like VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The 'Routing' category is expanded, showing 'IPv4 Management and Interfaces', 'IPv6 Management and Interfaces', and 'IPv6 Neighbors'. The main content area has a breadcrumb trail: 'Routing > IPv6 Management and Interfaces > IPv6 Neighbors'. A 'Save' link is in the top right. A 'Clear Neighbor Table' dialog box is open, containing radio buttons for 'All', 'Dynamic', 'Static', and 'N/A' (which is selected). Below the dialog are 'Apply' and 'Cancel' buttons. Underneath is the 'IPv6 Neighbor Table' header, followed by a table with columns: 'Interface', 'IPv6 Address', 'MAC Address', 'Status', and 'Router'. The table is empty, with the text '0 results found.' below it. At the bottom of the table are 'Add', 'Edit', and 'Delete' buttons.

Fig 11.2.11 Default IPv6 neighbor page



Save

Routing > IPv6 Management and Interfaces > IPv6 Neighbors

- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ **Routing**
- ▼ IPv4 Management and Interface
- ▲ IPv6 Management and Interface
 - IPv6 Interface
 - IPv6 Addresses
 - IPv6 Routes
 - IPv6 Neighbors**
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Add Neighbor

Interface	VLAN	1
IP Address	2005::1	
MAC Address	1a:2d:3c:4f:5d:6a	

Apply

Close

Fig 11.2.12 Add IPv6 neighbor page

11.3.1 RIP Routes Management

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source & the destination network. It is one of a family of IP Routing protocols and is an Interior Gateway Protocol (IGP) designed to distribute routing information within an Autonomous System (AS).

It is a distance vector routing protocol which has default AD value 120 & works on the application layer of OSI model. It uses port number 520. Typically, the best path is the path with the fewest hops. A hop is another router through which packets must travel to reach the destination. If RIP receives a RIP update from another router/switch that contains a path with fewer hops than the path stored in the route table, the system replaces the older route with the newer one. The system then includes the new path in the updates it sends to other RIP routers. A router/switch running RIP sends the contents of its routing table to each of its adjacent routers every 30 seconds by default.

Features of RIP:

Updates of the network are exchanged periodically.

Updates (routing information) are always broadcast.

Full routing tables are sent in updates.

Routers/Switches always trust on routing information received from neighbor routers. This is also known as Routing on rumor.

The disadvantages of RIP include:

Increased network traffic: RIP checks with its neighboring routers every 30 seconds, which increases network traffic.

Maximum hop count limitation: RIP has a maximum hop count of 15, which means that on large networks, other remote routers may not be able to be reached.

Comparison of RIP v1 & RIP v2

RIPv1	RIPv2
Classful	Classless
Automatic summarization to the class boundary	Manual summarization on per interface basis
Network masks not included in the advertisements	Network masks included in the advertisements
Advertisements use broadcast destination address 255.255.255.255	Advertisements use reserved multicast destination address 224.0.0.9
No authentication support	2 authentication methods (clear text, MD5)

Steps to Configure RIP in E3000 with Web GUI

1. Create any VLAN for routing purpose from 2 to 4094.
2. Assign IP address to created VLAN as per other connected router/switch IP address as they required to be in same network.
3. Go to Interface where you connected L3 Switch/Router and assign Created VLAN in access mode.
4. Enable RIP.
5. Add connected Network ID to RIP
6. Check the learn route with RIP.

Step 1: Create VLAN for routing purpose

COMMANDO

Save | Logout | Reboot | Debug

VLAN VLAN Create VLAN

Available VLAN Created VLAN

VLAN 3 VLAN 4 VLAN 5 VLAN 6 VLAN 7 VLAN 8 VLAN 9 VLAN 10

VLAN 1 VLAN 2

Apply

VLAN Table

Showing All entries Showing 1 to 2 of 2 entries

<input type="checkbox"/>	VLAN	Name	Type	VLAN Interface State
<input type="checkbox"/>	1	default	Default	Enabled
<input type="checkbox"/>	2	VLAN0002	Static	Enabled

Edit Delete

Fig 11.3.1 Creating VLAN 2 Page

Step 2: Assign IP address to created VLAN

COMMANDO

Save | Logout | Reboot | Debug

Routing IPv4 Management and Interfaces IPv4 Interface

IPv4 Interface Table

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status	Roles
<input type="checkbox"/>	VLAN 1	Static	192.168.0.1	255.255.255.0	Valid	primary

Add Edit Delete

Fig 11.3.2 Add IP address for VLAN Page

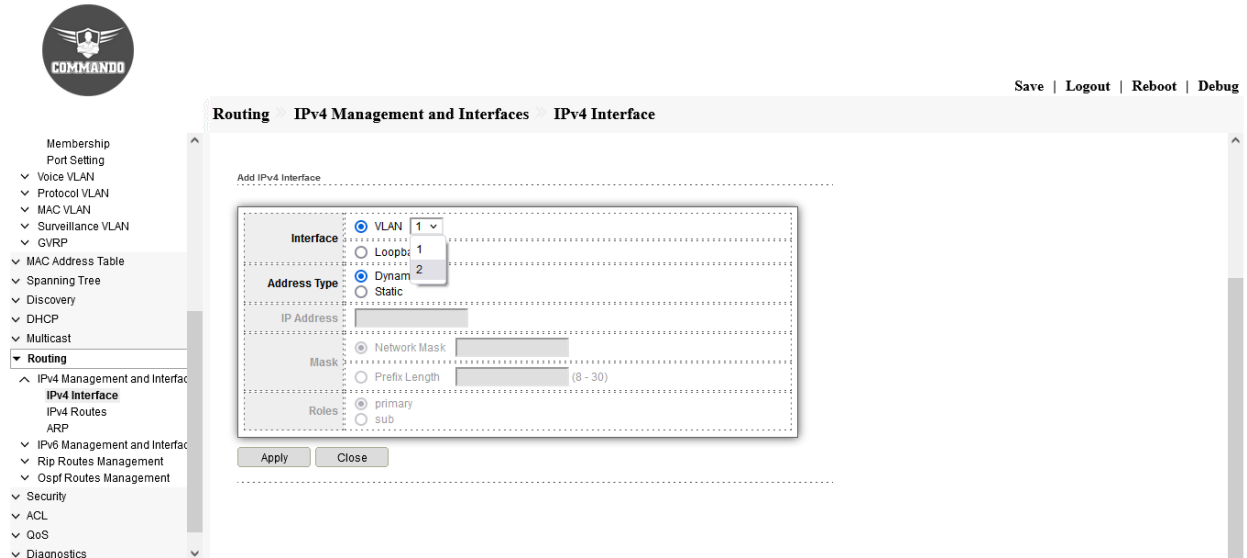


Fig 11.3.3 Selecting VLAN for providing IP address Page

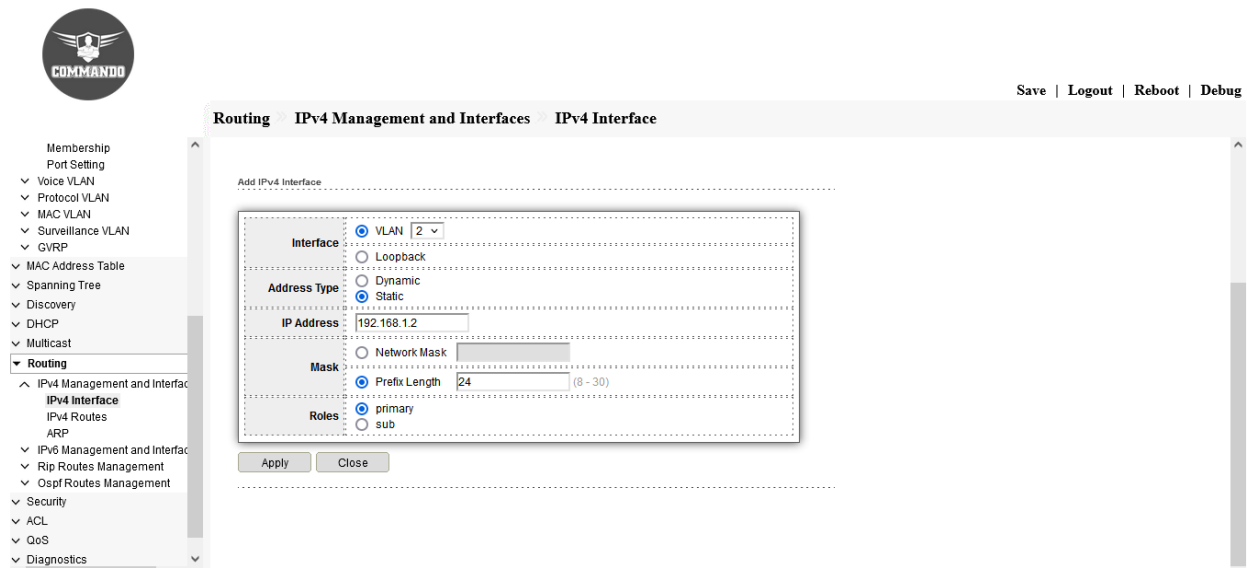


Fig 11.3.4 Add Static VLAN IP address with subnet mask Page

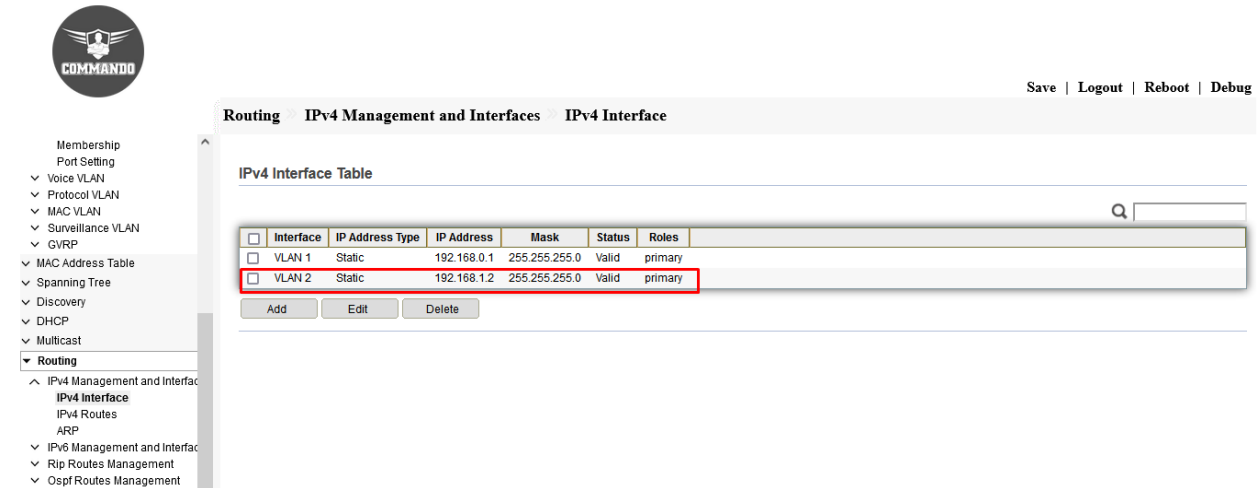


Fig 11.3.5 Assign IP address to created VLAN Page

Step 3: Configuration Interface connected to Other L3 device and assign Created VLAN in access mode.

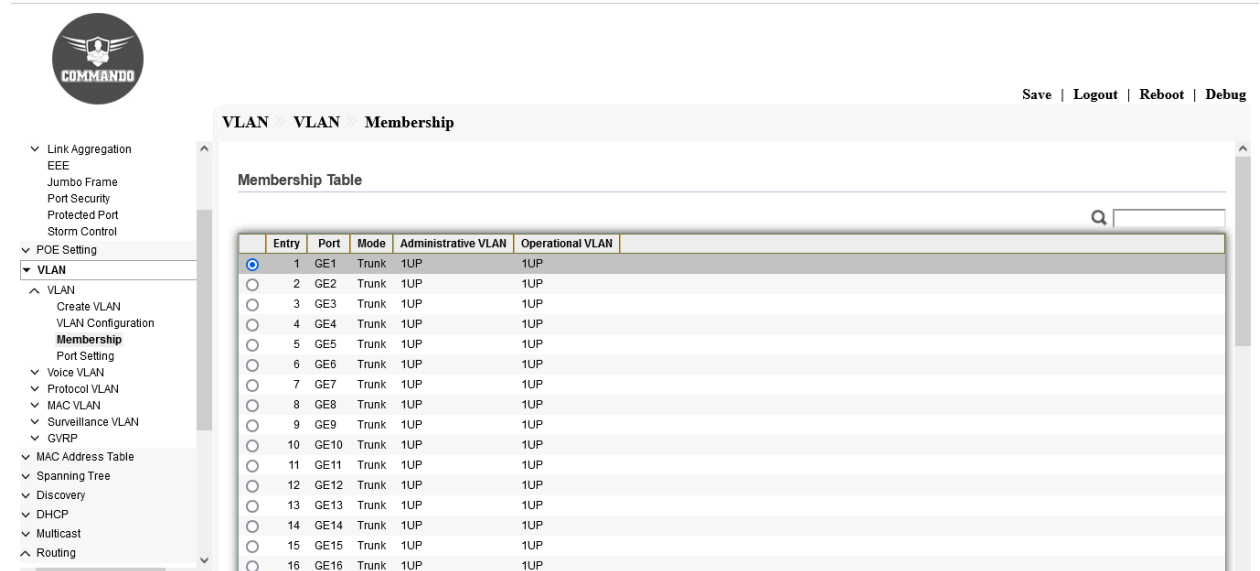


Fig 11.3.6 Selecting Interface to assign new VLAN membership page

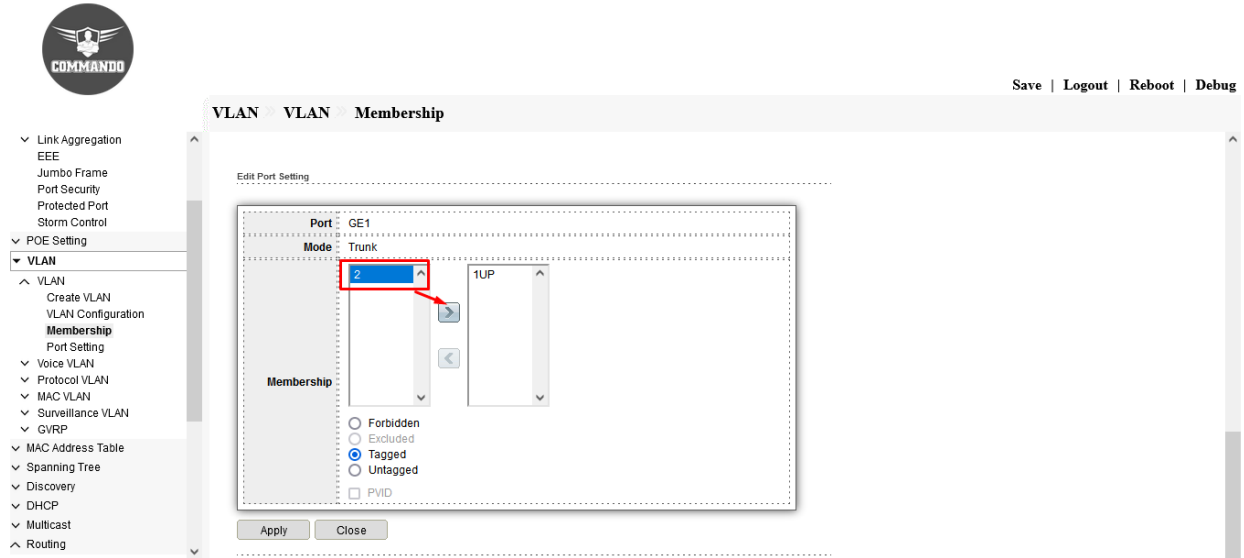


Fig 11.3.7 Edit Port setting for new VLAN membership page

Note: Remove VLAN 1 from port membership.

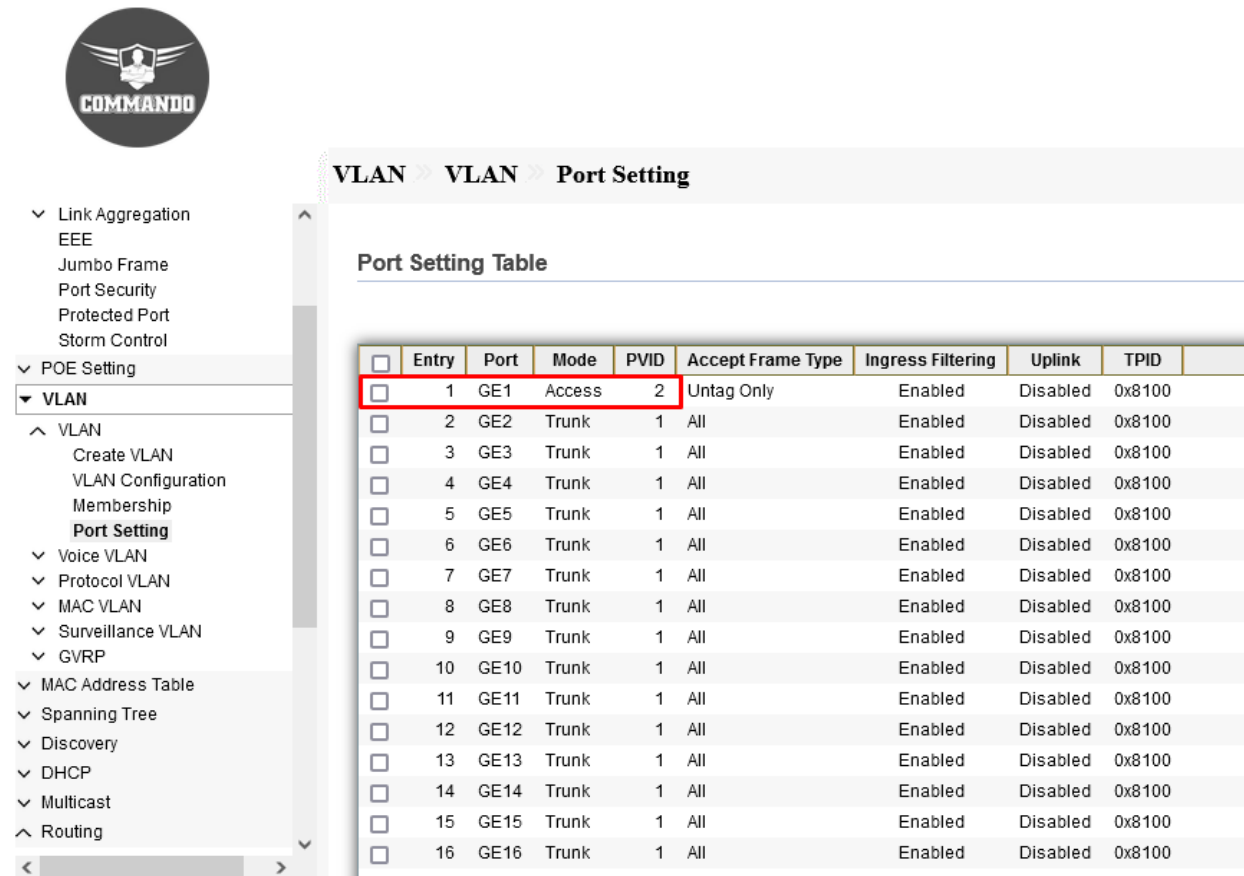
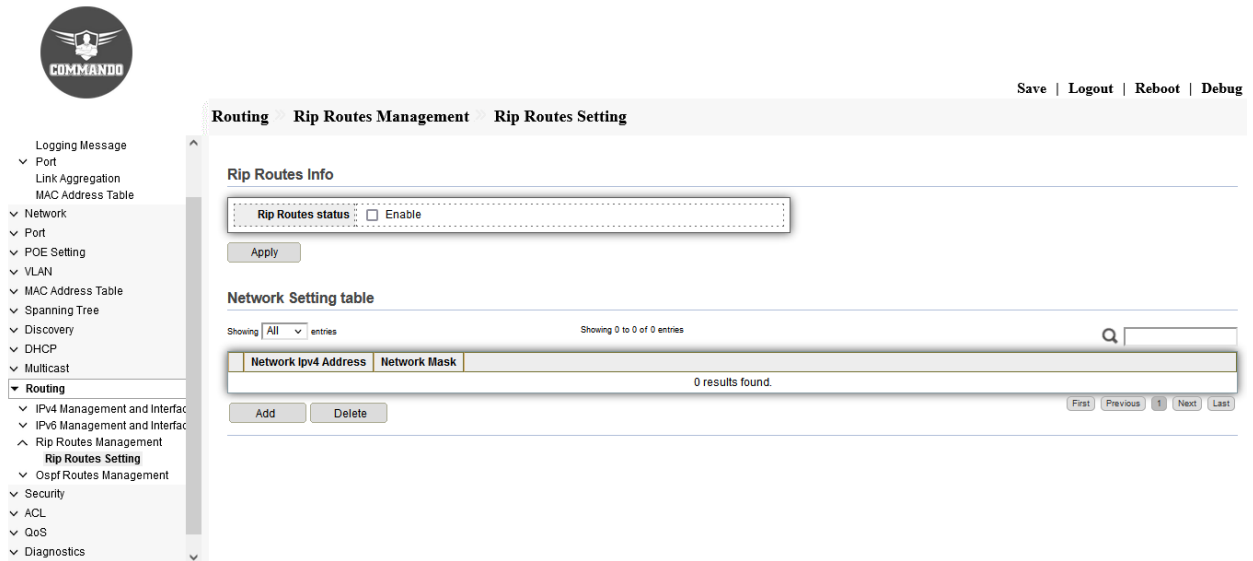


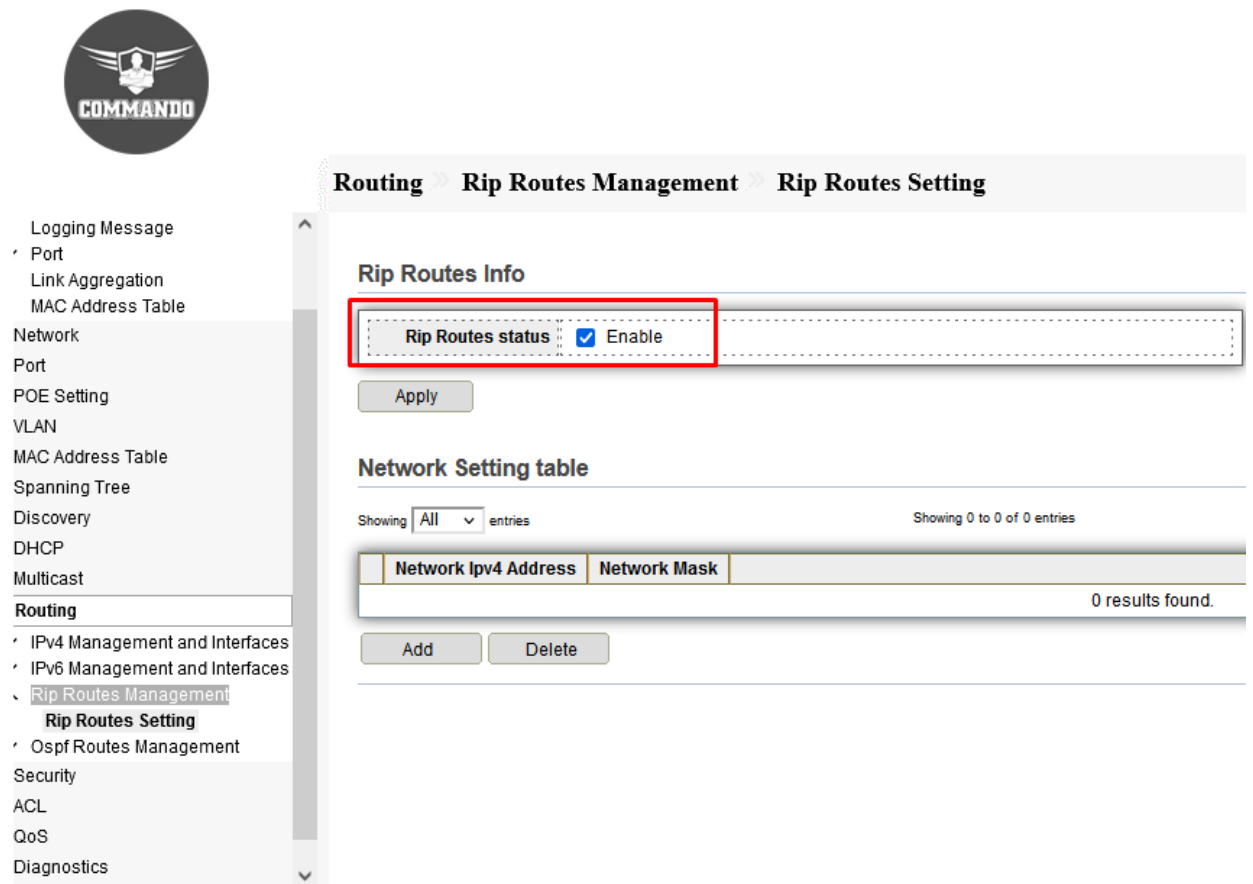
Fig 11.3.8 New VLAN membership Table page

Step 4: Enable RIP



The screenshot shows the COMMANDO web interface for configuring RIP routes. The breadcrumb navigation is **Routing > Rip Routes Management > Rip Routes Setting**. In the top right corner, there are links for **Save | Logout | Reboot | Debug**. The left sidebar contains a navigation tree with categories like Logging Message, Port, Link Aggregation, MAC Address Table, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, **Routing** (expanded), IPv4 Management and Interface, IPv6 Management and Interface, Ospf Routes Management, Security, ACL, QoS, and Diagnostics. The main content area is titled **Rip Routes Info** and features a **Rip Routes status** field with an unchecked **Enable** checkbox and an **Apply** button. Below this is the **Network Setting table**, which shows **Showing 0 to 0 of 0 entries** and a table with columns **Network Ipv4 Address** and **Network Mask**. The table is currently empty, displaying **0 results found.** and includes **Add** and **Delete** buttons.

Fig 11.3.9 Default RIP route setting Page



This screenshot shows the same COMMANDO web interface as Fig 11.3.9, but with the **Rip Routes status** checkbox checked, indicating that RIP is now enabled. The breadcrumb navigation remains **Routing > Rip Routes Management > Rip Routes Setting**. The left sidebar navigation tree is identical. The main content area shows the **Rip Routes Info** section with the **Enable** checkbox checked and the **Apply** button. The **Network Setting table** section below it also shows **Showing 0 to 0 of 0 entries** and **0 results found.** with **Add** and **Delete** buttons.

Fig 11.3.10 Enabling RIP in Switch Page

Note: After Enabling RIP then only you can add the connected network's ID in the RIP.

Step 5: Add connected Network ID to RIP

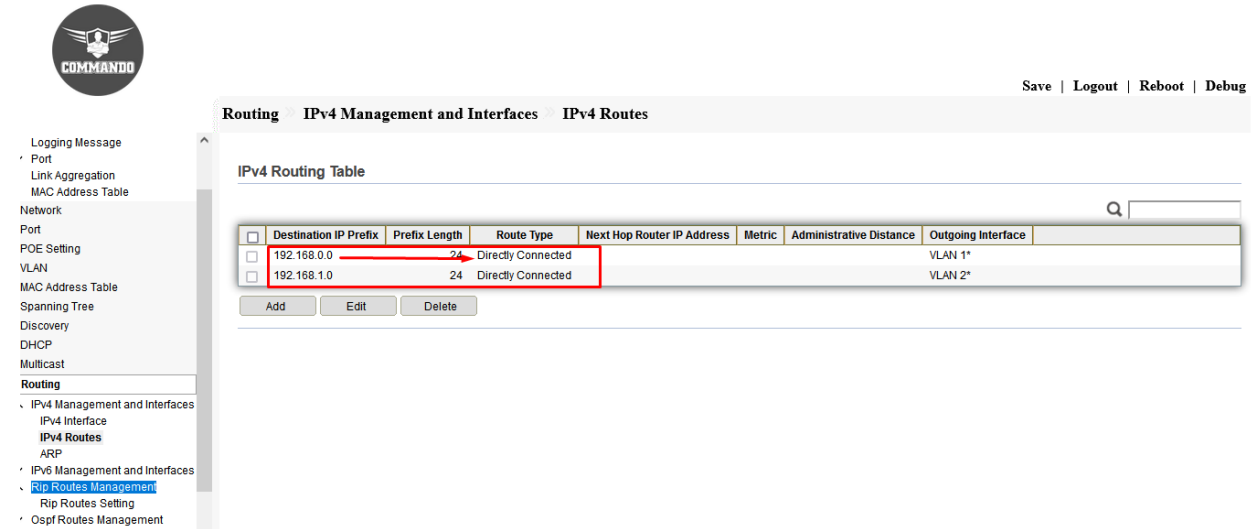


Fig 11.3.11 To know connected Network in switch page

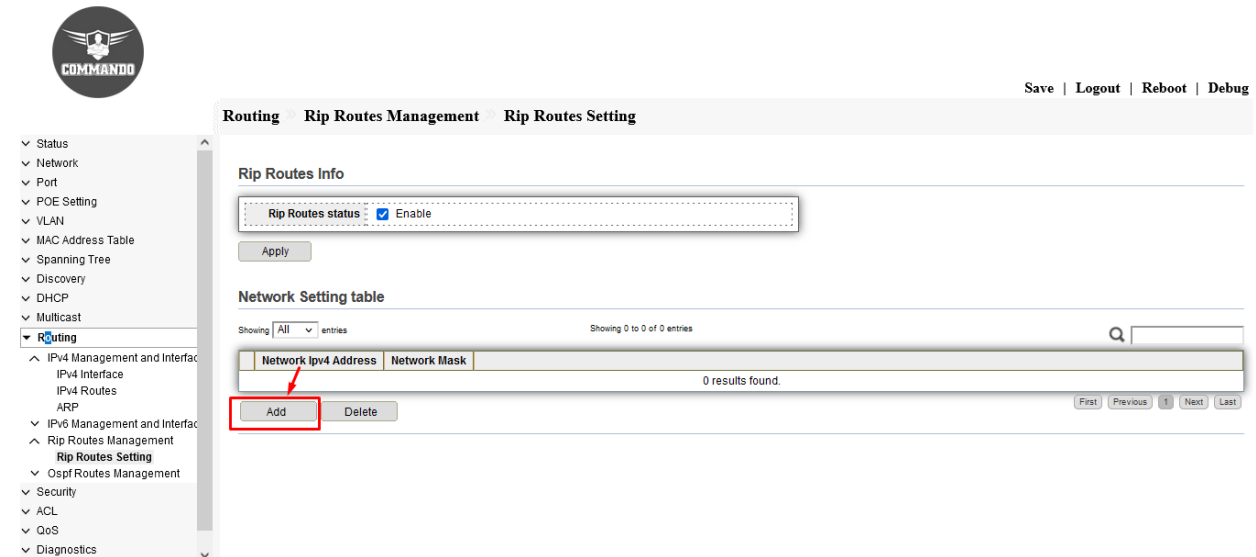


Fig 11.3.12 Add Connected Network ID in RIP Process Page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ **Routing**
 - ▲ IPv4 Management and Interface
 - IPv4 Interface
 - IPv4 Routes
 - ARP
 - ▼ IPv6 Management and Interface
 - ▲ Rip Routes Management
 - Rip Routes Setting**
 - ▼ Ospf Routes Management

Routing > Rip Routes Management > Rip Routes Setting

Network Setting table

Network Ipv4 Address	192.168.1.0
Network Mask	255.255.255.0

Apply Close

Fig 11.3.13 Network ID setting in RIP Page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ **Routing**
 - ▲ IPv4 Management and Interface
 - IPv4 Interface
 - IPv4 Routes
 - ARP
 - ▼ IPv6 Management and Interface
 - ▲ Rip Routes Management
 - Rip Routes Setting**
 - ▼ Ospf Routes Management

Routing > Rip Routes Management > Rip Routes Setting

Rip Routes Info

Rip Routes status Enable

Apply

Network Setting table

Showing All entries

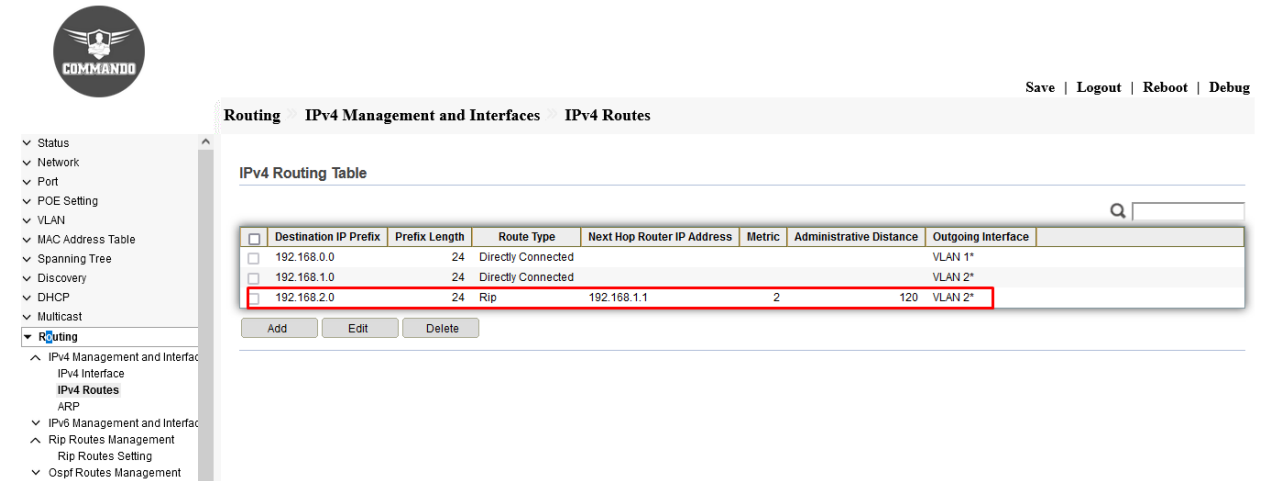
Showing 1 to 2 of 2 entries

	Network Ipv4 Address	Network Mask
<input type="checkbox"/>	192.168.0.0	255.255.255.0
<input type="checkbox"/>	192.168.1.0	255.255.255.0

Add Delete

Fig 11.3.14 Network ID setting Table page

Step 6: Check RIP Route



COMMANDO

Save | Logout | Reboot | Debug

Routing > IPv4 Management and Interfaces > IPv4 Routes

IPv4 Routing Table

<input type="checkbox"/>	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
<input type="checkbox"/>	192.168.0.0	24	Directly Connected				VLAN 1*
<input type="checkbox"/>	192.168.1.0	24	Directly Connected				VLAN 2*
<input type="checkbox"/>	192.168.2.0	24	Rip	192.168.1.1	2	120	VLAN 2*

Add Edit Delete

Routing

- IPv4 Management and Interfaces
 - IPv4 Interface
 - IPv4 Routes**
 - ARP
- IPv6 Management and Interfaces
- Rip Routes Management
 - Rip Routes Setting
- Ospf Routes Management

Fig 11.3.15 IPv4 Routing Table page

11.4.1 OSPF Routes Management

OSPF is an Interior Gateway Protocol (IGP) is link-state Interior Gateway Protocol (IGP) developed by the Internet Engineering Task Force (IETF). OSPF Version 2 as defined in RFC 2328 is designed for IPv4. OSPF constructs network topologies and routing tables by dividing an Autonomous System (AS) into one or more logical areas, Advertising routes by sending Link State Advertisements (LSAs), Exchanging OSPF packets between devices in an OSPF area to synchronize routing information.

In an OSPF network, each router generates a link-state advertisement (LSA) based on its surrounding network topology and transmits this LSA in an update packet to other routers in the network. The OSPF works by Exchanging Hello packets to establish OSPF neighbor relationships, Flooding LSAs to advertise link state information from their LSDBs to create a weighted, directed graph, Using an SPF algorithm to calculate and generate routes, Maintaining and updating routing tables by any topology changes.

OSPF has five types of packets:

Hello packet

Hello packets are sent periodically by OSPF-enabled interfaces to discover and maintain OSPF neighbor relationships. These packets contain information about the Designated Router (DR), Backup Designated Router (BDR), and known neighbors on the same network.

Database Description (DD) packet

After an adjacency is established, it uses DD packets to describe their own LSDBs for LSDB synchronization. A DD packet contains the header of each LSA in an LSDB and is the summary of all LSAs.

Link State Request (LSR) packet

After DD packets exchanged, they send LSR packets to request each other's LSAs. The LSR packets contain the summaries of the requested LSAs.

Link State Update (LSU) packet

It uses an LSU packet to transmit LSAs requested by its neighbors or to flood its own updated LSAs. The LSU packet contains a set of LSAs.

Link State Acknowledgment Packets

These packet to make the flooding of link state advertisements reliable, flooded advertisements are explicitly acknowledged. This acknowledgment is accomplished through the sending and receiving of Link State Acknowledgment packets.

OSPF Network Types:

Broadcast

Networks using Ethernet or Fiber Distributed Data Interface (FDDI) at the link layer are broadcast networks by default.

Non-Broadcast Multi-Access (NBMA)

Networks using frame relay (FR) or X.25 at the link layer are NBMA networks by default.

Point-to-Multipoint (P2MP)

No networks are P2MP networks by default, regardless of the link layer protocol used by the network. Networks may be changed to P2MP networks. Typical practice is to change partial-meshed NBMA networks to P2MP networks.

Point-to-Point (P2P)

Networks using Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), or Link Access Procedure Balanced (LAPB) at the link layer are P2P networks.

Common terms used in OSPF Process:

Router ID

A router ID is a 32-bit integer, which uniquely identifies an OSPF router in an AS. Each OSPF router has a router ID. A router ID is in the same format as an IP address. To

ensure OSPF stability in actual network deployment, it is recommended that the IP address of a loopback interface on a router be used as the router ID of this router. A router ID can be manually configured or automatically selected by a router. If no router ID is manually configured for a router, the router automatically selects an interface IP address as its router ID.

The router ID selection rules are as follows:

1. The router preferentially selects the largest IP address among loopback interface addresses as the router ID.
2. If no loopback interface is configured, the router selects the largest IP address among interface addresses as the router ID.
3. A switch can obtain a router ID again only after a router ID is reconfigured for the switch or an OSPF router ID is reconfigured and the OSPF process restarts.

DR/BDR Election process:

DR election rules are used to elect a DR only when routers with different router IDs or configured with different DR priorities are started at the same time. The election rules are that the device with the highest DR priority is elected as DR and the device with the second highest DR priority as BDR. A router with a DR priority of 0 can be a DR other only. If routers have the same DR priority, the router with the greatest router ID is elected as the DR, the router with the second greatest router ID becomes the BDR, and other routers are DR others.

Area

There are five types of OSPF areas: Backbone area (area 0), Standard area, Stub area, totally stubby area, and not-so-stubby area (NSSA).

OSPF Route

There are six types of route types like Intra-Area (O), Inter-Area (O IA), External Type 1 (E1), NSSA Type 1 (N1), External Type 2 (E2), NSSA Type 2 (N2) .

OSPF authentication

OSPF supports null, simple password authentication and MD5 authentication. OSPF MD5 authentication can be configured globally or by interface. Plain text & MD5 authentication among neighboring routers within an area is supported: Configurable routing interface parameters include interface output cost, re-transmission interval, interface transmit delay, router priority, router dead & hello intervals, & authentication key.

Steps to Configure OSPF in E3000 with Web-GUI

1. Create any VLAN for routing purpose from 2 to 4094.
2. Assign IP address to created VLAN as per other connected router/switch IP address as they required to be in same network.
3. Go to Interface where you connected L3 Switch/Router and assign Created VLAN in access mode.
4. Enable OSPF.
5. Add connected Network ID to OSPF
6. Check OSPF Route

Step 1 : Create VLAN for routing purpose

The screenshot shows the 'Create VLAN' configuration page. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, and VLAN. The 'VLAN' section is expanded to show 'Create VLAN'. The main area has two columns: 'Available VLAN' (VLAN 3-10) and 'Created VLAN' (VLAN 1, VLAN 2). 'VLAN 2' is highlighted with a red box. Below is a 'VLAN Table' with two entries: '1 default Default Enabled' and '2 VLAN0002 Static Enabled'. The 'Add' button is highlighted with a red box.

Save | Logout | Reboot | Debug

VLAN VLAN Create VLAN

Available VLAN Created VLAN

VLAN 3 VLAN 4 VLAN 5 VLAN 6 VLAN 7 VLAN 8 VLAN 9 VLAN 10

VLAN 1 VLAN 2

Apply

VLAN Table

Showing All entries Showing 1 to 2 of 2 entries

<input type="checkbox"/>	VLAN	Name	Type	VLAN Interface State
<input type="checkbox"/>	1	default	Default	Enabled
<input type="checkbox"/>	2	VLAN0002	Static	Enabled

Edit Delete

Fig 11.4.1 Creating VLAN 2 Page

Step 2: Assign IP address to created VLAN

The screenshot shows the 'IPv4 Interface' configuration page. The navigation menu on the left is expanded to 'Routing' > 'IPv4 Management and Interfaces' > 'IPv4 Interface'. The main area shows an 'IPv4 Interface Table' with one entry: 'VLAN 1 Static 192.168.0.1 255.255.255.0 Valid primary'. The 'Add' button is highlighted with a red box.

Save | Logout | Reboot | Debug

Routing IPv4 Management and Interfaces IPv4 Interface

IPv4 Interface Table

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status	Roles
<input type="checkbox"/>	VLAN 1	Static	192.168.0.1	255.255.255.0	Valid	primary

Add Edit Delete

Fig 11.4.2 Add IP address for VLAN Page

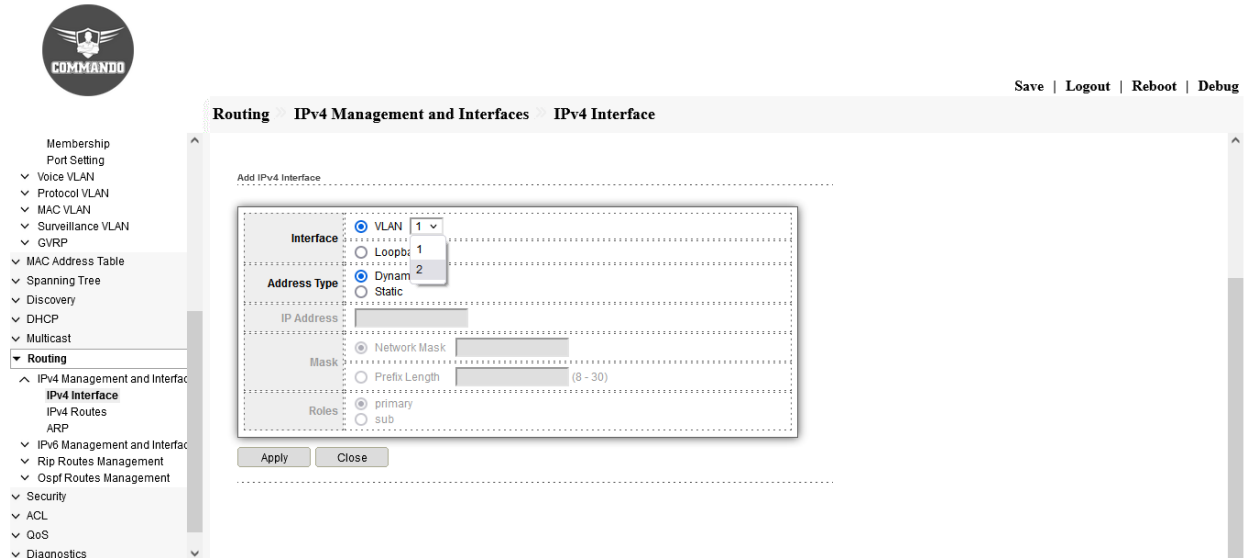


Fig 11.4.3 Selecting VLAN for providing IP address Page

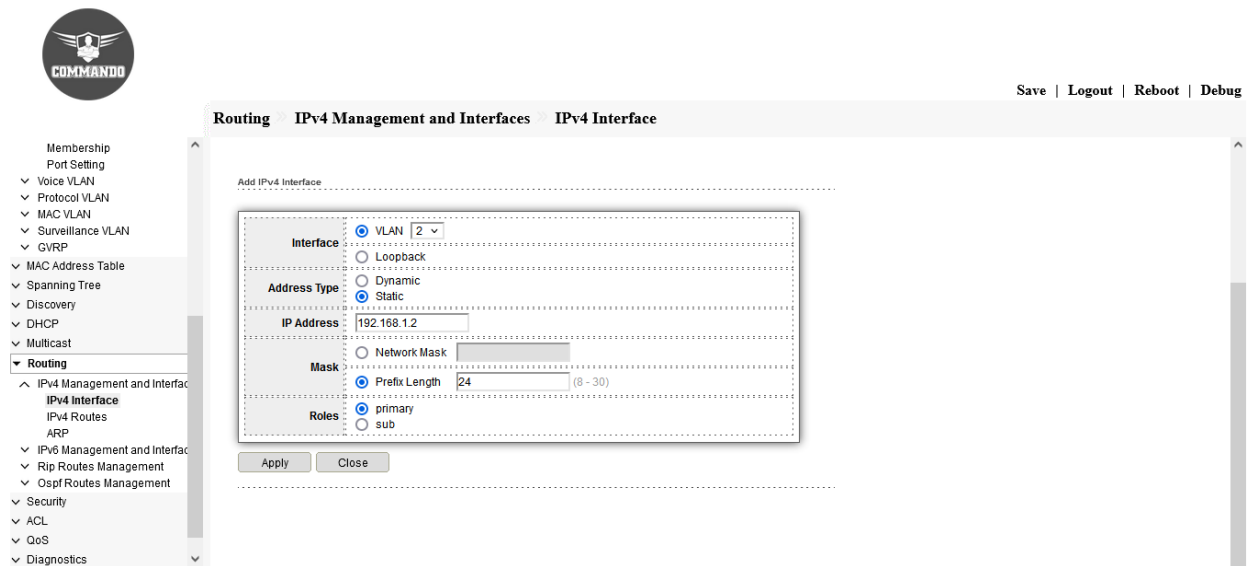


Fig 11.4.4 Add Static VLAN IP address with subnet mask Page

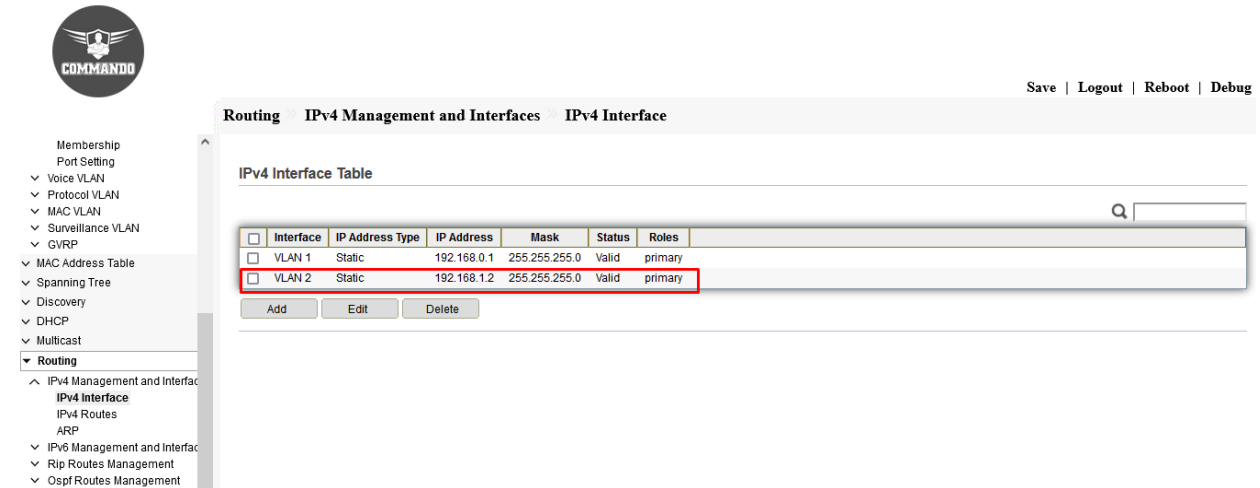


Fig 11.4.5 Assign IP address to created VLAN Page

Step 3: Configuration Interface connected to Other L3 device and assign Created VLAN in access mode.

