COMMANDO C2000 Managed Switch Web Manual

SoliderOS Version 1.4 Onwards

Trademarks and Permissions

COMMANDO Networks trademarks are trademarks of COMMANDO Networks Ltd.The COMMANDO trademarks, service marks ("Marks") and other COMMANDO trademarks are the property of COMMANDO Networks. COMMANDO Soilder 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 orrepresentations 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

Chapter 1 Introduction

COMMANDO Soldier C2000 Series Switches offers a state of art quality product that can serve on real time high-speed Performance with dual input power AC as well as DC, Covers larger physical distance upto 250 meters with copper cables as compared to other brands best switches. This series is having advance L2+ and basic 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 Web-based Graphical User Interface (WEBUI) , Command Line interface (CLI) , RADIUS/TACACS+, LLDP/LLDP-MED, Time based PoE/PoE+/PoE++ Scheduling, DHCP server as well as zero touch provisioning Whichever is suitable to our esteem customers.

COMMANDO Soldier C2000 Series Switches Series are fixed-configuration, with flexible uplinks Gigabit Ethernet switches that provide enterprise-class access for campus and branch applications. Designed for the digital workplace, these are optimized for today's mobile and IoT needs. These switches are powerful and flexible enough for users to deploy PoE/PoE+/PoE++ standard supplies up to 90W of power per port 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. The 90W PoE++; IEEE 802.3bt technology drives high-power infrastructure for smart building systems, safe cities, thin clients, and a lot more. Facility managers and building owners can adopt the standard to future-proof their all PoE/PoE+/PoE++ networks requirements. The outcome for them is lower installation and wiring costs. COMMANDO Soldier C2000 Series provide easy device rack and wall mounting, on boarding, configuration, monitoring, and troubleshooting. These fully managed switches can provide advanced L2+ and basic Layer 3 features as well as supports IEEE 802.3af-compliant PoE (Power over Ethernet), 802.3at-compliant PoE+ (Power over Ethernet plus) and IEEE802.3bt type-4 (Power over Ethernet plus plus). Each switchport is capable to

deliver 15.4 W PoE, 30 W PoE+ and 90W PoE++ power on all ports along with automated power (ON/OFF) scheduling. All Switches are PoE/PoE+/PoE++ capable to provide power across all access ports for wireless APs, security cameras, and other IoT devices. Designed for operational simplicity to lower total cost of ownership, they enable scalable, secure, and energy-efficient business operations with intelligent and automated services.

COMMANDO Soldier C2000 Series Switches RJ-45 auto sensing/auto PoE/PoE+/PoE++ 10/100/1000 ports with auto MDIX capabilities which also removes speed and duplex mismatches automatically as well as covers larger physical distance with copper pairs compared to other brands best switches . This series switches supports 8K MAC address tables , 4.1MB Packet Buffer memory , 10K bytes Jumbo Frames, Ipv4/IPv6 with 1024 static routing entries,s(MAC/IP/Port based), Port aggregation upto 8 ports, VLAN, Voice VLAN, GVRP, DHCP Server,DHCP Client, DHCP Snooping, DHCP Snooping option82, DHCP Relay, 802.1X authentication, centralized MAC authentication, Guest VLAN, RADIUS authentication, SSH 2.0, Port isolation, Port security, MAC address learning limit, IP Source guard, Dynamic ARP inspection, preventing man-in-the-middle attacks and ARP DoS attacks, IP/Port/MAC binding. COMMANDO Soldier C2000 Series Switches Management is made easy via a web-based Graphical User Interface (WEBUI/) or industry-standard Command Line Interface (CLI), with administration traffic protected via SSL or SSH encryption. SNMP (v1/v2c/v3) and RMON support enables the switch to be polled for valuable status information and allows it to send traps when abnormal events occur.

COMMANDO Soldier C2000 Series Switches with easy installation, configuration, monitoring, and troubleshooting and greatly reduces initial installation, configurationas well as administration costs. This series has improved HTTP base firmware upgrade as well as CLI based Updates which are freely available to all users without any cost or license fee for all times . These series switches supports Flexible service control with various ACLs to flexibly control ports. It also supports port-based VLAN assignment, MAC address-based VLAN assignment, protocol-based VLAN assignment, and network segment-based VLAN assignment. These secure and flexible VLAN assignment modes are used in networks where users

move frequently. It also supports GARP VLAN Registration Protocol (GVRP), which dynamically distributes, registers, and propagates VLAN attributes to ensure correct VLAN configuration and reduce network administrator workloads. This series switches supports SSH v1/v2/v3, RMON, and port-based traffic statistics.
COMMANDO Soldier C2000 Series Switches are the ideal solution for the most advanced small and medium organizations looking for the best combination of features, performance, and value. These switches are purposely designed for converged networks where voice, video, data are all carried on a single network platform. This series comes with fan/fanless switches models along with Small form-factor, fanless as well fan design for silent operation. Perfect for noise sensitive environments. Fan based Switches have Temperature- and load-based fan-speed control combines accurate monitoring with minimized system acoustic noise. The Fan based switches also feature built-in smart fans that monitor and detect temperature changes, adjusting the fan speed for maximum efficiency. At lower temperatures, the fans run at a lower speed, reducing both the power consumption and noise output of the switch.These cost effective switches, with a reasonable PoE/PoE+ power budget up to 800W along with PoE/PoE+/PoE++ configurable scheduler to automated Power ON/OFF connected PoE/PoE+/PoE++ devices as per scheduled timing.

The document is a user guide for COMMANDO Web demonstration web pages on C2000.The C2000 acts as a web server to accept http connection request and replies web pages so that user can get configuration or change configuration to C2000 by web access.