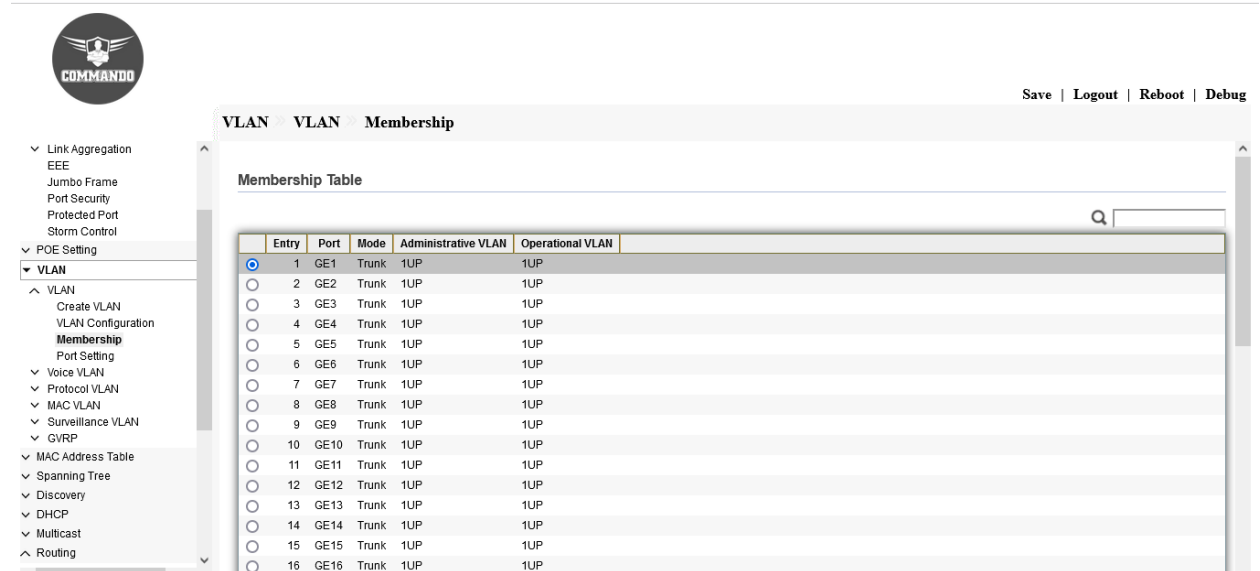


Fig 11.4.6 Selecting Interface to assign new VLAN membership page

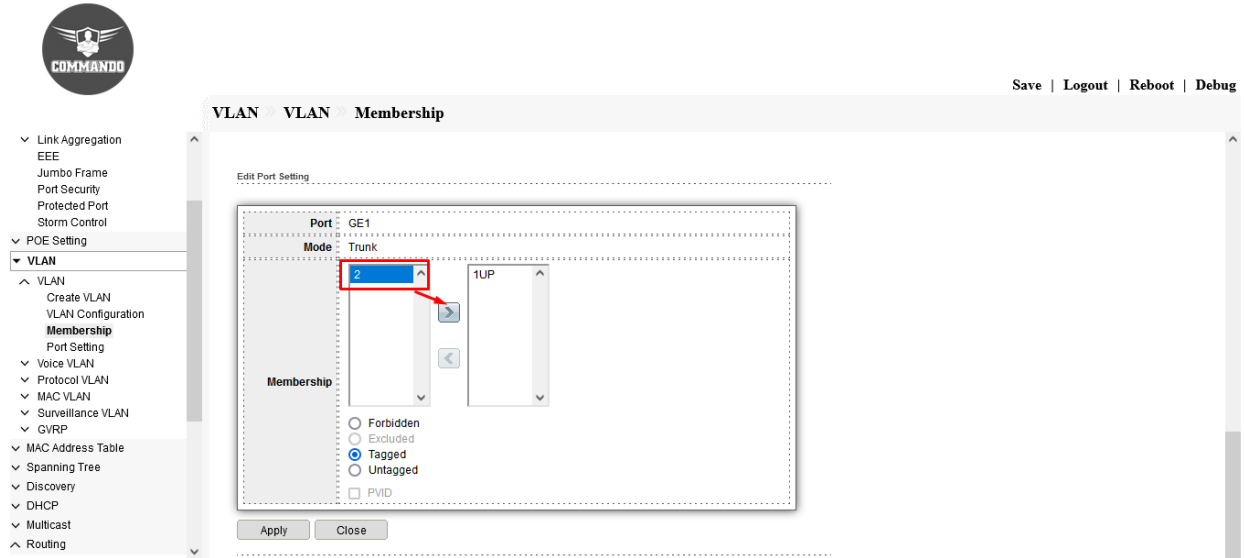


Fig 11.4.7 Edit Port setting for new VLAN membership page

Note: Remove VLAN 1 from access.

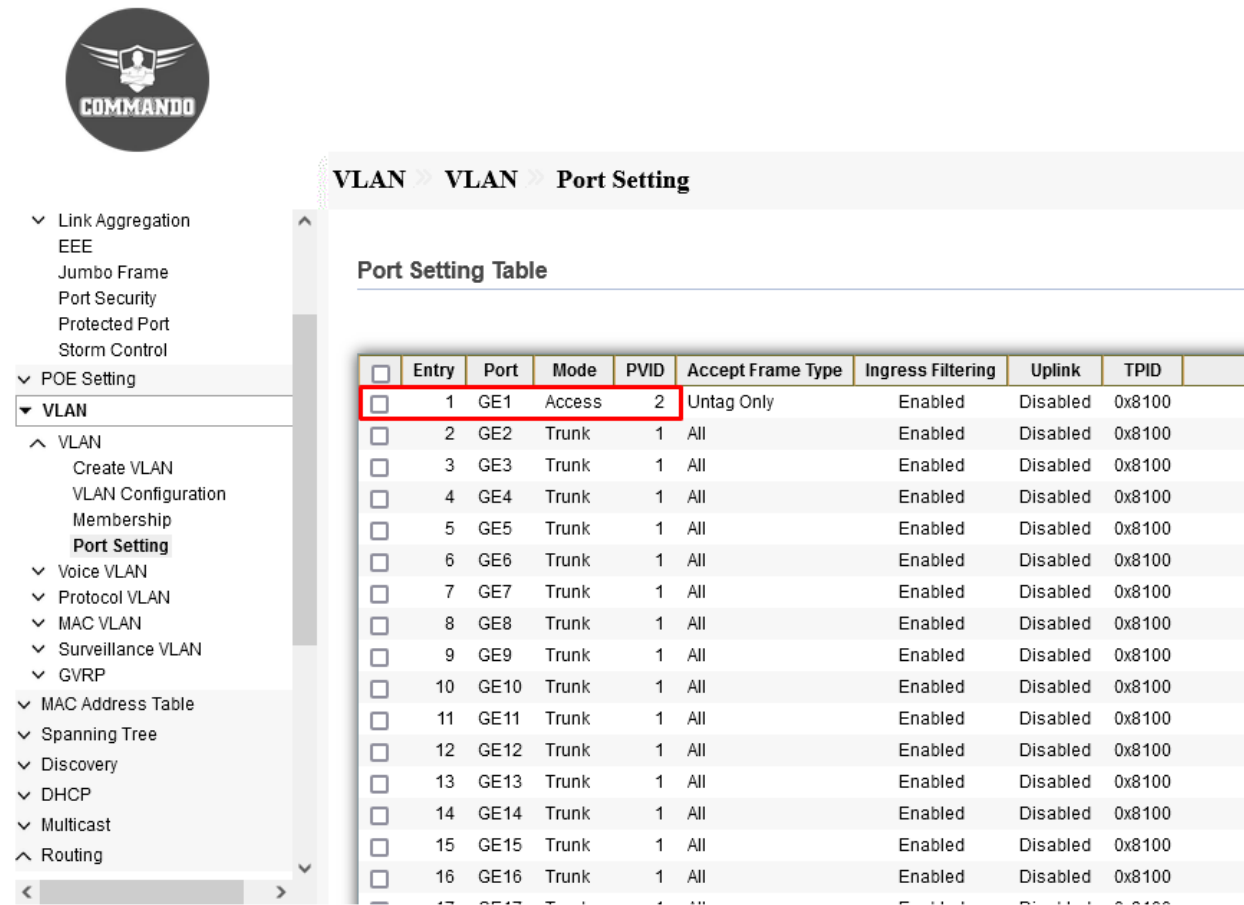



Fig 11.4.8 New VLAN membership Table page

Step 4: Enable OSPF



Routing » Ospf Routes Management » Ospf Routes Setting

OSPF Routes Info

OSPF Routes status Enable

Apply

Area Network Setting table


Showing All entries Showing 0 to 0 of 0 entries

Area Id	Network Ipv4 Address	Network Mask
0 results found.		

Add Delete

- Status
- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interface
 - IPv4 Interface
 - IPv4 Routes
 - ARP
 - IPv6 Management and Interface
 - Rip Routes Management
 - Rip Routes Setting
 - Ospf Routes Management
 - Ospf Routes Setting**
- Security
- ACL
- QoS

Fig 11.4.9 Default OSPF route setting Page



Save | Logout | Reboot | Debug

Routing » Ospf Routes Management » Ospf Routes Setting

OSPF Routes Info

OSPF Routes status Enable

Apply

Area Network Setting table

Showing All entries Showing 0 to 0 of 0 entries

Area Id	Network Ipv4 Address	Network Mask
0 results found.		

Add Delete

First Previous 1 Next Last

- Status
- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing**
 - IPv4 Management and Interface
 - IPv4 Interface
 - IPv4 Routes
 - ARP
 - IPv6 Management and Interface
 - Rip Routes Management
 - Rip Routes Setting
 - Ospf Routes Management
 - Ospf Routes Setting**
- Security
- ACL
- QoS

Fig 11.4.10 Enabling OSPF in Switch Page

Note: After Enabling OSPF then only you can add the connected network's ID in the OSPF Process.

Step 5: Add connected Network ID to OSPF

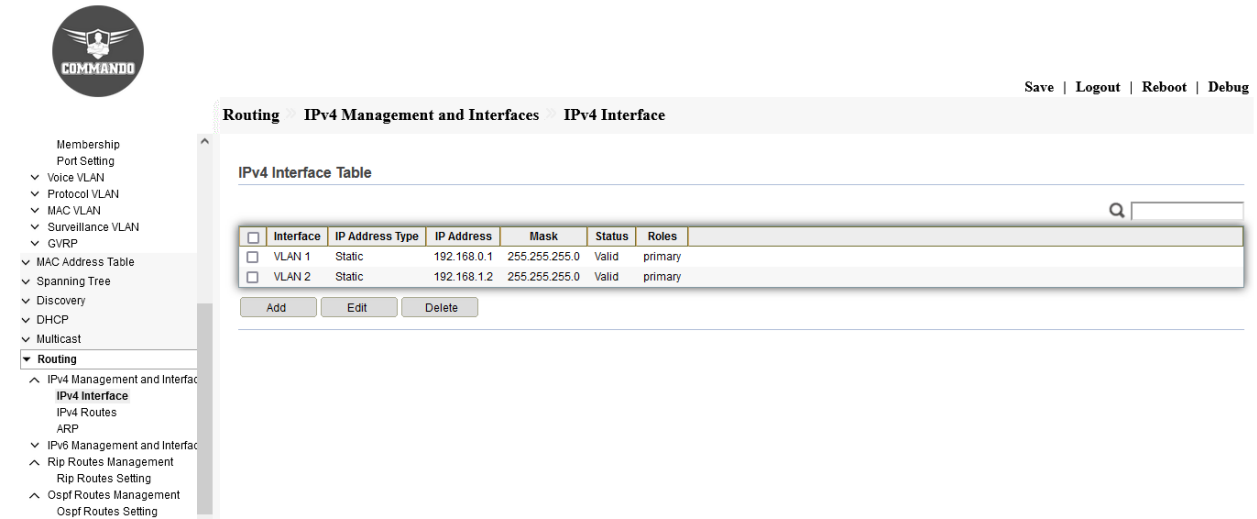


Fig 11.4.11 To know connected Network in switch page

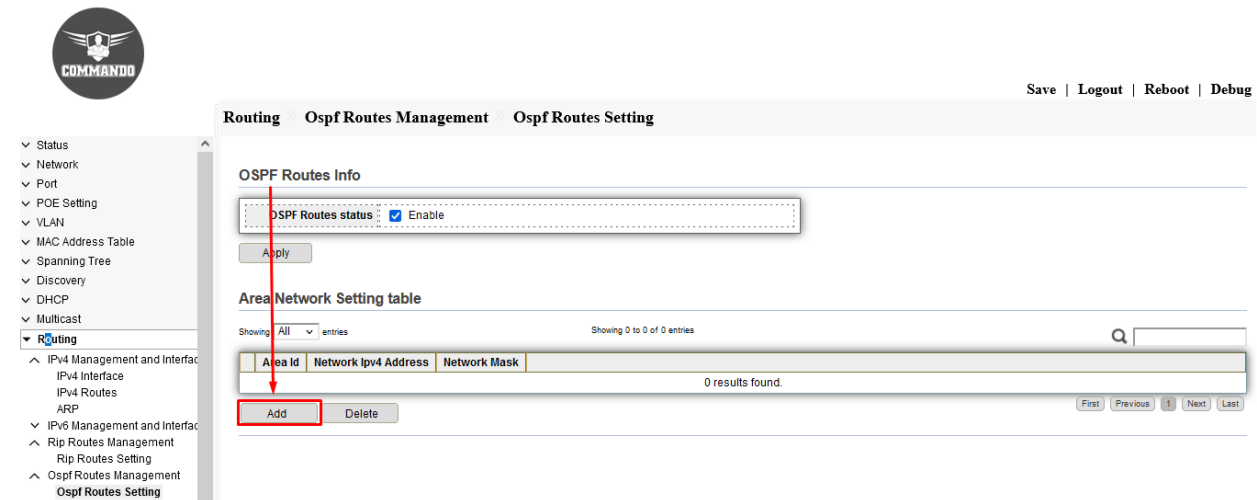


Fig 11.4.12 Add Connected Network ID in OSPF Process Page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ **Routing**
 - ▲ IPv4 Management and Interface
 - IPv4 Interface
 - IPv4 Routes
 - ARP
 - ▼ IPv6 Management and Interface
 - ▲ Rip Routes Management
 - Rip Routes Setting
 - ▲ Ospf Routes Management
 - Ospf Routes Setting**

Routing » Ospf Routes Management » Ospf Routes Setting

Area Network Setting table

Area Id	<input type="text" value="0.0.0.0"/>	A.B.C.D
Network Ipv4 Address	<input type="text" value="192.168.0.0"/>	
Network Mask	<input type="text" value="255.255.255.0"/>	

Fig 11.4.13 Network ID setting in OSPF Page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ **Routing**
 - ▲ IPv4 Management and Interface
 - IPv4 Interface
 - IPv4 Routes
 - ARP
 - ▼ IPv6 Management and Interface
 - ▲ Rip Routes Management
 - Rip Routes Setting
 - ▲ Ospf Routes Management
 - Ospf Routes Setting**

Routing » Ospf Routes Management » Ospf Routes Setting

OSPF Routes Info

OSPF Routes status Enable

Area Network Setting table

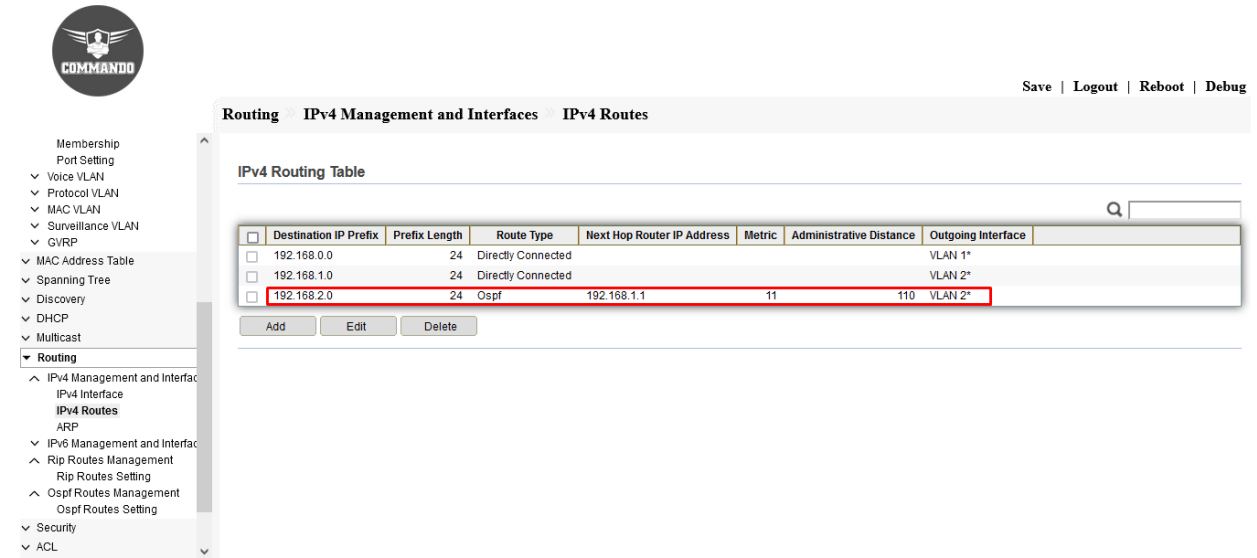
Showing entries

Showing 1 to 2 of 2 entries

	Area Id	Network Ipv4 Address	Network Mask
<input type="checkbox"/>	0.0.0.0	192.168.0.0	255.255.255.0
<input type="checkbox"/>	0.0.0.0	192.168.1.0	255.255.255.0

Fig 11.4.14 Network ID setting Table page

Step 6: Check OSPF Route



The screenshot displays the COMMANDO network management interface. On the left is a navigation menu with categories like Membership, Port Setting, Voice VLAN, Protocol VLAN, MAC VLAN, Surveillance VLAN, GVRP, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, IPv4 Management and Interfaces, IPv6 Management and Interfaces, Rip Routes Management, Ospf Routes Management, Security, and ACL. The 'Routing' section is expanded to show 'IPv4 Management and Interfaces' and 'IPv4 Routes'. The main content area is titled 'IPv4 Routing Table' and contains a table with the following data:


<input type="checkbox"/>	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
<input type="checkbox"/>	192.168.0.0	24	Directly Connected				VLAN 1*
<input type="checkbox"/>	192.168.1.0	24	Directly Connected				VLAN 2*
<input type="checkbox"/>	192.168.2.0	24	Ospf	192.168.1.1	11	110	VLAN 2*

Below the table are three buttons: 'Add', 'Edit', and 'Delete'. The OSPF route row is highlighted with a red border.

Fig 11.4.15 OSPF Learned Routing Table page

Chapter 12 Security

Group Header: Security

After clicking Security , following four corresponding web pages tabs are opened.

RADIUS: This page allow user to add, edit or delete RADIUS server settings and modify default parameter of RADIUS server. Remote Authorization Dial-In User Service (RADIUS) servers provide a centralized 802.1X or MAC-based network access control. The device can be configured to be a RADIUS client that can use a RADIUS server to provide centralized security, and as a RADIUS server.

TACACS+: TACACS (Terminal Access Controller Access Control System plus) that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

AAA: An AAA server is a server program that handles user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting (AAA) services. Authentication is the process of identifying an individual, usually based on a username and password.

Method List: AAA Method Lists can be used to assign a list of methods for Authentication, Authorization, Accounting. Methods Lists can be used to specify the order. If authentication service is not available or was not successful from the first method, second method can be used and so on.

Login Authentication: You can assign authentication methods to the various management access methods, such as SSH, Telnet, HTTP, and HTTPS. The authentication can be performed locally or on a RADIUS/TACACS+ server. Login authenticate with a username and password that is part of the configuration of the security appliance.

Authentication Manager: You can control access to your network through Switch by using authentication methods such as 802.1X, MAC Based and Web Based.

Property: Authentication manager implementation that delegates responsibility for authentication to one or more authentication providers.

Port Setting: The authentication manager port setting page control all the authentication methods, such as 802.1x, MAC authentication. It also handles network authentication requests and enforces authentication per port basis. The Auth Manager maintains operational data for all port-based network connection.

MAC-Based Local Account: Use MAC-based authentication to authenticate devices based on their physical media access control (MAC) address.

WEB-Based Local Account: WEB-Based Local Account can be defined as the process of verifying someone's identity by using pre-required details (Commonly username and password).

Sessions: Displays the web-based authentication settings for the specified interface.

DoS: A Denial of Service (DoS) attack is an attempt to make a switch unavailable to its users. DoS attacks saturate the switch with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a switch CPU overload.

Property: A denial-of-service attack is a malicious attempt to overwhelm switch with traffic to disrupt its normal operations. A denial-of-service (DoS) attack occurs when legitimate users are unable to access and send traffic, or other network resources due to the actions of a malicious attacker. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

Port Setting: You can protect your network against DoS (Denial of Service) attacks from flooding your network with unwanted requests using DoS Protection, block or allow specific client devices to access your network using Access Control, or you can prevent ARP spoofing and ARP attacks using IP & MAC Binding by port setting.

Dynamic ARP Inspection--> Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

Property: DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface). When DAI is enabled, the switch drops ARP packet if the sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database.

Statistics: Displays statistics for forwarded, dropped, MAC validation failure, IP packets.

DHCP Snooping: DHCP snooping is a series of techniques applied to improve the security of a DHCP infrastructure. When DHCP servers are allocating IP addresses to the clients on the LAN, DHCP snooping can be configured on LAN switches to prevent malicious or malformed DHCP traffic, or rogue DHCP servers.

Property: DHCP snooping is a security feature which acts as a firewall between untrusted hosts and trusted DHCP servers. Snooping prevents false DHCP responses and monitor clients. They can prevent man-in-the-middle attacks and authenticate host devices.

Statistics: Display DHCP snooping packet statistic which gives information about trusted ports.

Option82 Property: You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address exhaustion in LAN network.

Option82 Circuit ID: The DHCP Option 82 Circuit ID feature enhances validation security.

IP Source Guard: IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

Port Setting: When IP Source Guard is configured on a port, traffic coming on that port will be dropped unless there is a DHCP snooping entry to allow it.

IMPV Binding: This page allow user to add static IP source guard entry and browse all IP source guard entries that learned by DHCP snooping or statically create by user.

Save Database: This page allow user to configure DHCP snooping database which can backup and restore dynamic DHCP snooping entries.

12.1 RADIUS (Remote Authorization Dial-In User Service)

RADIUS is a protocol that was originally designed to authenticate remote users to a dial-in access server. RADIUS is now used in a wide range of authentication scenarios. The device reads the user name and password. The device creates a message called an Access-Request message and sends it to the RADIUS server. Remote Authorization Dial-In User Service (RADIUS) servers provide a centralized 802.1X or MAC-based network access control. The device is a RADIUS client that can use a RADIUS server to provide centralized security.

An organization can establish a Remote Authorization Dial-In User Service (RADIUS) server to provide centralized 802.1X or MAC-based network access control for all its devices. In this way, authentication and authorization can be handled on a single server for all devices in the organization. To configure and view This page allow user to add, edit or delete RADIUS server settings and modify default parameter of RADIUS server. To configure and view RADIUS, click **Security >> RADIUS**

COMMANDO

Save |

Security > RADIUS

Use Default Parameter

Retry	<input type="text" value="3"/>	(1 - 10, default 3)
Timeout	<input type="text" value="3"/>	Sec (1 - 30, default 3)
Key String	<input type="text"/>	

Apply

RADIUS Table

Showing All entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Server Address	Server Port	Priority	Retry	Timeout	Usage
0 results found.						

Add Edit Delete

Fig 12.1.1 Default RADIUS Table page

RADIUS Configuration:

Click on “Security”, then “RADIUS” from menu. Now Click on “Add”, then select “Address Type [Hostname/IPv4/IPv6]”, Enter “Server Address”, “Server Port”, “Priority”, “Key String”, “Retry”, “Timeout” value & “Usage” and Click on “Apply”.

Configuration object and description:

Address Type: Select the Address Type. There are three options as follows

Hostname: Select the Server by Hostname.

IPv4: Select the IPv4 address type.

IPv6: Select the IPv6 address type.

Server Address: Enter the RADIUS server by IP address.

Server Port: Enter the RADIUS server by Port Number.

Priority: Enter the order in which this RADIUS server is used. Zero is the highest priority RADIUS server and is the first server used. If it cannot establish a session with the high priority server, the device tries the next highest priority server.

Key String: Enter the default key string used for authenticating and encrypting between the device and the RADIUS server. This key must match the key configured on the RADIUS server.

Retry: Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred.

Timeout: Enter the number of seconds that the device waits for an answer from the RADIUS server before retrying the query or switching to the next server.

Usage: Enter the RADIUS server authentication type. The options are:

Login- RADIUS server is used for authenticating users that ask to administer the device.

802.1X- RADIUS server is used for 802.1x authentication.

All-RADIUS server is used for authenticating user that ask to administer the device and for 802.1X authentication.



Security > RADIUS

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
 - RADIUS**
 - TACACS+
 - ▼ AAA
 - ▼ Authentication Manager
 - ▼ DoS
 - ▼ Dynamic ARP Inspection
 - ▼ DHCP Snooping
 - ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Add RADIUS Server

Address Type	<input type="radio"/> Hostname
	<input checked="" type="radio"/> IPv4
	<input type="radio"/> IPv6
Server Address	<input type="text" value="192.168.0.50"/>
Server Port	<input type="text" value="1812"/> (0 - 65535, default 1812)
Priority	<input type="text" value="10"/> (0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default <input type="text"/>
Retry	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 10, default 3)
Timeout	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> Sec (1 - 30, default 3)
Usage	<input type="radio"/> Login
	<input type="radio"/> 802.1X
	<input checked="" type="radio"/> All

Apply Close

Fig 12.1.2 Add RADIUS server page



Save |

Security > RADIUS

- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security**
 - RADIUS**
 - TACACS+
 - AAA
 - Authentication Manager
 - DoS
 - Dynamic ARP Inspection
 - DHCP Snooping
 - IP Source Guard
- ACL
- QoS
- Diagnostics
- Management

Use Default Parameter

Retry	<input type="text" value="3"/>	(1 - 10, default 3)
Timeout	<input type="text" value="3"/>	Sec (1 - 30, default 3)
Key String	<input type="text"/>	

Apply

RADIUS Table

Showing entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Server Address	Server Port	Priority	Retry	Timeout	Usage
<input type="checkbox"/>	192.168.0.50	1812	10	3	3	All

Add Edit Delete

Fig 12.1.3 RADIUS Table page

12.2 TACACS+ (Terminal Access Controller Access Control Server Plus)

TACACS+, stands for Terminal Access Controller Access Control Server, is a security protocol used in AAA framework to provide centralized authentication for users who want to gain access to the network. The TACACS+ protocol provides detailed accounting information and flexible administrative control over the authentication, authorization, and accounting process. TACACS+ uses Transmission Control Protocol (TCP) for its transport. TACACS+ provides security by encrypting all traffic between the NAS and the process. An organization can establish a Terminal Access Controller Access Control System (TACACS+) server to provide centralized security for all of its devices. In this way, authentication and authorization can be handled on a single server for all devices in the organization. This page to add, edit or delete TACACS+ server settings and modify default parameter of TACACS+ server.

To view and configure TACACS+, click **Security >> TACACS+**

The screenshot shows the COMMANDO web interface. On the left is a navigation menu with categories like Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, RADIUS, TACACS+, AAA, Authentication Manager, DoS, Dynamic ARP Inspection, DHCP Snooping, IP Source Guard, ACL, QoS, Diagnostics, and Management. The 'Security' menu is expanded, and 'TACACS+' is selected. The main content area is titled 'Security > TACACS+'. It features a 'Use Default Parameter' section with a 'Timeout' field containing '5' and a 'Key String' field. Below this is an 'Apply' button. The 'TACACS+ Table' section shows a table with columns for 'Server Address', 'Server Port', 'Priority', and 'Timeout'. The table is currently empty, displaying 'Showing 0 to 0 of 0 entries' and '0 results found.' Below the table are 'Add', 'Edit', and 'Delete' buttons. A 'Save' link is visible in the top right corner.

Fig 12.2.1 Default TACACS+ Table page

TACACS+ Configuration:

Click on “Security”, then “TACACS+” from menu. Now Click on “Add”, then select “Address Type [Hostname/IPv4/IPv6]”, Enter “Server Address”, “Server Port”, “Priority”, “Key String”, “Timeout” value and Click on “Apply”.

Configuration object and description:

Address Type: Select the Address Type. The Three options like Hostname, IPv4, IPv6.

Hostname: Select the Server by Hostname.

IPv4: Select the IPv4 address type.

IPv6: Select the IPv6 address type.

Server Address: Enter the TACACS+ server by IP address.

Server Port: Enter the TACACS+ server by Port Number.

Priority: Enter the order in which this TACACS+ server is used. Zero is the highest priority TACACS+ server and is the first server used. If it cannot establish a session with the high priority server, the device tries the next highest priority server.

Key String: Enter the default key string used for authenticating and encrypting between the device and the TACACS+ server. This key must match the key configured on the TACACS+ server.

Timeout: Enter the amount of time that passes before the connection between the device and the TACACS+ server times out.

Authentication: Provides authentication of regular and 802.1X users logging onto the device by using usernames and user-defined passwords.

Authorization: Performed at login. After the authentication session is completed, an authorization session starts using the authenticated username. The RADIUS server then checks user privileges.

Accounting: Enable accounting of login sessions using the RADIUS server. This enables a system administrator to generate accounting reports from the RADIUS server.



- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+**
 - ✓ AAA
 - ✓ Authentication Manager
 - ✓ DoS
 - ✓ Dynamic ARP Inspection
 - ✓ DHCP Snooping
 - ✓ IP Source Guard
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Save

Security > TACACS+

Add TACACS+ Server

Address Type	<input type="radio"/> Hostname
	<input checked="" type="radio"/> IPv4
	<input type="radio"/> IPv6
Server Address	<input type="text" value="192.168.0.50"/>
Server Port	<input type="text" value="49"/> (0 - 65535, default 49)
Priority	<input type="text" value="2"/> (0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default
	<input type="text"/>
Timeout	<input checked="" type="checkbox"/> Use Default
	<input type="text" value="5"/> Sec (1 - 30, default 5)

Fig 12.2.2 Add TACACS+ server page



- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+**
 - ✓ AAA
 - ✓ Authentication Manager
 - ✓ DoS
 - ✓ Dynamic ARP Inspection
 - ✓ DHCP Snooping
 - ✓ IP Source Guard
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Save |

Security > TACACS+

Use Default Parameter	
Timeout	<input type="text" value="5"/> Sec (1 - 30, default 5)
Key String	<input type="text"/>

TACACS+ Table

Showing entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Server Address	Server Port	Priority	Timeout
<input type="checkbox"/>	192.168.0.50	49	2	5

Fig 12.2.3 TACACS+ table page

12.3 AAA

Authentication, authorization, and accounting (AAA) is a system for tracking user activities on an IP-based network and controlling their access to network resources. AAA is often implemented as a dedicated server. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is permitted access to the network. If the credentials do not match, authentication fails, and network access is denied.

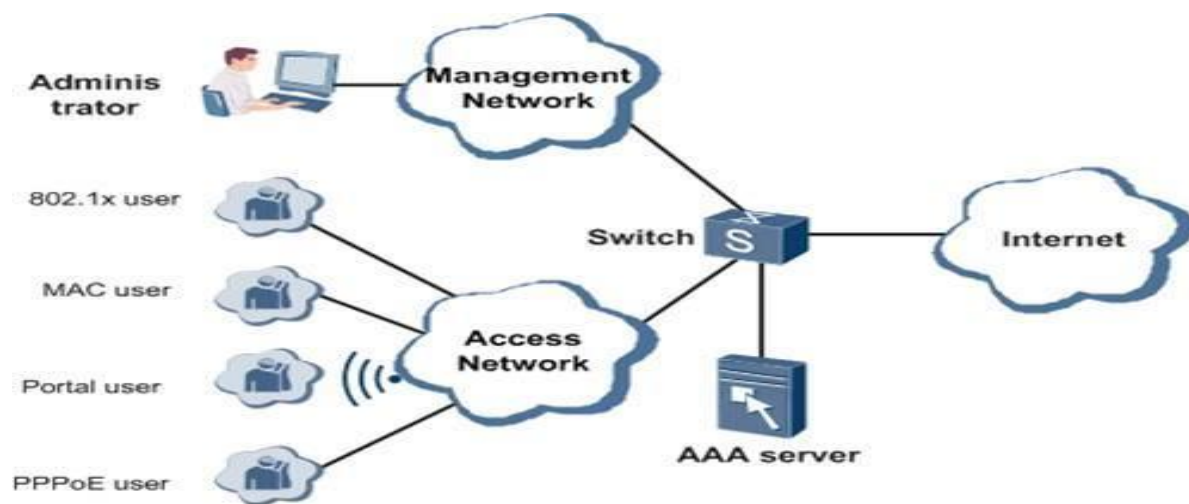
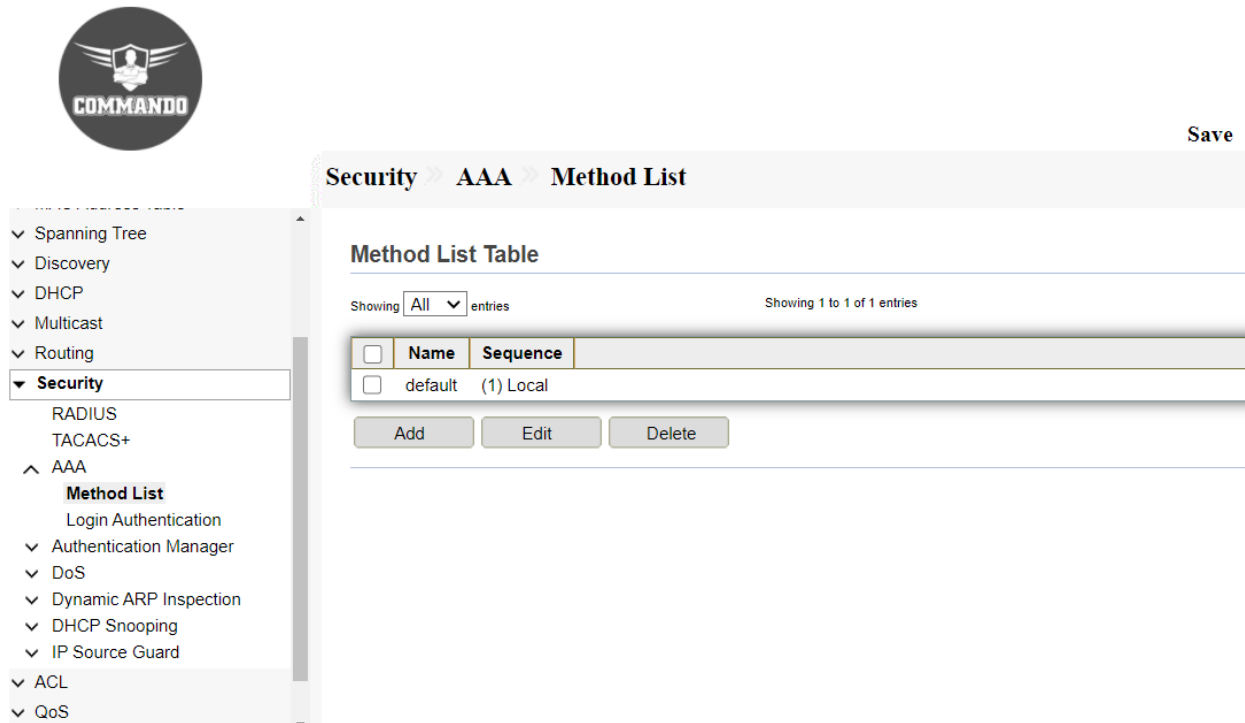


Fig 12.3.1 AAA Server Concept

12.3.1 AAA Method List

AAA stands for authentication, authorization, and accounting. AAA is a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. AAA provides authentication, authorization, and accounting functions for users, preventing unauthorized users from logging in to a switch and improving system security. AAA Method Lists can be used to assign a list of methods for Authentication, Authorization, Accounting. Methods Lists can be used to specify the order. If authentication service is not available or was not successful from the first method, second method can be used and so on.

To view and configure AAA Method List, click **Security >> AAA >> Method List**.



COMMANDO

Save

Security > AAA > Method List

Method List Table

Showing All entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Name	Sequence
<input type="checkbox"/>	default	(1) Local

Add Edit Delete

Fig 12.3.2 Default AAA Method List table page



- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security**
 - RADIUS
 - TACACS+
 - AAA
 - Method List**
 - Login Authentication
 - Authentication Manager
 - DoS
 - Dynamic ARP Inspection
 - DHCP Snooping
 - IP Source Guard
- ACL
- QoS
- Diagnostics
- Management

Security >> AAA >> Method List

Add Method List

Name	COMMANDO
Method 1	<input type="radio"/> Empty <input type="radio"/> None <input checked="" type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+
Method 2	<input type="radio"/> Empty <input type="radio"/> None <input type="radio"/> Local <input checked="" type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+
Method 3	<input type="radio"/> Empty <input type="radio"/> None <input type="radio"/> Local <input type="radio"/> Enable <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+
Method 4	<input type="radio"/> Empty <input type="radio"/> None <input checked="" type="radio"/> Local <input type="radio"/> Enable <input type="radio"/> RADIUS <input type="radio"/> TACACS+

Fig 12.3.3 Edit AAA Method List page



Save |

Security > AAA > Method List

- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ^ AAA
 - Method List**
 - Login Authentication
 - ✓ Authentication Manager
 - ✓ DoS
 - ✓ Dynamic ARP Inspection
 - ✓ DHCP Snooping
 - ✓ IP Source Guard
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Method List Table

Showing All entries

Showing 1 to 2 of 2 entries

<input type="checkbox"/>	Name	Sequence
<input type="checkbox"/>	default	(1) Local
		(1) Local
<input type="checkbox"/>	COMMANDO	(2) Enable
		(3) RADIUS
		(4) Local

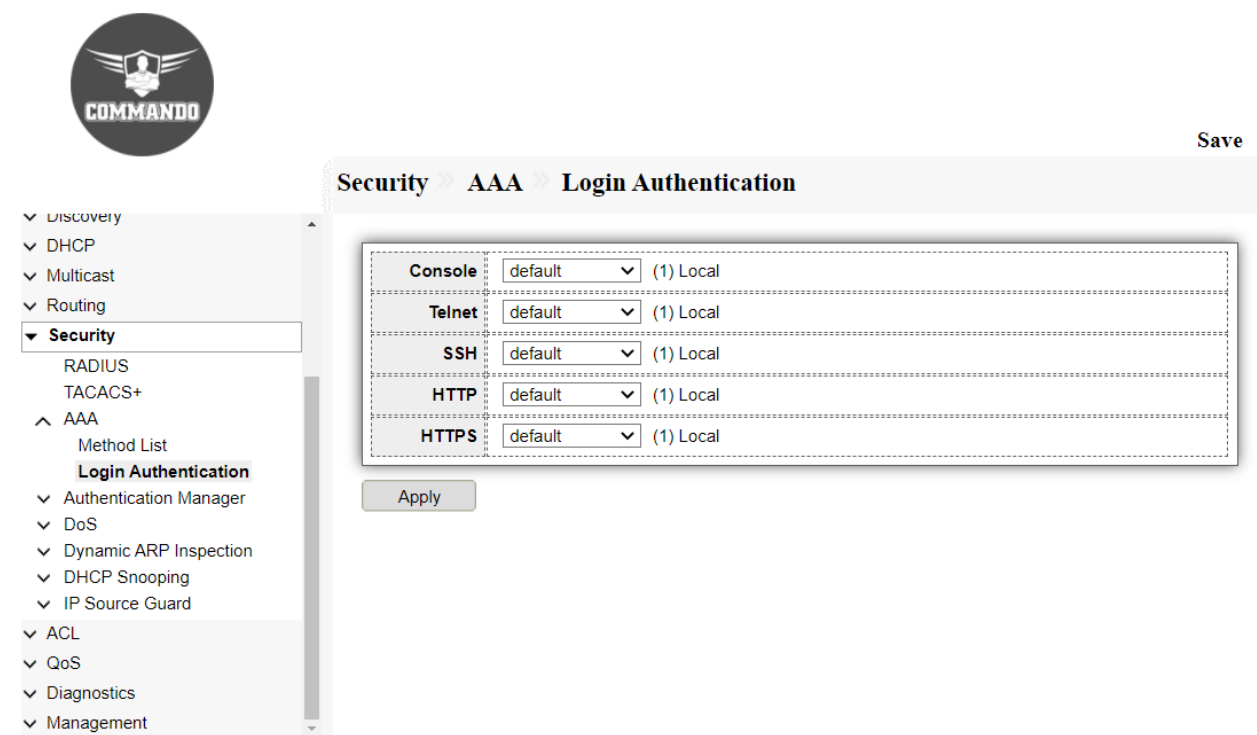
Add Edit Delete

Fig 12.3.4 AAA Method List Table page

12.3.2 Login Authentication

Local AAA means that you are performing AAA without the use of an external database. When performing local AAA, you can authenticate with a username and password that is part of the configuration of the switch. Authentication is based on each user having a unique set of login credentials for gaining network access. The AAA server compares a user's authentication credentials with other user credentials stored in a AAA database.

To view and configure the login authentication, click **Security >> AAA >> Login Authentication**.



The screenshot shows the COMMANDO web interface for configuring AAA Login Authentication. The breadcrumb path is **Security > AAA > Login Authentication**. A **Save** button is located in the top right corner. On the left, a navigation tree is visible with the following items: Discovery, DHCP, Multicast, Routing, **Security** (expanded), RADIUS, TACACS+, AAA (expanded), Method List, **Login Authentication** (highlighted), Authentication Manager, DoS, Dynamic ARP Inspection, DHCP Snooping, IP Source Guard, ACL, QoS, Diagnostics, and Management.

The main configuration area contains a table with the following settings:

Console	default	(1) Local
Telnet	default	(1) Local
SSH	default	(1) Local
HTTP	default	(1) Local
HTTPS	default	(1) Local

Below the table is an **Apply** button.

Fig 12.3.5 AAA Login Authentication page



Save

Security > AAA > Login Authentication

- Discovery
- DHCP
- Multicast
- Routing
- Security**
 - RADIUS
 - TACACS+
 - AAA
 - Method List
 - Login Authentication**
 - Authentication Manager
 - DoS
 - Dynamic ARP Inspection
 - DHCP Snooping
 - IP Source Guard
- ACL
- QoS
- Diagnostics
- Management

Console	default	(1) Local
Telnet	COMMANDO	(1) Local (2) Enable (3) RADIUS (4) Local
SSH	default	(1) Local
HTTP	default	(1) Local
HTTPS	COMMANDO	(1) Local (2) Enable (3) RADIUS (4) Local

Apply

Fig 12.3.6 Setting AAA Login Authentication page

12.4 Authentication Manager

You can control access to your network through Switch by using authentication methods such as 802.1X, MAC Based and Web Based. Authentication prevents unauthenticated devices and users from gaining access to your LAN. For 802.1X and MAC Based authentication, end devices must be authenticated before they receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server.

12.4.1 Property

These are the following Authentication Type:

802.1X: Use IEEE 802.1x to do authentication

MAC-Based: Use MAC address to do authentication

WEB-Based: Use MAC address to do authentication

To view and configure Authentication Manager Property, click **Security >> Authentication Manager >> Property**.

The screenshot displays the COMMANDO web interface for configuring the Authentication Manager Property. The breadcrumb trail indicates the path: Security > Authentication Manager > Property. The configuration form includes the following fields:

- Authentication Type:** Radio buttons for 802.1x, MAC-Based, and WEB-Based.
- Guest VLAN:** A radio button for Enable and a dropdown menu.
- MAC-Based User ID Format:** A dropdown menu showing 'XXXXXXXXXX'.

Below the configuration form is the **Port Mode Table**, which lists the authentication settings for various ports:

Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode	
		802.1x	MAC-Based	WEB-Based						
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Fig 12.4.1 Default Authentication Manager Port Mode Table page



Security > Authentication Manager > Property

- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
 - RADIUS
 - TACACS+
 - ✓ AAA
 - ^ Authentication Manager
 - Property
 - Port Setting
 - MAC-Based Local Account
 - WEB-Based Local Account
 - Sessions
 - ✓ DoS
 - ✓ Dynamic ARP Inspection
 - ✓ DHCP Snooping
 - ✓ IP Source Guard
 - ✓ ACL

Authentication Type 802.1x
 MAC-Based
 WEB-Based

Guest VLAN Enable
1

MAC-Based User ID Format

Apply

Port Mode Table

	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
<input checked="" type="checkbox"/>	1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input checked="" type="checkbox"/>	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input checked="" type="checkbox"/>	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Fig 12.4.2 Authentication Manager Selecting Ports page



- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▲ Authentication Manager
 - Property
 - Port Setting
 - MAC-Based Local Account
 - WEB-Based Local Account
 - Sessions
 - ▼ DoS
 - ▼ Dynamic ARP Inspection
 - ▼ DHCP Snooping
 - ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Security > Authentication Manager > Property

Edit Port Mode

Port	GE1-GE3	
Authentication Type	<input checked="" type="checkbox"/> 802.1x	
	<input checked="" type="checkbox"/> MAC-Based	
	<input type="checkbox"/> WEB-Based	
Host Mode	<input type="radio"/> Multiple Authentication	
	<input type="radio"/> Multiple Hosts	
	<input checked="" type="radio"/> Single Host	
Order	Available Type	Select Type
	WEB-Based	802.1x MAC-Based
Method	Available Method	Select Method
		RADIUS Local
Guest VLAN	<input checked="" type="checkbox"/> Enable	
VLAN Assign Mode	<input type="radio"/> Disable	
	<input type="radio"/> Reject	
	<input checked="" type="radio"/> Static	

Apply Close

Fig 12.4.3 Authentication Manager Property edit page



Security > Authentication Manager > Property

Authentication Type

802.1x

MAC-Based

WEB-Based

Guest VLAN

Enable

1

MAC-Based User ID Format

XXXXXXXXXXXX

Apply

Port Mode Table

	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
<input type="checkbox"/>	1	GE1	Enabled	Enabled	Disabled	Single Host	802.1x, MAC-Based	RADIUS, Local	Enabled	Static
<input type="checkbox"/>	2	GE2	Enabled	Enabled	Disabled	Single Host	802.1x, MAC-Based	RADIUS, Local	Enabled	Static
<input type="checkbox"/>	3	GE3	Enabled	Enabled	Disabled	Single Host	802.1x, MAC-Based	RADIUS, Local	Enabled	Static
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Fig 12.4.4 Authentication Manager Property Port Mode Table page

12.4.2 Port Setting

802.1X: 802.1X is an IEEE standard for port-based network access control (PNAC). It provides an authentication mechanism for devices seeking to access a LAN.

During the authentication process, the switch completes multiple message exchanges between the end device and the authentication server. While 802.1X authentication is in process, only 802.1X traffic and control traffic can transit through the network.

To view and configure the Authentication Manager Port Setting, click **Security >> Authentication Manager >> Port Setting**.

COMMANDO

Save | Logout | Reboot

Security > Authentication Manager > Port Setting

Port Setting Table

Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters			Web-Based Parameters		
					Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login	
<input type="checkbox"/>	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	16	GE16	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	17	GE17	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	18	GE18	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	19	GE19	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	20	GE20	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	21	GF71	Disabled	Disabled	256	3600	60	60	30	30	30	2	3

Fig 12.4.5 Authentication Manager Property Port Mode Table page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▲ Authentication Manager
 - Property
 - Port Setting**
 - MAC-Based Local Account
 - WEB-Based Local Account
 - Sessions
 - ▼ DoS
 - ▼ Dynamic ARP Inspection
 - ▼ DHCP Snooping
 - ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Port Setting Table

<input checked="" type="checkbox"/>	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters				Web-Based Parameters	
						Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login	
<input checked="" type="checkbox"/>	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	16	GE16	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	17	GE17	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	18	GE18	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	19	GE19	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	20	GE20	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	
<input checked="" type="checkbox"/>	21	GE21	Disabled	Disabled	256	3600	60	60	30	30	30	2	3	

Fig 12.4.6 Authentication Manager Property Selecting Port page



Security > Authentication Manager > Port Setting

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▲ Authentication Manager
 - Property
 - Port Setting
 - MAC-Based Local Account
 - WEB-Based Local Account
 - Sessions
 - ▼ DoS
 - ▼ Dynamic ARP Inspection
 - ▼ DHCP Snooping
 - ▼ IP Source Guard
 - ▼ ACL
 - ▼ QoS
 - ▼ Diagnostics
 - ▼ Management

Edit Port Setting

Port	GE1-GE28		
Port Control	<input type="radio"/> Disabled <input checked="" type="radio"/> Force Authorized <input type="radio"/> Force Unauthorized <input type="radio"/> Auto		
Reauthentication	<input type="checkbox"/> Enable		
Max Hosts	<input type="text" value="256"/>	(1 - 256, default 256)	
Common Timer			
Reauthentication	<input type="text" value="360000"/>	Sec (300 - 2147483647, default 3600)	
Inactive	<input type="text" value="600"/>	Sec (60 - 65535, default 60)	
Quiet	<input type="text" value="600"/>	Sec (0 - 65535, default 60)	
802.1x Parameters			
TX Period	<input type="text" value="30"/>	Sec (1 - 65535, default 30)	
Supplicant Timeout	<input type="text" value="30"/>	Sec (1 - 65535, default 30)	
Server Timeout	<input type="text" value="30"/>	Sec (1 - 65535, default 30)	
Max Request	<input type="text" value="2"/>	(1 - 10, default 2)	
Web-Based Parameters			
Max Login	<input type="text" value="3"/>	(3 - 10, default 3)	

Apply Close

Fig 12.4.7 Authentication Manager Property edit port setting page



Save | Logout | Reboot | Debug

Security > Authentication Manager > Port Setting

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▲ Authentication Manager
 - Property
 - Port Setting
 - MAC-Based Local Account
 - WEB-Based Local Account
 - Sessions
 - ▼ DoS
 - ▼ Dynamic ARP Inspection
 - ▼ DHCP Snooping

Port Setting Table

Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters				Web-Based Parameters	
					Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login	
<input type="checkbox"/>	1	GE1	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	2	GE2	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	3	GE3	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	4	GE4	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	5	GE5	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	6	GE6	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	7	GE7	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	8	GE8	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	9	GE9	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	10	GE10	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	11	GE11	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	12	GE12	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	13	GE13	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	14	GE14	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	15	GE15	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3
<input type="checkbox"/>	16	GE16	Force Authorized	Disabled	256	360000	600	600	30	30	30	2	3

Fig 12.4.8 Authentication Manager Port setting table page

12.4.3 MAC-Based Local Account

The 802.1X authentication method only works if the end device is 802.1X-enabled, but many single-purpose network devices such as printers and IP phones do not support the 802.1X protocol. You can configure MAC RADIUS authentication on interfaces that are connected to network devices that do not support 802.1X and for which you want to allow to access the LAN. When an end device that is not 802.1X-enabled is detected on the interface, the switch transmits the MAC address of the device to the authentication server. The server then tries to match the MAC address with a list of MAC addresses in its database. If the MAC address matches an address in the list, the end device is authenticated.

To view and configure MAC-Based Local Account, click **Security >> Authentication Manger >> MAC-Based Local Account**.

MAC-Based Configuration:

Click on "Security", then "Authentication Manager" >> "MAC-Based Local Account" from menu. Click on "Add" & enter "MAC Address" Select "Port Control [Force Authorized/ Force Unauthorized/Auto]" & Enter "VLAN" ID.

Next enter Assigned Timer parameters like "Reauthentication", "Inactive" value & Click on "Apply".

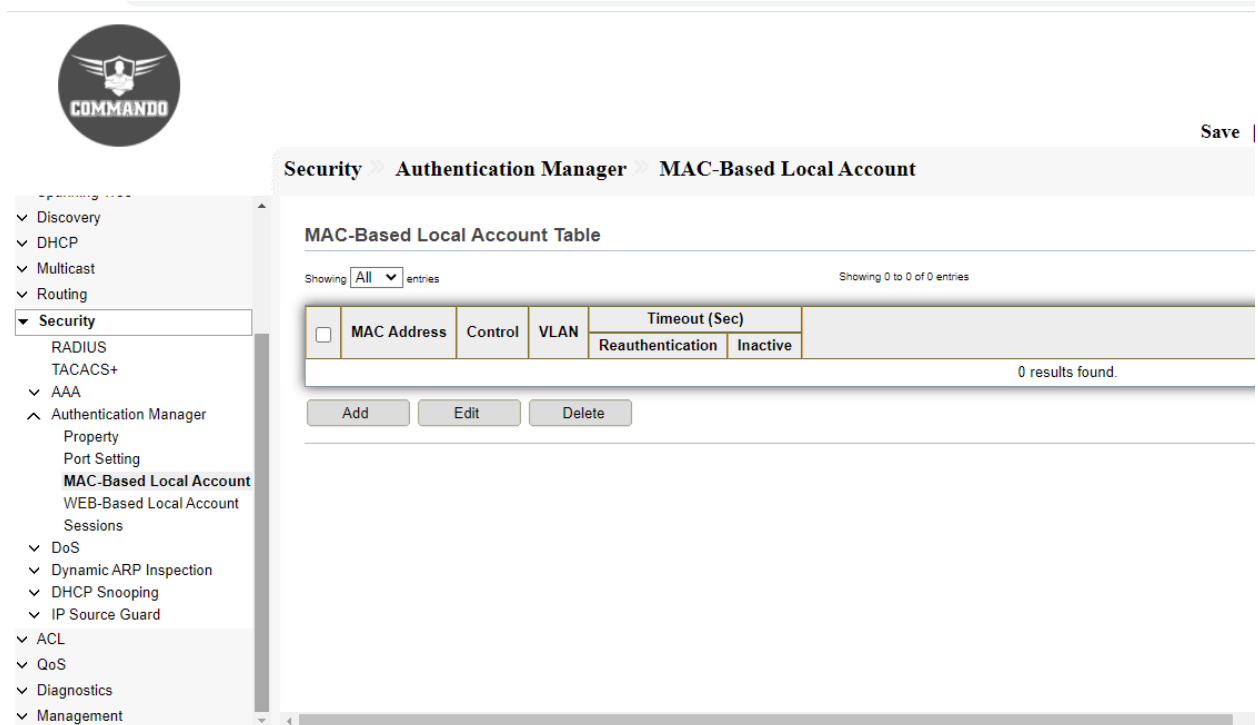


Fig 12.4.9 Authentication Manager Default MAC -Based Local Account page

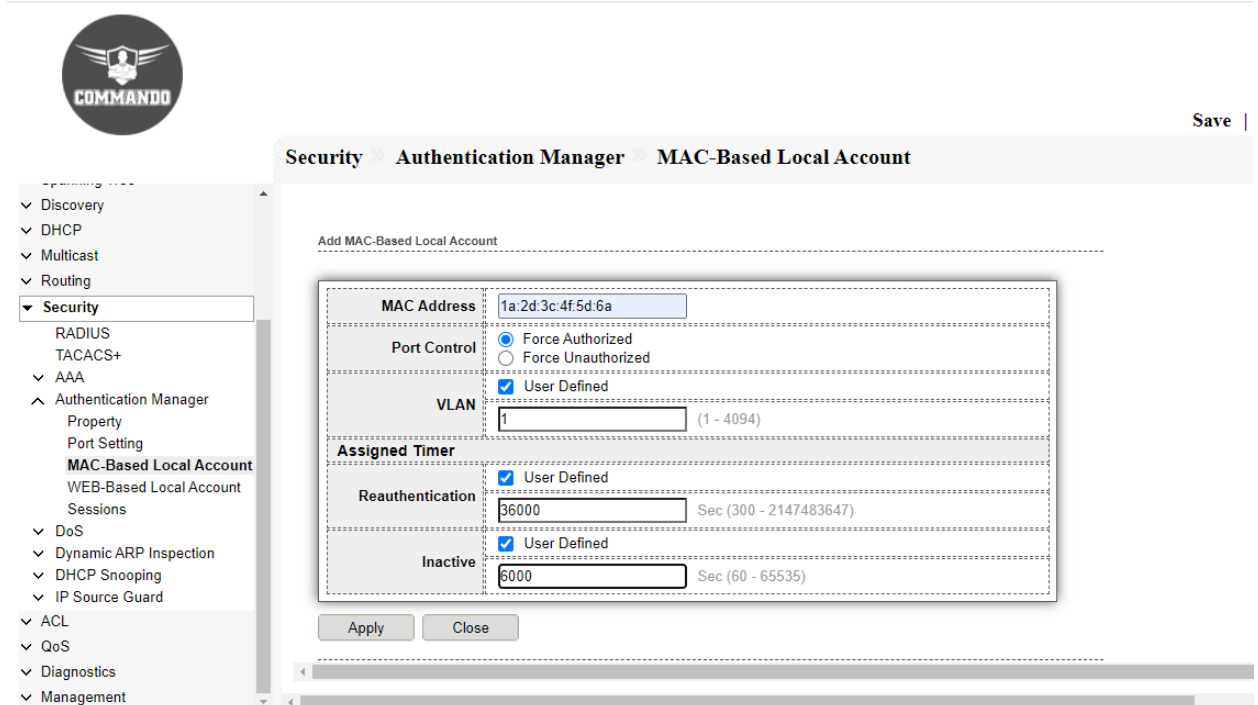


Fig 12.4.10 Authentication Manager MAC -Based user defined Local Account page



Save

Security > Authentication Manager > MAC-Based Local Account

MAC-Based Local Account Table

Showing **All** entries Showing 1 to 1 of 1 entries

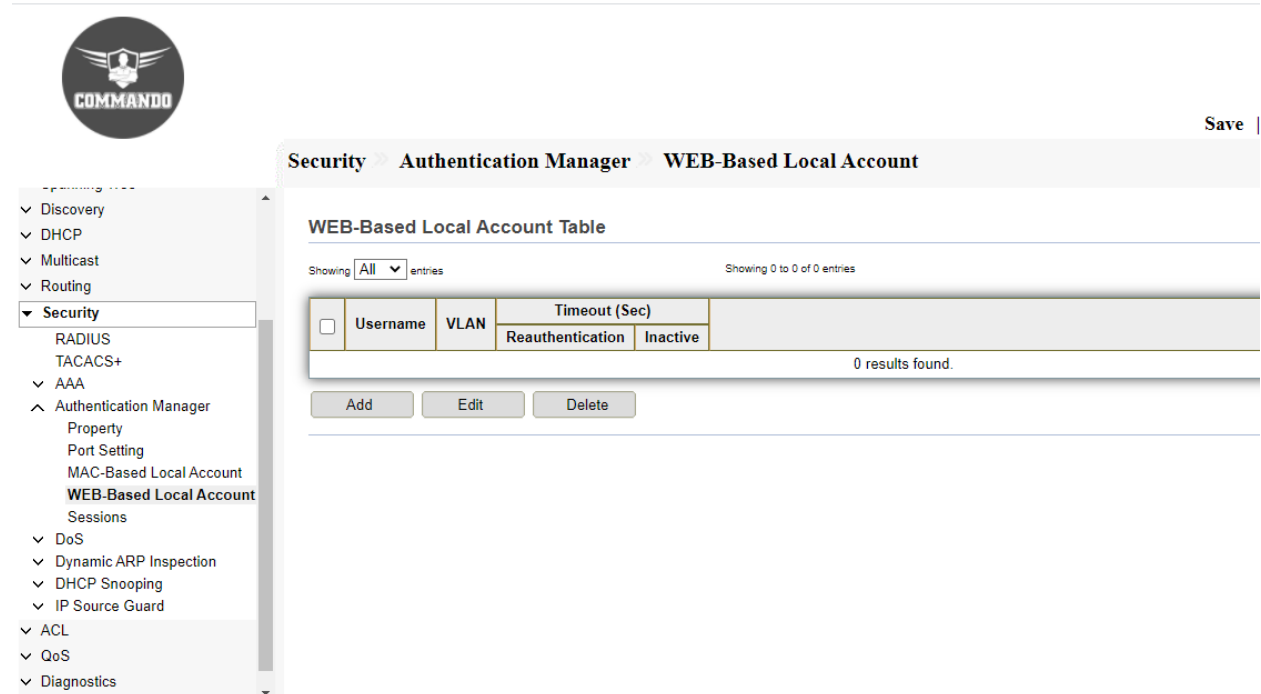
<input type="checkbox"/>	MAC Address	Control	VLAN	Timeout (Sec)	
				Reauthentication	Inactive
<input type="checkbox"/>	1A:2D:3C:4F:5D:6A	Force Authorized	1	36000	6000

Fig 12.4.11 MAC -Based user defined Local Account Table page

12.4.4 WEB-Based Local Account

WEB-Based authentication enables you to authenticate users on switches by redirecting Web browser requests to a login page that requires users to input a valid username and password before they can access the network.

To view and configure WEB-Based Local Account, click **Security >> Authentication Manger >> WEB-Based Local Account**.



The screenshot displays the Commando network management interface. On the left is a navigation sidebar with a tree structure. The 'Security' menu is expanded, showing sub-items like RADIUS, TACACS+, AAA, Authentication Manager, DoS, Dynamic ARP Inspection, DHCP Snooping, IP Source Guard, ACL, QoS, and Diagnostics. Under 'Authentication Manager', 'WEB-Based Local Account' is selected. The main content area shows the configuration page for 'WEB-Based Local Account'. At the top right, there is a 'Save' link. Below the breadcrumb 'Security > Authentication Manager > WEB-Based Local Account', the page title 'WEB-Based Local Account Table' is displayed. A dropdown menu shows 'Showing All entries' and 'Showing 0 to 0 of 0 entries'. A table with the following structure is shown:

	Username	VLAN	Timeout (Sec)	
			Reauthentication	Inactive
0 results found.				

Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

Fig 12.4.12 Default WEB-Based Local Account Table page

WEB-Based Configuration:

Click on “Security”, then “Authentication Manager” >> ” WEB-Based Local Account” from menu. Click on “Add” & enter “Username”, “Password” and “VLAN” ID.

Next enter Assigned Timer parameters like “Reauthentication”, “Inactive” value. &Click on “Apply”.



Save |

Security > Authentication Manager > WEB-Based Local Account

- Discovery
- DHCP
- Multicast
- Routing
- Security
 - RADIUS
 - TACACS+
 - AAA
 - Authentication Manager
 - Property
 - Port Setting
 - MAC-Based Local Account
 - WEB-Based Local Account
 - Sessions
 - DoS
 - Dynamic ARP Inspection
 - DHCP Snooping
 - IP Source Guard
 - ACL
 - QoS
 - Diagnostics

Add WEB-Based Local Account

Username	COMMANDOPC
Password	*****
Confirm Password	*****
VLAN	<input checked="" type="checkbox"/> User Defined 1 (1 - 4094)
Assigned Timer	
Reauthentication	<input checked="" type="checkbox"/> User Defined 360 Sec (300 - 2147483647)
Inactive	<input checked="" type="checkbox"/> User Defined 600 Sec (60 - 65535)

Apply Close

Fig 12.4.13 Add WEB-Based Local Account page



Save |

Security > Authentication Manager > WEB-Based Local Account

- Discovery
- DHCP
- Multicast
- Routing
- Security
 - RADIUS
 - TACACS+
 - AAA
 - Authentication Manager
 - Property
 - Port Setting
 - MAC-Based Local Account
 - WEB-Based Local Account
 - Sessions
 - DoS
 - Dynamic ARP Inspection
 - DHCP Snooping
 - IP Source Guard
 - ACL
 - QoS
 - Diagnostics
 - Management

WEB-Based Local Account Table

Showing All entries

Showing 1 to 1 of 1 entries

	Username	VLAN	Timeout (Sec)	
			Reauthentication	Inactive
<input type="checkbox"/>	COMMANDOPC	1	360	600

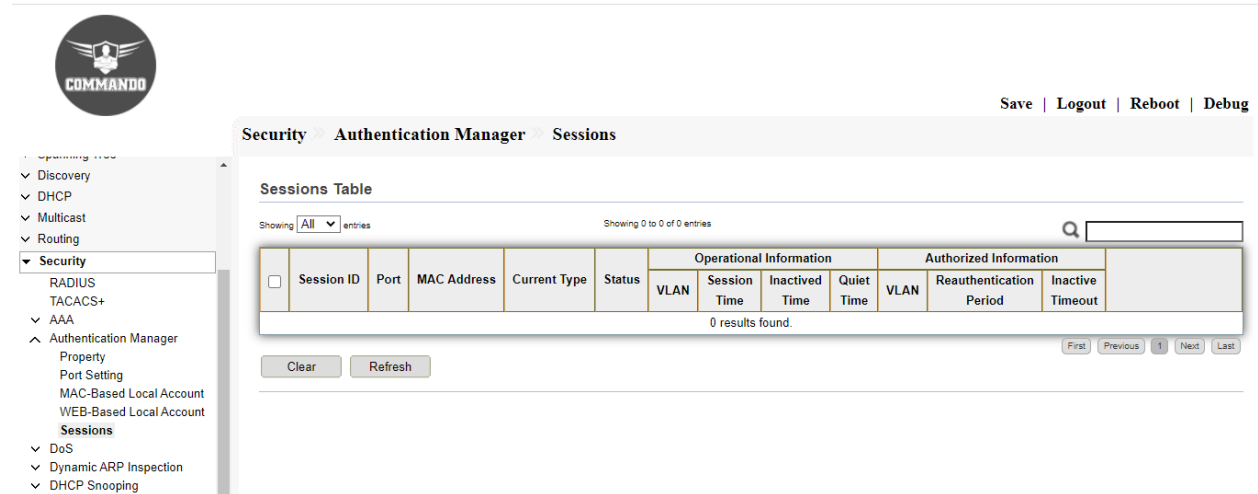
Add Edit Delete

Fig 12.4.14 WEB-Based Local Account table page

12.4.5 Sessions

This page shows all detail information of authentication sessions and allow user to select specific session. Session ID is unique of each session.

To view Sessions, click **Security >> Authentication Manger >> Sessions**.



The screenshot shows the COMMANDO web interface. On the left is a navigation tree with categories like Discovery, DHCP, Multicast, Routing, Security, AAA, Authentication Manager, DoS, and DHCP Snooping. The 'Sessions' link under 'Authentication Manager' is highlighted. The main content area is titled 'Security > Authentication Manager > Sessions' and includes links for 'Save', 'Logout', 'Reboot', and 'Debug'. Below the breadcrumb is a 'Sessions Table' section. It features a search bar, a dropdown for 'Showing All entries', and a status indicator 'Showing 0 to 0 of 0 entries'. The table has columns for Session ID, Port, MAC Address, Current Type, Status, Operational Information (VLAN, Session Time, Inactivated Time, Quiet Time), and Authorized Information (VLAN, Reauthentication Period, Inactive Timeout). The table is currently empty, displaying '0 results found.' and navigation buttons for 'Clear', 'Refresh', 'First', 'Previous', '1', 'Next', and 'Last'.

Fig 12.4.15 Authentication Manager Sessions Table page

12.5 DoS

A Denial of Service (DoS) attack is a hacker attempt to make a Switch unavailable to its users. DoS attacks saturate the switch with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a switch CPU overload.

The DoS protection feature is a set of predefined rules that protect the network from malicious attacks. The DoS Security Suite Settings enables activating the security suite. A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users. DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a switch CPU overload. The Denial of Service (DoS) Prevention feature assists the system administrator in resisting such attacks.

To view and configure Dos Global Setting, click **Security >> Dos >> Property**.



Security > DoS > Property

- √ Status
- √ Network
- √ Port
- √ POE Setting
- √ VLAN
- √ MAC Address Table
- √ Spanning Tree
- √ Discovery
- √ DHCP
- √ Multicast
- √ Routing
- ▼ Security
 - RADIUS
 - TACACS+
 - √ AAA
 - √ Authentication Manager
 - ^ DoS
 - Property**
 - Port Setting
 - √ Dynamic ARP Inspection
 - √ DHCP Snooping
 - √ IP Source Guard
- √ ACL
- √ QoS
- √ Diagnostics
- √ Management

POD	<input checked="" type="checkbox"/> Enable
Land	<input checked="" type="checkbox"/> Enable
UDP Blat	<input checked="" type="checkbox"/> Enable
TCP Blat	<input checked="" type="checkbox"/> Enable
DMAC = SMAC	<input checked="" type="checkbox"/> Enable
Null Scan Attack	<input checked="" type="checkbox"/> Enable
X-Mas Scan Attack	<input checked="" type="checkbox"/> Enable
TCP SYN-FIN Attack	<input checked="" type="checkbox"/> Enable
TCP SYN-RST Attack	<input checked="" type="checkbox"/> Enable
ICMP Fragment	<input checked="" type="checkbox"/> Enable
TCP-SYN	<input checked="" type="checkbox"/> Enable Note: Source Port < 1024
TCP Fragment	<input checked="" type="checkbox"/> Enable Note: Offset = 1
Ping Max Size	<input checked="" type="checkbox"/> Enable IPv4 <input checked="" type="checkbox"/> Enable IPv6 <input type="text" value="512"/> Byte (0 - 65535, default 512)
TCP Min Hdr size	<input checked="" type="checkbox"/> Enable <input type="text" value="20"/> Byte (0 - 31, default 20)
IPv6 Min Fragment	<input checked="" type="checkbox"/> Enable <input type="text" value="1240"/> Byte (0 - 65535, default 1240)
Smurf Attack	<input checked="" type="checkbox"/> Enable <input type="text" value="0"/> Netmask Length (0 - 32, default 0)

Apply

Fig 12.5.1 DoS property page



Security >> DoS >> Port Setting

- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ✓ AAA
 - ✓ Authentication Manager
 - ^ DoS
 - Property
 - Port Setting**
 - ✓ Dynamic ARP Inspection
 - ✓ DHCP Snooping
 - ✓ IP Source Guard
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	
<input type="checkbox"/>	1	GE1	Disabled	
<input type="checkbox"/>	2	GE2	Disabled	
<input type="checkbox"/>	3	GE3	Disabled	
<input type="checkbox"/>	4	GE4	Disabled	
<input type="checkbox"/>	5	GE5	Disabled	
<input type="checkbox"/>	6	GE6	Disabled	
<input type="checkbox"/>	7	GE7	Disabled	
<input type="checkbox"/>	8	GE8	Disabled	
<input type="checkbox"/>	9	GE9	Disabled	
<input type="checkbox"/>	10	GE10	Disabled	
<input type="checkbox"/>	11	GE11	Disabled	
<input type="checkbox"/>	12	GE12	Disabled	
<input type="checkbox"/>	13	GE13	Disabled	
<input type="checkbox"/>	14	GE14	Disabled	
<input type="checkbox"/>	15	GE15	Disabled	

Fig 12.5.2 Default DoS Port Setting page



Security » DoS » Port Setting

- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▼ Authentication Manager
 - ^ DoS
 - Property
 - Port Setting**
 - ▼ Dynamic ARP Inspection
 - ▼ DHCP Snooping
 - ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Port Setting Table

<input checked="" type="checkbox"/>	Entry	Port	State
<input checked="" type="checkbox"/>	1	GE1	Disabled
<input checked="" type="checkbox"/>	2	GE2	Disabled
<input checked="" type="checkbox"/>	3	GE3	Disabled
<input checked="" type="checkbox"/>	4	GE4	Disabled
<input checked="" type="checkbox"/>	5	GE5	Disabled
<input checked="" type="checkbox"/>	6	GE6	Disabled
<input checked="" type="checkbox"/>	7	GE7	Disabled
<input checked="" type="checkbox"/>	8	GE8	Disabled
<input checked="" type="checkbox"/>	9	GE9	Disabled
<input checked="" type="checkbox"/>	10	GE10	Disabled
<input checked="" type="checkbox"/>	11	GE11	Disabled
<input checked="" type="checkbox"/>	12	GE12	Disabled

Fig 12.5.3 Selecting Port DoS Setting page



Save | Logout |

Security > DoS > Port Setting

- RADIUS
- TACACS+
- ▼ AAA
- ▼ Authentication Manager
- ▲ DoS
 - Property
 - Port Setting**
- ▼ Dynamic ARP Inspection
- ▼ DHCP Snooping
- ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Edit Port Setting

Port	GE1-GE28,LAG1-LAG8
State	<input checked="" type="checkbox"/> Enable

Apply Close

Fig 12.5.4 DoS Port Setting Table after enable all ports page



Security » DoS » Port Setting

- RADIUS
- TACACS+
- ✓ AAA
- ✓ Authentication Manager
- ^ DoS
 - Property
 - Port Setting**
 - ✓ Dynamic ARP Inspection
 - ✓ DHCP Snooping
 - ✓ IP Source Guard
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	
<input type="checkbox"/>	1	GE1	Enabled	
<input type="checkbox"/>	2	GE2	Enabled	
<input type="checkbox"/>	3	GE3	Enabled	
<input type="checkbox"/>	4	GE4	Enabled	
<input type="checkbox"/>	5	GE5	Enabled	
<input type="checkbox"/>	6	GE6	Enabled	
<input type="checkbox"/>	7	GE7	Enabled	

Fig 12.5.5 DoS Port Setting Table after enabled ports page

12.6 Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings. This capability protects the network from certain "man-in-the-middle" attacks. Use the Dynamic ARP Inspection pages to configure settings of Dynamic ARP Inspection. This page allow user to configure global and per interface settings of Dynamic ARP Inspection.

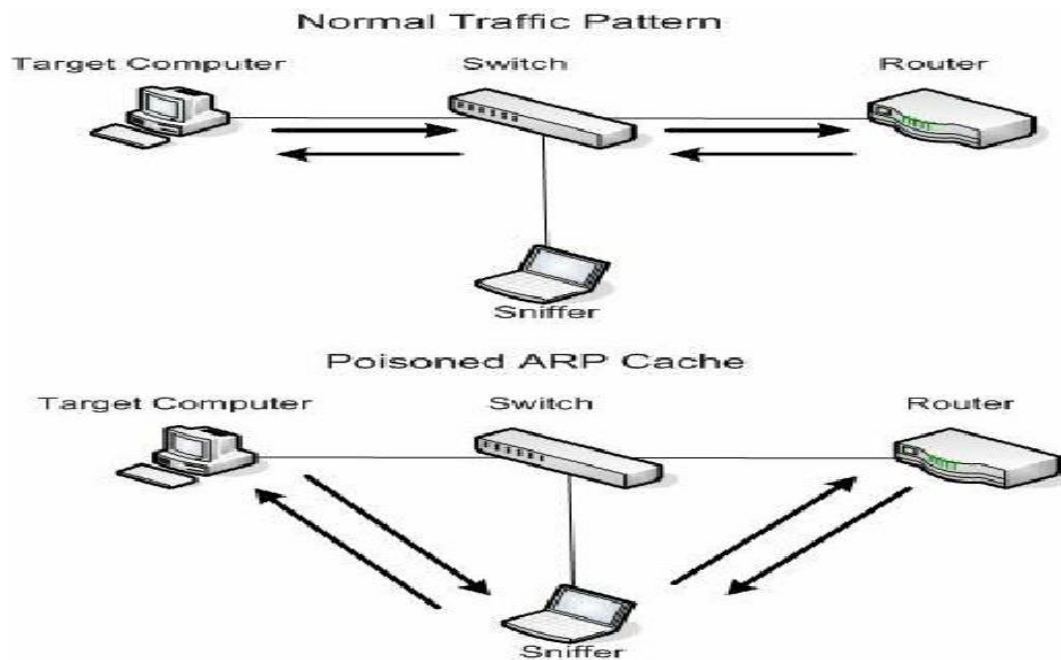


Fig 12.6.1 Dynamic ARP Inspection (DAI) Poisoned ARP Cache Concept

12.6.1 Dynamic ARP Inspection

ARP inspection is performed only on untrusted interfaces. ARP packets that are received on the trusted interface are simply forwarded. If the ARP Packet Validation option is selected (Properties page), the following additional validation checks are performed:

Source MAC: Compares the packet's source MAC address in the Ethernet header against the sender's MAC address in the ARP request. This check is performed on both ARP requests and responses.

Destination MAC: compares the packet's destination MAC address in the Ethernet header against the destination interface's MAC address. This check is performed for ARP responses.

IP Addresses: Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0

To view and configure Dynamic ARP Inspection Setting, , click **Security >> Dynamic ARP Inspection >> Property**.

The screenshot shows the Commando network management interface. The breadcrumb navigation is **Security > Dynamic ARP Inspection > Property**. The main configuration area has a **State** toggle set to **Enable**. Below it, there are two lists: **Available VLAN** and **Selected VLAN**, with **VLAN 1** selected in the latter. An **Apply** button is present. Below the configuration area is the **Port Setting Table**, which contains the following data:

	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited

Fig 12.6.2 Dynamic ARP Inspection (DAI) port setting table page



- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▼ Authentication Manager
 - ▼ DoS
 - ▲ Dynamic ARP Inspection
 - Property**
 - Statistics
 - ▼ DHCP Snooping
 - ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Security > Dynamic ARP Inspection > Property

State Enable

VLAN

Available VLAN

Selected VLAN

VLAN 1

Apply

Port Setting Table

<input checked="" type="checkbox"/>	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
<input checked="" type="checkbox"/>	1	GE1	Disabled	Disabled	Disabled	Disabled	10
<input checked="" type="checkbox"/>	2	GE2	Disabled	Disabled	Disabled	Disabled	10
<input checked="" type="checkbox"/>	3	GE3	Disabled	Disabled	Disabled	Disabled	10

Fig 12.6.3 Dynamic ARP Inspection (DAI) port selection page



- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▼ Authentication Manager
 - ▼ DoS
 - ▲ Dynamic ARP Inspection
 - Property**
 - Statistics
 - ▼ DHCP Snooping
 - ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Security > Dynamic ARP Inspection > Property

Save

Edit Port Setting

Port: GE1-GE28 LAG1-LAG8

Trust: Enable

Source MAC Address: Enable

Destination MAC Address: Enable

IP Address: Enable
 Allow Zero (0.0.0.0)

Rate Limit: 10 pps (1 - 50, default 0, 0 is Unlimited)

Apply Close

Fig 12.6.4 Dynamic ARP Inspection (DAI) Edit Port Setting page



- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ✓ AAA
 - ✓ Authentication Manager
 - ✓ DoS
 - ^ Dynamic ARP Inspection
 - Property**
 - Statistics
 - ✓ DHCP Snooping
 - ✓ IP Source Guard
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Security > Dynamic ARP Inspection > Property

Port Setting Table

<input type="checkbox"/>	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
<input type="checkbox"/>	1	GE1	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	2	GE2	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	3	GE3	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	4	GE4	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	5	GE5	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	6	GE6	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	7	GE7	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	8	GE8	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	9	GE9	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	10	GE10	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	11	GE11	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	12	GE12	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	13	GE13	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	14	GE14	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	15	GE15	Enabled	Enabled	Enabled	Enabled	10
<input type="checkbox"/>	16	GE16	Enabled	Enabled	Enabled	Enabled	10

Fig 12.6.5 DAI Port Setting Table page after enabling ports page

12.6.2 Dynamic ARP Inspection (DAI) Statistics

This page allow user to browse all statistics that recorded by Dynamic ARP Inspection function. Displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with DAI enabled (active).

To view Dynamic ARP Inspection Statistics, click **Security >> Dynamic ARP Inspection >> Statistics**.

COMMANDO

Save | Logout | Reboot |

Security > Dynamic ARP Inspection > Statistics

Statistics Table

<input type="checkbox"/>	Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0
<input type="checkbox"/>	7	GE7	0	0	0	0	0	0
<input type="checkbox"/>	8	GE8	0	0	0	0	0	0
<input type="checkbox"/>	9	GE9	0	0	0	0	0	0
<input type="checkbox"/>	10	GE10	0	0	0	0	0	0
<input type="checkbox"/>	11	GE11	0	0	0	0	0	0

Fig 12.6.7 Dynamic ARP Inspection (DAI) Statistics Table page

12.7 DHCP Snooping

DHCP Snooping is a layer 2 security technology incorporated into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. DHCP Snooping prevents unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. This page allow user to configure global and per interface settings of DHCP Snooping.

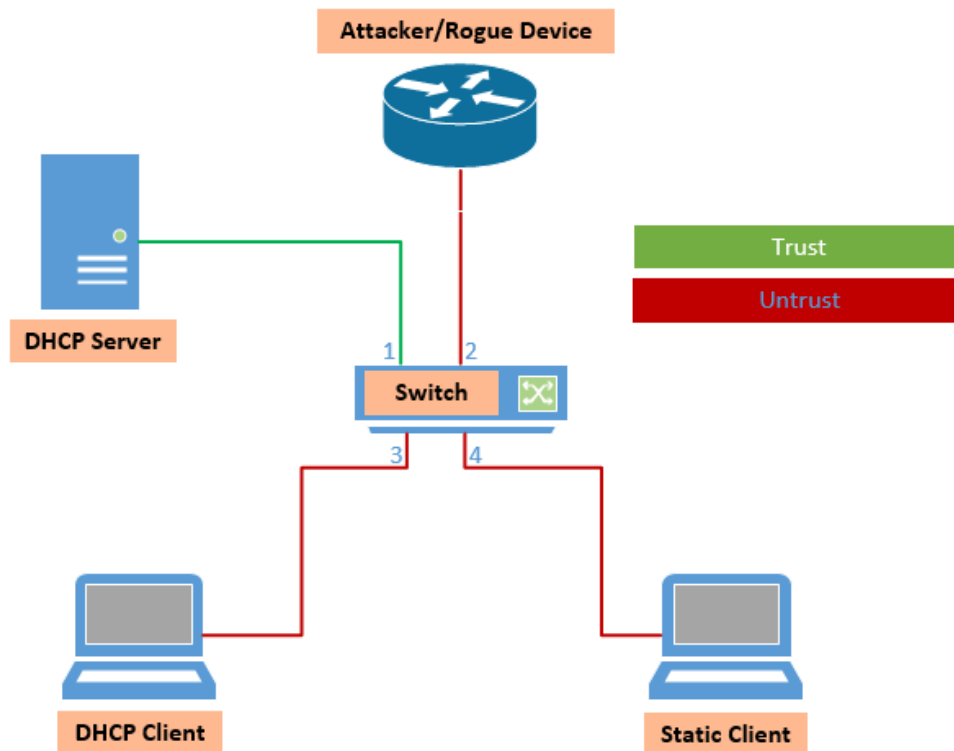


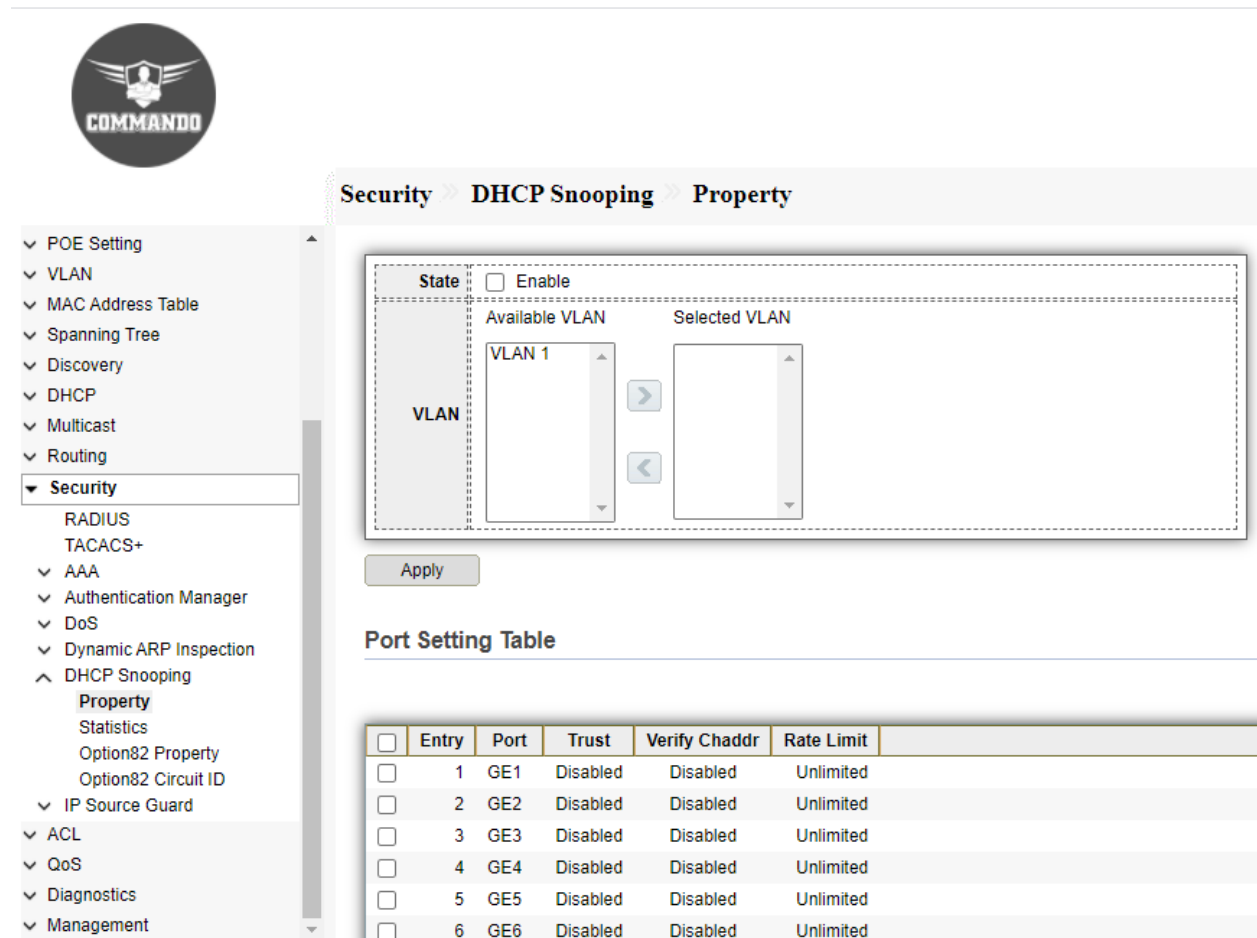
Fig 12.7.1 DHCP Snooping Concept

12.8.1 DHCP Snooping Property

DHCP snooping provides a security mechanism to prevent receiving false DHCP response packets and to log DHCP addresses. It does this by treating ports on the device as either trusted or untrusted. A trusted port is a port that is connected to a DHCP server and is allowed to assign DHCP addresses. DHCP messages received on trusted ports are allowed to pass through the device.

An untrusted port is a port that is not allowed to assign DHCP addresses. By default, all ports are considered untrusted until you declare them trusted.

To view and configure DHCP Snooping, click **Security >> DHCP Snooping >> Property**.



The screenshot displays the Commando network management interface. On the left is a navigation menu with categories like POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, and Management. The 'Security' menu is expanded, showing sub-items like RADIUS, TACACS+, AAA, Authentication Manager, DoS, Dynamic ARP Inspection, DHCP Snooping (with 'Property' selected), Statistics, Option82 Property, Option82 Circuit ID, IP Source Guard, ACL, QoS, Diagnostics, and Management.

The main content area has a breadcrumb trail: **Security > DHCP Snooping > Property**. Below this is a configuration panel with a 'State' section containing an unchecked 'Enable' checkbox. Underneath is a 'VLAN' section with two list boxes: 'Available VLAN' (containing 'VLAN 1') and 'Selected VLAN' (empty), with right and left arrow buttons between them. An 'Apply' button is located below the VLAN section.

Below the configuration panel is the 'Port Setting Table'.

<input type="checkbox"/>	Entry	Port	Trust	Verify Chaddr	Rate Limit
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	Disabled	Unlimited

Fig 12.8.1 Default DHCP Snooping Port setting Table page



- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security**
 - RADIUS
 - TACACS+
 - AAA
 - Authentication Manager
 - DoS
 - Dynamic ARP Inspection
 - DHCP Snooping
 - Property**
 - Statistics
 - Option82 Property
 - Option82 Circuit ID
 - IP Source Guard
- ACL
- QoS
- Diagnostics
- Management

Security > DHCP Snooping > Property

State: Enable

VLAN:

Available VLAN	Selected VLAN
	VLAN 1

Apply

Port Setting Table

<input checked="" type="checkbox"/>	Entry	Port	Trust	Verify Chaddr	Rate Limit
<input checked="" type="checkbox"/>	1	GE1	Disabled	Disabled	Unlimited
<input checked="" type="checkbox"/>	2	GE2	Disabled	Disabled	Unlimited
<input checked="" type="checkbox"/>	3	GE3	Disabled	Disabled	Unlimited
<input checked="" type="checkbox"/>	4	GE4	Disabled	Disabled	Unlimited
<input checked="" type="checkbox"/>	5	GE5	Disabled	Disabled	Unlimited
<input checked="" type="checkbox"/>	6	GE6	Disabled	Disabled	Unlimited

Fig 12.8.2 DHCP Snooping for selected Port setting page



- Multicast
- Routing
- Security**
 - RADIUS
 - TACACS+
 - AAA
 - Authentication Manager
 - DoS
 - Dynamic ARP Inspection
 - DHCP Snooping
 - Property**
 - Statistics
 - Option82 Property
 - Option82 Circuit ID
 - IP Source Guard
- ACL
- QoS
- Diagnostics
- Management

Save | Logout

Security > DHCP Snooping > Property

Edit Port Setting

Port	GE1-GE28,LAG1-LAG8
Trust	<input checked="" type="checkbox"/> Enable
Verify Chaddr	<input checked="" type="checkbox"/> Enable
Rate Limit	<input type="text" value="200"/> pps (1 - 300, default 0), 0 is Unlimited

Apply Close

Fig 12.8.3 Created VLAN DHCP Snooping State page



Security >> DHCP Snooping >> Property

- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ✓ AAA
 - ✓ Authentication Manager
 - ✓ DoS
 - ✓ Dynamic ARP Inspection
 - ^ DHCP Snooping
 - Property**
 - Statistics
 - Option82 Property
 - Option82 Circuit ID
 - ✓ IP Source Guard
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

State: Enable

VLAN

Available VLAN	Selected VLAN
	VLAN 1

Apply

Port Setting Table

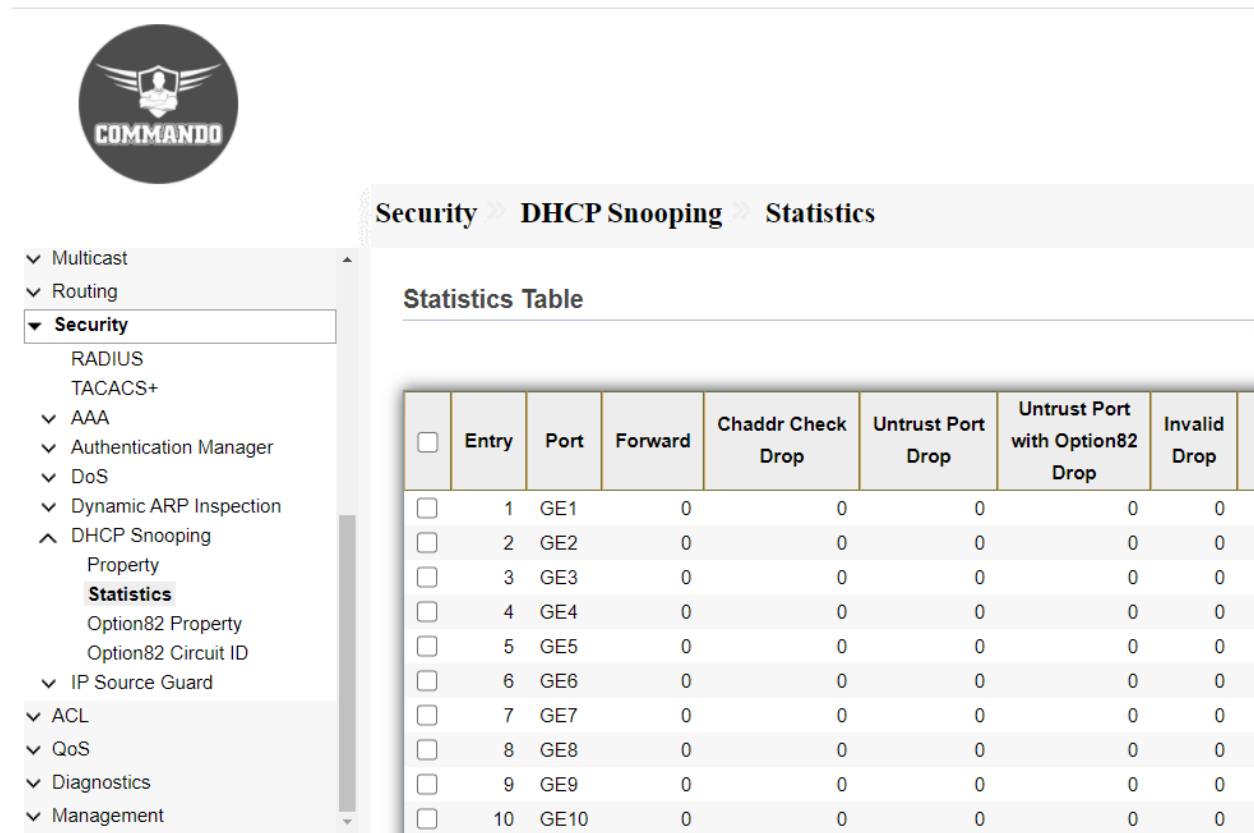
<input type="checkbox"/>	Entry	Port	Trust	Verify Chaddr	Rate Limit
<input type="checkbox"/>	1	GE1	Enabled	Enabled	200
<input type="checkbox"/>	2	GE2	Enabled	Enabled	200
<input type="checkbox"/>	3	GE3	Enabled	Enabled	200
<input type="checkbox"/>	4	GE4	Enabled	Enabled	200
<input type="checkbox"/>	5	GE5	Enabled	Enabled	200
<input type="checkbox"/>	6	GE6	Enabled	Enabled	200

Fig 12.8.4 DHCP Snooping Port setting Table After Enabling Ports page

12.8.2 Statistics

This page allows users to browse all statistics that's recorded by DHCP snooping function. Display information about trusted ports and display DHCP snooping trust.

To view the DHCP Snooping Statistics, click **Security >> DHCP Snooping >> Statistics**.



COMMANDO

Security > DHCP Snooping > Statistics

Statistics Table

<input type="checkbox"/>	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop
<input type="checkbox"/>	1	GE1	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0
<input type="checkbox"/>	7	GE7	0	0	0	0	0
<input type="checkbox"/>	8	GE8	0	0	0	0	0
<input type="checkbox"/>	9	GE9	0	0	0	0	0
<input type="checkbox"/>	10	GE10	0	0	0	0	0

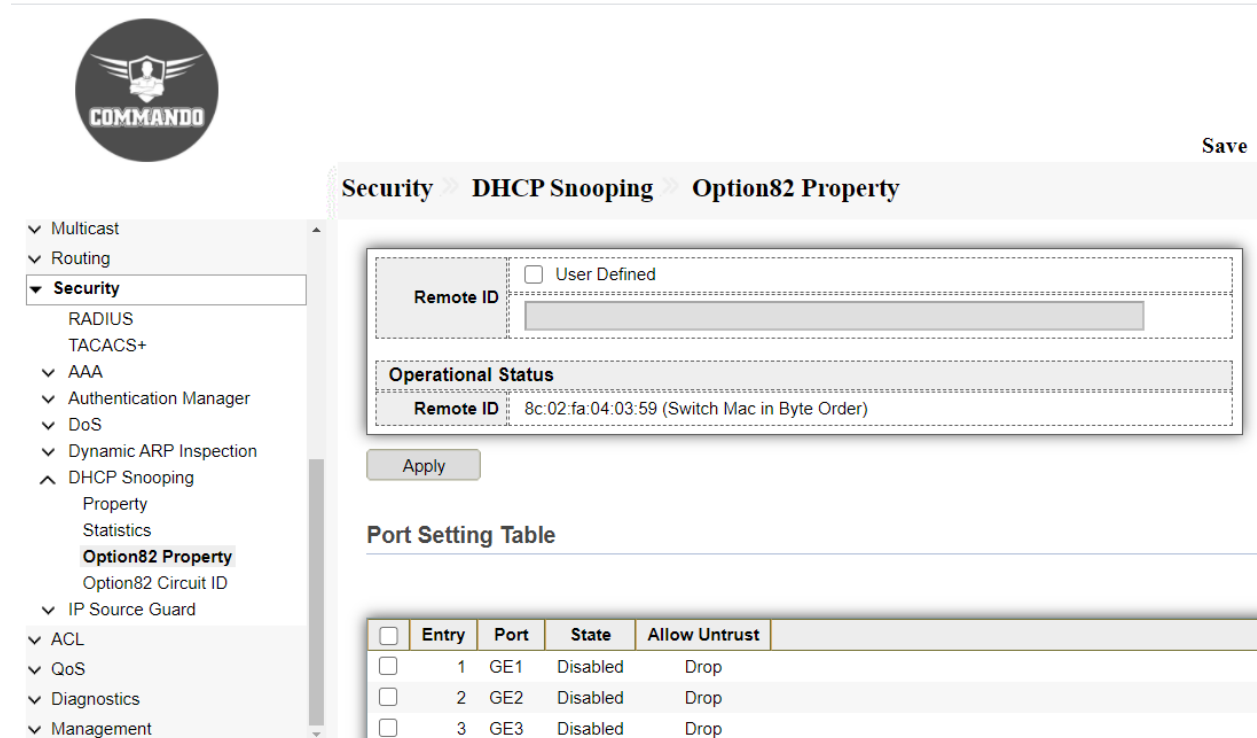
Fig 12.8.5 DHCP Snooping statistics Table page

12.8.3 Option82 Property

Option 82 (DHCP Relay Agent Information Option) passes port and agent information to a central DHCP server, indicating where an assigned IP address physically connects to the network.

The main goal of option 82 is to help to the DHCP server select the best IP subnet (network pool) from which to obtain an IP address. This DHCP Snooping Option82 allow user to set string of DHCP option82 remote ID filed. The string will attach in option82.


To view and configure DHCP Snooping Option82 Property, click **Security >> DHCP Snooping >> Option82 Property**.



The screenshot displays the Commando network management interface. On the left is a navigation menu with categories like Multicast, Routing, Security, AAA, Authentication Manager, DoS, Dynamic ARP Inspection, DHCP Snooping, IP Source Guard, ACL, QoS, Diagnostics, and Management. The 'Security' menu is expanded to show 'Option82 Property'. The main content area has a breadcrumb trail: Security > DHCP Snooping > Option82 Property. At the top right is a 'Save' button. The configuration area contains a 'Remote ID' field with a 'User Defined' checkbox and an empty text input. Below this is an 'Operational Status' section with a 'Remote ID' field containing the value '8c:02:fa:04:03:59 (Switch Mac in Byte Order)'. An 'Apply' button is located below the operational status. At the bottom is a 'Port Setting Table' with the following data:

	Entry	Port	State	Allow Untrust
<input type="checkbox"/>	1	GE1	Disabled	Drop
<input type="checkbox"/>	2	GE2	Disabled	Drop
<input type="checkbox"/>	3	GE3	Disabled	Drop

Fig 12.8.6 Default DHCP Snooping Option82 Port setting table page



Save |

Security > DHCP Snooping > Option82 Property

- ▼ Multicast
- ▼ Routing
- ▼ Security
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▼ Authentication Manager
 - ▼ DoS
 - ▼ Dynamic ARP Inspection
 - ▲ DHCP Snooping
 - Property
 - Statistics
 - Option82 Property**
 - Option82 Circuit ID
 - ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Remote ID User Defined

Remote ID


Operational Status

Remote ID 00:02:fa:04:03:59

Port Setting Table

<input checked="" type="checkbox"/>	Entry	Port	State	Allow Untrust
<input checked="" type="checkbox"/>	1	GE1	Disabled	Drop
<input checked="" type="checkbox"/>	2	GE2	Disabled	Drop
<input checked="" type="checkbox"/>	3	GE3	Disabled	Drop

Fig 12.8.7 DHCP Snooping Option82 Port Selecting Ports page



Save | Logout

Security > DHCP Snooping > Option82 Property

- ▼ AAA
- ▼ Authentication Manager
- ▼ DoS
- ▼ Dynamic ARP Inspection
- ▲ DHCP Snooping
 - Property
 - Statistics
 - Option82 Property**
 - Option82 Circuit ID
- ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Edit Port Setting

Port GE1-GE28,LAG1-LAG8

State Enable

Allow Untrust
 Keep
 Drop
 Replace

Fig 12.8.8 DHCP Snooping Option82 Edit Port Setting page



- √ Spanning Tree
- √ Discovery
- √ DHCP
- √ Multicast
- √ Routing
- ▼ Security
 - RADIUS
 - TACACS+
 - √ AAA
 - √ Authentication Manager
 - √ DoS
 - √ Dynamic ARP Inspection
 - ∧ DHCP Snooping
 - Property
 - Statistics
 - Option82 Property**
 - Option82 Circuit ID
 - √ IP Source Guard
- √ ACL
- √ QoS
- √ Diagnostics
- √ Management

Security > DHCP Snooping > Option82 Property

Remote ID User Defined

Operational Status
Remote ID 00:02:fa:04:03:59

Apply

Port Setting Table

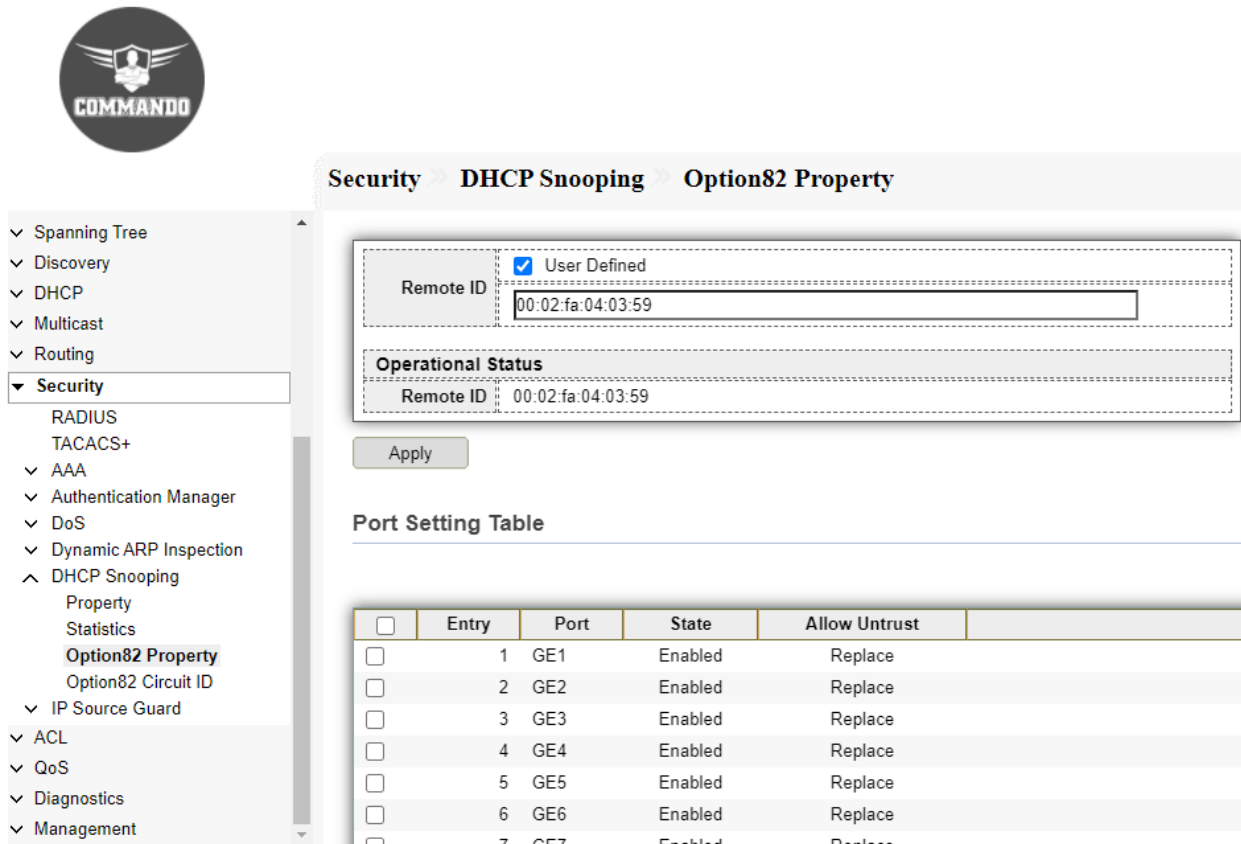
<input type="checkbox"/>	Entry	Port	State	Allow Untrust
<input type="checkbox"/>	1	GE1	Enabled	Replace
<input type="checkbox"/>	2	GE2	Enabled	Replace
<input type="checkbox"/>	3	GE3	Enabled	Replace
<input type="checkbox"/>	4	GE4	Enabled	Replace
<input type="checkbox"/>	5	GE5	Enabled	Replace
<input type="checkbox"/>	6	GE6	Enabled	Replace
<input type="checkbox"/>	7	GE7	Enabled	Replace

Fig 12.8.9 DHCP Snooping Option82 Edit Port Setting Table page after Enabling Ports page

12.8.4 Option82 Circuit ID

This page allow user to set string of DHCP option82 circuit ID filed. The string would attach in option82 if option inserted.

To view and configure DHCP Snooping Option82 Circuit ID, click **Security >> DHCP Snooping >> Option82 Circuit ID**.



COMMANDO

Security > DHCP Snooping > Option82 Property

Remote ID User Defined
00:02:fa:04:03:59

Operational Status
Remote ID 00:02:fa:04:03:59

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Allow Untrust
<input type="checkbox"/>	1	GE1	Enabled	Replace
<input type="checkbox"/>	2	GE2	Enabled	Replace
<input type="checkbox"/>	3	GE3	Enabled	Replace
<input type="checkbox"/>	4	GE4	Enabled	Replace
<input type="checkbox"/>	5	GE5	Enabled	Replace
<input type="checkbox"/>	6	GE6	Enabled	Replace
<input type="checkbox"/>	7	GE7	Enabled	Replace

Fig 12.8.10 DHCP Snooping Option82 Circuit ID Table page



- ▼ Multicast
- ▼ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▼ Authentication Manager
 - ▼ DoS
 - ▼ Dynamic ARP Inspection
 - ▲ DHCP Snooping
 - Property
 - Statistics
 - Option82 Property
 - Option82 Circuit ID**
 - ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Security > DHCP Snooping > Option82 Circuit ID

Option82 Circuit ID Table

Showing entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Port	VLAN	Circuit ID
0 results found.			

Fig 12.8.11 DHCP Snooping Add Option82 Circuit ID page



- ▼ Multicast
- ▼ Routing
- ▼ **Security**
 - RADIUS
 - TACACS+
 - ▼ AAA
 - ▼ Authentication Manager
 - ▼ DoS
 - ▼ Dynamic ARP Inspection
 - ▲ DHCP Snooping
 - Property
 - Statistics
 - Option82 Property
 - Option82 Circuit ID**
 - ▼ IP Source Guard
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Save |

Security > DHCP Snooping > Option82 Circuit ID

Add Option82 Circuit ID

Port	<input type="text" value="GE7"/>
VLAN	<input type="text" value="1"/> (1 - 4094) (Keep empty to set without VLAN)
Circuit ID	<input type="text" value="2"/>

Fig 12.8.12 DHCP SnoopingOption82 Circuit ID Table after enabling GE7 port page

12.9 IP Source Guard

IP Source Guard is a security feature that can be used to prevent traffic attacks caused when a host tries to use the IP address of its neighbor. When IP Source Guard is enabled, the device only transmits client IP traffic to IP addresses contained in the DHCP Snooping Binding database.

This includes both addresses added by DHCP Snooping and manually added entries. If the packet matches an entry in the database, the device forwards it. If not, it is dropped.

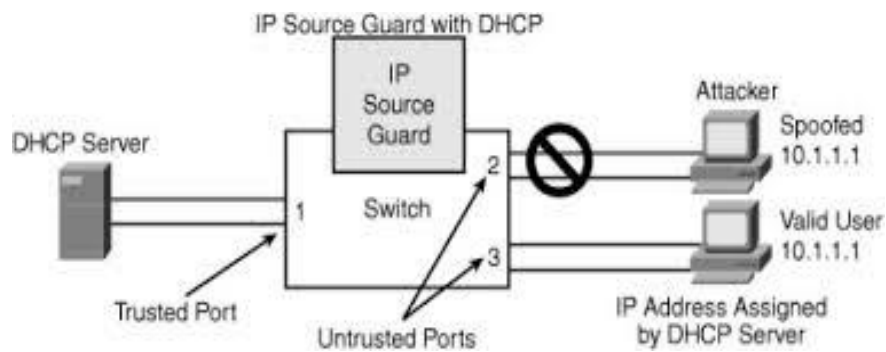
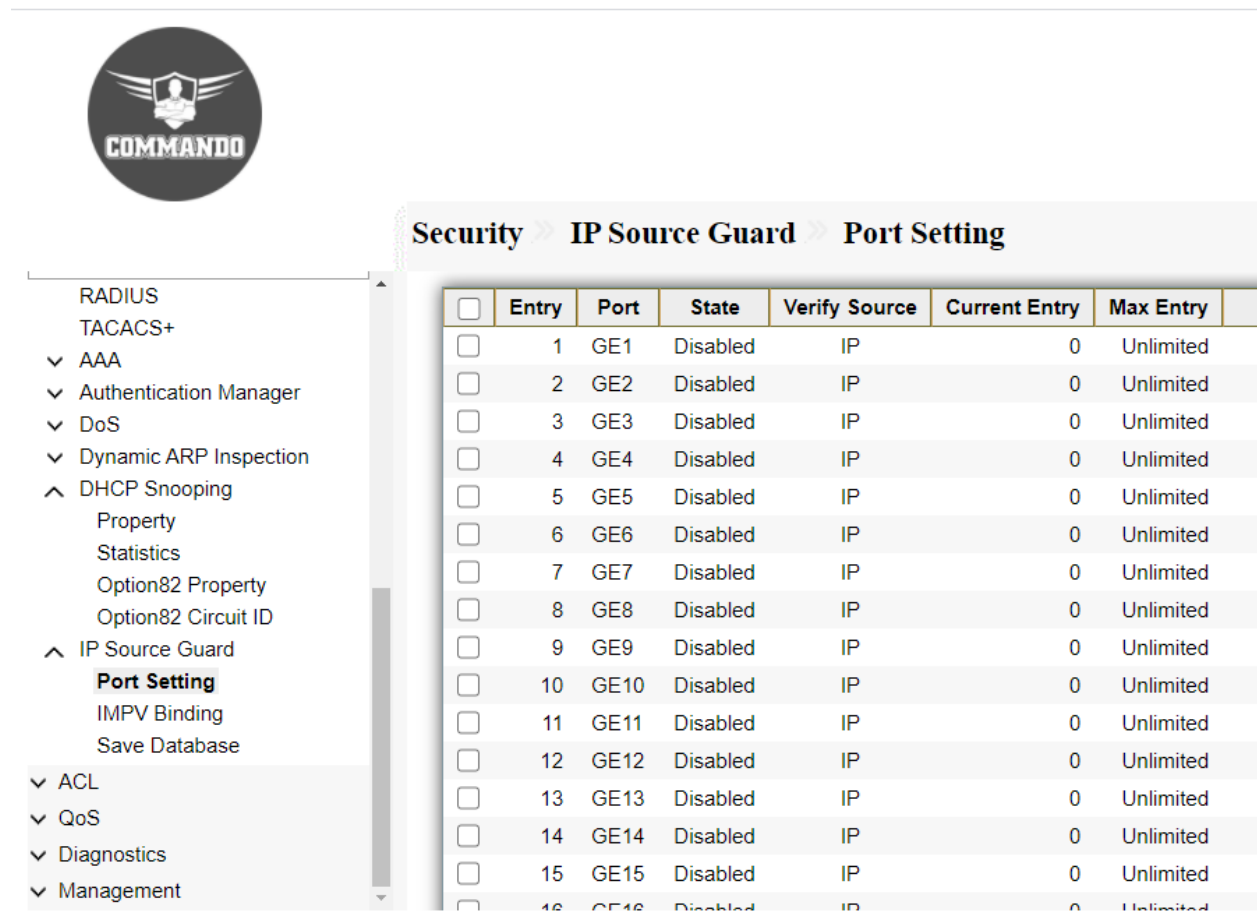


Fig 12.9.1 IP Source Guard concept

12.9.1 IP Source Guard Port Setting

Use the IP Source Guard pages to configure settings of IP Source Guard. Use the IP Source Guard pages to configure settings of IP Source Guard.

To view and configure IP source guard Port Setting, click **Security >> IP Source Guard >> Port Setting**.



The screenshot shows the COMMANDO network management interface. On the left is a navigation tree with the following items: RADIUS, TACACS+, AAA, Authentication Manager, DoS, Dynamic ARP Inspection, DHCP Snooping (with sub-items: Property, Statistics, Option82 Property, Option82 Circuit ID), IP Source Guard (with sub-items: **Port Setting**, IMPV Binding, Save Database), ACL, QoS, Diagnostics, and Management. The main content area is titled "Security >> IP Source Guard >> Port Setting" and contains a table with the following data:

<input type="checkbox"/>	Entry	Port	State	Verify Source	Current Entry	Max Entry
<input type="checkbox"/>	1	GE1	Disabled	IP	0	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	IP	0	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	IP	0	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	IP	0	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	IP	0	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	IP	0	Unlimited
<input type="checkbox"/>	7	GE7	Disabled	IP	0	Unlimited
<input type="checkbox"/>	8	GE8	Disabled	IP	0	Unlimited
<input type="checkbox"/>	9	GE9	Disabled	IP	0	Unlimited
<input type="checkbox"/>	10	GE10	Disabled	IP	0	Unlimited
<input type="checkbox"/>	11	GE11	Disabled	IP	0	Unlimited
<input type="checkbox"/>	12	GE12	Disabled	IP	0	Unlimited
<input type="checkbox"/>	13	GE13	Disabled	IP	0	Unlimited
<input type="checkbox"/>	14	GE14	Disabled	IP	0	Unlimited
<input type="checkbox"/>	15	GE15	Disabled	IP	0	Unlimited
<input type="checkbox"/>	16	GE16	Disabled	IP	0	Unlimited

Fig 12.9.2 IP source guard default Port Setting table page



- RADIUS
- TACACS+
- AAA
- Authentication Manager
- DoS
- Dynamic ARP Inspection
- DHCP Snooping
 - Property
 - Statistics
 - Option82 Property
 - Option82 Circuit ID
- IP Source Guard
 - Port Setting**
 - IMPV Binding
 - Save Database
- ACL
- QoS
- Diagnostics
- Management

Security >> IP Source Guard >> Port Setting

<input checked="" type="checkbox"/>	Entry	Port	State	Verify Source	Current Entry	Max Entry
<input checked="" type="checkbox"/>	1	GE1	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	2	GE2	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	3	GE3	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	4	GE4	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	5	GE5	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	6	GE6	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	7	GE7	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	8	GE8	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	9	GE9	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	10	GE10	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	11	GE11	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	12	GE12	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	13	GE13	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	14	GE14	Disabled	IP	0	Unlimited
<input checked="" type="checkbox"/>	15	GE15	Disabled	IP	0	Unlimited

Fig 12.9.3 IP source guard Selecting Ports for Setting page



- RADIUS
- TACACS+
- AAA
- Authentication Manager
- DoS
- Dynamic ARP Inspection
- DHCP Snooping
 - Property
 - Statistics
 - Option82 Property
 - Option82 Circuit ID
- IP Source Guard
 - Port Setting**
 - IMPV Binding
 - Save Database
- ACL
- QoS
- Diagnostics
- Management

Save

Security >> IP Source Guard >> Port Setting

Edit Port Setting

Port	GE1-GE28,LAG1-LAG8
State	<input checked="" type="checkbox"/> Enable
Verify Source	<input type="radio"/> IP <input checked="" type="radio"/> IP-MAC
Max Entry	<input type="text" value="2"/> (1 - 50, default 0), 0 is Unlimited

Apply Close

Fig 12.9.4 Edit IP source guard Ports Setting page



Security >> IP Source Guard >> Port Setting

- RADIUS
- TACACS+
- ✓ AAA
- ✓ Authentication Manager
- ✓ DoS
- ✓ Dynamic ARP Inspection
- ^ DHCP Snooping
 - Property
 - Statistics
 - Option82 Property
 - Option82 Circuit ID
- ^ IP Source Guard
 - Port Setting**
 - IMPV Binding
 - Save Database
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Verify Source	Current Entry	Max Entry
<input type="checkbox"/>	1	GE1	Enabled	IP-MAC	0	2
<input type="checkbox"/>	2	GE2	Enabled	IP-MAC	0	2
<input type="checkbox"/>	3	GE3	Enabled	IP-MAC	0	2
<input type="checkbox"/>	4	GE4	Enabled	IP-MAC	0	2
<input type="checkbox"/>	5	GE5	Enabled	IP-MAC	0	2
<input type="checkbox"/>	6	GE6	Enabled	IP-MAC	0	2
<input type="checkbox"/>	7	GE7	Enabled	IP-MAC	0	2
<input type="checkbox"/>	8	GE8	Enabled	IP-MAC	0	2
<input type="checkbox"/>	9	GE9	Enabled	IP-MAC	0	2
<input type="checkbox"/>	10	GE10	Enabled	IP-MAC	0	2
<input type="checkbox"/>	11	GE11	Enabled	IP-MAC	0	2
<input type="checkbox"/>	12	GE12	Enabled	IP-MAC	0	2

Fig 12.9.5 IP source guard Port Setting table after setting page

12.9.2 IMPV Binding

This page allow user to add static IP source guard entry and browse all IP source guard entries that learned by DHCP snooping or statically create by user.

To view and configure IP Source Guard IMPV Binding, click **Security >> IP Source Guard >> IMPV Binding**.

The screenshot shows the Commando web interface. On the left is a navigation menu with categories like Dynamic ARP Inspection, DHCP Snooping, IP Source Guard, and ACL. The main content area is titled "Security > IP Source Guard > IMPV Binding". At the top right of the main area are links for "Save", "Logout", "Reboot", and "Debug". Below the breadcrumb is the title "IP-MAC-Port-VLAN Binding Table". There is a search bar and a status indicator "Showing 0 to 0 of 0 entries". A table with columns "Port", "VLAN", "MAC Address", "IP Address", "Binding", "Type", and "Lease Time" is shown, with "0 results found." below it. At the bottom of the table are "Add", "Edit", and "Delete" buttons, and pagination controls for "First", "Previous", "1", "Next", and "Last".

Fig 12.9.6 IP Source Guard Default IMPV Binding Table page

The screenshot shows the Commando web interface for adding a binding. The navigation menu on the left includes RADIUS, TACACS+, AAA, Authentication Manager, DoS, Dynamic ARP Inspection, DHCP Snooping, IP Source Guard, and ACL. The main content area is titled "Security > IP Source Guard > IMPV Binding" and has a "Save" link at the top right. The page title is "Add IP-MAC-Port-VLAN Binding". A form is displayed with fields for "Port" (GE10), "VLAN" (1), "Binding" (IP-Port-VLAN selected), "MAC Address" (empty), and "IP Address" (192.168.0.3 / 255.255.255.255). There are "Apply" and "Close" buttons at the bottom of the form.

Fig 12.9.7 Add IP Source Guard IP-MAC-Port-VLAN Binding page



Save | Logout |

Security > IP Source Guard > IMPV Binding

IP-MAC-Port-VLAN Binding Table

Showing All entries

Showing 1 to 1 of 1 entries



<input type="checkbox"/>	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
<input type="checkbox"/>	GE10	1	N/A	192.168.0.3 / 255.255.255.255	IP-Port-VLAN	Static	N/A

Add Edit Delete

First Prev

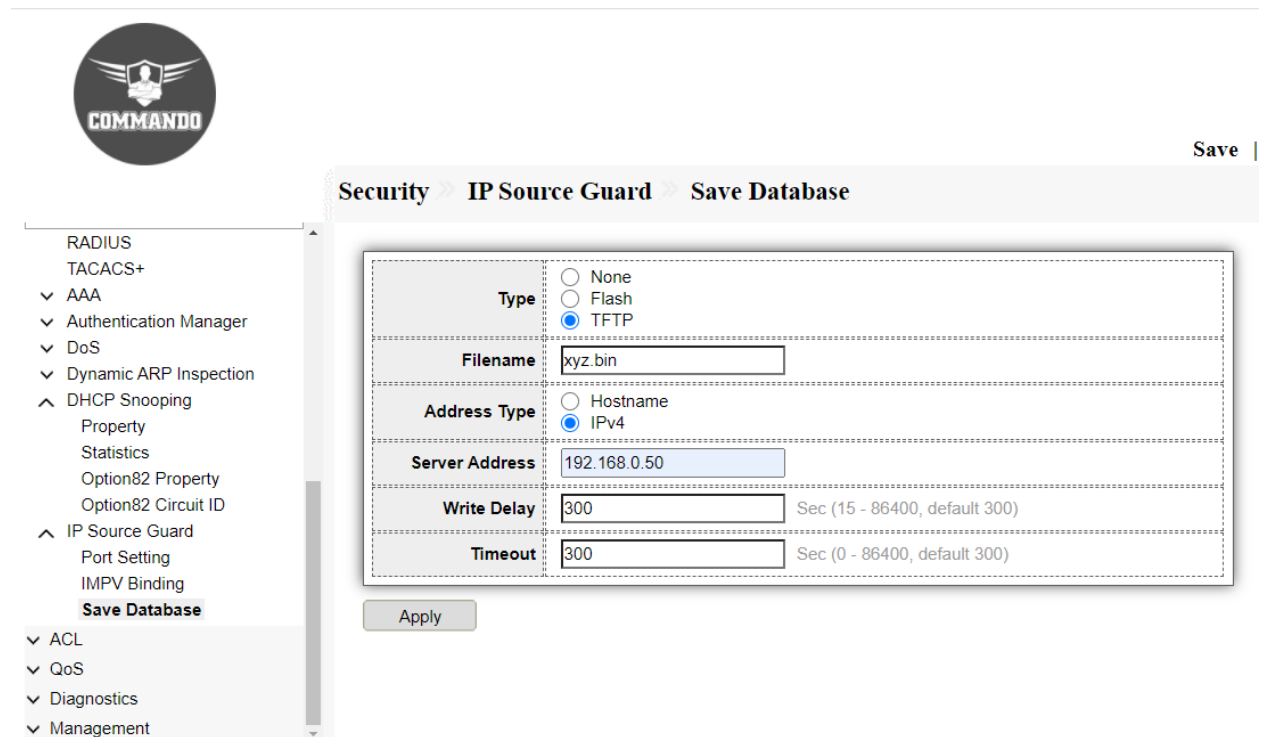
- RADIUS
- TACACS+
- AAA
- Authentication Manager
- DoS
- Dynamic ARP Inspection
- DHCP Snooping
 - Property
 - Statistics
 - Option82 Property
 - Option82 Circuit ID
- IP Source Guard
 - Port Setting
 - IMPV Binding**
 - Save Database
- ACL
- QoS
- Diagnostics
- Management

Fig 12.9.8 IP Source Guard IP-MAC-Port-VLAN Binding Table page

12.9.3 Save Database

This page allow user to configure DHCP snooping database which can backup and restore dynamic DHCP snooping entries.

To Save DHCP Snooping Database, click **Security >> DHCP Snooping >> Save Database**.



The screenshot shows the configuration page for the IP Source Guard Save Database. On the left is a navigation menu with the following items: RADIUS, TACACS+, AAA, Authentication Manager, DoS, Dynamic ARP Inspection, DHCP Snooping (expanded), IP Source Guard (expanded), and Save Database (highlighted). The main content area has a breadcrumb trail: Security > IP Source Guard > Save Database. The configuration form includes the following fields:

Type	<input type="radio"/> None
	<input type="radio"/> Flash
	<input checked="" type="radio"/> TFTP
Filename	<input type="text" value="xyz.bin"/>
Address Type	<input type="radio"/> Hostname
	<input checked="" type="radio"/> IPv4
Server Address	<input type="text" value="192.168.0.50"/>
Write Delay	<input type="text" value="300"/> Sec (15 - 86400, default 300)
Timeout	<input type="text" value="300"/> Sec (0 - 86400, default 300)

An **Apply** button is located below the form.

Fig 12.9.9 IP Source Guard Save Database page

Chapter 13 ACL

MAC ACL: MAC ACLs are used to filter traffic on a specific source MAC address or range of MAC addresses.

MAC ACE: When a frame is received on a port, the switch processes the frame through the first ACL. If the frame matches an ACE filter of the first ACL, the ACE action takes place. If the frame matches none of the ACE filters, the next ACL is processed.

IPv4 ACL: An ACL contains the hosts that are permitted or denied access to the network device. The IPv4-based ACL is a list of sources IPv4 addresses that use Layer 3 information to permit or deny access to traffic. IPv4 ACLs restrict IP-related traffic based on the configured IP filters.

IPv4 ACE: An Access Control List (ACL) is a list of one or more Access Control Entries (ACEs), where each ACE consists of a matching criterion and an action on IPv4 packets (permit or deny). Each ace has a sequence number to define the order, list of match criteria.

IPv6 ACL: IPv6 ACLs support the same options as IPv4 ACLs including source, destination IP, source, and destination ports. You can enable only IPv4 traffic in your network by blocking IPv6 traffic.

IPv6 ACE: An Access Control List (ACL) is a list of one or more Access Control Entries (ACEs), where each ACE consists of a matching criterion and an action on IPv6 Packets (permit or deny). Each ace has a sequence number to define the order, list of match criteria.

ACL Binding:

This page shows configuration of MAC, IPv4 & IPv6 Access List. An Access Control List (ACL) is an ordered list of classification filters and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE). Each ACE is made up of filters that distinguish traffic groups and associated actions.

A single ACL may contain one or more ACEs, which are matched against the contents of incoming frames. Either a DENY or PERMIT action is applied to frames whose contents match the filter.

13.1 MAC ACL

MAC-based ACLs are used to filter traffic based on Layer 2 fields. MAC-based ACLs check all frames for a match. This page allow user to add or delete ACL rule. A rule cannot be deleted if under binding.

To view and configure MAC ACL, click **ACL >> MAC ACL**.

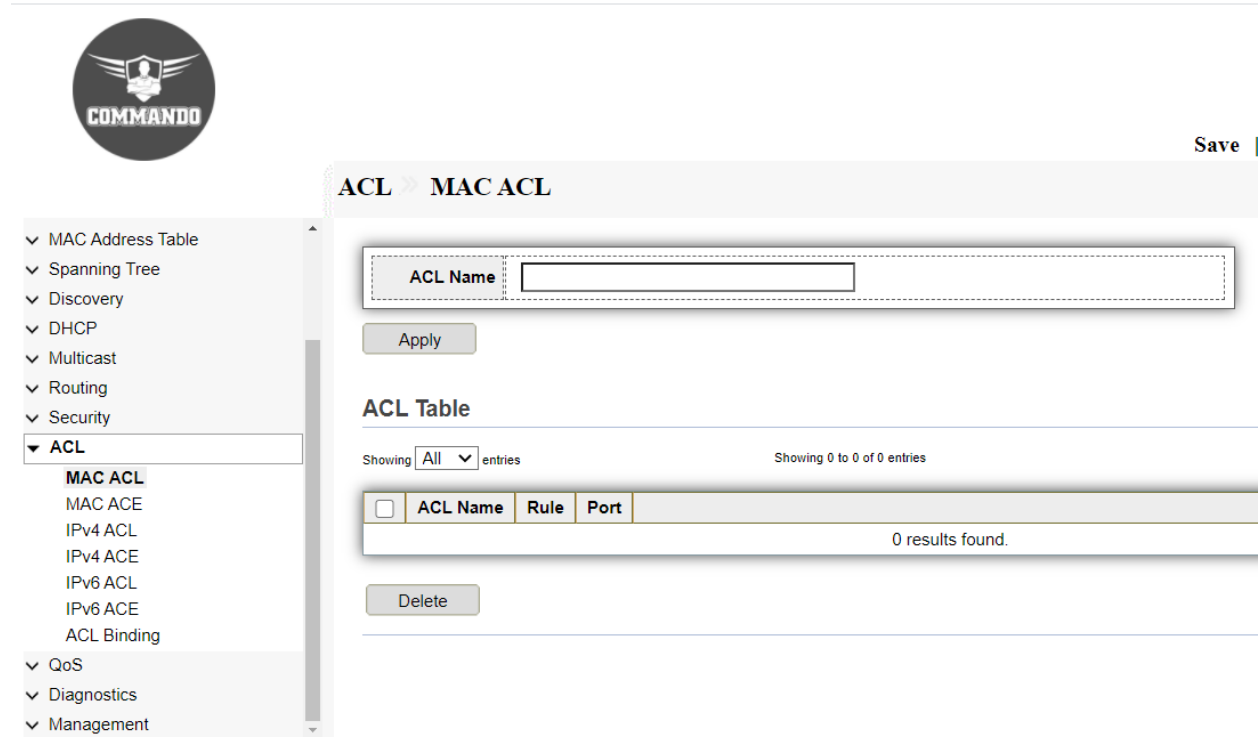


Fig 13.1.1 Default MAC ACL Table page



Save

ACL > MAC ACL

- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ▼ **ACL**
 - MAC ACL**
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL
 - IPv6 ACE
 - ACL Binding
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

ACL Name

Apply

ACL Table

Showing All entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	ACL Name	Rule	Port
<input type="checkbox"/>	COMMANDO	0	

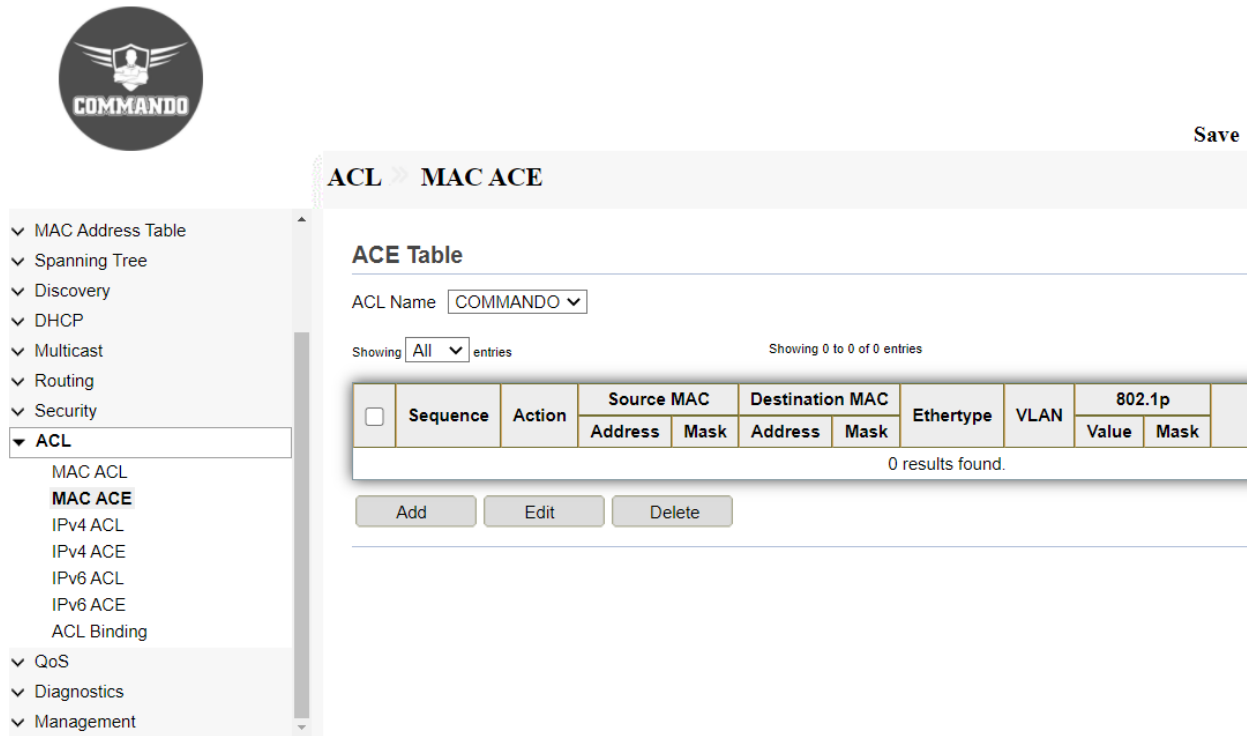
Delete

Fig 13.1.2 MAC ACL Table after creating COMMANDO page

13.2 MAC ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding.

To view and configure MAC ACE, click **ACL >> MAC ACE**



The screenshot shows the COMMANDO web interface for configuring MAC ACE. On the left is a navigation menu with categories like MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The ACL section is expanded, showing sub-items: MAC ACL, MAC ACE (highlighted), IPv4 ACL, IPv4 ACE, IPv6 ACL, IPv6 ACE, and ACL Binding. The main content area is titled 'ACL > MAC ACE' and includes a 'Save' button in the top right. Below the title is the 'ACE Table' configuration section, which includes a dropdown for 'ACL Name' set to 'COMMANDO'. It shows 'Showing All entries' and 'Showing 0 to 0 of 0 entries'. A table with columns for Sequence, Action, Source MAC (Address, Mask), Destination MAC (Address, Mask), Ethertype, VLAN, and 802.1p (Value, Mask) is displayed, currently containing no data. Below the table are 'Add', 'Edit', and 'Delete' buttons. The text '0 results found.' is centered below the table.

Fig 13.2.1 Default MAC ACE page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
 - ▼ ACL
 - MAC ACL
 - MAC ACE**
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL
 - IPv6 ACE
 - ACL Binding
 - ▼ QoS
 - ▼ Diagnostics
 - ▼ Management

ACL > MAC ACE

Add ACE

ACL Name	COMMANDO	
Sequence	10	(1 - 2147483647)
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Source MAC	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)	
Destination MAC	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)	
Ethertype	<input checked="" type="checkbox"/> Any 0x <input type="text"/> (0x600 ~ 0xFFFF)	
VLAN	<input type="checkbox"/> Any <input type="text"/> (1 - 4094)	
802.1p	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Value / Mask) (0 - 7)	

Apply Close

Fig 13.2.2 Add MAC ACE page



Save | Logout |

ACL > MAC ACE

ACE Table

ACL Name **COMMANDO**

Showing All entries

Showing 1 to 1 of 1 entries

Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
		Address	Mask	Address	Mask			Value	Mask
<input type="checkbox"/>	10 Deny	Any	Any	Any	Any	Any	1	Any	Any

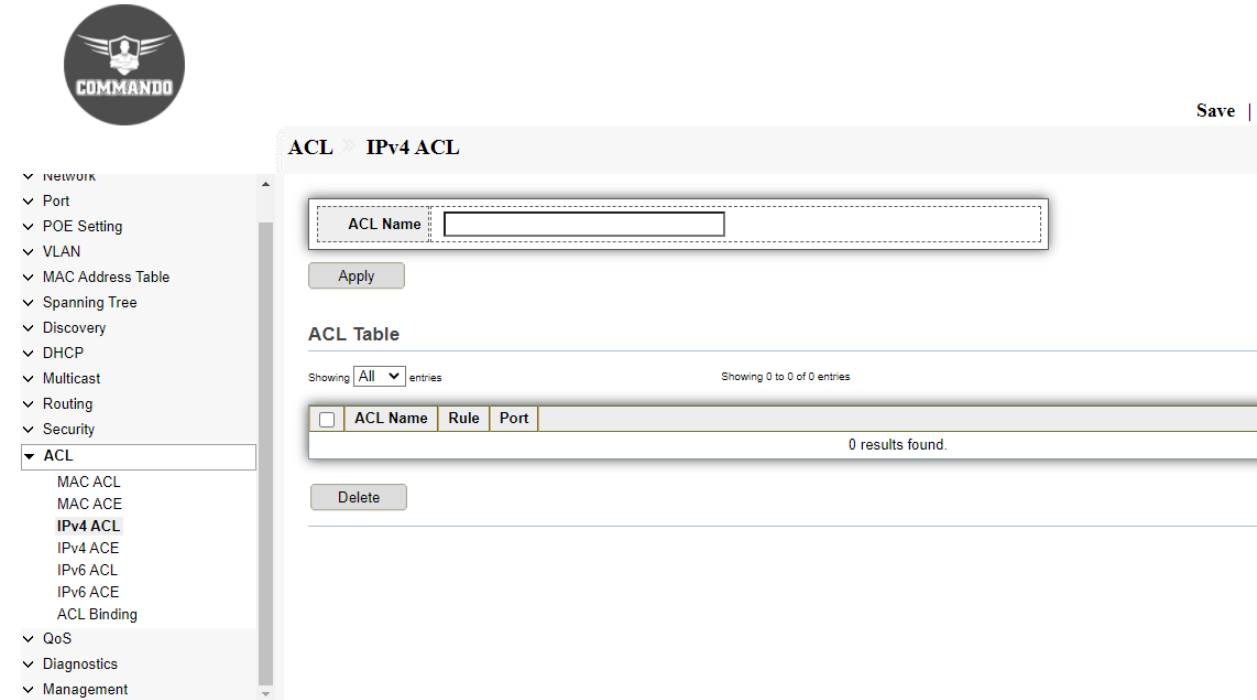
Add Edit Delete

Fig 13.2.3 MAC ACE Table page

13.3 IPv4 ACL

IPv4-based ACLs are used to check IPv4 packets, while other types of frames, such as ARPs, are not checked. This page allow user to add or delete IPv4 ACL rule. A rule cannot be deleted if under binding.

To view and configure IPv4 ACL, click **ACL >> IPv4 ACL**



The screenshot shows the COMMANDO network management interface. On the left is a navigation menu with categories like network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The ACL section is expanded, showing sub-items: MAC ACL, MAC ACE, IPv4 ACL (highlighted), IPv4 ACE, IPv6 ACL, IPv6 ACE, and ACL Binding. The main content area is titled 'ACL > IPv4 ACL' and includes a 'Save |' link. It features an 'ACL Name' input field with an 'Apply' button below it. Underneath is an 'ACL Table' section with a 'Showing All entries' indicator and 'Showing 0 to 0 of 0 entries'. A table with columns for 'ACL Name', 'Rule', and 'Port' is shown, containing '0 results found.' and a 'Delete' button.

Fig 13.3.1 Default ACL Table page

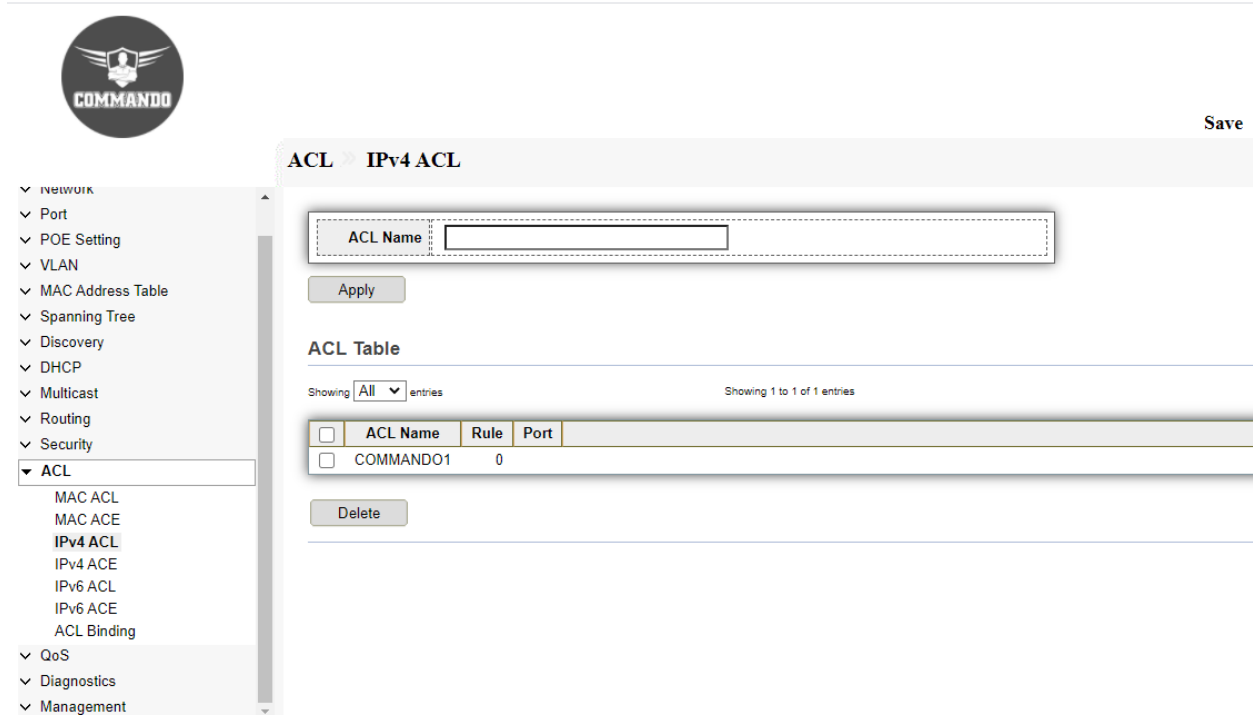


Fig 13.3.2 Edit IPv4 ACL Name page

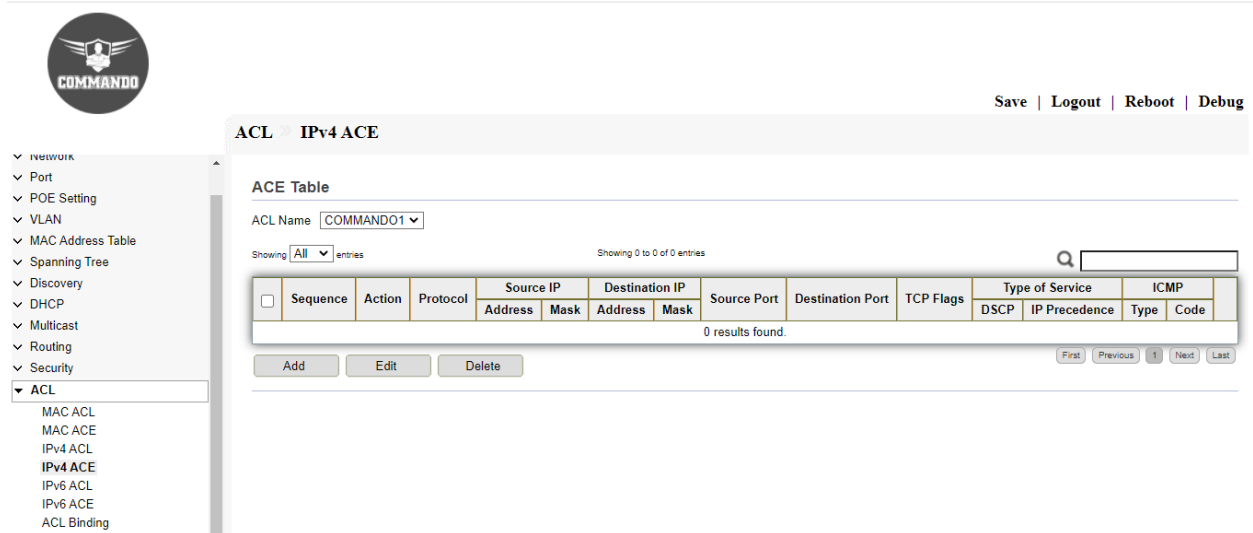
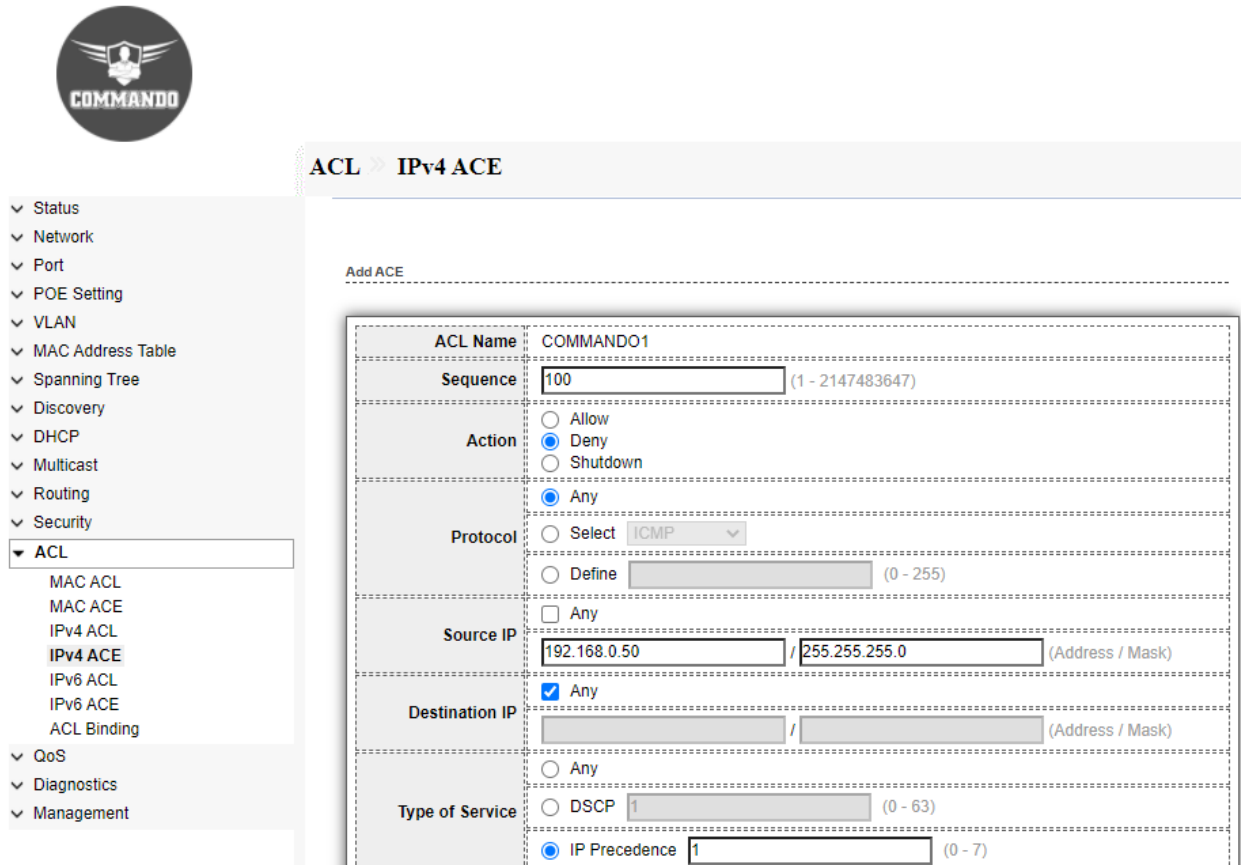


Fig 13.3.3 IPv4 ACL Table after creating COMMANDO1 ACL page

13.4 IPv4 ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding.

To display IPv4 ACE page, click **ACL >> IPv4 ACE**




The screenshot shows the 'IPv4 ACE' configuration page in the COMMANDO interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The 'ACL' category is expanded, showing sub-items: MAC ACL, MAC ACE, IPv4 ACL, IPv4 ACE (selected), IPv6 ACL, IPv6 ACE, and ACL Binding.

The main configuration area is titled 'ACL > IPv4 ACE' and contains an 'Add ACE' section. The configuration form is as follows:

ACL Name	COMMANDO1
Sequence	100 (1 - 2147483647)
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> Select ICMP
Source IP	<input type="radio"/> Define <input type="text"/> (0 - 255) <input type="checkbox"/> Any
Source IP	<input type="text"/> 192.168.0.50 / <input type="text"/> 255.255.255.0 (Address / Mask)
Destination IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
Type of Service	<input type="radio"/> Any <input type="radio"/> DSCP <input type="text"/> 1 (0 - 63) <input checked="" type="radio"/> IP Precedence <input type="text"/> 1 (0 - 7)

Fig 13.4.1 Default IPv4 ACE Table page



Save | Logout | Reboot |

ACL IPv4 ACE

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ **ACL**
 - MAC ACL
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL
 - IPv6 ACE
 - ACL Binding
- ▼ QoS


ACE Table

ACL Name:

Showing **All** entries Showing 1 to 1 of 1 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code
<input type="checkbox"/>	100	Deny	Any (IP)	192.168.0.50	255.255.255.0	Any	Any							1

Fig 13.4.2 Add IPv4 ACE page



ACL IPv6 ACL

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ **ACL**
 - MAC ACL
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL**
 - IPv6 ACE
 - ACL Binding
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

ACL Name

ACL Table

Showing **All** entries Showing 0 to 0 of 0 entries

	ACL Name	Rule	Port
0 results found.			

Fig 13.4.3 IPv4 ACE Table page

13.5 IPv6 ACL

The IPv6-Based ACL page displays and enables the creation of IPv6 ACLs, which check pure IPv6-based traffic. IPv6 ACLs do not check IPv6-over-IPv4 or ARP packets. This page allow user to add or delete Ipv6 ACL rule. A rule cannot be deleted if under binding.

To view and configure IPv6 ACL page, click **ACL >> IPv6 ACL**

The screenshot shows the COMMANDO network management interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The 'ACL' category is expanded, showing sub-items: MAC ACL, MAC ACE, IPv4 ACL, IPv4 ACE, IPv6 ACL (highlighted), IPv6 ACE, and ACL Binding. The main content area is titled 'ACL >> IPv6 ACL'. It features a form for creating a new ACL with an 'ACL Name' input field and an 'Apply' button. Below this is an 'ACL Table' section with a dropdown menu set to 'All' entries and a status 'Showing 0 to 0 of 0 entries'. A table with columns 'ACL Name', 'Rule', and 'Port' is shown, containing no data and a message '0 results found.' at the bottom right. A 'Delete' button is located below the table.

Fig 13.5.1 Default IPv6 ACL Table page



- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
 - ▼ **ACL**
 - MAC ACL
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL**
 - IPv6 ACE
 - ACL Binding
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

ACL >> IPv6 ACL

ACL Name

Apply

ACL Table

Showing **All** entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	ACL Name	Rule	Port
<input type="checkbox"/>	COMMANDO2	0	

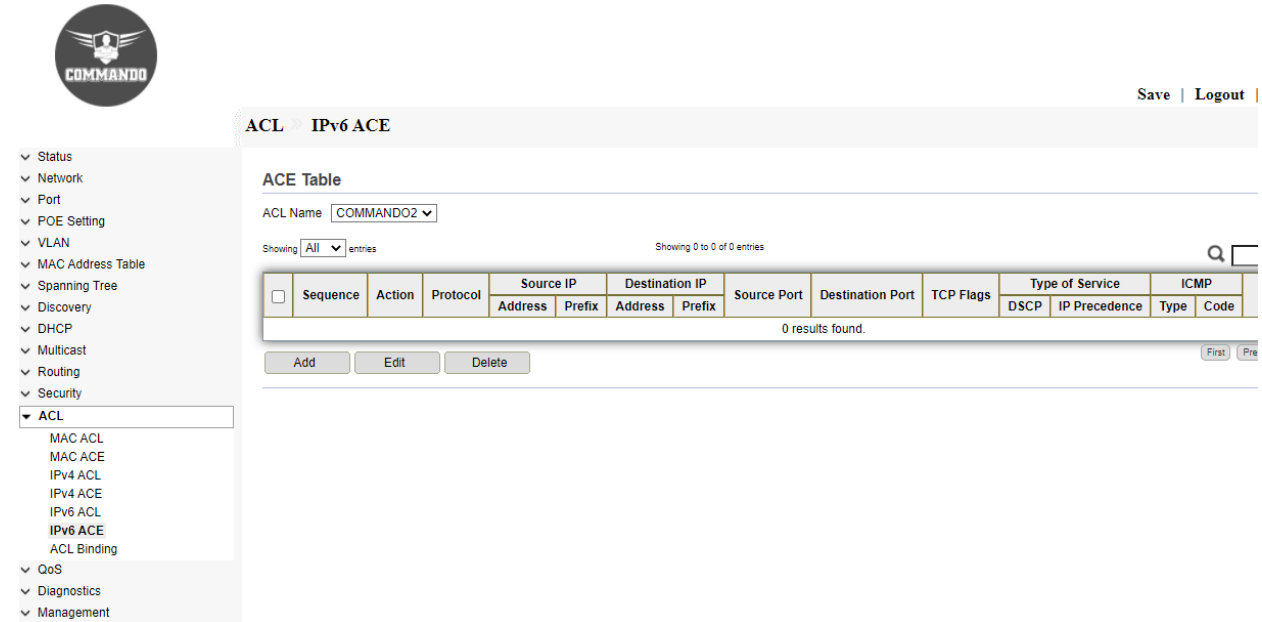
Delete

Fig 13.5.2 IPv6 ACL Table after changing page

13.6 IPv6 ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding.

To view and configure IPv6 ACE page, click **ACL >> IPv6 ACE**



The screenshot shows the COMMANDO web interface for configuring IPv6 ACE rules. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The ACL menu is expanded, showing sub-items: MAC ACL, MAC ACE, IPv4 ACL, IPv4 ACE, IPv6 ACL, IPv6 ACE, and ACL Binding. The main content area is titled 'ACL > IPv6 ACE' and includes a 'Save | Logout' link. Below the title is the 'ACE Table' section, where the 'ACL Name' is set to 'COMMANDO2'. It shows 'Showing All entries' and 'Showing 0 to 0 of 0 entries'. A table with columns for Sequence, Action, Protocol, Source IP (Address, Prefix), Destination IP (Address, Prefix), Source Port, Destination Port, TCP Flags, Type of Service (DSCP, IP Precedence), and ICMP (Type, Code) is displayed. The table is currently empty, with '0 results found.' below it. At the bottom of the table are 'Add', 'Edit', and 'Delete' buttons, and 'First' and 'Pre' navigation buttons.

Fig 13.6.1 Default IPv6 ACE Table page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
 - ▼ ACL
 - MAC ACL
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL
 - IPv6 ACE
 - ACL Binding
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

ACL > IPv6 ACE

Add ACE

ACL Name	COMMANDO2
Sequence	1000 (1 - 2147483647)
Action	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Shutdown
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> Select TCP
	<input type="radio"/> Define (0 - 255)
Source IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Prefix (0 - 128))
Destination IP	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Prefix (0 - 128))
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP (0 - 63) <input type="radio"/> IP Precedence (0 - 7)

Fig 13.6.2 Add IPv6 ACE page



- ▼ network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
 - ▼ ACL
 - MAC ACL
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL
 - IPv6 ACE
 - ACL Binding
- ▼ QoS
- ▼ Diagnostics

Save | Logout

ACL > IPv6 ACE

ACE Table

ACL Name COMMANDO2

Showing All entries

Showing 1 to 1 of 1 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service	
				Address	Prefix	Address	Prefix				DSCP	IP Preced
<input type="checkbox"/>	1000	Shutdown	Any (IP)	Any	Any	Any	Any					Any

Add Edit Delete

Fig 13.6.3 IPv6 ACE table after adding ACE page

13.7 ACL Binding

When an ACL is bound to an interface (port, LAG or VLAN), its ACE rules are applied to packets arriving at that interface. Packets that do not match any of the ACEs in the ACL are matched to a default rule, whose action is to drop unmatched packets.

Although each interface can be bound to only one ACL, multiple interfaces can be bound to the same ACL by grouping them into a policy-map and binding that policy-map to the interface.

After an ACL is bound to an interface, it cannot be edited, modified, or deleted until it is removed from all the ports to which it is bound or in use. This page allow user to bind or unbind ACL rule to or from interface. IPv4 and IPv6 ACL cannot be bound to the same port simultaneously.

To view and configure ACL Binding page, click **ACL >> ACL Binding**



ACL > ACL Binding

- ✓ NETWORK
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ▼ **ACL**
 - MAC ACL
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL
 - IPv6 ACE
 - ACL Binding**
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

ACL Binding Table

<input type="checkbox"/>	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	GE1			
<input type="checkbox"/>	2	GE2			
<input type="checkbox"/>	3	GE3			
<input type="checkbox"/>	4	GE4			
<input type="checkbox"/>	5	GE5			
<input type="checkbox"/>	6	GE6			
<input type="checkbox"/>	7	GE7			
<input type="checkbox"/>	8	GE8			
<input type="checkbox"/>	9	GE9			
<input type="checkbox"/>	10	GE10			
<input type="checkbox"/>	11	GE11			
<input type="checkbox"/>	12	GE12			
<input type="checkbox"/>	13	GE13			
<input type="checkbox"/>	14	GE14			
<input type="checkbox"/>	15	GE15			

Fig 13.7.1 ACL Binding Table page



ACL >> ACL Binding

- network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL**
 - MAC ACL
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL
 - IPv6 ACE
 - ACL Binding**
- QoS
- Diagnostics
- Management

ACL Binding Table

<input checked="" type="checkbox"/>	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
<input checked="" type="checkbox"/>	1	GE1			
<input checked="" type="checkbox"/>	2	GE2			
<input checked="" type="checkbox"/>	3	GE3			
<input checked="" type="checkbox"/>	4	GE4			
<input checked="" type="checkbox"/>	5	GE5			
<input checked="" type="checkbox"/>	6	GE6			
<input checked="" type="checkbox"/>	7	GE7			
<input checked="" type="checkbox"/>	8	GE8			
<input checked="" type="checkbox"/>	9	GE9			
<input checked="" type="checkbox"/>	10	GE10			
<input checked="" type="checkbox"/>	11	GE11			
<input checked="" type="checkbox"/>	12	GE12			
<input checked="" type="checkbox"/>	13	GE13			
<input checked="" type="checkbox"/>	14	GE14			
<input checked="" type="checkbox"/>	15	GE15			

Fig 13.7.2 Selecting port for ACL Binding page



ACL > ACL Binding

- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL**
 - MAC ACL
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL
 - IPv6 ACE
 - ACL Binding**
- QoS
- Diagnostics
- Management

Add ACL Binding

Port	GE1-GE28,LAG1-LAG8
Note: ACL cannot be bound without any rules configured.	
MAC ACL	COMMANDO
IPv4 ACL	COMMANDO1
IPv6 ACL	None

Apply Close

Fig 13.7.3 Add ACL Binding page



ACL > ACL Binding

- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ▼ **ACL**
 - MAC ACL
 - MAC ACE
 - IPv4 ACL
 - IPv4 ACE
 - IPv6 ACL
 - IPv6 ACE
 - ACL Binding**
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

ACL Binding Table

<input type="checkbox"/>	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	GE1		COMMANDO	
<input type="checkbox"/>	2	GE2		COMMANDO	
<input type="checkbox"/>	3	GE3		COMMANDO	
<input type="checkbox"/>	4	GE4		COMMANDO	
<input type="checkbox"/>	5	GE5		COMMANDO	
<input type="checkbox"/>	6	GE6		COMMANDO	
<input type="checkbox"/>	7	GE7		COMMANDO	
<input type="checkbox"/>	8	GE8		COMMANDO	
<input type="checkbox"/>	9	GE9		COMMANDO	
<input type="checkbox"/>	10	GE10		COMMANDO	
<input type="checkbox"/>	11	GE11		COMMANDO	
<input type="checkbox"/>	12	GE12		COMMANDO	
<input type="checkbox"/>	13	GE13		COMMANDO	
<input type="checkbox"/>	14	GE14		COMMANDO	

Fig 13.7.4 ACL Binding Table after Enabled GE1 port page

Chapter 14 QoS

General: Quality of service (QoS) refers to any technology that manages data traffic to reduce packet loss, latency, and jitter on the network. QoS controls and manages network resources by setting priorities for specific types of data on the network.

Property: The QoS global properties include default values for QoS rule parameters, unit of measure, and QoS authentication timeouts.

Queue Scheduling: QoS Queue scheduling is a scheduling methodology of network traffic based upon QoS (Quality of Service). Here, the frames or packets are mapped to internal forwarding queues based on its QoS information, which are then services according to a queuing scheme.

CoS Mapping: Class of Service (CoS) is a queuing discipline. An algorithm compares fields of packets or CoS tags to classify packets and to assign to queues of differing priority.

DSCP Mapping: A Differentiated Services Code Point (DSCP) is a packet header value that can be used to request high priority or best effort delivery for traffic. DSCP Mapping is used to determine traffic classification for network data.

IP Precedence Mapping: IP Precedence allows you to specify the class of service (CoS) for a packet. You use the three precedence bits in the type of service (ToS) field of the IP version 4 (IPv4) header for this purpose. The traffic classified according to the user IP Precedence value is mapped.

Rate Limit: Use the Rate Limit pages to define values that determine how much traffic the switch can receive and send on specific port or queue.

Ingress / Egress Port: We can configure ingress port rate limit and egress port rate limit. The ingress/egress rate limit can be configured on the switch interface. Excess bandwidth above ingress/egress rate limit is discarded.

Egress Queue: Egress queues for each port for three kinds of queue scheduling algorithms like Strict-Priority Queue (SP) and Weighted Round Robin (WRR).

13.1 QoS General

Generally, in IP network, all the packets are treated equally without priority difference following the First-in, First-out (FIFO) policy. That is, they make best effort to transmit the packets to the destination, not making any commitment or guarantee of the transmission reliability, delay or to satisfy other performance requirements. To deliver better service with the limited network resources, QoS monitors the traffic of the specific user on the ingress, so that it can make a better use of the assigned resource. The port traffic limit is the port-based traffic limit used for limiting the general speed of packet output on the port. Traffic Priority IP TOS, DSCP and 802.1p, etc. IP packet TOS byte of IP header has eight bits. The first three bits indicate the IP priority with the value ranging from 0 to 7. Bits 3 to 6 indicate the TOS priority, ranging from 0 to 15. The TOS byte of IP header is re-defined to DS field. Wherein, the DSCP priority is indicated by the first six bits (bits 0 to 5) with the value ranging from 0 to 63, and the last two bits (bits 6 and 7) are currently unused. 802.1p priority is in the layer-2 packet header and has each host supporting the protocol 802.1Q is added with a 4-byte 802.1Q tag head behind the source address in the original Ethernet frame head when sending data packets. The 4-byte 802.1Q tag head contains 2-byte tag protocol Identifier (TPID) whose value is 8100, and 2-byte tag control information (TCI). This information is added to IP packet with 802.1Q tag.

When congestion occurs, several packets will compete for the resources. Two kinds of queue scheduling algorithms are used to overcome the problem. These two kinds of queue scheduling algorithms are Strict-Priority Queue (SP) and Weighted Round Robin (WRR).

14.1.1 Property

Quality of Service (QoS) prioritizes traffic so that more important traffic can pass first. This result is a performance improvement for critical network traffic. E3000 Series Switches allow setting QoS on per port basis with queuing.

To view and configure QoS Property, click **QoS >> General >> Property**.

The screenshot displays the 'QoS > General > Property' configuration page. On the left is a navigation menu with categories like Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, and QoS. Under QoS, 'Property' is selected. The main content area shows the 'QoS > General > Property' breadcrumb and a configuration box with the following settings:

- State:** Enable
- Trust Mode:**
 - CoS
 - DSCP
 - CoS-DSCP
 - IP Precedence

Below the configuration box is an 'Apply' button and a 'Port Setting Table'.

	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
<input type="checkbox"/>	1	GE1	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	2	GE2	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	3	GE3	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	4	GE4	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	5	GE5	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	6	GE6	0	Enabled	Disabled	Disabled	Disabled

Fig 14.1.1 Default QoS Port Setting table page



- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS**
 - General
 - Property**
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping
 - Rate Limit
 - Diagnostics
 - Management

QoS > General > Property

State	<input checked="" type="checkbox"/> Enable
Trust Mode	<input type="checkbox"/> CoS
	<input type="checkbox"/> DSCP
	<input checked="" type="checkbox"/> CoS-DSCP
	<input type="checkbox"/> IP Precedence

Apply

Port Setting Table

	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
<input type="checkbox"/>	1	GE1	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	2	GE2	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	3	GE3	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	4	GE4	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	5	GE5	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	6	GE6	0	Enabled	Disabled	Disabled	Disabled

Fig 14.1.2 Enable QoS on Switch page



- network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
 - General
 - Property**
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping
- Rate Limit
- Diagnostics
- Management

QoS » General » Property

State Enable

Trust Mode CoS
 DSCP
 CoS-DSCP
 IP Precedence

Apply

Port Setting Table

	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
<input type="checkbox"/>	1	GE1	0	Enabled	Disabled	Disabled	Disabled
<input checked="" type="checkbox"/>	2	GE2	0	Enabled	Disabled	Disabled	Disabled
<input checked="" type="checkbox"/>	3	GE3	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	4	GE4	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	5	GE5	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	6	GE6	0	Enabled	Disabled	Disabled	Disabled

Fig 14.1.3 Selecting Ports for QoS setting page



- network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
 - General
 - Property
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping
- Rate Limit
- Diagnostics
- Management

QoS > General > Property

State Enable

Trust Mode CoS
 DSCP
 CoS-DSCP
 IP Precedence

Apply

Port Setting Table

	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
<input type="checkbox"/>	1	GE1	0	Enabled	Disabled	Disabled	Disabled
<input checked="" type="checkbox"/>	2	GE2	0	Enabled	Disabled	Disabled	Disabled
<input checked="" type="checkbox"/>	3	GE3	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	4	GE4	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	5	GE5	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	6	GE6	0	Enabled	Disabled	Disabled	Disabled

Fig 14.1.4 Edit Ports setting for Qos page



- Status
- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
 - General
 - Property
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping
- Rate Limit

Save |

QoS > General > Property

State Enable

Trust Mode CoS
 DSCP
 CoS-DSCP
 IP Precedence

Apply

Port Setting Table

	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
<input type="checkbox"/>	1	GE1	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	2	GE2	2	Enabled	Disabled	Enabled	Disabled
<input type="checkbox"/>	3	GE3	2	Enabled	Disabled	Enabled	Disabled
<input type="checkbox"/>	4	GE4	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	5	GE5	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	6	GE6	0	Enabled	Disabled	Disabled	Disabled

Fig 14.1.5 QoS Port Setting table page

14.1.2 Queue Scheduling

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue and queue 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled, Strict Priority (SP) and Weighted Round Robin (WRR).

Strict Priority (SP): Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.

Weighted Round Robin (WRR): In WRR mode the number of packets sent from the queue is proportional to the weight of the queue higher the weight, the with more priority frames are sent.

The queuing modes can be selected on the Queue page. When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with queue-8 (the highest priority queue) and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced. It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in Strict Priority. In this case traffic for the SP queues is always sent before traffic from the WRR queues. After the SP queues have been emptied, traffic from the WRR queues is forwarded.

To view and configure Queue Scheduling, click **QoS >> General >> Queue Scheduling**



- ∨ Port
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ **QoS**
 - ∧ General
 - Property
 - Queue Scheduling**
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping
 - ∨ Rate Limit
- ∨ Diagnostics
- ∨ Management

QoS >> General >> Queue Scheduling

Queue Scheduling Table

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	<input checked="" type="radio"/>	<input type="radio"/>	1	
2	<input checked="" type="radio"/>	<input type="radio"/>	2	
3	<input checked="" type="radio"/>	<input type="radio"/>	3	
4	<input checked="" type="radio"/>	<input type="radio"/>	4	
5	<input checked="" type="radio"/>	<input type="radio"/>	5	
6	<input checked="" type="radio"/>	<input type="radio"/>	9	
7	<input checked="" type="radio"/>	<input type="radio"/>	13	
8	<input checked="" type="radio"/>	<input type="radio"/>	15	

Apply

Fig 14.1.6 Default QoS Scheduling table page



QoS >> General >> Queue Scheduling

- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ▼ **QoS**
 - ^ General
 - Property
 - Queue Scheduling**
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping
 - ✓ Rate Limit
- ✓ Diagnostics
- ✓ Management

Queue Scheduling Table

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="1"/>	6.67%
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="2"/>	13.33%
3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="3"/>	20%
4	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="4"/>	26.67%
5	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="5"/>	33.33%
6	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="9"/>	
7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="13"/>	
8	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="15"/>	

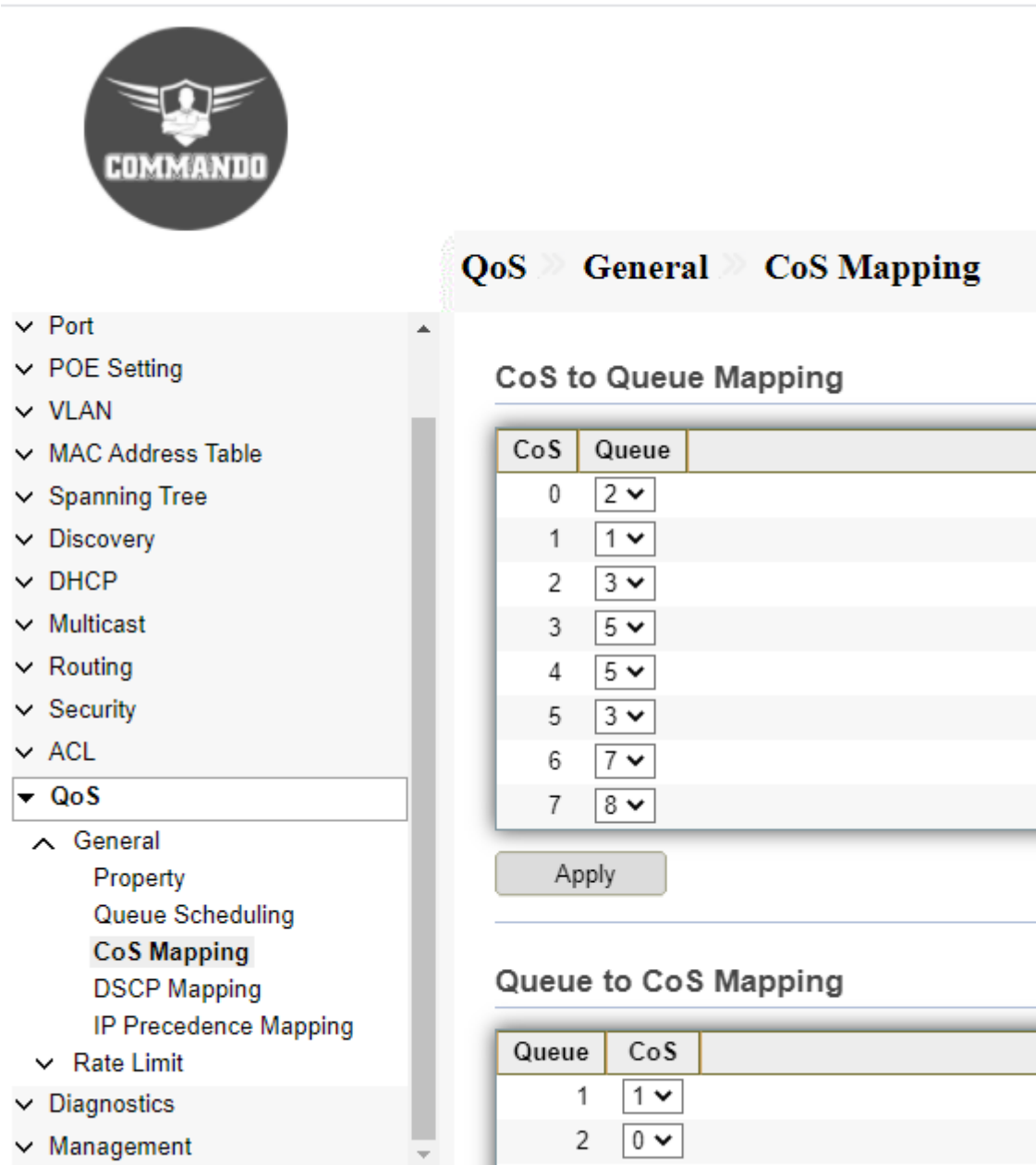
Apply

Fig 14.1.7 QoS Scheduling changing Queue Method page

14.1.3 CoS Mapping

The CoS to Queue table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports. CoS/802.1p priority for egress traffic from each queue can be set.

To view and configure CoS Mapping, click **QoS >> General >> CoS Mapping**



The screenshot shows the COMMANDO network management interface. On the left is a navigation menu with a tree structure. The 'QoS' section is expanded, and 'CoS Mapping' is selected. The main content area shows the 'CoS to Queue Mapping' configuration page. At the top of this page is a breadcrumb trail: 'QoS >> General >> CoS Mapping'. Below the breadcrumb is a table for mapping CoS values to Queue numbers. The table has two columns: 'CoS' and 'Queue'. The rows show CoS values from 0 to 7, each with a corresponding Queue value selected in a dropdown menu. Below the table is an 'Apply' button. Further down, there is a section for 'Queue to CoS Mapping' with a table showing Queue numbers 1 and 2, each with a corresponding CoS value selected in a dropdown menu.

COMMANDO

QoS >> General >> CoS Mapping

CoS to Queue Mapping

CoS	Queue
0	2
1	1
2	3
3	5
4	5
5	3
6	7
7	8

Apply

Queue to CoS Mapping

Queue	CoS
1	1
2	0

Fig 14.1.8 CoS to Queue Mapping Changing Queue values page



- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ▼ **QoS**
 - ^ General
 - Property
 - Queue Scheduling
 - CoS Mapping**
 - DSCP Mapping
 - IP Precedence Mapping
 - ✓ Rate Limit
- ✓ Diagnostics
- ✓ Management

QoS >> General >> CoS Mapping

6	7 ▼
7	8 ▼

Apply

Queue to CoS Mapping

Queue	CoS
1	1 ▼
2	0 ▼
3	2 ▼
4	3 ▼
5	1 ▼
6	1 ▼
7	6 ▼
8	7 ▼

Apply

Fig 14.1.9 Queue to CoS Mapping Changing Queue values page

14.1.4 DSCP Mapping

The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. we can change DSCP value for egress traffic from each queue.

To view and configure DSCP Mapping, click **QoS >> General >> DSCP Mapping**.



QoS >> General >> DSCP Mapping

DSCP to Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	1 ▾	16 [CS2]	3 ▾	32 [CS4]	5 ▾	48 [CS6]	7 ▾
1	1 ▾	17	3 ▾	33	5 ▾	49	7 ▾
2	1 ▾	18 [AF21]	3 ▾	34 [AF41]	5 ▾	50	7 ▾
3	1 ▾	19	3 ▾	35	5 ▾	51	7 ▾
4	1 ▾	20 [AF22]	3 ▾	36 [AF42]	5 ▾	52	7 ▾
5	1 ▾	21	3 ▾	37	5 ▾	53	7 ▾
6	1 ▾	22 [AF23]	3 ▾	38 [AF43]	5 ▾	54	7 ▾
7	1 ▾	23	3 ▾	39	5 ▾	55	7 ▾
8 [CS1]	2 ▾	24 [CS3]	4 ▾	40 [CS5]	6 ▾	56 [CS7]	8 ▾
9	2 ▾	25	4 ▾	41	6 ▾	57	8 ▾
10 [AF11]	2 ▾	26 [AF31]	4 ▾	42	6 ▾	58	8 ▾
11	2 ▾	27	4 ▾	43	6 ▾	59	8 ▾
12 [AF12]	2 ▾	28 [AF32]	4 ▾	44	6 ▾	60	8 ▾
13	2 ▾	29	4 ▾	45	6 ▾	61	8 ▾
14 [AF13]	2 ▾	30 [AF33]	4 ▾	46 [EF]	6 ▾	62	8 ▾
15	2 ▾	31	4 ▾	47	6 ▾	63	8 ▾

Apply

Fig 14.1.11 Default DSCP to Queue Mapping page



QoS » General » DSCP Mapping

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ **QoS**
 - ^ General
 - Property
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping**
 - IP Precedence Mapping
- ▼ Rate Limit
- ▼ Diagnostics
- ▼ Management

DSCP to Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	1 ▼	16 [CS2]	3 ▼	32 [CS4]	5 ▼	48 [CS6]	7 ▼
1	1 ▼	17	3 ▼	33	5 ▼	49	7 ▼
2	1 ▼	18 [AF21]	3 ▼	34 [AF41]	5 ▼	50	5 ▼
3	7 ▼	19	6 ▼	35	5 ▼	51	7 ▼
4	1 ▼	20 [AF22]	3 ▼	36 [AF42]	7 ▼	52	7 ▼
5	1 ▼	21	3 ▼	37	5 ▼	53	7 ▼
6	1 ▼	22 [AF23]	3 ▼	38 [AF43]	5 ▼	54	7 ▼
7	1 ▼	23	3 ▼	39	5 ▼	55	7 ▼
8 [CS1]	5 ▼	24 [CS3]	5 ▼	40 [CS5]	5 ▼	56 [CS7]	5 ▼
9	2 ▼	25	4 ▼	41	6 ▼	57	8 ▼
10 [AF11]	2 ▼	26 [AF31]	4 ▼	42	6 ▼	58	8 ▼
11	2 ▼	27	4 ▼	43	6 ▼	59	8 ▼
12 [AF12]	2 ▼	28 [AF32]	4 ▼	44	6 ▼	60	8 ▼
13	2 ▼	29	4 ▼	45	6 ▼	61	8 ▼
14 [AF13]	2 ▼	30 [AF33]	4 ▼	46 [EF]	6 ▼	62	8 ▼
15	2 ▼	31	4 ▼	47	6 ▼	63	8 ▼

Apply

Fig 14.1.12 Changing DSCP to Queue Mapping page



QoS » General » DSCP Mapping

- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ▼ **QoS**
 - ^ General
 - Property
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping**
 - IP Precedence Mapping
 - ✓ Rate Limit
- ✓ Diagnostics
- ✓ Management

Apply

Queue to DSCP Mapping

Queue	DSCP
1	0 [CS0] ▼
2	8 [CS1] ▼
3	16 [CS2] ▼
4	24 [CS3] ▼
5	22 [AF23] ▼
6	4 ▼
7	48 [CS6] ▼
8	56 [CS7] ▼

Apply

Fig 14.1.13 Changing Queue to DSCP Mapping page

14.1.5 IP Precedence Mapping

This page allow user to configure IP Precedence to Queue mapping and Queue to IP Precedence mapping.

To view and configure IP Precedence Mapping, click **QoS >> General >> IP Precedence Mapping**.



- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ **QoS**
 - ∧ General
 - Property
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping**
 - ∨ Rate Limit
- ∨ Diagnostics
- ∨ Management

QoS >> General >> IP Precedence Mapping

IP Precedence to Queue Mapping

IP Precedence	Queue
0	1 ▾
1	2 ▾
2	3 ▾
3	4 ▾
4	5 ▾
5	6 ▾
6	7 ▾
7	8 ▾

Apply

Queue to IP Precedence Mapping

Fig 14.1.15 IP Precedence to queue Mapping page



- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ▼ **QoS**
 - ^ General
 - Property
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping**
 - ✓ Rate Limit
- ✓ Diagnostics
- ✓ Management

QoS >> General >> IP Precedence Mapping

IP Precedence to Queue Mapping

IP Precedence	Queue
0	1 ▼
1	2 ▼
2	2 ▼
3	7 ▼
4	6 ▼
5	8 ▼
6	3 ▼
7	4 ▼

Apply

Queue to IP Precedence Mapping

Queue	IP Precedence
-------	---------------

Fig 14.1.16 Changing IP Precedence to Queue Mapping values page



QoS » General » IP Precedence Mapping

Apply

Queue to IP Precedence Mapping

Queue	IP Precedence
1	0 ▼
2	1 ▼
3	2 ▼
4	3 ▼
5	4 ▼
6	5 ▼
7	6 ▼
8	7 ▼

Apply

Navigation Menu:

- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS**
 - General
 - Property
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping**
 - Rate Limit
- Diagnostics
- Management

Fig 14.1.17 Queue to IP Precedence Mapping page



- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ▼ **QoS**
 - ^ General
 - Property
 - Queue Scheduling
 - CoS Mapping
 - DSCP Mapping
 - IP Precedence Mapping**
 - ✓ Rate Limit
- ✓ Diagnostics
- ✓ Management

QoS >> General >> IP Precedence Mapping

Apply

Queue to IP Precedence Mapping

Queue	IP Precedence
1	0 ▼
2	1 ▼
3	6 ▼
4	1 ▼
5	4 ▼
6	1 ▼
7	4 ▼
8	4 ▼

Apply

Fig 14.1.18 Changing Queue to IP Precedence Mapping values page

14.2 Rate Limit

Rate limiting simply means that the switch will slow down traffic on a port to keep it from exceeding the limit that you set. Rate Limit pages to define values that determine how much traffic the switch can receive and send on specific port or queue. With Rate Limit configured, we can protect the network bandwidth from being occupied too much by some of the clients.

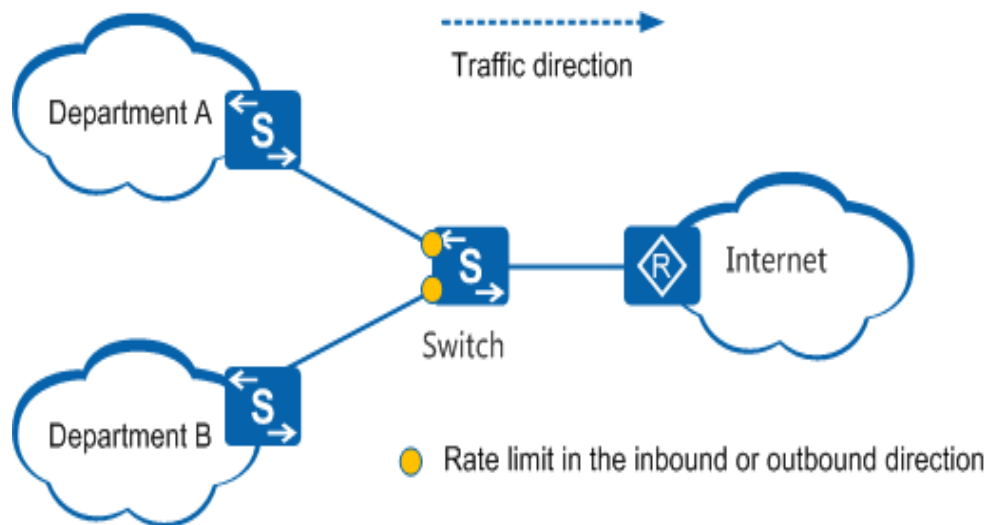


Fig 14.2.1 Rate Limiting concept

14.2.1 Ingress / Egress Port

This page allow user to configure ingress port rate limit and egress port rate limit.

The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded in inbound and outbound direction.

To view and configure Ingress / Egress Port, click **QoS >> Rate Limit >> Ingress / Egress Port**.



QoS >> Rate Limit >> Ingress / Egress Port

Ingress / Egress Port Table

<input type="checkbox"/>	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
<input type="checkbox"/>	1	GE1	Disabled		Disabled	
<input type="checkbox"/>	2	GE2	Disabled		Disabled	
<input type="checkbox"/>	3	GE3	Disabled		Disabled	
<input type="checkbox"/>	4	GE4	Disabled		Disabled	
<input type="checkbox"/>	5	GE5	Disabled		Disabled	
<input type="checkbox"/>	6	GE6	Disabled		Disabled	
<input type="checkbox"/>	7	GE7	Disabled		Disabled	
<input type="checkbox"/>	8	GE8	Disabled		Disabled	
<input type="checkbox"/>	9	GE9	Disabled		Disabled	
<input type="checkbox"/>	10	GE10	Disabled		Disabled	
<input type="checkbox"/>	11	GE11	Disabled		Disabled	

Navigation menu on the left:

- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS**
 - General
 - Rate Limit
 - Ingress / Egress Port**
 - Egress Queue
- Diagnostics
- Management

Fig 14.2.1 Ingress / Egress Port Table page



- ∨ Port
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ **QoS**
 - ∨ General
 - ∧ Rate Limit
 - Ingress / Egress Port**
 - Egress Queue
- ∨ Diagnostics
- ∨ Management

QoS » Rate Limit » Ingress / Egress Port

Ingress / Egress Port Table

<input checked="" type="checkbox"/>	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
<input checked="" type="checkbox"/>	1	GE1	Disabled		Disabled	
<input checked="" type="checkbox"/>	2	GE2	Disabled		Disabled	
<input checked="" type="checkbox"/>	3	GE3	Disabled		Disabled	
<input checked="" type="checkbox"/>	4	GE4	Disabled		Disabled	
<input checked="" type="checkbox"/>	5	GE5	Disabled		Disabled	
<input checked="" type="checkbox"/>	6	GE6	Disabled		Disabled	
<input checked="" type="checkbox"/>	7	GE7	Disabled		Disabled	
<input checked="" type="checkbox"/>	8	GE8	Disabled		Disabled	
<input checked="" type="checkbox"/>	9	GE9	Disabled		Disabled	
<input checked="" type="checkbox"/>	10	GE10	Disabled		Disabled	
<input checked="" type="checkbox"/>	11	GE11	Disabled		Disabled	

Fig 14.2.2 Selecting Ingress / Egress Port page



Save |

QoS > Rate Limit > Ingress / Egress Port

- ∨ Port
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ **QoS**
 - ∨ General
 - ∧ Rate Limit
 - Ingress / Egress Port**
 - Egress Queue
- ∨ Diagnostics
- ∨ Management

Edit Ingress / Egress Port

Port	GE1-GE28
Ingress	<input checked="" type="checkbox"/> Enable
	<input type="text" value="2000"/> Kbps (16 - 1000000)
Egress	<input checked="" type="checkbox"/> Enable
	<input type="text" value="1000000"/> Kbps (16 - 1000000)

Fig 14.2.3 Edit Rate Ingress / Egress Port page



QoS » Rate Limit » Ingress / Egress Port

- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ▼ **QoS**
 - ✓ General
 - ^ Rate Limit
 - Ingress / Egress Port**
 - Egress Queue
- ✓ Diagnostics
- ✓ Management

Ingress / Egress Port Table

<input type="checkbox"/>	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
<input type="checkbox"/>	1	GE1	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	2	GE2	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	3	GE3	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	4	GE4	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	5	GE5	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	6	GE6	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	7	GE7	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	8	GE8	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	9	GE9	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	10	GE10	Enabled	2000	Enabled	1000000
<input type="checkbox"/>	11	GE11	Enabled	2000	Enabled	1000000

Fig 14.2.4 Selecting Ingress / Egress Port page

14.2.2 Egress Queue

Egress rate limiting is performed by shaping the output load.

To view and configure Egress Queue, click **QoS >> Rate Limit >> Egress Queue**.

The screenshot shows the 'Egress Queue Table' page in the COMMANDO interface. The page includes a navigation menu on the left, a search bar, and a table with the following structure:

Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue 7		Queue 8	
		State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
<input type="checkbox"/>	1 GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	2 GE2	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	3 GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	4 GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	5 GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	6 GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	7 GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	8 GE8	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	9 GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	10 GE10	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	11 GE11	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	12 GE12	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	13 GE13	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	14 GE14	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

Fig 14.2.7 Default Egress Queue Table page

The screenshot shows the 'Egress Queue Table' page in the COMMANDO interface. The page includes a navigation menu on the left, a search bar, and a table with the following structure:

Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue 7		Queue 8	
		State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
<input type="checkbox"/>	1 GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	2 GE2	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input checked="" type="checkbox"/>	3 GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input checked="" type="checkbox"/>	4 GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input checked="" type="checkbox"/>	5 GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	6 GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	7 GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	8 GE8	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	9 GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	10 GE10	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	11 GE11	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	12 GE12	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	13 GE13	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	14 GE14	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

Fig 14.2.8 Selecting Egress Queue ports page



QoS Rate Limit Egress Queue

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ▼ QoS
 - ✓ General
 - ^ Rate Limit
 - Ingress / Egress Port
 - Egress Queue**
- ✓ Diagnostics
- ✓ Management

Edit Egress Queue

Port	GE2-GE5
Queue 1	<input checked="" type="checkbox"/> Enable <input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 2	<input checked="" type="checkbox"/> Enable <input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 3	<input checked="" type="checkbox"/> Enable <input type="text" value="3000"/> Kbps (16 - 1000000)
Queue 4	<input checked="" type="checkbox"/> Enable <input type="text" value="400"/> Kbps (16 - 1000000)
Queue 5	<input checked="" type="checkbox"/> Enable <input type="text" value="60000"/> Kbps (16 - 1000000)
Queue 6	<input type="checkbox"/> Enable <input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 7	<input type="checkbox"/> Enable <input type="text" value="1000000"/> Kbps (16 - 1000000)
Queue 8	<input type="checkbox"/> Enable <input type="text" value="1000000"/> Kbps (16 - 1000000)

Fig 14.2.9 Edit Egress Queue page



Save | Logout | Reboot |

QoS > Rate Limit > Egress Queue

- ∨ Status
- ∨ Network
- ∨ Port
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ QoS
 - ∨ General
 - ∧ Rate Limit
 - Ingress / Egress Port
 - Egress Queue**
- ∨ Diagnostics
- ∨ Management

Egress Queue Table

	Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6	
			State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
<input type="checkbox"/>	1	GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	2	GE2	Enabled	1000000	Enabled	1000000	Enabled	3008	Enabled	400	Enabled	60000	Disabled	
<input type="checkbox"/>	3	GE3	Enabled	1000000	Enabled	1000000	Enabled	3008	Enabled	400	Enabled	60000	Disabled	
<input type="checkbox"/>	4	GE4	Enabled	1000000	Enabled	1000000	Enabled	3008	Enabled	400	Enabled	60000	Disabled	
<input type="checkbox"/>	5	GE5	Enabled	1000000	Enabled	1000000	Enabled	3008	Enabled	400	Enabled	60000	Disabled	
<input type="checkbox"/>	6	GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	7	GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	8	GE8	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	9	GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	10	GE10	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	11	GE11	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	12	GE12	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
<input type="checkbox"/>	13	GE13	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

Fig 14.2.10 Egress Queue Table after Editing Queue page

Chapter 15 Diagnostics

Logging: Log files of a switch are classified into user log files and diagnostic log files.

Property: A diagnostic log file records the service processing flow and fault information. These logs sent to the log buffer, console, or terminal monitors.

Remote Server: You can set up a switch to automatically transfer diagnostic information to a remote server. If a fault occurs, you can provide your customer support.

Ping: Ping (Packet Internet Groper) tests the connection between two network nodes by sending packets to a host and measure the round-trip time.

Traceroute: Traceroute is used to display the route (path) each node has passed to reach the tested host, and measure transit delays of packets across entire path to host.

Copper Test: The Copper Test feature of the switch tests whether a port can link up or not through an RJ45 connector and helps to determine the cable performance and can carry out diagnostic test on the cable that is plugged on Switch ports to see its online status. With this information in hand, you can troubleshoot an interface.

Fiber Module: SFP module is available in two form-factors: GBIC or SFP. The operational information reported by the Small Form-factor Pluggable (SFP) transceiver are shown by E3000 Series Switches.

UDLD: UDLD (Unidirectional Link Detection) is a layer 1/2 protocol (unrelated to spanning tree) that protects the upper layer protocols from causing loops in the network. Unidirectional link occurs when traffic is transmitted between neighbors in one direction only which can cause spanning-tree topology loops.

Property: When a unidirectional link is detected, UDLD shuts down the affected LAN port and alerts the user. Unidirectional links can cause a variety of problems, including spanning tree topology loops. UDLD is a Layer 2 protocol that works with the Layer 1 protocols to determine the physical status of a link.

Neighbor: After enabling UDLD on the connected interface of the other switch, we can see that the local switch has detected its neighbor and updated the link's status to bidirectional. UDLD is capable of tracking multiple neighbors per interface.

15.1 Logging

Log files of a switch are classified into user log files and diagnostic log files. To Enable/Disable the global logging services these pages are used. When the logging service is enabled, Console Logging, RAM Logging, Flash Logging can be configured.

15.1.1 Property

To enable/disable the logging service, click **Diagnostic >> Logging >> Property**. By default, Console port showing informational messages.

COMMANDO

Diagnostics >> Logging >> Property

- State: Enable
- Aggregation: Enable
- Aging Time: Sec (15 - 3600, default 300)

Console Logging

- State: Enable
- Minimum Severity: (Note: Emergency, Alert, Critical, Error, Warning, Notice, Informational)

RAM Logging

- State: Enable
- Minimum Severity: (Note: Emergency, Alert, Critical, Error, Warning, Notice, Informational)

Flash Logging

- State: Enable
- Minimum Severity: (Note: Emergency, Alert, Critical, Error, Warning, Notice, Informational)

Fig 15.1.1 Diagnostic Logging Property page



Diagnostics » Logging » Property

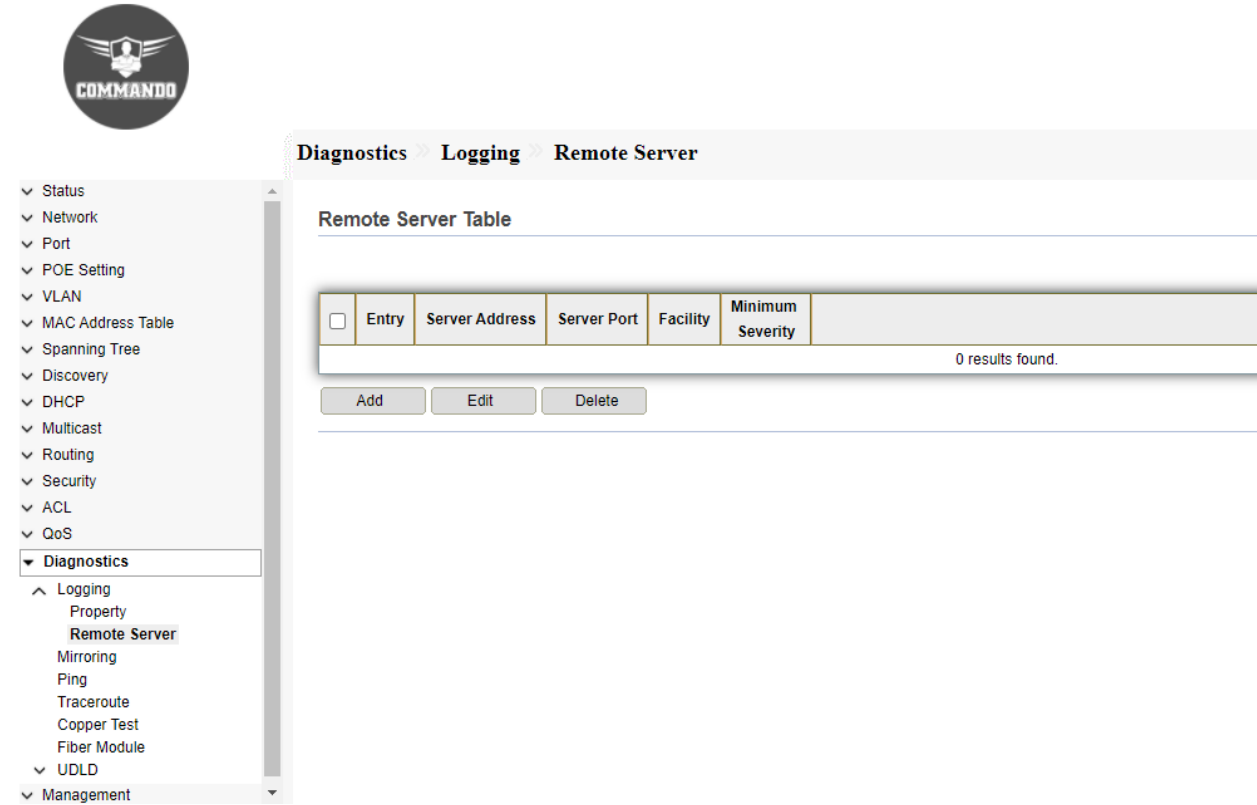
- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ **Diagnostics**
 - ^ Logging
 - Property**
 - Remote Server
 - Mirroring
 - Ping
 - Traceroute
 - Copper Test
 - Fiber Module
 - ▼ UDLD

State	<input checked="" type="checkbox"/> Enable
Aggregation	<input checked="" type="checkbox"/> Enable
Aging Time	<input type="text" value="300"/> Sec (15 - 3600, default 300)
Console Logging	
State	<input checked="" type="checkbox"/> Enable
Minimum Severity	<input type="text" value="Warning"/> Note: Emergency, Alert, Critical, Error, Warning
RAM Logging	
State	<input checked="" type="checkbox"/> Enable
Minimum Severity	<input type="text" value="Critical"/> Note: Emergency, Alert, Critical
Flash Logging	
State	<input type="checkbox"/> Enable
Minimum Severity	<input type="text" value="Informational"/> Note: Emergency, Alert, Critical, Error, Warning, Notice, Informational

Fig 15.1.2 Changing Diagnostic Logging Property options page

15.1.2 Remote Server

To configure the remote logging server, click **Diagnostic >> Logging >> Remote Server**.



The screenshot displays the COMMANDO web interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, Logging, Property, Remote Server, Mirroring, Ping, Traceroute, Copper Test, Fiber Module, UDLD, and Management. The 'Diagnostics' menu is expanded, and 'Remote Server' is selected. The main content area shows the breadcrumb 'Diagnostics > Logging > Remote Server' and a table titled 'Remote Server Table'. The table has columns for 'Entry', 'Server Address', 'Server Port', 'Facility', and 'Minimum Severity'. Below the table, it indicates '0 results found.' and provides 'Add', 'Edit', and 'Delete' buttons.

<input type="checkbox"/>	Entry	Server Address	Server Port	Facility	Minimum Severity
0 results found.					

Fig 15.1.3 Diagnostic Logging Default remote server page



Diagnostics > Logging > Remote Server

- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ▼ **Diagnostics**
 - ^ Logging
 - Property
 - Remote Server**
 - Mirroring
 - Ping
 - Traceroute
 - Copper Test
 - Fiber Module
 - ✓ UDLD

Add Remote Server

Address Type	<input type="radio"/> Hostname
	<input checked="" type="radio"/> IPv4
	<input type="radio"/> IPv6
Server Address	<input type="text" value="192.168.0.50"/>
Server Port	<input type="text" value="514"/> (1 - 65535, default 514)
Facility	<input type="text" value="Local 4"/>
Minimum Severity	<input type="text" value="Critical"/>
	Note: Emergency, Alert, Critical

Apply Close

Fig 15.1.4 Diagnostic Logging Add remote server page



Diagnostics » Logging » Remote Server

Remote Server Table

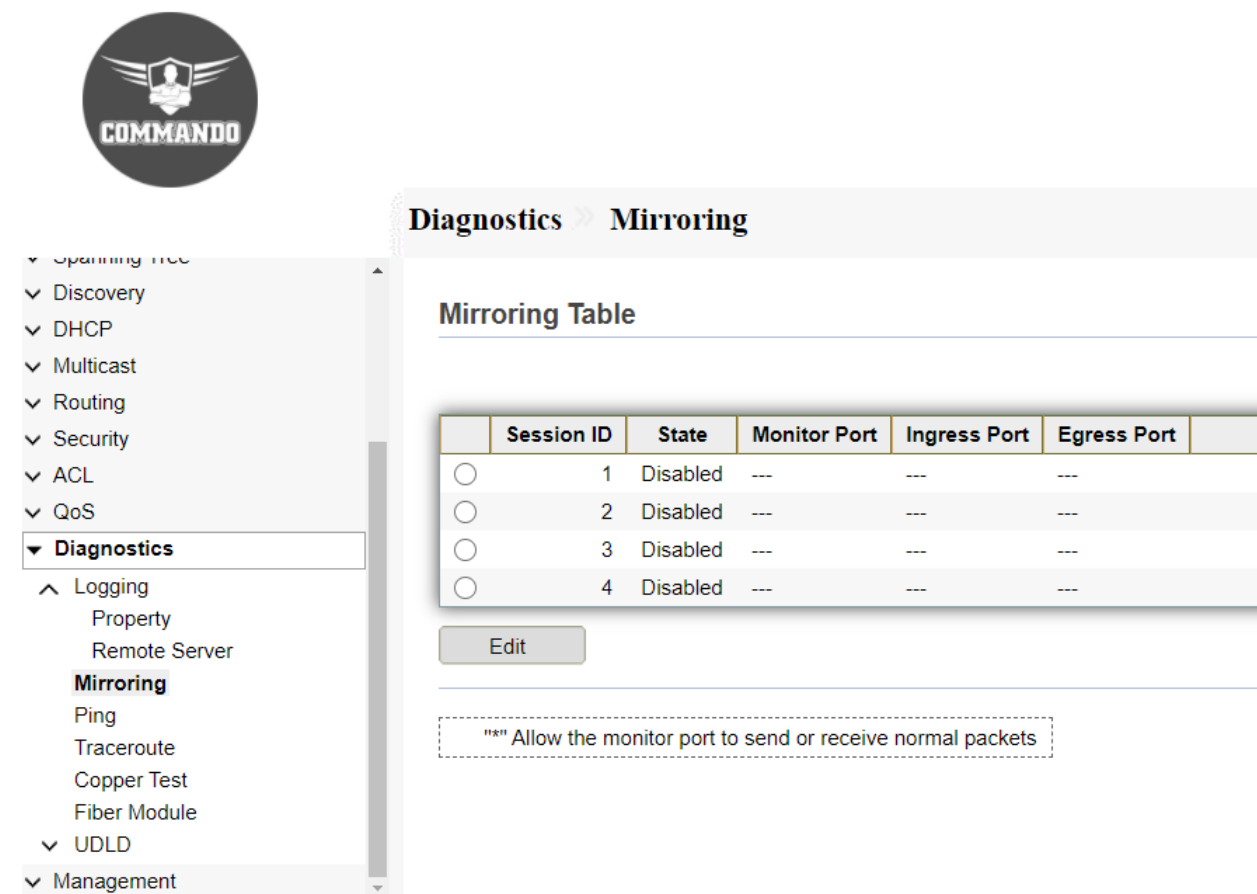
<input type="checkbox"/>	Entry	Server Address	Server Port	Facility	Minimum Severity	
<input type="checkbox"/>	1	192.168.0.50	514	Local 4	Critical	

Fig 15.1.5 Diagnostic Logging remote server Table page

15.2 Mirroring

Port mirroring is used on a network device to send a copy of network packets seen on other ports or multiple switch ports, or an entire VLAN to a network monitoring connection on another port on the device. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion detection system. A network analyzer connected to the monitoring port processes the data packets for diagnosing, debugging, and performance monitoring. Mirroring does not guarantee that all traffic from the source port(s) is received on the analyzer (destination) port. If more data is sent to the analyzer port than it can support, some data might be lost. Port mirroring lets you mirror the incoming (ingress) and outgoing (egress) traffic of a single port to a predefined destination port.

The mirroring option is ideal for performing diagnostics by allowing traffic that is being sent to and received from one or more source ports to be replicated out a monitoring/target port. To configure Port Mirroring, click **Port >> Mirroring**.



COMMANDO

Diagnostics > Mirroring

Mirroring Table

	Session ID	State	Monitor Port	Ingress Port	Egress Port	
<input type="radio"/>	1	Disabled	---	---	---	
<input type="radio"/>	2	Disabled	---	---	---	
<input type="radio"/>	3	Disabled	---	---	---	
<input type="radio"/>	4	Disabled	---	---	---	

*** Allow the monitor port to send or receive normal packets

Fig 15.2.1 Mirroring Table page



Diagnostics > Mirroring

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ▼ **Diagnostics**
 - ^ Logging
 - Property
 - Remote Server
 - Mirroring**
 - Ping
 - Traceroute
 - Copper Test
 - Fiber Module
- ✓ UDLD
- ✓ Management

Allow the monitor port to send or receive normal packets

Edit Mirroring

Session ID	1	
State	<input checked="" type="checkbox"/> Enable	
Monitor Port	GE17	
	<input type="checkbox"/> Send or Receive Normal Packet	
Ingress Port	Available Port	Selected Port
	LAG1 LAG2 LAG3 LAG4 LAG5 LAG6 LAG7 LAG8	GE2
Egress Port	Available Port	Selected Port
	LAG1 LAG2 LAG3 LAG4 LAG5 LAG6 LAG7 LAG8	GE4

Apply Close

Fig 15.2.2 Edit Port Mirroring page



- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ▼ **Diagnostics**
 - ^ Logging
 - Property
 - Remote Server
 - Mirroring**
 - Ping
 - Traceroute
 - Copper Test
 - Fiber Module
- ✓ UDLD
- ✓ Management

Diagnostics > Mirroring

Mirroring Table

	Session ID	State	Monitor Port	Ingress Port	Egress Port
<input type="radio"/>	1	Enabled	GE17	GE2	GE4
<input type="radio"/>	2	Disabled	---	---	---
<input type="radio"/>	3	Disabled	---	---	---
<input type="radio"/>	4	Disabled	---	---	---

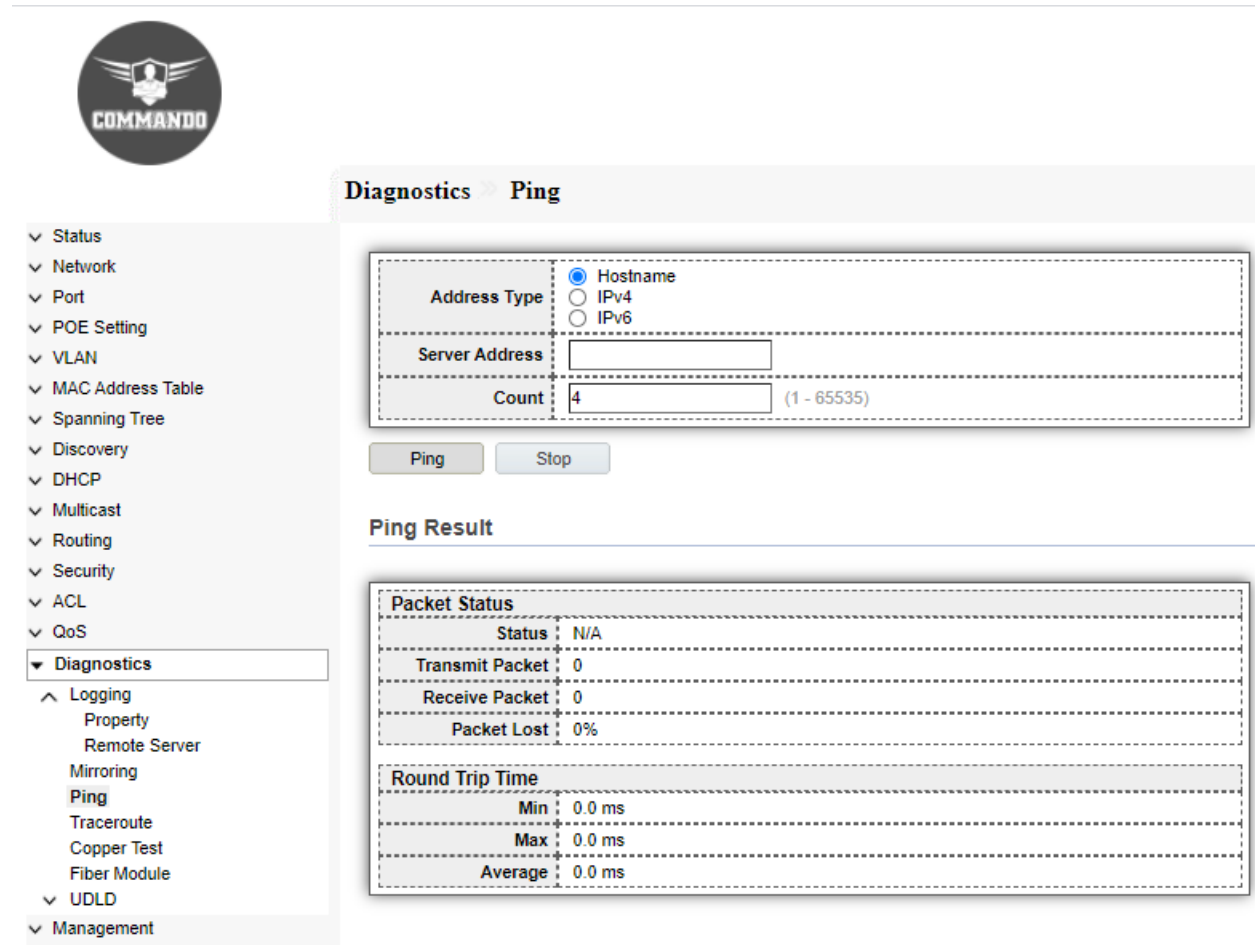
Edit

** Allow the monitor port to send or receive normal packets

Fig 15.2.3 Mirroring Table after configuring GE1 as monitor port page

15.2 Ping

Ping (Packet Internet Groper) tests the connection between two network nodes by sending packets to a host and measure the round-trip time. You can Ping to any IP or Hostname for that click **Diagnostic >> Ping**.



The screenshot displays the COMMANDO network management interface. On the left is a sidebar menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, Logging, Property, Remote Server, Mirroring, Ping, Traceroute, Copper Test, Fiber Module, UDLD, and Management. The 'Diagnostics' section is expanded, and 'Ping' is selected.

The main content area is titled 'Diagnostics > Ping'. It contains a configuration form with the following fields:

- Address Type:** Radio buttons for Hostname (selected), IPv4, and IPv6.
- Server Address:** An empty text input field.
- Count:** A text input field containing '4', with '(1 - 65535)' to its right.

Below the form are two buttons: 'Ping' and 'Stop'.

The 'Ping Result' section contains a table with the following data:

Packet Status	
Status	N/A
Transmit Packet	0
Receive Packet	0
Packet Lost	0%

Round Trip Time	
Min	0.0 ms
Max	0.0 ms
Average	0.0 ms

Fig 15.2.1 Diagnostic Default Ping test page



Diagnostics > Ping

- ✓ Status
- ✓ Network
- ✓ Port
- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ▼ **Diagnostics**
 - ^ Logging
 - Property
 - Remote Server
 - Mirroring
 - Ping**
 - Traceroute
 - Copper Test
 - Fiber Module
 - ✓ UDLD
 - ✓ Management

Address Type	<input type="radio"/> Hostname
	<input checked="" type="radio"/> IPv4
	<input type="radio"/> IPv6
Server Address	<input type="text" value="192.168.0.10"/>
Count	<input type="text" value="8"/> (1 - 65535)

Ping Result

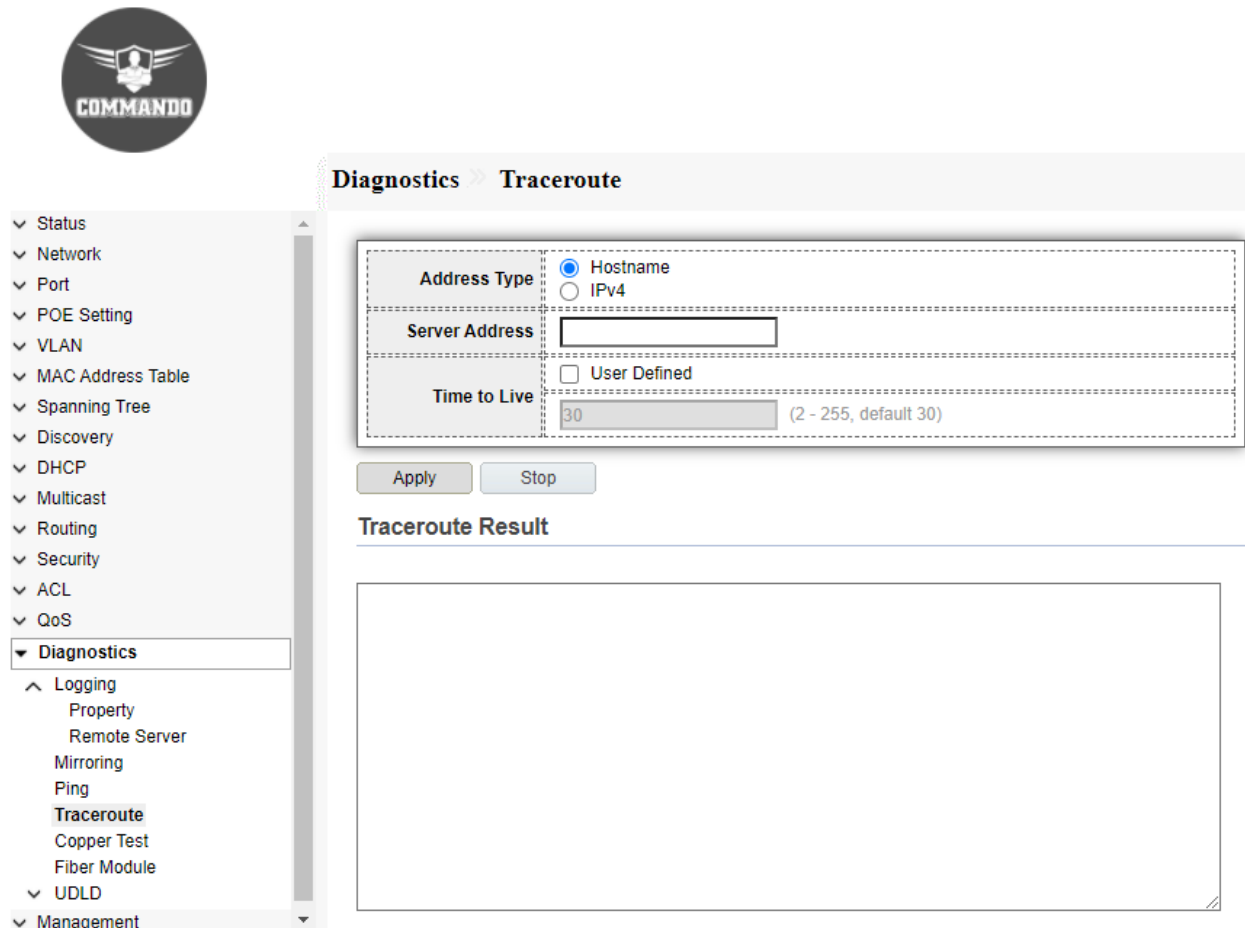
Packet Status	
Status	Success
Transmit Packet	8
Receive Packet	8
Packet Lost	0 %

Round Trip Time	
Min	Max
0 ms	0 ms
Average	0 ms

Fig 15.2.2 Diagnostic Ping test result page

15.3 Traceroute

Traceroute discovers the IP routes along which packets were forwarded by sending an IP packet to the target host and back to the device. The Trace route page shows each hop between the device and a target host, and the round-trip time to each such hop. You can Traceroute any IP or Hostname for that click **Diagnostic >> Traceroute**.



The screenshot displays the COMMANDO network management interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, Logging, Property, Remote Server, Mirroring, Ping, Traceroute, Copper Test, Fiber Module, UDLD, and Management. The 'Diagnostics' menu is expanded, and 'Traceroute' is selected. The main content area is titled 'Diagnostics >> Traceroute'. It contains a configuration form with the following fields: 'Address Type' with radio buttons for 'Hostname' (selected) and 'IPv4'; 'Server Address' with an empty text input field; and 'Time to Live' with a checkbox for 'User Defined' (unchecked) and a numeric input field set to '30' (with a note '(2 - 255, default 30)'). Below the form are 'Apply' and 'Stop' buttons. Underneath is a section titled 'Traceroute Result' with a large empty rectangular area for the output.

Fig 15.3.1 Diagnostic Traceroute Default test page



Diagnostics » Traceroute

Address Type	<input type="radio"/> Hostname
	<input checked="" type="radio"/> IPv4
Server Address	<input type="text" value="192.168.0.10"/>
Time to Live	<input checked="" type="checkbox"/> User Defined
	<input type="text" value="3"/> (2 - 255, default 30)

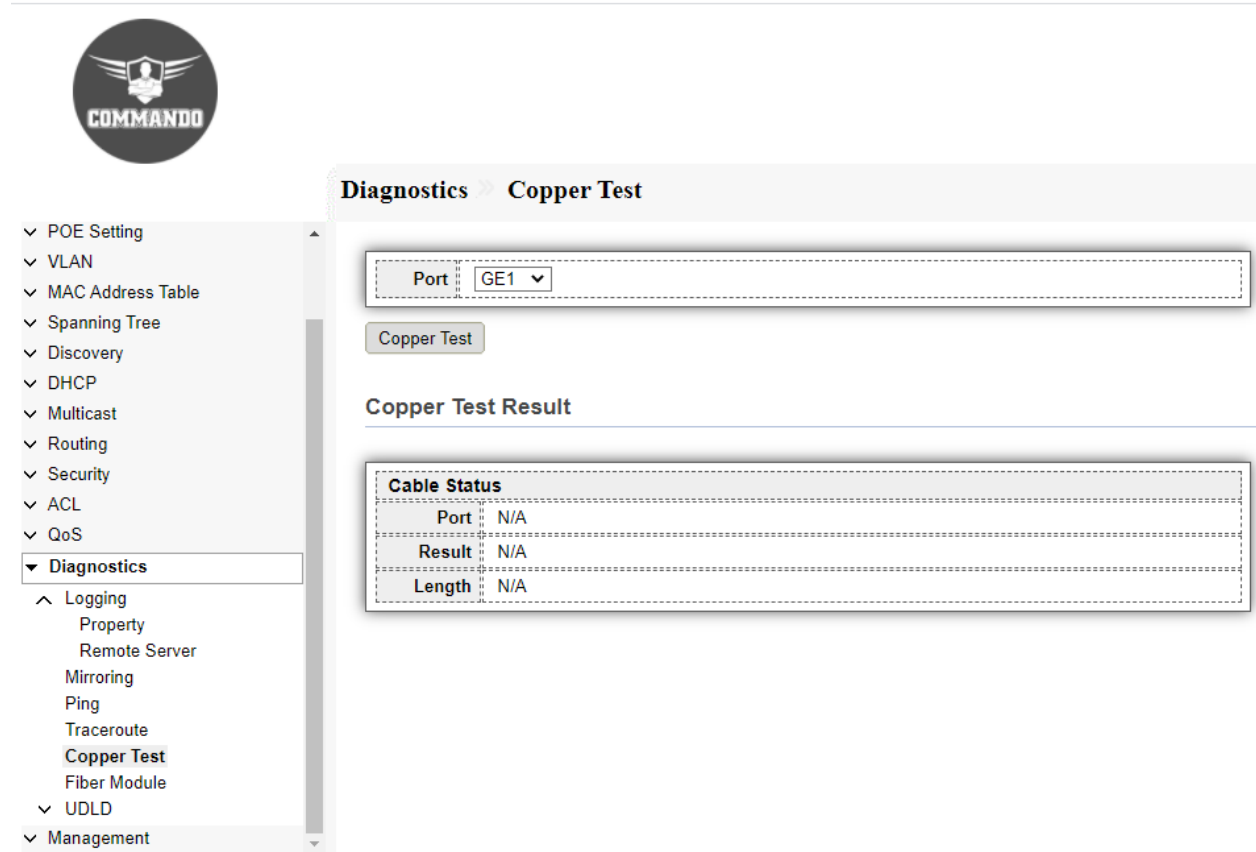
Traceroute Result

```
traceroute to 192.168.0.10 (192.168.0.10), 3 hops max, 38 byte packets
1 192.168.0.10 (192.168.0.10) 0.000 ms 0.000 ms 0.000 ms
Trace complete
```

Fig 15.3.2 Traceroute result page

15.4 Copper Test

The Copper Test feature of the switch tests whether a port can link up or not through an RJ45 connector and helps to determine the cable performance and can carry out diagnostic test on the cable that is plugged on Switch ports to see its online status. With this information in hand, you can troubleshoot an interface. For copper length diagnostic, click **Diagnostic > Copper Test**.



The screenshot displays the COMMANDO network management interface. On the left is a sidebar menu with various configuration options, including 'Diagnostics' which is expanded to show 'Copper Test'. The main content area is titled 'Diagnostics > Copper Test'. It features a 'Port' dropdown menu currently set to 'GE1', a 'Copper Test' button, and a 'Cable Status' table. The table has three rows: 'Port', 'Result', and 'Length', each with a value of 'N/A'.

Cable Status	
Port	N/A
Result	N/A
Length	N/A

15.4.1 Diagnostic Default Copper Test Result page



- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ▼ **Diagnostics**
 - ^ Logging
 - Property
 - Remote Server
 - Mirroring
 - Ping
 - Traceroute
 - Copper Test**
 - Fiber Module
- ✓ UDLD
- ✓ Management

Diagnostics > **Copper Test**

Port	GE10 ▼
------	--------

Copper Test

Copper Test Result

Cable Status	
Port	GE10
Result	OK
Length	10.0 M

Fig 15.4.2 Diagnostic Copper Test Result page

15.5 Fiber Module

The Fiber Module Status page displays the operating conditions reported by the SFP (Small Form-factor Pluggable) transceiver. The Optical Module Status page displays the operational information reported by the Small Form-factor Pluggable (SFP) transceiver.

To view and configure the Optical Module Diagnostic, click **Diagnostic >> Fiber Module**.

Save | Logout | Reboot

Diagnostics > Fiber Module

Fiber Module Table

Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
0 results found.							

Refresh Detail

Fig 15.5.1 Diagnostic Default Fiber Module Table page

Save | Logout | Reboot | Debug

Diagnostics Fiber Module

Fiber Module Table

Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
<input type="radio"/> TE1	52.62	3.31	17.69	0.25	0.00	Insert	Loss
<input type="radio"/> TE2	28.42	3.41	7.22	0.63	0.00	Insert	Loss
<input type="radio"/> TE3	19.79	3.31	28.99	0.25	0.33	Insert	Normal
<input type="radio"/> TE4	N/S	N/S	N/S	N/S	N/S	Remove	Loss

Refresh Detail

Fig 15.5.2 Fiber Module Table page

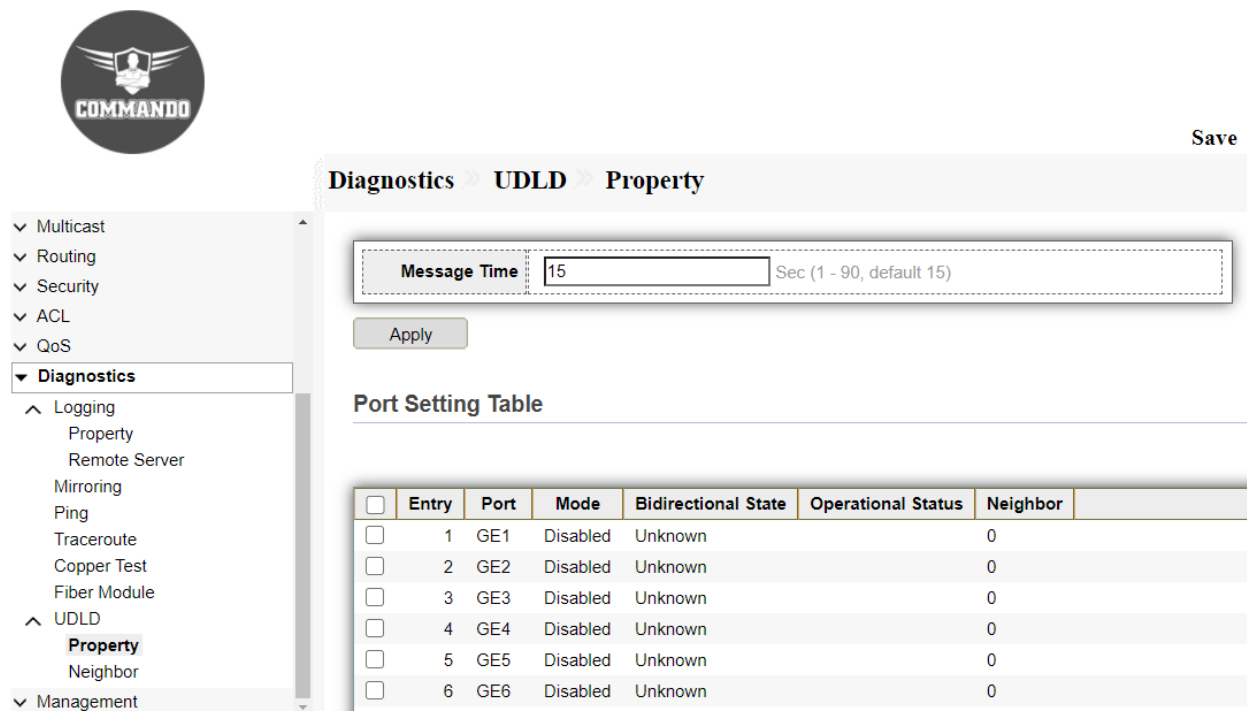
15.6 UDLD

UDLD (Unidirectional Link Detection) is a layer 1/2 protocol (unrelated to spanning tree) that protects the upper layer protocols from causing loops in the network. Unidirectional link occurs when traffic is transmitted between neighbors in one direction only which can cause spanning-tree topology loops. After enabling UDLD on the connected interface of the other switch, we can see that the local switch has detected its neighbor and updated the link's status to bidirectional.

15.6.1 Property

When a unidirectional link is detected, UDLD shuts down the affected LAN port and alerts the user. Unidirectional links can cause a variety of problems, including spanning tree topology loops. UDLD is a Layer 2 protocol that works with the Layer 1 protocols to determine the physical status of a link. This page allow user to configure global and per interface settings of UDLD.

To view and configure UDLD Property, click **Diagnostics >> UDLD >> Property**.



COMMANDO

Save

Diagnostics > UDLD > Property

Message Time: Sec (1 - 90, default 15)

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
<input type="checkbox"/>	1	GE1	Disabled	Unknown		0
<input type="checkbox"/>	2	GE2	Disabled	Unknown		0
<input type="checkbox"/>	3	GE3	Disabled	Unknown		0
<input type="checkbox"/>	4	GE4	Disabled	Unknown		0
<input type="checkbox"/>	5	GE5	Disabled	Unknown		0
<input type="checkbox"/>	6	GE6	Disabled	Unknown		0

Fig 15.6.1 UDLD Default Port Setting Table page



Save

Diagnostics > UDLD > Property

- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ **Diagnostics**
 - ▲ Logging
 - Property
 - Remote Server
 - Mirroring
 - Ping
 - Traceroute
 - Copper Test
 - Fiber Module
 - ▲ UDLD
 - Property**
 - Neighbor
- ▼ Management

Message Time Sec (1 - 90, default 15)

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
<input checked="" type="checkbox"/>	1	GE1	Disabled	Unknown		0
<input checked="" type="checkbox"/>	2	GE2	Disabled	Unknown		0
<input checked="" type="checkbox"/>	3	GE3	Disabled	Unknown		0
<input type="checkbox"/>	4	GE4	Disabled	Unknown		0
<input type="checkbox"/>	5	GE5	Disabled	Unknown		0
<input type="checkbox"/>	6	GE6	Disabled	Unknown		0

Fig 15.6.2 UDLD Port selection page



Save

Diagnostics > UDLD > Property

- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ **Diagnostics**
 - ▲ Logging
 - Property
 - Remote Server
 - Mirroring
 - Ping
 - Traceroute
 - Copper Test
 - Fiber Module
 - ▲ UDLD
 - Property**
 - Neighbor
- ▼ Management

Message Time Sec (1 - 90, default 15)

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
<input type="checkbox"/>	1	GE1	Normal	Unknown	Link up	0
<input type="checkbox"/>	2	GE2	Normal	Unknown	Link down	0
<input type="checkbox"/>	3	GE3	Normal	Unknown	Link down	0
<input type="checkbox"/>	4	GE4	Disabled	Unknown		0
<input type="checkbox"/>	5	GE5	Disabled	Unknown		0
<input type="checkbox"/>	6	GE6	Disabled	Unknown		0

Fig 15.6.3 UDLD Edit Port Setting page



Save

Diagnostics >> UDLD >> Property

- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ▼ **Diagnostics**
 - ^ Logging
 - Property
 - Remote Server
 - Mirroring
 - Ping
 - Traceroute
 - Copper Test
 - Fiber Module
 - ^ UDLD
 - Property**
 - Neighbor
- ✓ Management

Message Time Sec (1 - 90, default 15)

Apply

Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor	
<input type="checkbox"/>	1	GE1	Normal	Unknown	Link up	0	
<input type="checkbox"/>	2	GE2	Normal	Unknown	Link down	0	
<input type="checkbox"/>	3	GE3	Normal	Unknown	Link down	0	
<input type="checkbox"/>	4	GE4	Disabled	Unknown		0	
<input type="checkbox"/>	5	GE5	Disabled	Unknown		0	
<input type="checkbox"/>	6	GE6	Disabled	Unknown		0	
<input type="checkbox"/>	7	GE7	Disabled	Unknown		0	

Fig 15.6.4 UDLD Port Setting Table page

15.6.2 UDLD Neighbor

After enabling UDLD on the connected interface of the other switch, we can see that the local switch has detected its neighbor and updated the link's status to bidirectional. UDLD is capable of tracking multiple neighbors per interface.

To view and configure Neighbor page, click **Diagnostics >> UDLD >> Neighbor**

COMMANDO

Save

Diagnostics >> UDLD >> Neighbor

Neighbor Table

Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval
0 results found.							

Refresh

Fig 15.6.4 UDLD Neighbor Table page

Chapter 16 Management

User Account: Use the Management pages to configure settings for the switch management features.

Management Access: These pages describe access rules for various management methods.

Management VLAN: Management VLAN is used for managing the switch from a remote location by using protocols such as telnet, SSH, SNMP etc. Normally the Management VLAN is VLAN 1, but you can use and configure any VLAN as a management VLAN. You can also configure Management IP address other than 192.168.0.1 and default gateway for Management VLAN.

Management Service: You can manage a switch through Telnet, SSH, HTTP, HTTPS, SNMP via web system and console port.

Management ACL: The management ACL contains rules that define a match condition for an inbound IP packet. You set a rule to allow or deny access to a matching inbound IP packet.

Management ACE: This section describes how to create ACLs and add rules (ACEs) to them.

Firmware: Firmware upgrade or backup firmware image through HTTP or TFTP to enhance functionality of switch.

Upgrade: Upgrade or backup firmware image through HTTP or TFTP server.

Active image: Network administrator can have dual image stored in switch and any one can be used as active image and other as backup image.

Configuration: Upgrade or backup configuration file through HTTP or TFTP server.

Upgrade: Upgrade or backup configuration file through HTTP or TFTP server.

Save Configuration: Configuration file to be saved.

SNMP: The Simple Network Management Protocol (SNMP) is a necessary tool for every network administrator. With an SNMP management station, you can graph the performance of network devices. With SNMP, network managers can view or modify network device information, and troubleshoot according to notifications sent by those devices in a timely manner.

View: E3000 Series Switch supports three SNMP versions: SNMPv1, SNMPv2c and SNMPv3.

Group: SNMP Groups are used to combine the SNMP users based on access privileges and authorization to different SNMP views at the MIBs.

Community: SNMP community string is a user ID or password that is sent along with a Get-Request. An SNMP community string is used to allow access to statistics within a managed device or router. A device can access data within other connected devices with the correct community string.

User: Specify the SNMP username on the host that connects to the SNMP agent and display the SNMP users.

Engine ID: The Engine ID is only used by SNMPv3 entities to uniquely identify them. Each SNMP agent maintains local information that is used in SNMPv3 message exchanges.

Trap Event: Monitored device (SNMP agent) send Traps are alert messages sent from a remote SNMP-enabled device to a central collector, the "SNMP manager".

Notification: SNMP uses traps otherwise known as notifications to notify the SNMP manager of network events.

RMON: RMON (Remote Network Monitoring) together with the SNMP system allows the network manager to monitor remote network devices efficiently. RMON reduces traffic flow between the NMS and managed devices, which is convenient to manage large networks.

Statistics: Traffic statistics (such as the total number of packets on a network segment during a certain time period, or total number of correct packets that are sent to a host).

Based on SNMP protocol, the NMS collects network data by communicating with Agents.

History: You can create a RMON history entry for an interface to gather information about network traffic within that interface.

Event: A RMON event is the action that occurs when an associated RMON alarm is triggered. When an alarm event occurs, it can be configured to generate a log event, a trap to an SNMP network management station, or both.

Alarm: A RMON alarm allows you to monitor a MIB object for a desired transitory state. An alarm periodically takes samples of the object's value and compares them to the configured thresholds.

These pages show tools like SNMP, RMON, Firmware upgrade, user account, save configuration, Alarm, Notification details. To upgrade firmware, User can upgrade firmware through HTTP, or Configuration restore, or Configuration backup.

Restore Factory Default: Erase/Remove all current configuration.

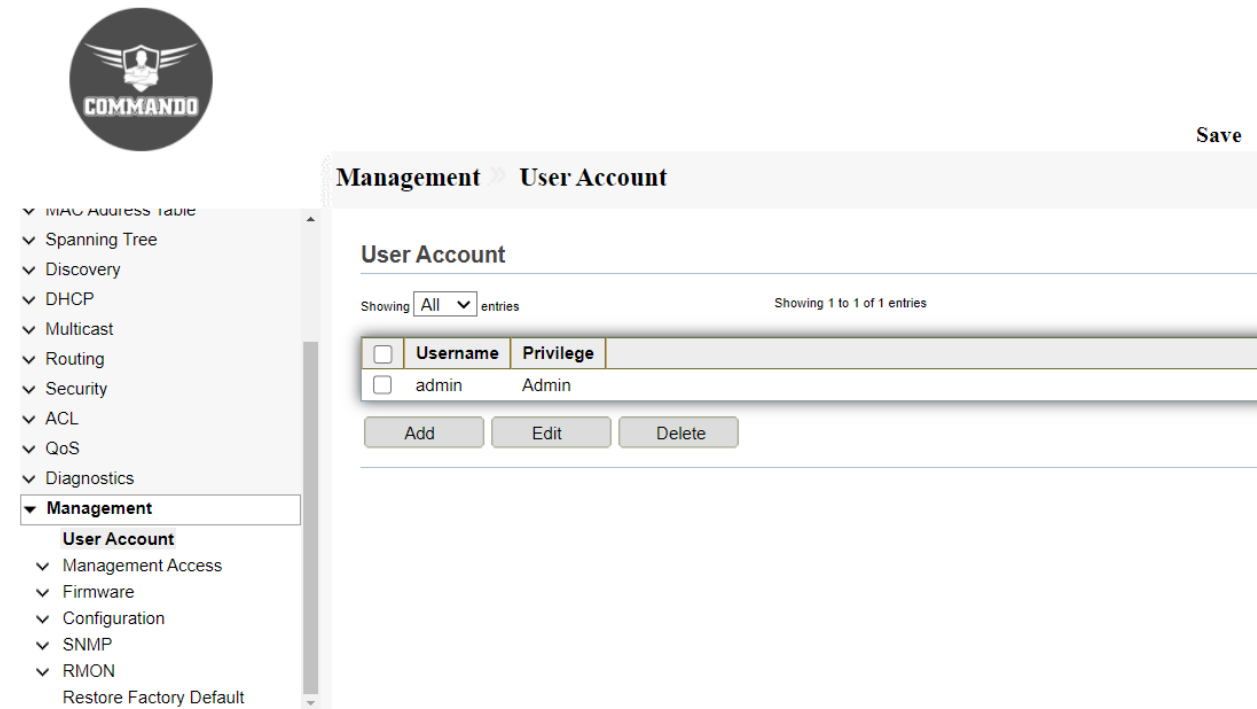
16.1 User Account

This page shows User account configuration where new Username & Password can be set to access the switch. Use this page to add and delete users and change the passwords of existing users.

To view and configure User Account, click **Management >> User Account**

Note: 1. By default, Username is “admin” and password: ***** written on backside of device.

2. Username “admin” can be changed and removed as per requirement.



The screenshot displays the Commando network management interface. On the left is a navigation tree with categories like MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. Under Management, 'User Account' is selected. The main content area is titled 'Management >> User Account' and contains a 'Save' button in the top right. Below the title is a 'User Account' section with a dropdown menu set to 'All' and 'Showing 1 to 1 of 1 entries'. A table lists the user 'admin' with 'Admin' privilege. Below the table are 'Add', 'Edit', and 'Delete' buttons.

<input type="checkbox"/>	Username	Privilege
<input type="checkbox"/>	admin	Admin

Fig 16.1.1 Default User Account page

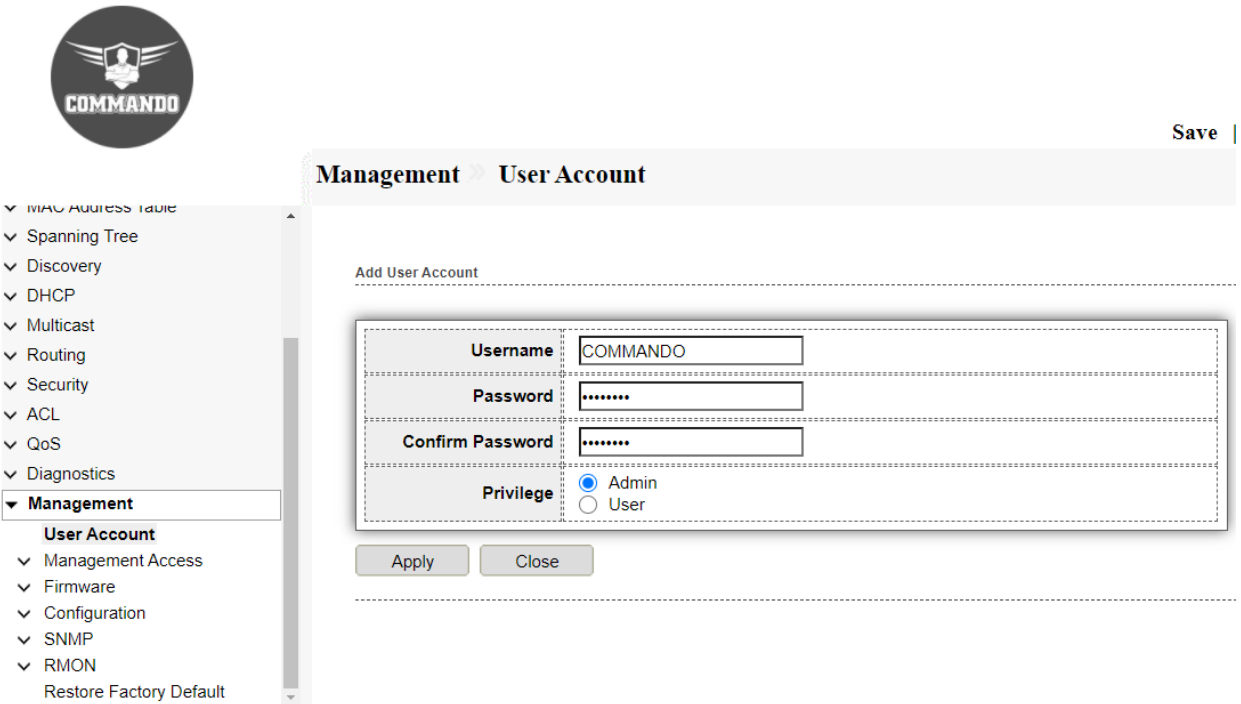


Fig 16.1.2 Add User Account having all privilege page

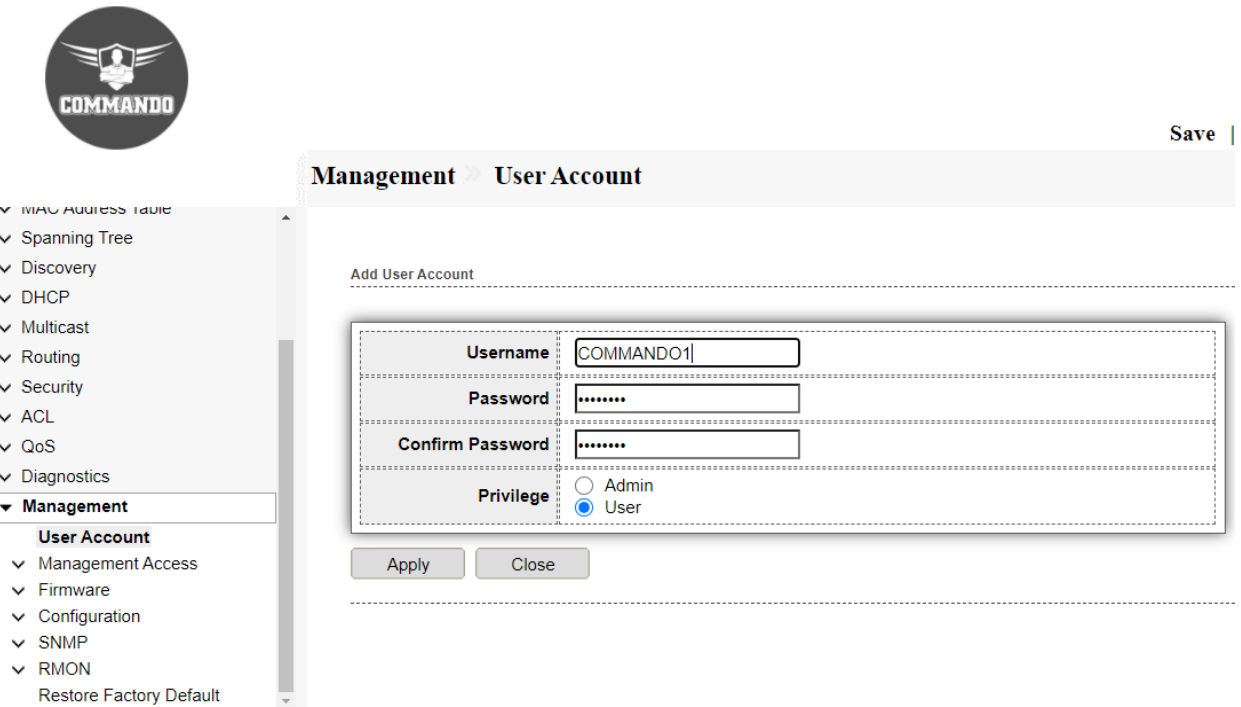


Fig 16.1.3 Add User Account having very limited access page

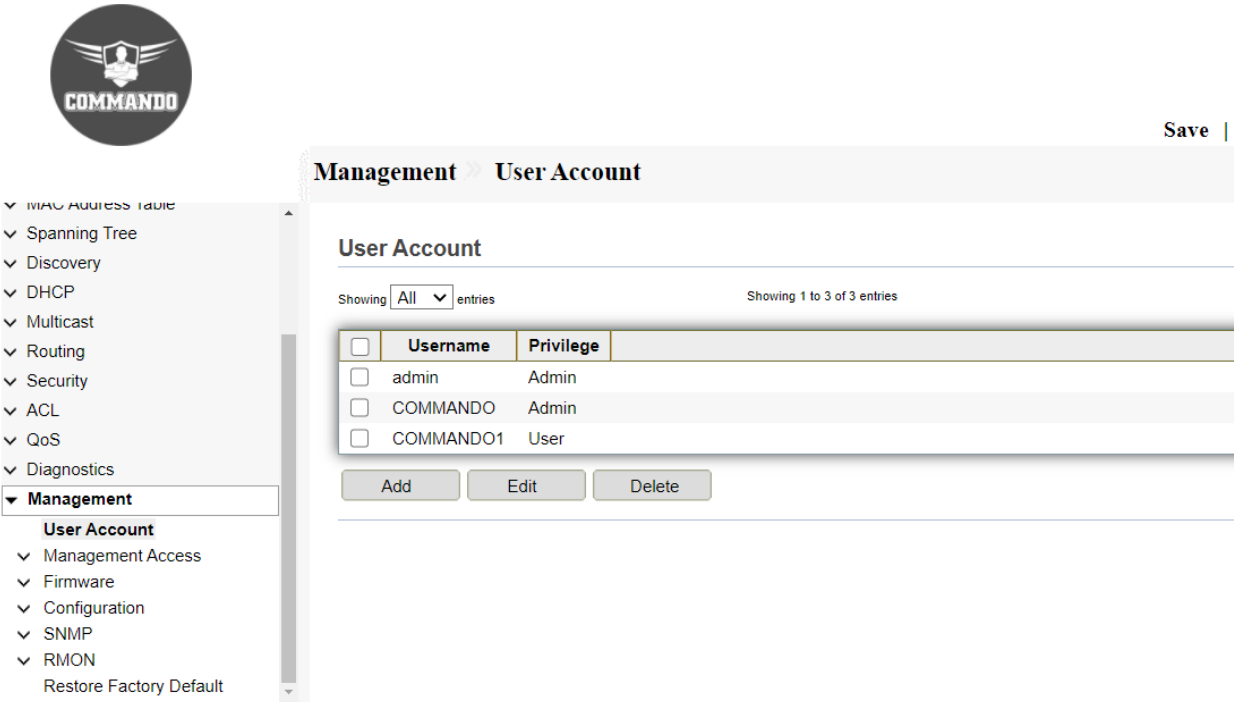


Fig 16.1.4 All User Account page

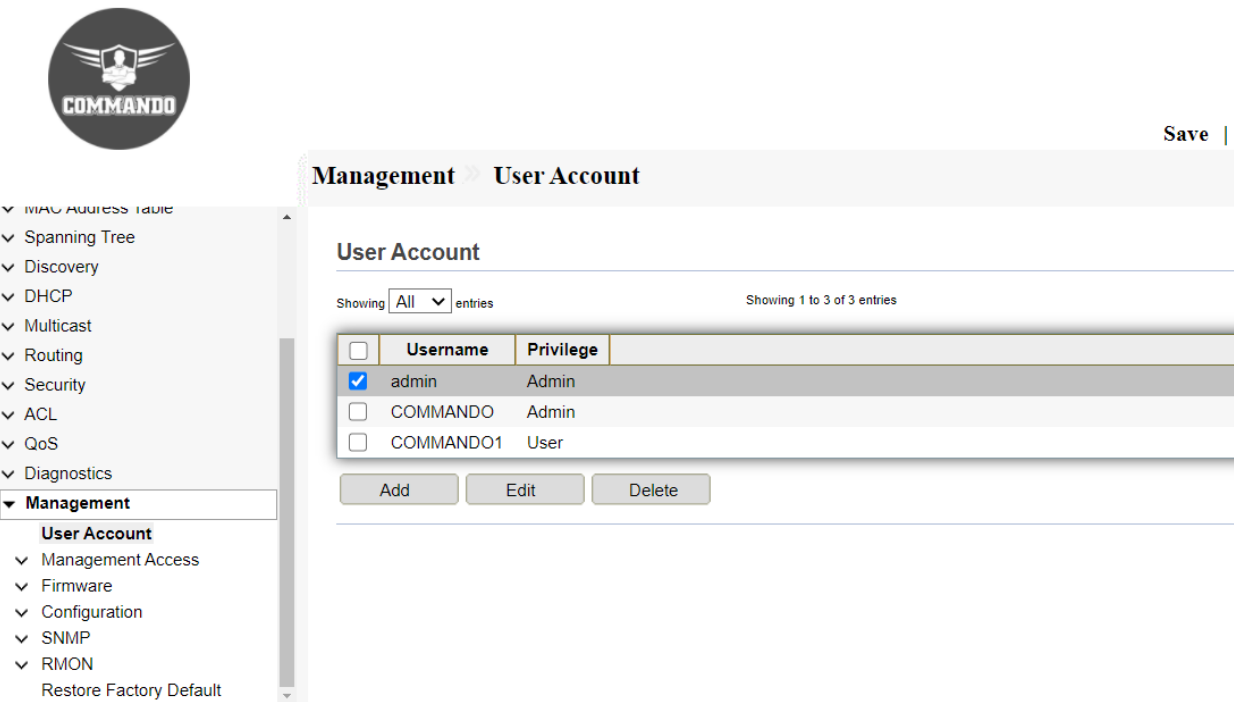



Fig 16.1.5 Selecting and Add/Edit/Delete User Account page



Save

Management » User Account


User Account

Showing **All** entries Showing 1 to 2 of 2 entries

<input type="checkbox"/>	Username	Privilege
<input type="checkbox"/>	COMMANDO	Admin
<input type="checkbox"/>	COMMANDO1	User

- ▼ IPv4 Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ **Management**
 - User Account**
 - ▼ Management Access
 - ▼ Firmware
 - ▼ Configuration
 - ▼ SNMP
 - ▼ RMON
 - Restore Factory Default

Fig 16.1.6 Deleting default admin account for security purpose page



Username:

Password:

Fig 16.1.7 Login with COMMANDO admin privilege account page

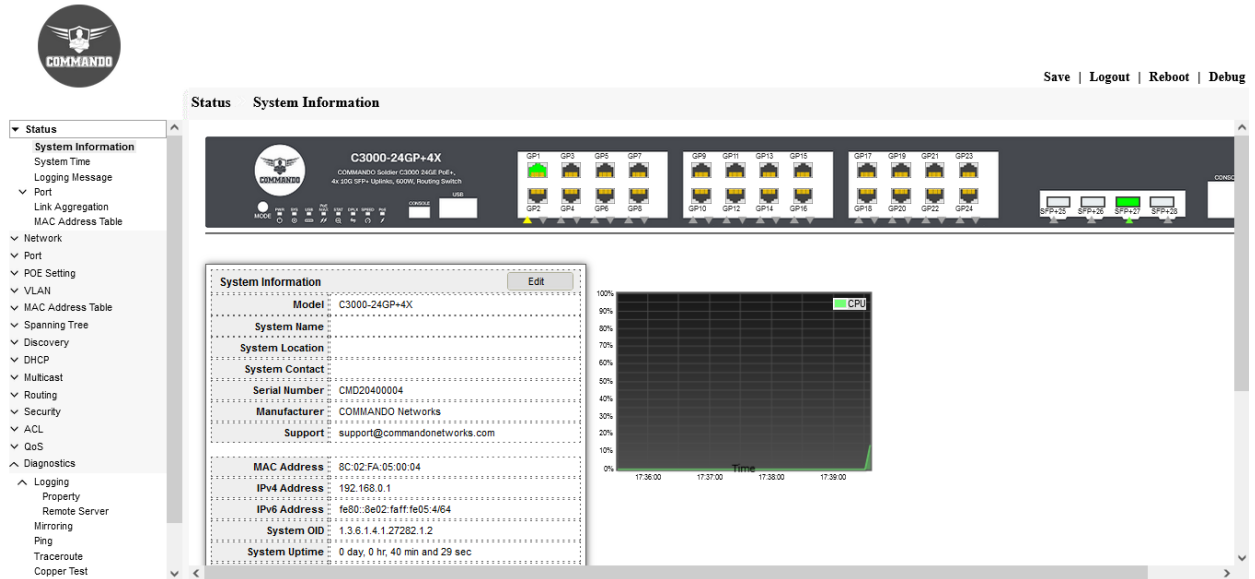


Fig 16.1.8 E3000 Switch access with COMMANDO admin privilege account page

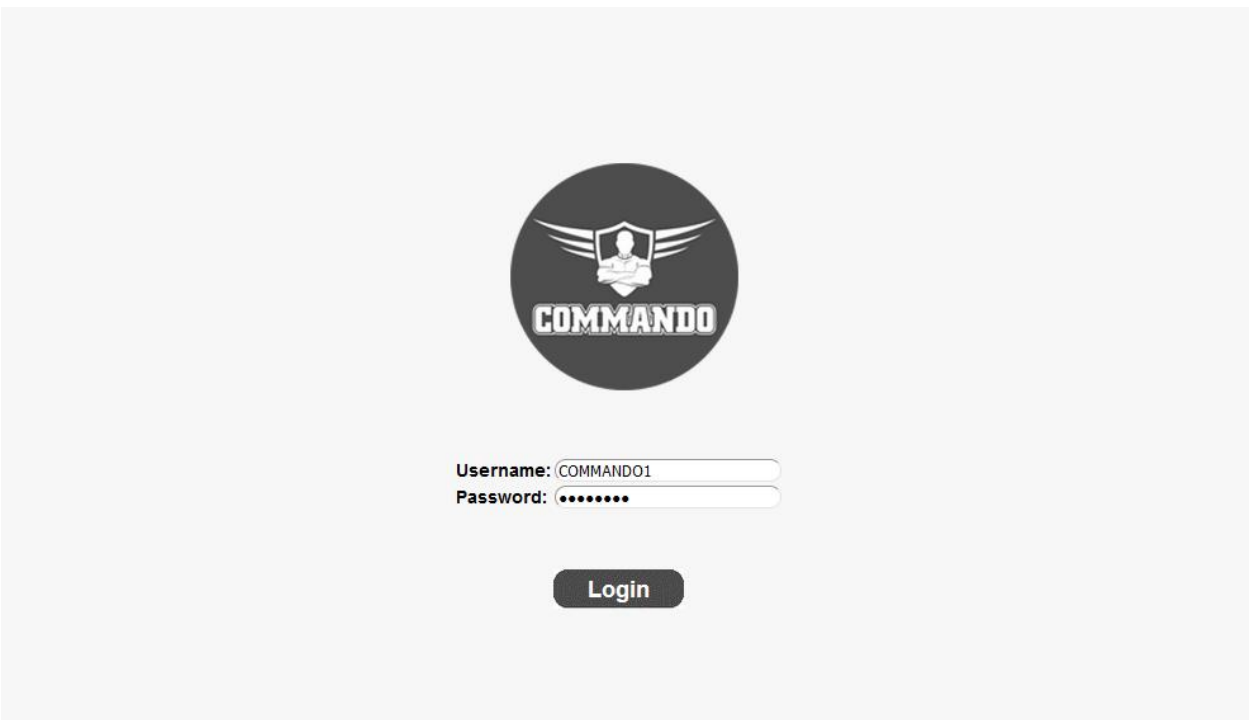


Fig 16.1.9 Login with COMMANDO1 user privilege account page



Save | Logout | Reboot | Debug

- Status
- System Information
- System Time
- Logging Message
- Port
- Link Aggregation
- MAC Address Table

Status System Information

C3000-24GP-4X
COMMANDO Series C3000 24GE PoE+, 4x 20G SFP+, 600W, Routing Switch

System Information

Model	C3000-24GP-4X
System Name	
System Location	
System Contact	
Serial Number	CMD20400004
Manufacturer	COMMANDO Networks
Support	support@commandonetworks.com
MAC Address	8C:02:FA:05:00:04
IPv4 Address	192.168.0.1
IPv6 Address	fe80::be02:faff:fe05:4/64
System OID	1.3.6.1.4.1.27282.1.2
System Uptime	0 day, 0 hr, 42 min and 45 sec

Fig 16.1.10 E3000 Switch access with COMMANDO1 user privilege account page

16.2 Management Access

Access profiles determine how to authenticate and authorize users accessing the device through various access methods. Access Profiles can limit management access from specific sources. Only users who pass both the active access profile and the management access authentication methods are given management access to the device.

16.2.1 Management Service

Methods for accessing for configuration, troubleshooting, and managing the E3000 Series Switches:

Telnet: Telnet enables a user to manage an account or device remotely. The name stands for "teletype network". Historically, Telnet provided access to a command-line interface on a remote host.

Secure Shell (SSH): Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2). SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport. The SSH (Secure Shell) is a method for secure login from a terminal to a managed device. It protects communication security and integrity with strong authentication and encryption. It is a secure alternative to the non-protected login protocols, such as telnet. In an SSH login session, the PC acts as the SSH client, and the switch acts as the SSH server.

Hypertext Transfer Protocol (HTTP): HTTP protocol transfers information between the browser and the server in clear text, allowing the network, through which the information passes, to see the information transmitted.

Secure HTTP (HTTPS): HTTPS (HTTP Secure) is an adaptation of HTTP (Hypertext Transfer Protocol) for secure communication. HTTPS creates a secure channel over an insecure network. If adequate cipher suites are used and the server's certificate is

verified and trusted, the communication data can be protected from eavesdroppers and man-in-the-middle attacks. HTTPS is also referred to as HTTP over TLS, or HTTP over SSL, because in HTTPS, communication data is encrypted by TLS (Transport Layer Security) or SSL (Secure Sockets Layer). Now a days, HTTPS is widely used on the internet for secure communication between websites and web browsers. In a local network, HTTPS can also be used for secure access to switches.

Simple Network Management Protocol (SNMP): Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. SNMP is widely used in network management for network monitoring. SNMP works by sending messages, called protocol data units (PDUs), to devices within your network that “speak” SNMP. These messages are called SNMP Get-Requests. Using these requests, network administrators can track virtually any data values they specify.

To view and enable Management Service click **Security >> Management Access >> Management Service**. To access the switch CLI enable “Telnet” Service.



Management > Management Access > Management Service

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ **Management**
 - User Account
 - Management Access
 - Management Service**
 - Management ACL
 - Management ACE
 - Firmware
 - Configuration
 - SNMP
 - RMON
 - Restore Factory Default

Management Service		
Telnet	<input checked="" type="checkbox"/>	Enable
SSH	<input checked="" type="checkbox"/>	Enable
HTTP	<input checked="" type="checkbox"/>	Enable
HTTPS	<input checked="" type="checkbox"/>	Enable
SNMP	<input checked="" type="checkbox"/>	Enable

Session Timeout		
Console	<input type="text" value="10"/>	Min (0 - 65535, default 10)
Telnet	<input type="text" value="1000"/>	Min (0 - 65535, default 10)
SSH	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTP	<input type="text" value="1000"/>	Min (0 - 65535, default 10)
HTTPS	<input type="text" value="10"/>	Min (0 - 65535, default 10)

Password Retry Count		
Console	<input type="text" value="3"/>	(0 - 120, default 3)
Telnet	<input type="text" value="3"/>	(0 - 120, default 3)
SSH	<input type="text" value="3"/>	(0 - 120, default 3)

Silent Time		
Console	<input type="text" value="0"/>	Sec (0 - 65535, default 0)
Telnet	<input type="text" value="0"/>	Sec (0 - 65535, default 0)
SSH	<input type="text" value="0"/>	Sec (0 - 65535, default 0)

Apply

Fig 16.2.1 Management services page



Management Management Access Management Service

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ **Management**
 - User Account
 - ▲ Management Access
 - Management Service**
 - Management ACL
 - Management ACE
 - ▼ Firmware
 - ▼ Configuration
 - ▼ SNMP
 - ▼ RMON
 - Restore Factory Default

Management Service		
Telnet	<input checked="" type="checkbox"/>	Enable
SSH	<input checked="" type="checkbox"/>	Enable
HTTP	<input checked="" type="checkbox"/>	Enable
HTTPS	<input checked="" type="checkbox"/>	Enable
SNMP	<input checked="" type="checkbox"/>	Enable

Session Timeout		
Console	<input type="text" value="1000"/>	Min (0 - 65535, default 10)
Telnet	<input type="text" value="10000"/>	Min (0 - 65535, default 10)
SSH	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTP	<input type="text" value="1000"/>	Min (0 - 65535, default 10)
HTTPS	<input type="text" value="10"/>	Min (0 - 65535, default 10)

Password Retry Count		
Console	<input type="text" value="30"/>	(0 - 120, default 3)
Telnet	<input type="text" value="20"/>	(0 - 120, default 3)
SSH	<input type="text" value="10"/>	(0 - 120, default 3)

Silent Time		
Console	<input type="text" value="10000"/>	Sec (0 - 65535, default 0)
Telnet	<input type="text" value="0"/>	Sec (0 - 65535, default 0)
SSH	<input type="text" value="0"/>	Sec (0 - 65535, default 0)

Apply

Fig 16.2.2 Enabling Management services with different session timeout page



Management Management Access Management Service

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ **Management**
 - User Account
 - ▲ Management Access
 - Management Service**
 - Management ACL
 - Management ACE
 - ▼ Firmware
 - ▼ Configuration
 - ▼ SNMP
 - ▼ RMON
 - Restore Factory Default

Management Service		
Telnet	<input type="checkbox"/>	Enable
SSH	<input checked="" type="checkbox"/>	Enable
HTTP	<input checked="" type="checkbox"/>	Enable
HTTPS	<input checked="" type="checkbox"/>	Enable
SNMP	<input checked="" type="checkbox"/>	Enable

Session Timeout		
Console	<input type="text" value="1000"/>	Min (0 - 65535, default 10)
Telnet	<input type="text" value="10000"/>	Min (0 - 65535, default 10)
SSH	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTP	<input type="text" value="1000"/>	Min (0 - 65535, default 10)
HTTPS	<input type="text" value="10"/>	Min (0 - 65535, default 10)

Password Retry Count		
Console	<input type="text" value="30"/>	(0 - 120, default 3)
Telnet	<input type="text" value="20"/>	(0 - 120, default 3)
SSH	<input type="text" value="10"/>	(0 - 120, default 3)

Silent Time		
Console	<input type="text" value="10000"/>	Sec (0 - 65535, default 0)
Telnet	<input type="text" value="0"/>	Sec (0 - 65535, default 0)
SSH	<input type="text" value="0"/>	Sec (0 - 65535, default 0)

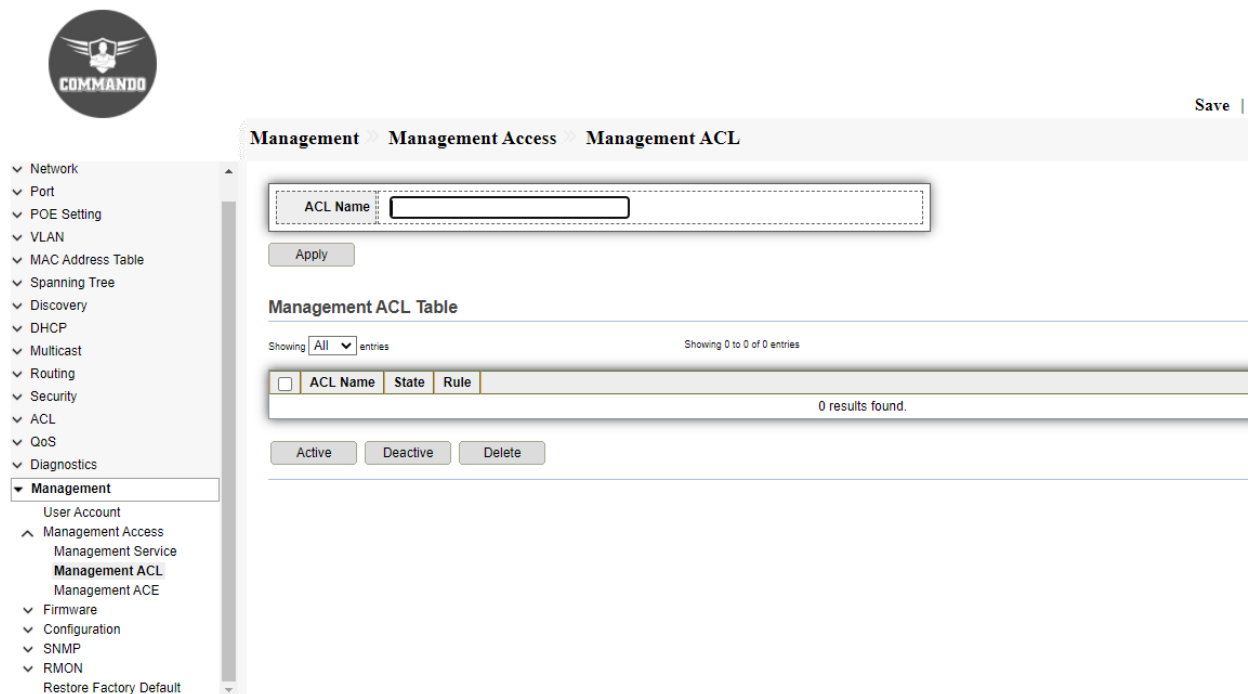
Apply

Fig 16.2.3 Disabling telnet Management services page

16.2.2 Management ACL

Management Access Control List (ACL) is an additional feature that you can configure on your network to enhance security. An access rule is created and applied to permit or deny access to the network or to a particular device inside the network. Displays information Table about Access Control List where you can Active, Deactivate or Delete the ACL.

To view and configure Management ACL, click **Security >> Management Access >> Management ACL**.



The screenshot shows the COMMANDO web interface for configuring Management ACL. On the left is a navigation menu with categories like Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, and Diagnostics. The 'Management' category is expanded, showing sub-items: User Account, Management Access, Management Service, Management ACL (highlighted), and Management ACE. The main content area has a breadcrumb trail: Management > Management Access > Management ACL. At the top right is a 'Save' button. Below the breadcrumb is a form with an 'ACL Name' input field and an 'Apply' button. The 'Management ACL Table' section shows a table with columns for 'ACL Name', 'State', and 'Rule'. The table is currently empty, displaying 'Showing 0 to 0 of 0 entries' and '0 results found.' Below the table are three buttons: 'Active', 'Deactive', and 'Delete'.

Fig 16.2.4 Default Management ACL Table page

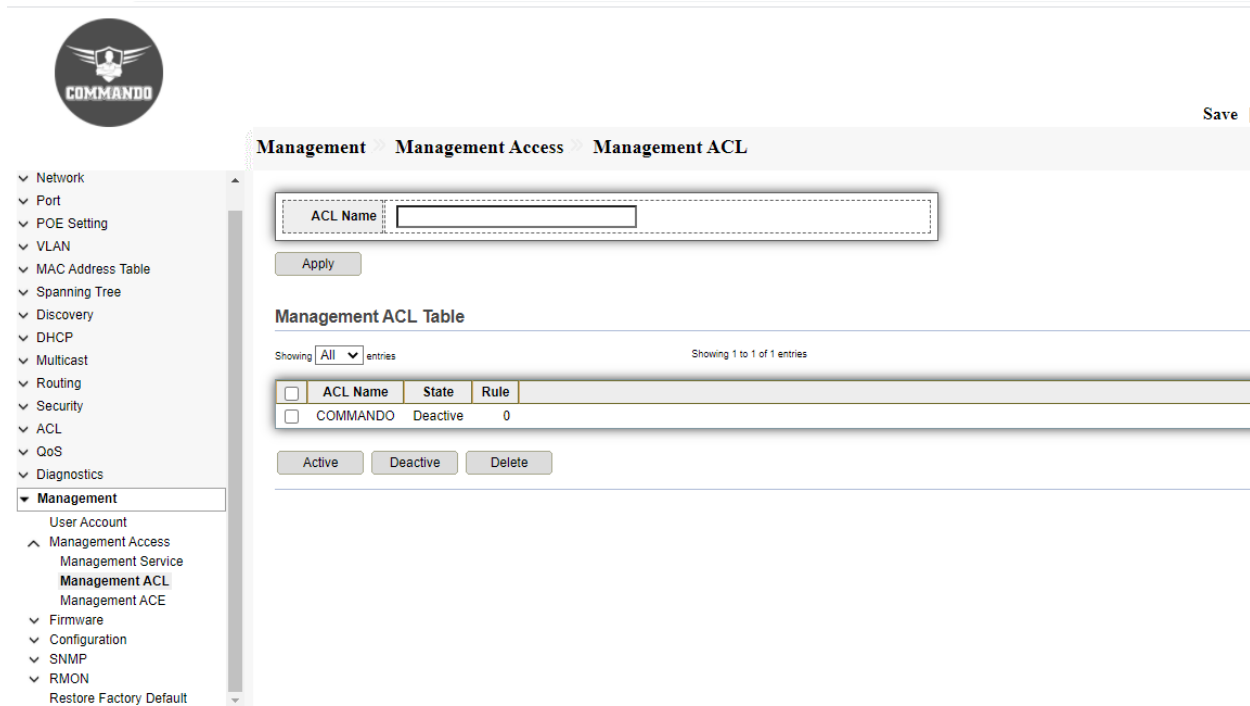


Fig 16.2.5 Adding Management ACL Name page

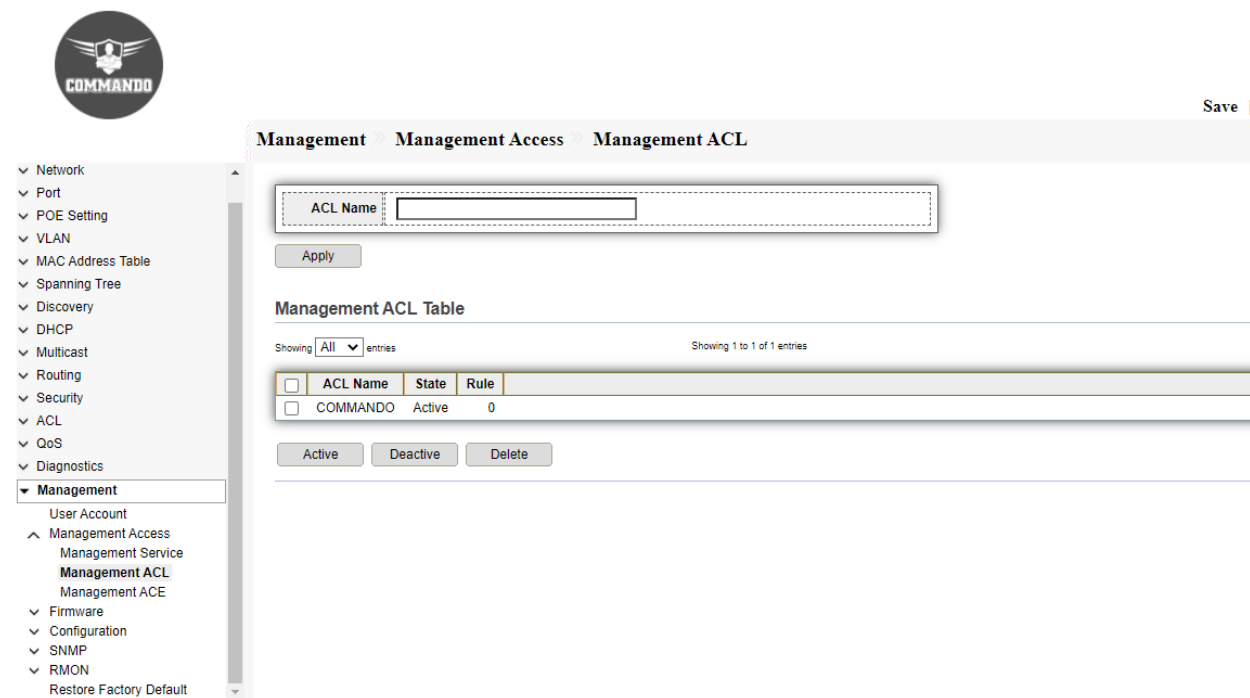
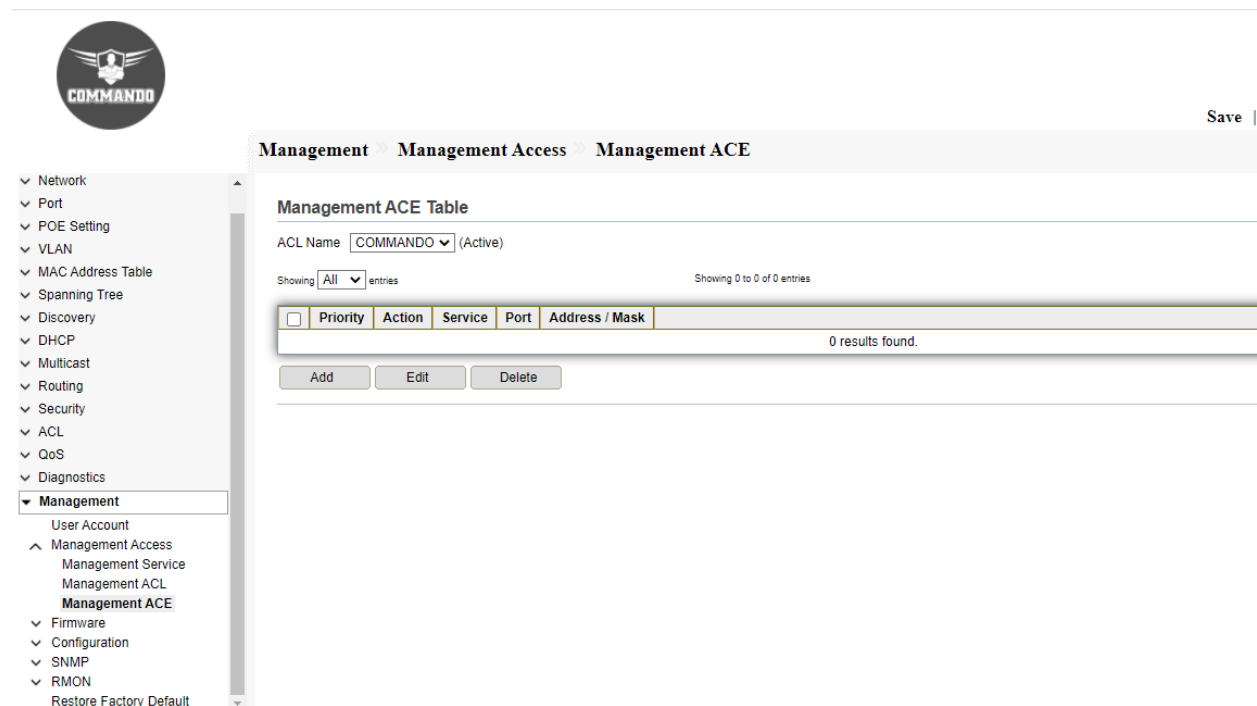


Fig 16.2.6 Activating Management ACL Table page

16.2.3 Management ACE

An Access Control List (ACL) is an ordered list of classification filters and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE). Each ACE is made up of filters that distinguish traffic groups and associated actions. A single ACL may contain one or more ACEs, which are matched against the contents of incoming frames. Either a DENY or PERMIT action is applied to frames whose contents match the filter. This is to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under active. New ACE cannot be added if ACL under active.

To view and configure Management ACE, click **Security >> Management Access >> Management ACE**.



The screenshot displays the COMMANDO web interface. On the left is a navigation menu with categories like Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, Management, Management Access, Management Service, Management ACL, Management ACE, Firmware, Configuration, SNMP, and RMON. The main content area shows the breadcrumb path: Management > Management Access > Management ACE. Below this is the 'Management ACE Table' section, which includes a dropdown for 'ACL Name' set to 'COMMANDO (Active)', a 'Showing All entries' indicator, and a table with columns for Priority, Action, Service, Port, and Address / Mask. The table is currently empty, displaying '0 results found.' Below the table are 'Add', 'Edit', and 'Delete' buttons. A 'Save' button is located in the top right corner of the interface.

Fig 16.2.7 Default Management ACE Table page



Management > Management Access > Management ACE

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ **Management**
 - User Account
 - ▲ Management Access
 - Management Service
 - Management ACL
 - Management ACE**
 - ▼ Firmware
 - ▼ Configuration
 - ▼ SNMP
 - ▼ RMON
 - Restore Factory Default

Add Management ACE

ACL Name	COMMANDO	
Priority	1 (1 - 65535)	
Service	<input type="radio"/> All <input type="radio"/> http <input checked="" type="radio"/> https <input type="radio"/> Snmp <input type="radio"/> SSH <input type="radio"/> Telnet	
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny	
Port	Available Port	Selected Port
	GE1 GE2 GE4 GE5 GE6 GE7 GE8 GE9	GE3
IP Version	<input checked="" type="radio"/> All <input type="radio"/> IPv4 <input type="radio"/> IPv6	
IPv4	/ 255.255.255.255	
IPv6	/ 128 (1 - 128)	

Apply Close

Fig 16.2.8 Add Management ACE Table page



Save |

Management > Management Access > Management ACE

- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ▼ **Management**
 - User Account
 - ^ Management Access
 - Management Service
 - Management ACL
 - Management ACE**
 - ✓ Firmware
 - ✓ Configuration
 - ✓ SNMP
 - ✓ RMON
 - Restore Factory Default

Management ACE Table

ACL Name COMMANDO (Active)

Showing All entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Priority	Action	Service	Port	Address / Mask
<input type="checkbox"/>	1	Deny	https	GE3	N/A

Fig 16.2.9 Management ACE Table after ACL Activation page

16.3 Firmware

This page allow user to upgrade or backup firmware image through HTTP or TFTP server.

16.3.1 Upgrade

To view and configure firmware upgrade or backup, click **Management >> Firmware >> Upgrade**.

Installing from the Local System (HTTP): Firmware may be directly uploaded to the switch from the local system. Click "Choose File" to select the firmware that needed to upgrade. And then click "Apply " to start Upgrading.

Installing from the Remote Server (TFTP): Firmware may be fetched by the switch from a remote machine serving the firmware file. The Server must be providing the file via TFTP. Select Upgrade Method "TFTP", Select "Address Type [Hostname/IPv4/IPv6]", Then Enter "Server Address" & "Filename" And then click "Apply " to start upgrading.

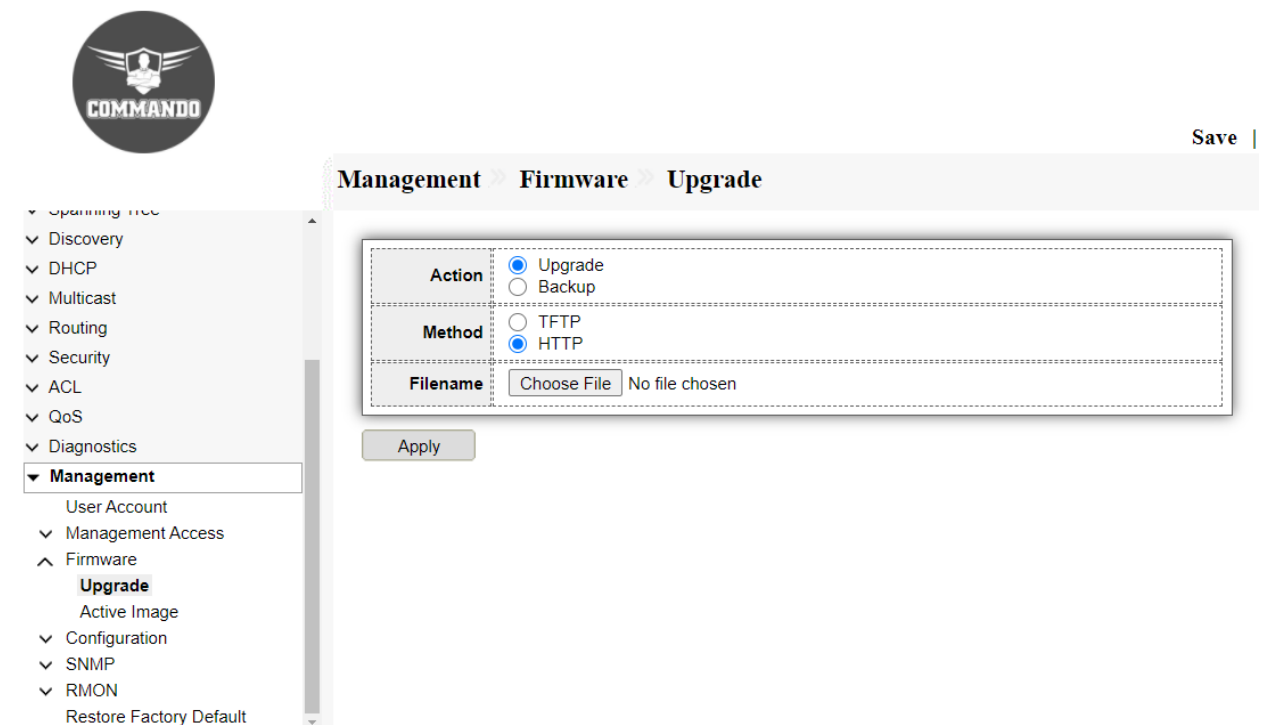


Fig 16.3.1 Default Firmware Upgrade page

Firmware Update Procedure to Firmware Version SoldierOS

Step 1 Collect the Firmware upgrade of switch.

Step 2: For Uploading prepared firmware file to COMMANDO Series E3000 by Web GUI by clicking Management >>Firmware>>Upgrade and select method HTTP choose file **vmlinux.bix**.

Step 3: Don't Power ON/OFF device. After successful uploading click reboot button on device. After that you must remove all browser history to login again with new firmware.

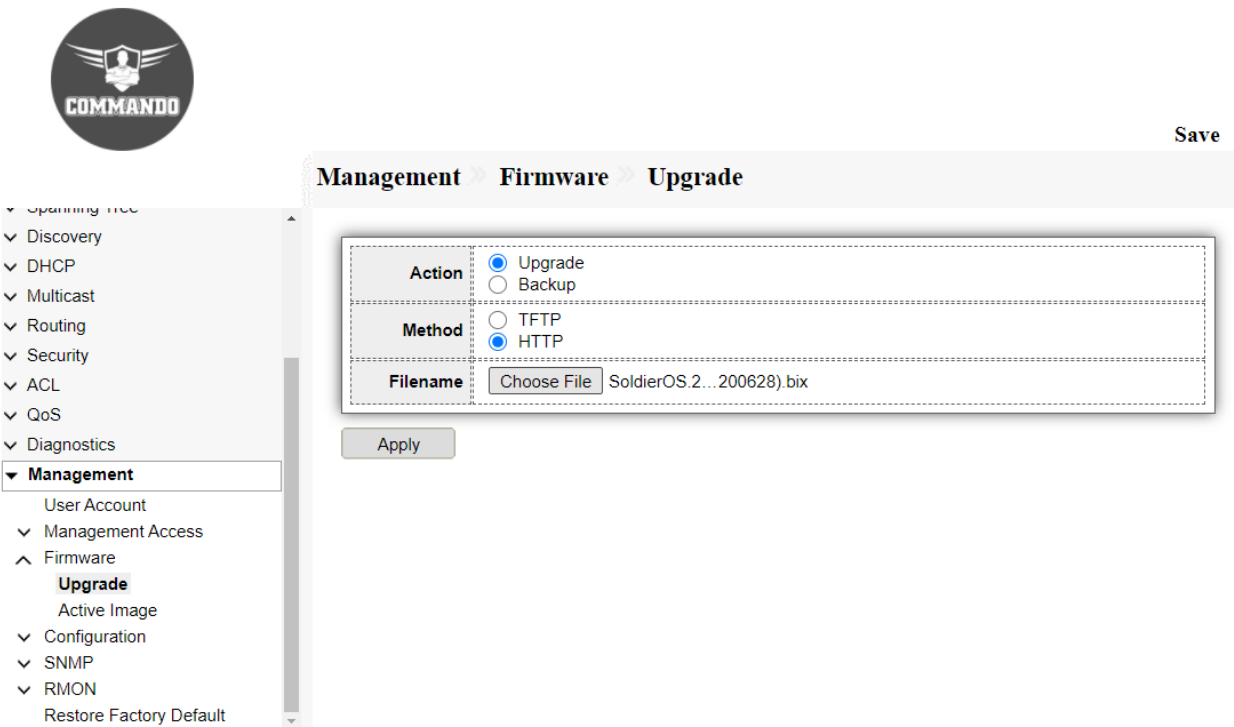


Fig 16.3.2 Firmware Upgrade page

16.3.2 Active Image

In all E3000 Series Switches support Dual Image. The switch stores two images. One image is set as the next start up image, and the other is set as the backup image. After you upgrade a firmware, the switch will automatically map the firmware file to the backup image. When the switch reboots, it will try to start up with the next startup image. When the switch fails to start up with the next startup image, it will try to start up with the backup image. In all E3000 Series Switches two images working in active and backup mode. When the active image is upgraded or unworkable, you can switch over services to the backup image to ensure normal running of the E3000 series Switches. No saved configuration is lost while changing images.

To view and configure Active Image, Click **Management>>Firmware>>Active Image**

The screenshot shows the COMMANDO web interface for configuring the Active Image. The navigation menu on the left includes options like Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, Management, User Account, Management Access, Management Service, Management ACL, Management ACE, Firmware, Upgrade, Active Image, Configuration, and SNMP. The main content area is titled 'Management Firmware Active Image' and contains the following information:

Active Image: Image0 Image1
Note: the image was selected for the next boot

Active Image

Firmware	Image0*
Version	SoldierOS.3Kv1.10
Name	
Size	8813783 Bytes
Created	2022-01-24 09:59:59

Backup Image

Firmware	Image1
Version	
Name	
Size	undefined Bytes
Created	

Apply

Fig 16.3.3 Firmware Active Image page

16.4 Configuration

The Configuration Management and Update Firmware features allow you to browse to save and retrieve files directly from your local system. This is the easiest and recommended method.

Alternatively, you can use a TFTP (Trivial File Transfer Protocol) server to centralize the storage of your configuration and firmware files. Free TFTP servers for Windows and Linux are available on the web. They are generally easy to install and setup.

16.4.1 Upgrade

This page allow user to upgrade or backup configuration file through HTTP or TFTP server.

To view and configure firmware upgrade or backup, click

Management >> Configuration >> Upgrade or Configuration >>Backup

COMMANDO

Management > Configuration > Upgrade

Action	<input checked="" type="radio"/> Upgrade <input type="radio"/> Backup
Method	<input type="radio"/> TFTP <input checked="" type="radio"/> HTTP
Configuration	<input checked="" type="radio"/> Running Configuration <input type="radio"/> Startup Configuration <input type="radio"/> Backup Configuration <input type="radio"/> RAM Log <input type="radio"/> Flash Log
Filename	<input type="button" value="Choose File"/> No file chosen

Fig 16.4.1 Configuration default upgrade page

Upgrading from the Local System (HTTP): Configuration can be directly uploaded to the switch from the local system. Select “Action [Upgrade]”, then configuration “Method [HTTP]”, “Configuration [Running/Startup/Backup]”, now click “Choose File” to select the file that needed to upgrade and click “Apply” to start upgrading.

Upgrading from the Remote Server (TFTP): Select “Action [Upgrade]”, then configuration “Method [TFTP]”, “Configuration [Running/Startup/Backup]”, Select “Address Type [Hostname/IPv4/IPv6]”, Then Enter “Server Address” & “Filename” And then click "Apply " to start upgrading.

Backup from the Local System (HTTP): Configuration can be directly backup. Select “Action [Backup]”, then configuration “Method [HTTP]”, “Configuration [Running/Startup/Backup]”, click “Apply” to start downloading back up file.

Backup from the Remote Server (TFTP): Configuration can be directly backup. Select “Action [Backup]”, then configuration “Method [TFTP]”, “Configuration [Running/Startup/Backup]”, click “Apply” to start downloading back up file.

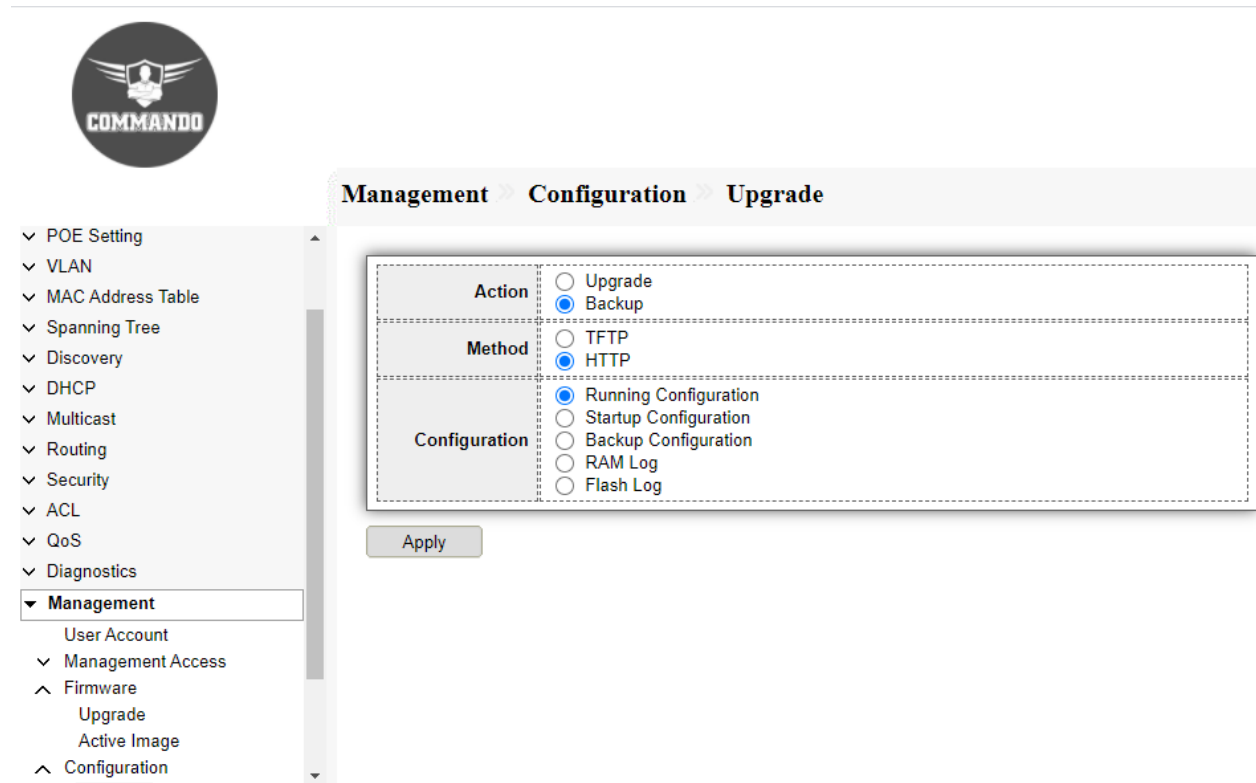


Fig 16.4.2 Backup of Configuration from running configuration page



Management » Configuration » Upgrade

- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ▼ **Management**
 - User Account
 - ✓ Management Access
 - ^ Firmware
 - Upgrade
 - Active Image
 - ^ Configuration

Backup Running Configuration completed successfully

Done

! This type of file can harm your computer. Do you want to keep running-config.cfg anyway? [Keep](#) [Discard](#)

Fig 16.4.3 Backup running configuration page

16.4.2 Save Configuration

This page allow user to manage configuration file saved on PC or TFTP server. This saves configuration in the switch, which may be used later to revert to the current state if changes lead to an undesirable configuration. All the customized settings Switch will be erased. The standard procedure is to restore the device to factory settings, wiping it clean of any configuration file data.

To Save Configuration, click **Management >> Configuration >> Save Configuration**.

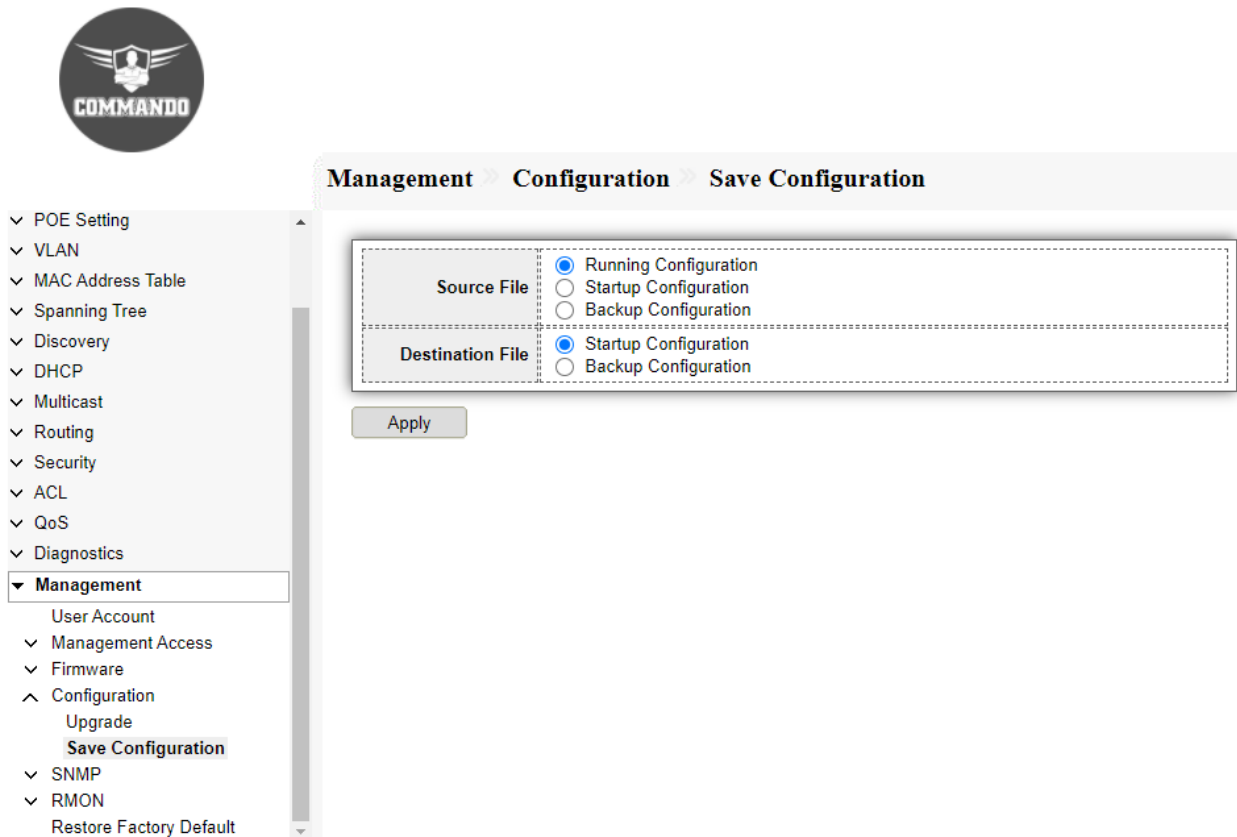


Fig 16.4.4 Save running Configuration to Startup Configuration page



- ✓ POE Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ▼ **Management**
 - User Account
 - ✓ Management Access
 - ✓ Firmware
 - ^ Configuration
 - Upgrade
 - Save Configuration**
 - ✓ SNMP
 - ✓ RMON
 - Restore Factory Default

Management > Configuration > Save Configuration

Source File	<input checked="" type="radio"/> Running Configuration
	<input type="radio"/> Startup Configuration
	<input type="radio"/> Backup Configuration
Destination File	<input type="radio"/> Startup Configuration
	<input checked="" type="radio"/> Backup Configuration

Apply

Fig 16.4.5 Save running Configuration to Backup Configuration page

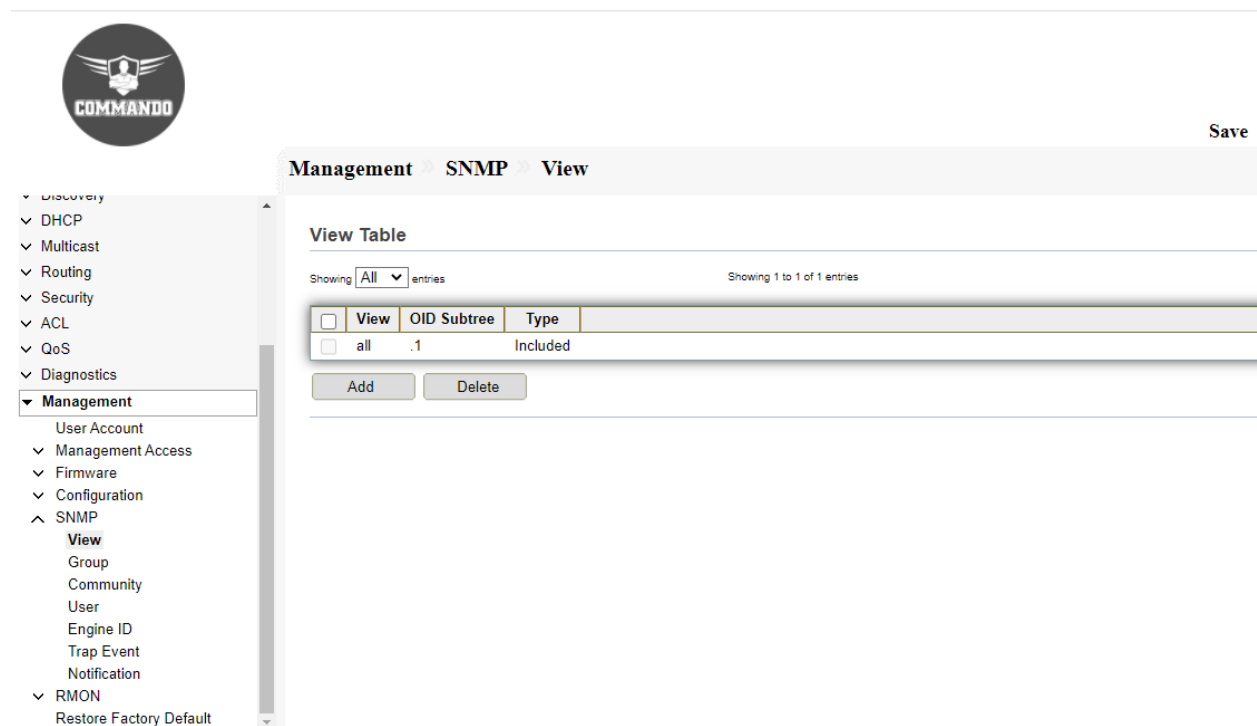
16.5 SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

16.5.1 View

A view is a user-defined label for a collection of MIB sub trees. Each sub tree ID is defined by the Object ID (OID) of the root of the relevant sub trees. Either well-known names can be used to specify the root of the desired sub tree or an OID can be entered.

To view and configure SNMP view table, click **Management >> SNMP >> View**.



The screenshot displays the Commando network management interface. On the left is a navigation tree with the following items: Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, **Management** (expanded), User Account, Management Access, Firmware, Configuration, SNMP (expanded), View (selected), Group, Community, User, Engine ID, Trap Event, Notification, RMON, and Restore Factory Default. The main content area shows the breadcrumb path **Management > SNMP > View** and a **Save** button. Below this is the **View Table** section, which includes a dropdown menu set to **All** entries and the text **Showing 1 to 1 of 1 entries**. A table with the following data is displayed:

<input type="checkbox"/>	View	OID Subtree	Type
<input type="checkbox"/>	all	.1	Included

Below the table are **Add** and **Delete** buttons.

Fig 16.5.1 Default SNMP View Table page



- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View**
 - Group
 - Community
 - User
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Management > SNMP > View

Add View

View	<input type="text" value="12"/>
OID Subtree	<input type="text" value="2"/>
Type	<input checked="" type="radio"/> Included <input type="radio"/> Excluded

Fig 16.5.2 SNMP add View page



- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View**
 - Group
 - Community
 - User
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Management > SNMP > View Save |

View Table

Showing entries Showing 1 to 2 of 2 entries

<input type="checkbox"/>	View	OID Subtree	Type
<input type="checkbox"/>	12	.2	Included
<input type="checkbox"/>	all	.1	Included

Fig 16.5.3 SNMP View Table page

16.5.2 Group

A group defines read/write privileges and a level of security. It becomes operational when it is associated with an SNMP user or community.

To view and configure SNMP group settings, click **Management >> SNMP >> Group**.

COMMANDO

Management > SNMP > Group Save |

Group Table

Showing **All** entries Showing 0 to 0 of 0 entries

	Group	Version	Security Level	View		
				Read	Write	Notify
<input type="checkbox"/>						

0 results found.

Configure [SNMP View](#) to associate a non-default view with a group.

- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group**
 - Community
 - User
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Fig 16.5.4 SNMP Default Group Table page



- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group**
 - Community
 - User
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Management > SNMP > Group

Add Group

Group	COMMANDO
Version	<input type="radio"/> SNMPv1 <input checked="" type="radio"/> SNMPv2 <input type="radio"/> SNMPv3
Security Level	<input type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
View	<input checked="" type="checkbox"/> Read all
	<input checked="" type="checkbox"/> Write all
	<input checked="" type="checkbox"/> Notify all

Apply Close

Fig 16.5.5 SNMP Add Group page



- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group**
 - Community
 - User
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Management > SNMP > Group

Group Table

Showing All entries Showing 1 to 1 of 1 entries

	Group	Version	Security Level	View		
				Read	Write	Notify
<input type="checkbox"/>	COMMANDO	SNMPv2	No Security	all	all	all

Configure [SNMP View](#) to associate a non-default view with a group.


Add Edit Delete

Fig 16.5.6 SNMP Group Table after adding group page

16.5.3 Community

Access rights in SNMPv1 and SNMPv2 are managed by defining communities in the Communities page. The community name is a type of shared password between the SNMP management station and the device. It is used to authenticate the SNMP management station.

To view and configure the SNMP community settings, click **Management >> SNMP >> Community**.



Management > SNMP > Community

Community Table

Showing entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Community	Group	View	Access
<input type="checkbox"/>	public		all	Read-Only

The access right of a community is defined by a group under advanced mode.
Configure [SNMP Group](#) to associate a group with a community.

- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group
 - Community**
 - User
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Fig 16.5.7 SNMP Community Table page



Management > SNMP > Community

Add Community

Community	COMMANDO
Type	<input type="radio"/> Basic <input checked="" type="radio"/> Advanced
View	all
Access	<input checked="" type="radio"/> Read-Only <input type="radio"/> Read-Write
Group	COMMANDO

Apply Close

- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group
 - Community**
 - User
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Fig 16.5.8 Add SNMP Community page



- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group
 - Community**
 - User
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Management >> SNMP >> Community

Community Table

Showing All entries

Showing 1 to 2 of 2 entries

<input type="checkbox"/>	Community	Group	View	Access
<input type="checkbox"/>	COMMANDO	COMMANDO		
<input type="checkbox"/>	public		all	Read-Only

The access right of a community is defined by a group under advanced mode. Configure [SNMP Group](#) to associate a group with a community.

Fig 16.5.9 SNMP Community Table after adding community page

16.5.4 User

An SNMP user is defined by the login credentials (username, passwords, and authentication method) and by the context and scope in which it operates by association with a group and an Engine ID.

The configured user has the attributes of its group, having the access privileges configured within the associated view.

To view and configure SNMP users, click **Management >> SNMP >> User**.

COMMANDO

Management > SNMP > User

User Table

Showing **All** entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	User	Group	Security Level	Authentication Method	Privacy Method	
0 results found.						

Configure [SNMP Group](#) to associate an SNMPv3 group with an SNMPv3 user.

- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group
 - Community
 - User**
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Fig 16.5.10 SNMP Default user Table page



Management > SNMP > User

- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group
 - Community
 - User**
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Add User

User	COMMANDO
Group	COMMANDO1
Security Level	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
Authentication	
Method	<input checked="" type="radio"/> None <input type="radio"/> MD5 <input type="radio"/> SHA
Password	
Privacy	
Method	<input checked="" type="radio"/> None <input type="radio"/> DES
Password	

Apply Close

Fig 16.5.11 SNMP Add user page



Management > SNMP > User

User Table

Showing **All** entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	User	Group	Security Level	Authentication Method	Privacy Method
<input type="checkbox"/>	COMMANDO	COMMANDO1	No Security	None	None

Configure [SNMP Group](#) to associate an SNMPv3 group with an SNMPv3 user.

- Management
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group
 - Community
 - User**
 - Engine ID
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

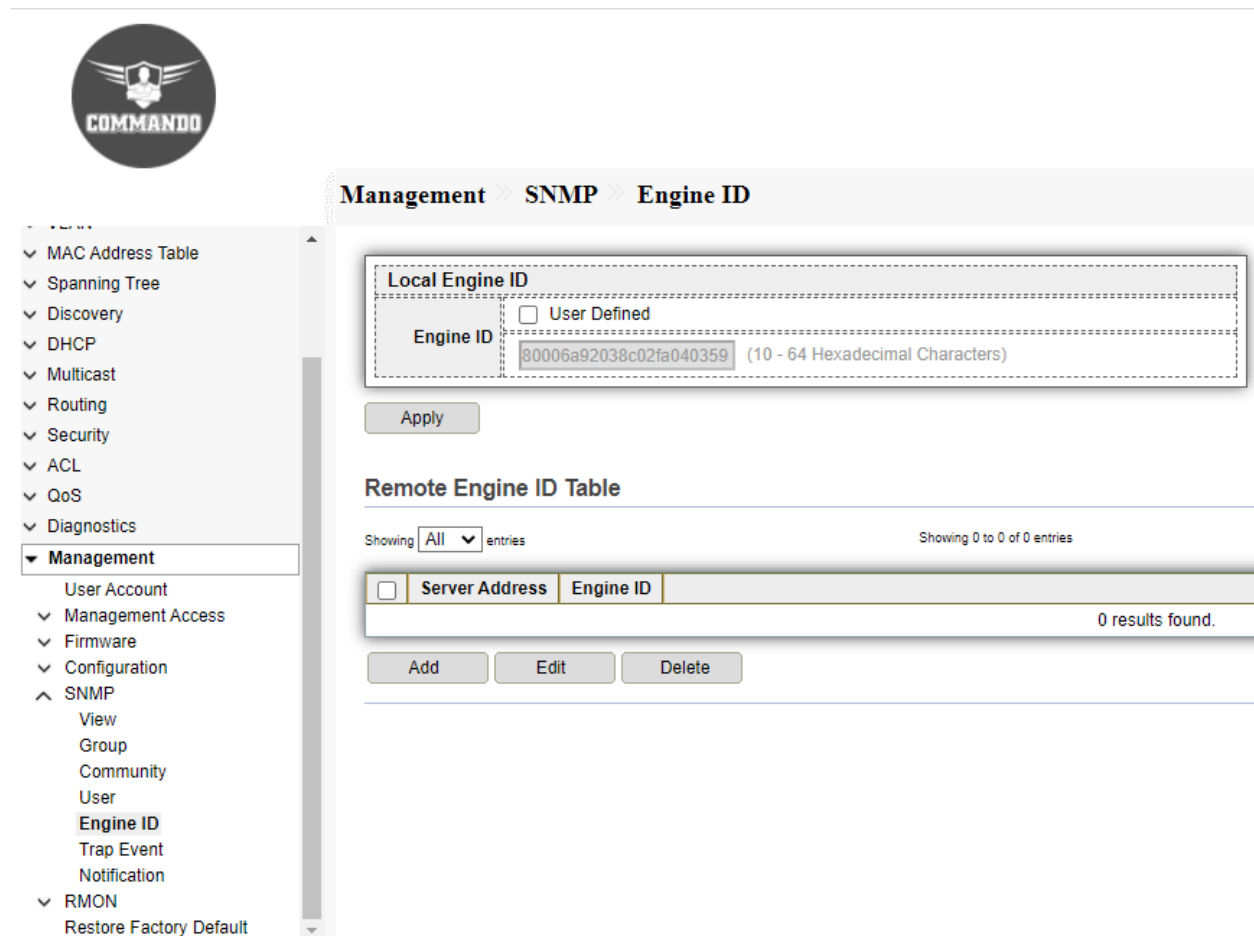
Fig 16.5.12 SNMP user Table after adding User page

16.5.5 Engine ID

The Engine ID is used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set) and sends trap messages to a manager. The agent's local information is encapsulated in fields in the message. Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is comprised of the enterprise number and the default MAC address.

This engine ID must be unique for the administrative domain, so that no two devices in a network have the same engine ID.

To view and configure and display SNMP local and remote engine ID, click **Management >> SNMP >> Engine ID**.



COMMANDO

Management > SNMP > Engine ID

Local Engine ID

User Defined

Engine ID: (10 - 64 Hexadecimal Characters)

Apply

Remote Engine ID Table

Showing **All** entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Server Address	Engine ID
0 results found.		

Add Edit Delete

Fig 16.5.13 SNMP Default Remote Engine ID Table page



Management » SNMP » Engine ID

Add Remote Engine ID

Address Type	<input type="radio"/> Hostname
	<input checked="" type="radio"/> IPv4
	<input type="radio"/> IPv6
Server Address	<input type="text" value="192.168.0.50"/>
Engine ID	<input type="text" value="08003e2834922a2323"/> (10 - 64 Hexadecimal Characters)

- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group
 - Community
 - User
 - Engine ID**
 - Trap Event
 - Notification
 - RMON
 - Restore Factory Default

Fig 16.5.14 SNMP Add Remote Engine ID page



Management » SNMP » Engine ID

Local Engine ID

User Defined

Engine ID (10 - 64 Hexadecimal Characters)

Apply

Remote Engine ID Table

Showing entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Server Address	Engine ID
<input type="checkbox"/>	192.168.0.50	08003e2834922a2323

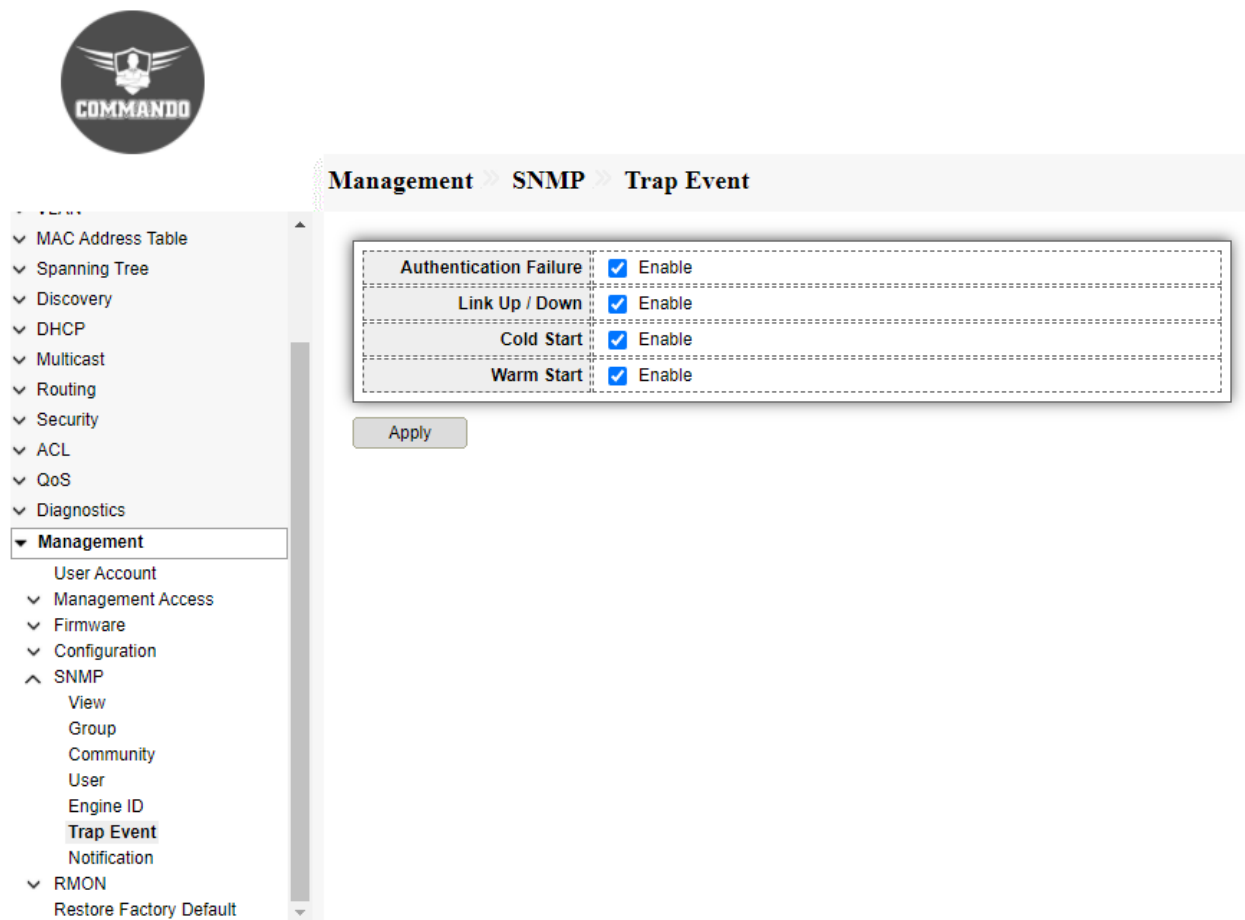
Add Edit Delete

Fig 16.5.15 SNMP Add Remote Engine ID page

16.5.6 Trap Event

The Trap Settings page enables configuring whether SNMP notifications are sent from the device, and for which cases.

To view and configure SNMP trap event, click **Management >> SNMP >> Trap Event**.



The screenshot shows the COMMANDO web interface. On the left is a navigation menu with the following items: MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, **Management** (expanded), User Account, Management Access, Firmware, Configuration, SNMP (expanded), View, Group, Community, User, Engine ID, **Trap Event** (highlighted), Notification, RMON, and Restore Factory Default. The main content area is titled "Management >> SNMP >> Trap Event" and contains a table with the following settings:

Authentication Failure	<input checked="" type="checkbox"/> Enable
Link Up / Down	<input checked="" type="checkbox"/> Enable
Cold Start	<input checked="" type="checkbox"/> Enable
Warm Start	<input checked="" type="checkbox"/> Enable

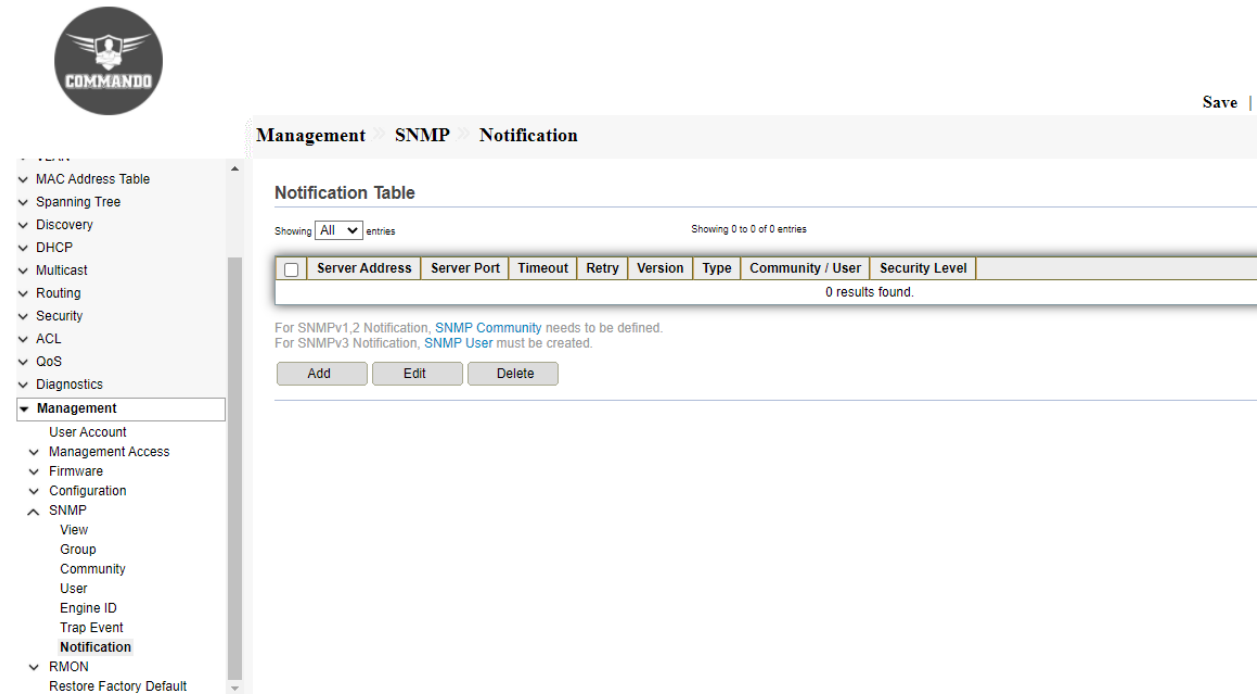
Below the table is an "Apply" button.

Fig 16.5.16 SNMP Trap Event page

16.5.7 Notification

An SNMP notification is a message sent from the device to the SNMP management station indicating that a certain event has occurred, such as a link up/down.

To view and configure the hosts to receive SNMPv1/v2/v3 notification, click **Management >> SNMP >> Notification**.



The screenshot displays the Commando network management interface. On the left is a navigation tree with the following items: MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, Management (expanded), User Account, Management Access, Firmware, Configuration, SNMP (expanded), View, Group, Community, User, Engine ID, Trap Event, Notification (highlighted), RMON, and Restore Factory Default. The main content area is titled "Management > SNMP > Notification" and includes a "Save" link. Below the breadcrumb is the "Notification Table" section, which shows "Showing 0 to 0 of 0 entries". A table with the following columns is displayed: (checkbox), Server Address, Server Port, Timeout, Retry, Version, Type, Community / User, and Security Level. Below the table, it states "0 results found." and provides instructions: "For SNMPv1,2 Notification, [SNMP Community](#) needs to be defined." and "For SNMPv3 Notification, [SNMP User](#) must be created." At the bottom of the table area are three buttons: "Add", "Edit", and "Delete".

Fig 16.5.17 SNMP Default Notification Table page



Management > SNMP > Notification

- Network
- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - View
 - Group
 - Community
 - User
 - Engine ID
 - Trap Event
 - Notification**
 - RMON
 - Restore Factory Default

Add Notification

Address Type	<input type="radio"/> Hostname <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text" value="192.168.0.50"/>
Version	<input type="radio"/> SNMPv1 <input type="radio"/> SNMPv2 <input checked="" type="radio"/> SNMPv3
Type	<input checked="" type="radio"/> Trap <input type="radio"/> Inform
Community / User	<input type="text" value="COMMANDO"/>
Security Level	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
Server Port	<input checked="" type="checkbox"/> Use Default <input type="text" value="162"/> (1 - 65535, default 162)
Timeout	<input checked="" type="checkbox"/> Use Default <input type="text" value="15"/> Sec (1 - 300, default 15)
Retry	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 255, default 3)

Fig 16.5.18 SNMP Add Notification page



Management > SNMP > Notification

- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ▼ **Management**
 - User Account
 - ✓ Management Access
 - ✓ Firmware
 - ✓ Configuration
 - ^ SNMP
 - View
 - Group
 - Community
 - User
 - Engine ID
 - Trap Event
 - Notification**
 - ✓ RMON
 - Restore Factory Default

Notification Table

Showing entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
<input type="checkbox"/>	192.168.0.50	162			SNMPv3	Trap	COMMANDO	No Security

For SNMPv1,2 Notification, **SNMP Community** needs to be defined.
For SNMPv3 Notification, **SNMP User** must be created.

Add

Edit

Delete

Fig 16.5.19 SNMP Notification Table page

16.6 RMON

RMON (Remote Networking Monitoring) is an SNMP specification that enables an SNMP agent in the device to proactively monitor traffic statistics over a given period and send traps to an SNMP manager. The local SNMP agent compares

RMON decreases the traffic between the manager and the device because the SNMP manager does not have to poll the device frequently for information, and enables the manager to get timely status reports, because the device reports events as they occur.

16.6.1 Statistics

The Statistics page displays detailed information regarding packet sizes and information regarding physical layer errors.

To view RMON Statistics, click **Management >> RMON >> Statistics**.

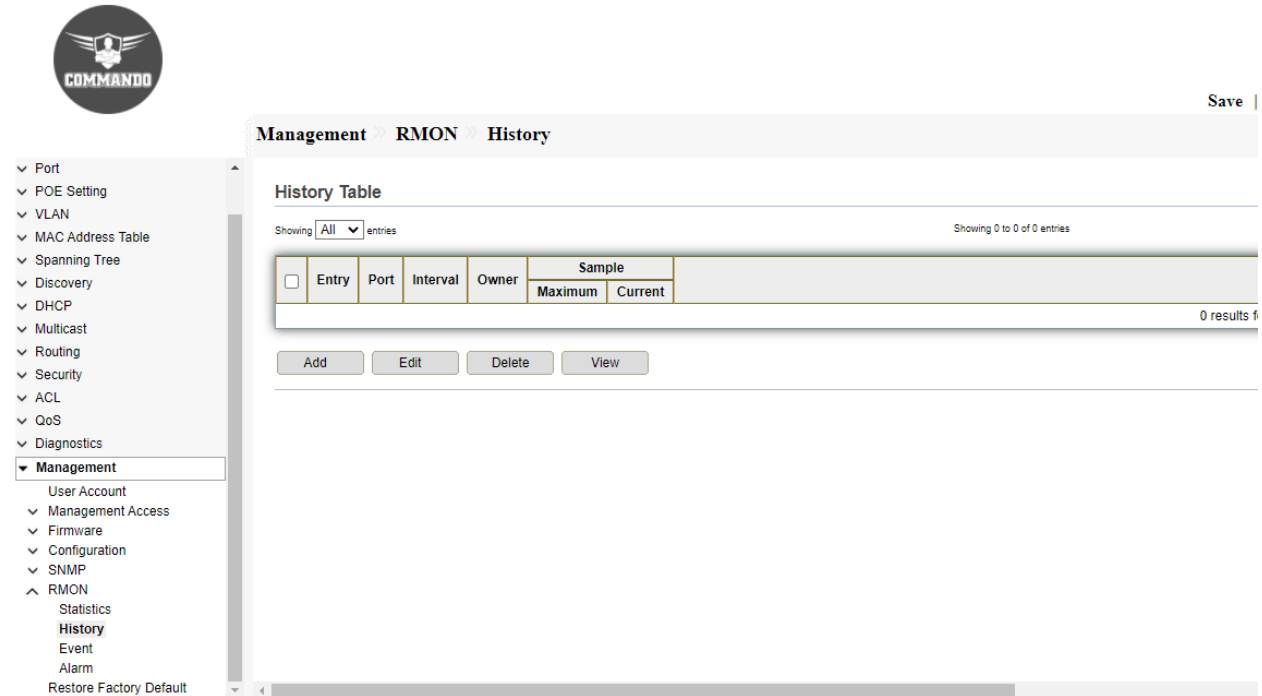
Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jammers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes
<input type="checkbox"/>	1 GE1	123710	0	1170	365	805	0	0	0	0	0	0	419	531	208	10	0	2
<input type="checkbox"/>	2 GE2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	3 GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4 GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5 GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	6 GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	7 GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	8 GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	9 GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	10 GE10	871385	0	3776	178	1123	0	0	0	0	0	0	1711	1188	277	56	487	80
<input type="checkbox"/>	11 GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	12 GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	13 GE13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	14 GE14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	15 GE15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	16 GE16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	17 GE17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	18 GE18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	19 GE19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fig 16.6.1 RMON Statistics Table page

16.6.2 History

The History Table page defines the sampling frequency, number of samples to store and the port from where to gather the data.

To view and configure RMON history, click **Management >> RMON >> History**.



The screenshot displays the COMMANDO web interface. On the left is a navigation tree with categories like Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, and Diagnostics. The 'Management' category is expanded, showing sub-items like User Account, Management Access, Firmware, Configuration, SNMP, RMON, Statistics, History, Event, and Alarm. The main content area shows the breadcrumb trail 'Management > RMON > History' and a 'Save' button. Below this is the 'History Table' section, which includes a dropdown menu set to 'All' entries and a status indicator 'Showing 0 to 0 of 0 entries'. The table has columns for 'Entry', 'Port', 'Interval', 'Owner', and 'Sample' (subdivided into 'Maximum' and 'Current'). Below the table are buttons for 'Add', 'Edit', 'Delete', and 'View'. The bottom of the page shows a 'Restore Factory Default' link.

Fig 16.6.2 RMON Default History Table page



Management > RMON > History

Add History

Entry	1
Port	GE10
Max Sample	50 (1 - 50, default 50)
Interval	1800 (1 - 3600, default 1800)
Owner	COMMANDO

Apply Close

Fig 16.6.3 RMON Add History page



Management >> RMON >> History

- ∨ Port
- ∨ POE Setting
- ∨ VLAN
- ∨ MAC Address Table
- ∨ Spanning Tree
- ∨ Discovery
- ∨ DHCP
- ∨ Multicast
- ∨ Routing
- ∨ Security
- ∨ ACL
- ∨ QoS
- ∨ Diagnostics
- ∨ **Management**
 - User Account
 - ∨ Management Access
 - ∨ Firmware
 - ∨ Configuration
 - ∨ SNMP
 - ∧ RMON
 - Statistics
 - History**
 - Event
 - Alarm
 - Restore Factory Default

History Table

Showing entries

<input type="checkbox"/>	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
<input type="checkbox"/>	1	GE10	1800	COMMANDO	50	50

Fig 16.6.4 RMON History Table page

16.6.3 Event

The Event Log Table page displays the log of events (actions) that occurred. Following types of events can be logged: Event Log or Trap or Event Log and Trap. The action in the event is performed when the event is bound to an alarm and the conditions of the alarm have occurred.

To view and configure RMON event, click **Management >> RMON >> Event**.

COMMANDO

Save |

Management > RMON > Event

Event Table

Showing All entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Entry	Community	Description	Notification	Time	Owner
0 results found.						

Add Edit Delete View

- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - RMON
 - Statistics
 - History
 - Event
 - Alarm
 - Restore Factory Default

Fig 16.6.5 RMON Default Event Table page



Management >> RMON >> Event

- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - RMON
 - Statistics
 - History
 - Event**
 - Alarm
 - Restore Factory Default

Add Event

Entry	1
Notification	<input type="radio"/> None <input type="radio"/> Event Log <input checked="" type="radio"/> Trap <input type="radio"/> Event Log and Trap
Community	COMMANDOLAN
Description	COMMANDO
Owner	COMMANDO

Apply Close

Fig 16.6.6 RMON Add Event page



Save |

Management >> RMON >> Event

- Port
- POE Setting
- VLAN
- MAC Address Table
- Spanning Tree
- Discovery
- DHCP
- Multicast
- Routing
- Security
- ACL
- QoS
- Diagnostics
- Management**
 - User Account
 - Management Access
 - Firmware
 - Configuration
 - SNMP
 - RMON
 - Statistics
 - History
 - Event**
 - Alarm
 - Restore Factory Default

Event Table

Showing All entries

Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Entry	Community	Description	Notification	Time	Owner
<input type="checkbox"/>	1	COMMANDOLAN	COMMANDO	Trap	(0) 0:00:00.00	COMMANDO

Add Edit Delete View

Fig 16.6.7 RMON Event Table page

16.6.4 Alarm

The Alarms page provides the ability to configure alarms and to bind them with events.

To view and configure RMON Alarm menu, click **Management >> RMON >> Alarm**.

The screenshot shows the 'Management > RMON > Alarm' page. On the left is a navigation menu with 'Management' expanded to show 'Alarm'. The main area is titled 'Alarm Table' and contains a table with columns: Entry, Port, Counter (Name, Value), Sampling, Interval, Owner, Trigger, Rising (Threshold, Event), and Falling (Threshold, Event). The table is currently empty, displaying '0 results found.' Below the table are 'Add', 'Edit', and 'Delete' buttons. At the top right of the page are links for 'Save', 'Logout', 'Reboot', and 'Debug'.

Fig 16.6.8 RMON Default Alarm page

The screenshot shows the 'Management > RMON > Alarm' page with the 'Add Alarm' form. The form is titled 'Add Alarm' and contains the following fields:

- Entry:** 1
- Port:** GE10
- Counter:** Oversize Packets
- Sampling:** Absolute (selected), Delta
- Interval:** 100 (Sec (1 - 2147483647, default 100))
- Owner:** COMMANDO
- Trigger:** Rising (selected), Falling, Rising and Falling
- Rising:**
 - Threshold:** 100 (0 - 2147483647, default 100)
 - Event:** 1 - COMMANDO
- Falling:**
 - Threshold:** 20 (0 - 2147483647, default 20)
 - Event:** 1 - COMMANDO

 At the bottom of the form are 'Apply' and 'Close' buttons. The left navigation menu is also visible, with 'Management' expanded to 'Alarm'.

Fig 16.6.9 RMON Add Alarm Counter page



Management > RMON > Alarm

Alarm Table

Showing entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
			Name	Value					Threshold	Event	Threshold	Event
<input type="checkbox"/>	1	GE10	OverSizePkts	0	Absolute	100	COMMANDO	Rising	100	COMMANDO	20	COMMANDO

Fig 16.6.10 RMON Alarm Table page

16.7 Restore Factory Default

E3000 Hardware also you can factory reset by software reset Command. Use Restore Factory Default, Click **Management>>Restore Factory Default** and again reboot the Switch to get factory default configuration in E3000 Series Switches.

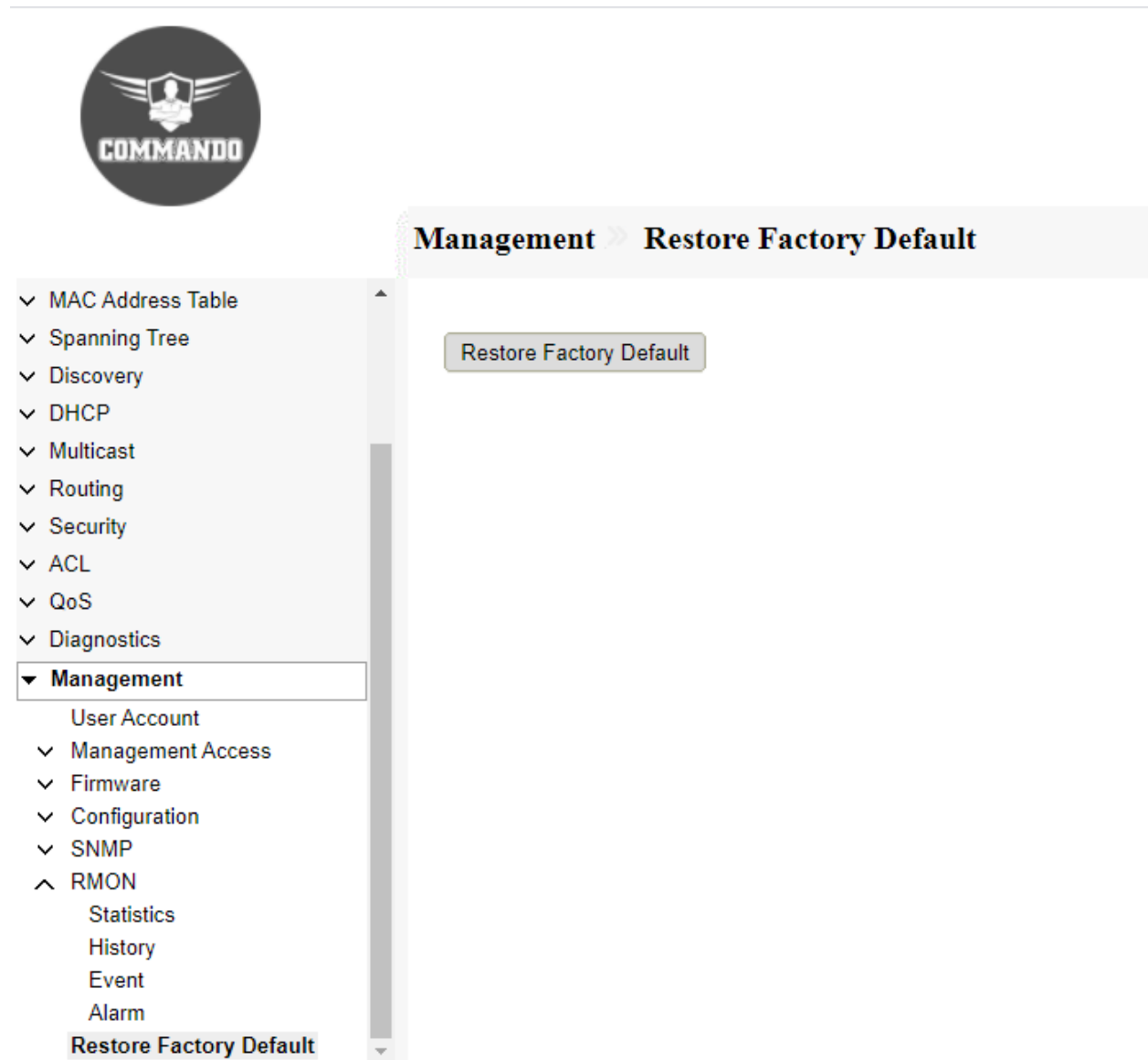


Fig 16.7.1 Restore Factory Default page

17. PoE/PoE+ Setting

Power over Ethernet (PoE) is technology that passes electric power over twisted-pair Ethernet cable to powered devices (PD), such as wireless access points, IP cameras, and VoIP phones in addition to the data that cable usually carries. It enables one RJ45 cable to provide both data connection and electric power to PDs instead of having a separate cable for each. PoE is IEEE802.3af, PoE+ is IEEE802.3at. Currently, the max amount of power provided over Cat5 cabling is 15.4 watts for PoE and 30W watts for PoE+ supported by E3000 series Switches.

Note: This topic is applicable only for PoE/PoE+ E3000 Series Switches.

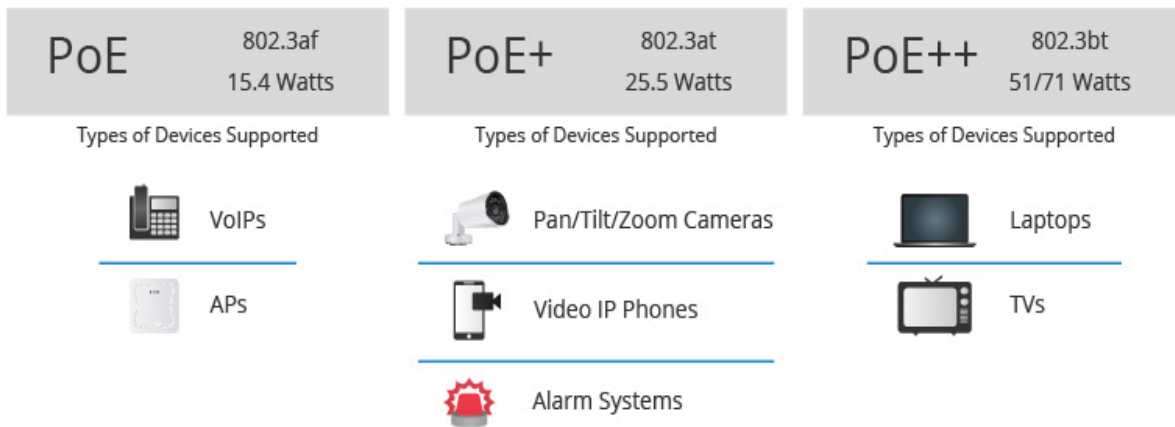
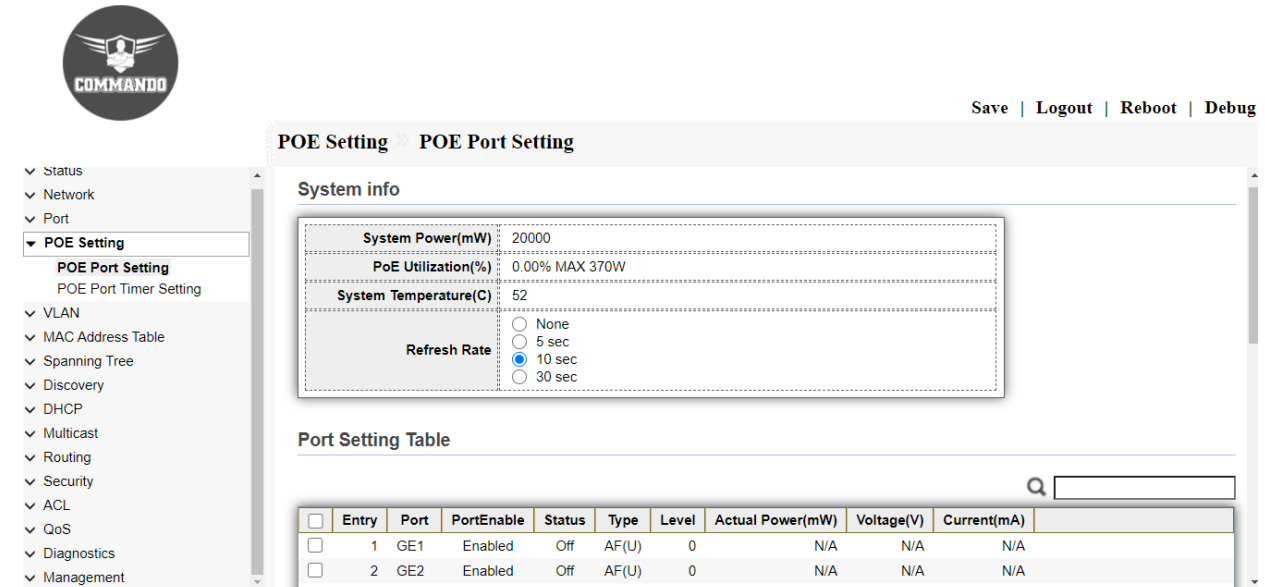


Fig 17.1 E3000 Series PoE/PoE+ Switches Concept

17.1.1 POE Port Setting

The PoE/PoE+ Settings page displays system PoE/PoE+ information for auto enabling PoE/PoE+ on the interfaces and monitoring the current power usage and maximum power limit per port.

For the POE Port Setting menu, click **POE Setting >> POE Port Setting**.



The screenshot shows the COMMANDO web interface for POE Port Setting. The left sidebar contains a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The main content area is titled "POE Setting" and "POE Port Setting". It features a "System info" section with a table of system parameters and a "Port Setting Table" below it. The "System info" table includes System Power(mW), PoE Utilization(%), System Temperature(C), and Refresh Rate. The "Port Setting Table" has columns for Entry, Port, PortEnable, Status, Type, Level, Actual Power(mW), Voltage(V), and Current(mA).

System info

System Power(mW)	20000
PoE Utilization(%)	0.00% MAX 370W
System Temperature(C)	52
Refresh Rate	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 30 sec

Port Setting Table

Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)
<input type="checkbox"/>	1	GE1	Enabled	Off	AF(U)	0	N/A	N/A
<input type="checkbox"/>	2	GE2	Enabled	Off	AF(U)	0	N/A	N/A

Fig 17.1.1 PoE Port Setting System Default Info page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
 - POE Port Setting
 - POE Port Timer Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

POE Setting > POE Port Setting

System info

System Power(mW)	26114
PoE Utilization(%)	1.65% MAX 370W
System Temperature(C)	52
Refresh Rate	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 30 sec

Port Setting Table

<input type="checkbox"/>	Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)
<input type="checkbox"/>	1	GE1	Enabled	Off	AF(U)	0	N/A	N/A	N/A
<input type="checkbox"/>	2	GE2	Enabled	On	AT(N)	4	3888	54	72
<input type="checkbox"/>	3	GE3	Enabled	On	AF(N)	3	2226	53	42
<input type="checkbox"/>	4	GE4	Enabled	Off	AF(U)	0	N/A	N/A	N/A
<input type="checkbox"/>	5	GE5	Enabled	Off	AF(U)	0	N/A	N/A	N/A

Fig 17.1.2 PoE Port Setting System Info after adding PoE devices page



- ▼ Status
- ▼ Network
- ▼ Port
- ▼ POE Setting
 - POE Port Setting
 - POE Port Timer Setting
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

Save

POE Setting > POE Port Setting

System info

System Power(mW)	25744
PoE Utilization(%)	1.55% MAX 370W
System Temperature(C)	52
Refresh Rate	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 30 sec

Port Setting Table

<input type="checkbox"/>	Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)
<input type="checkbox"/>	1	GE1	Enabled	Off	AF(U)	0	N/A	N/A	N/A
<input checked="" type="checkbox"/>	2	GE2	Enabled	On	AT(N)	4	3942	54	73
<input type="checkbox"/>	3	GE3	Enabled	On	AF(N)	3	1802	53	34
<input type="checkbox"/>	4	GE4	Enabled	Off	AF(U)	0	N/A	N/A	N/A
<input type="checkbox"/>	5	GE5	Enabled	Off	AF(U)	0	N/A	N/A	N/A

Fig 17.1.3 Selecting PoE Port for Setting page



- ✓ Status
- ✓ Network
- ✓ Port
- ▼ POE Setting
 - POE Port Setting
 - POE Port Timer Setting
- ✓ VLAN
- ✓ MAC Address Table
- ✓ Spanning Tree
- ✓ Discovery
- ✓ DHCP
- ✓ Multicast
- ✓ Routing
- ✓ Security
- ✓ ACL
- ✓ QoS
- ✓ Diagnostics
- ✓ Management

POE Setting > POE Port Setting

Edit Port Setting

Port	GE2
PortEnable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Apply

Close

Fig 17.1.4 Edit PoE Port Setting page

17.2 POE Port Timer Setting

PoE/PoE+ can be configured on the device for a specific period. This feature enables you to define, per port, the days in the week and the hours that PoE is enabled. By default, Power over Ethernet (PoE)-capable ports can deliver PoE/PoE+ power continuously. E3000 Series Switches auto ON/OFF PoE/PoE+ as per Scheduled time which makes them intelligent. PoE/PoE+ Scheduling is a feature which allows you to specify the amount of time that power is delivered to a PoE/PoE+ port. This can be used to save power when devices are not in use, or as a security feature to prevent access from being available outside of business hours. When the time is not active, PoE is disabled.

For the POE Port Timer Setting menu, click **POE Setting >> POE Port Timer Setting**.

The screenshot shows the COMMANDO web interface. On the left is a navigation menu with categories like Status, Network, Port, POE Setting, VLAN, MAC Address Table, Spanning Tree, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics, and Management. The main content area is titled "POE Setting > POE Port Timer Setting" and includes a "Port" dropdown menu set to "GE1". Below this is a search bar and a table of checkboxes for each day of the week (Mon-Sun) and hour of the day (00-23). All checkboxes are checked, indicating PoE is enabled for all days and hours. An "Apply" button is located below the table. In the top right corner, there are links for "Save", "Logout", "Reboot", and "Debug".

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Thu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fri	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Fig 17.2.1 Default PoE Port Timer Setting for GE1 page



Save | Logout | Reboot | Debug

- ▼ Status
- ▼ Network
- ▼ Port
- ▼ **POE Setting**
 - POE Port Setting
 - POE Port Timer Setting**
- ▼ VLAN
- ▼ MAC Address Table
- ▼ Spanning Tree
- ▼ Discovery
- ▼ DHCP
- ▼ Multicast
- ▼ Routing
- ▼ Security
- ▼ ACL
- ▼ QoS
- ▼ Diagnostics
- ▼ Management

POE Setting > **POE Port Timer Setting**

Port:

<input type="checkbox"/>	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Thu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fri	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sun	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Fig 17.2.2 Turning Off PoE Port and Setting timer for GE3 for Saturday and Sunday page