The COMMANDO SoldierOS IP Base switches Management is made easy via a web-based Graphical User Interface (WEBUI) access via HTTP/HTTPS or industry-standard Command Line Interface (CLI) via Console/Telnet with administration traffic protected via , SNMP v1/v2C/v3, SSH v1/v2, RMON v1/v2 which enables the switch to be polled for valuable status information and allows it to send traps when abnormal events occur.

Simplified Configuration and Management

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

Easy to manage via Console/web-Based Management (WEBUI)/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 WEBUI / 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 WebUI- 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 C2000 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 HyperTerminal 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

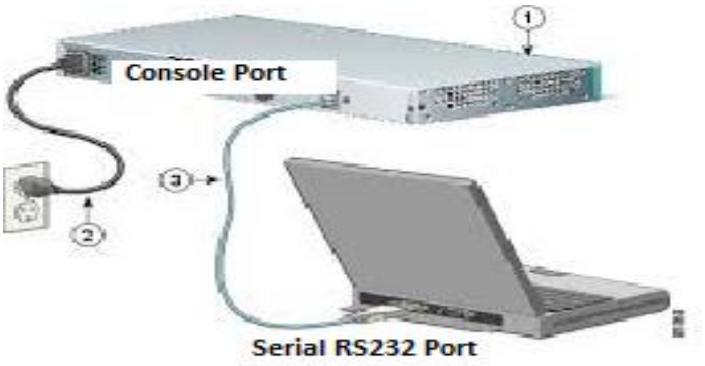
• No parity

• 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 of 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.



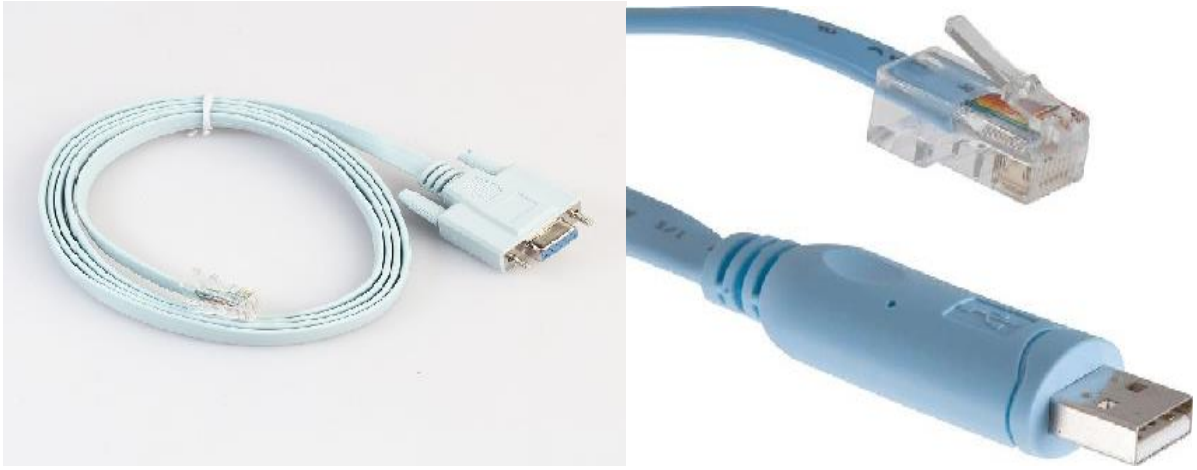


Fig-1. Connection of console port with PC/Laptop via console cable.

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

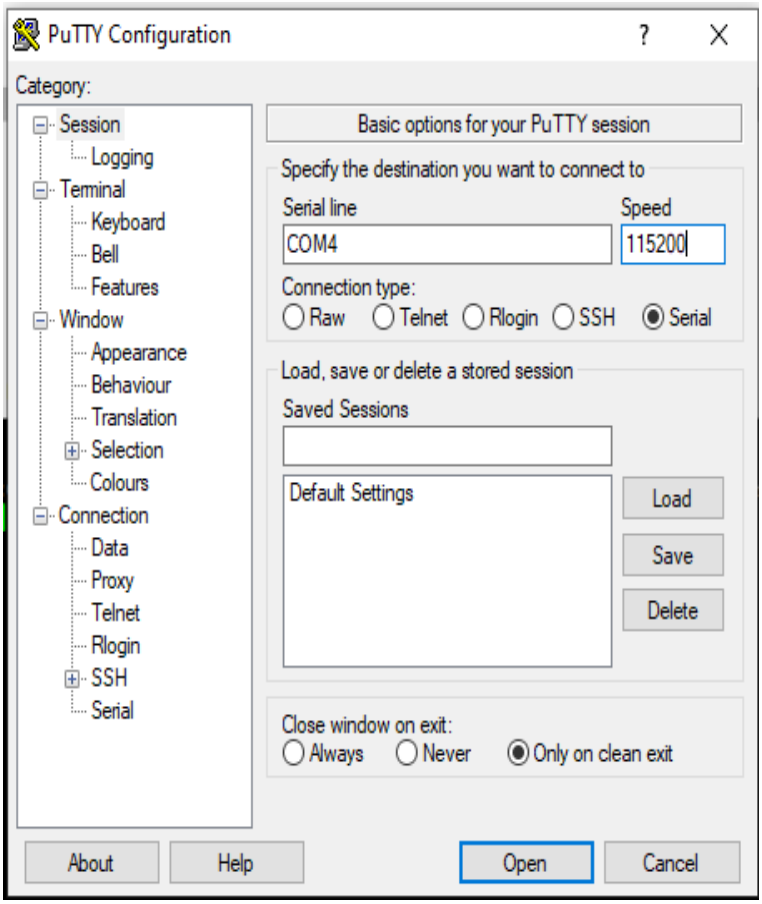


Fig-2. Putty configuration in PC for console port access

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.

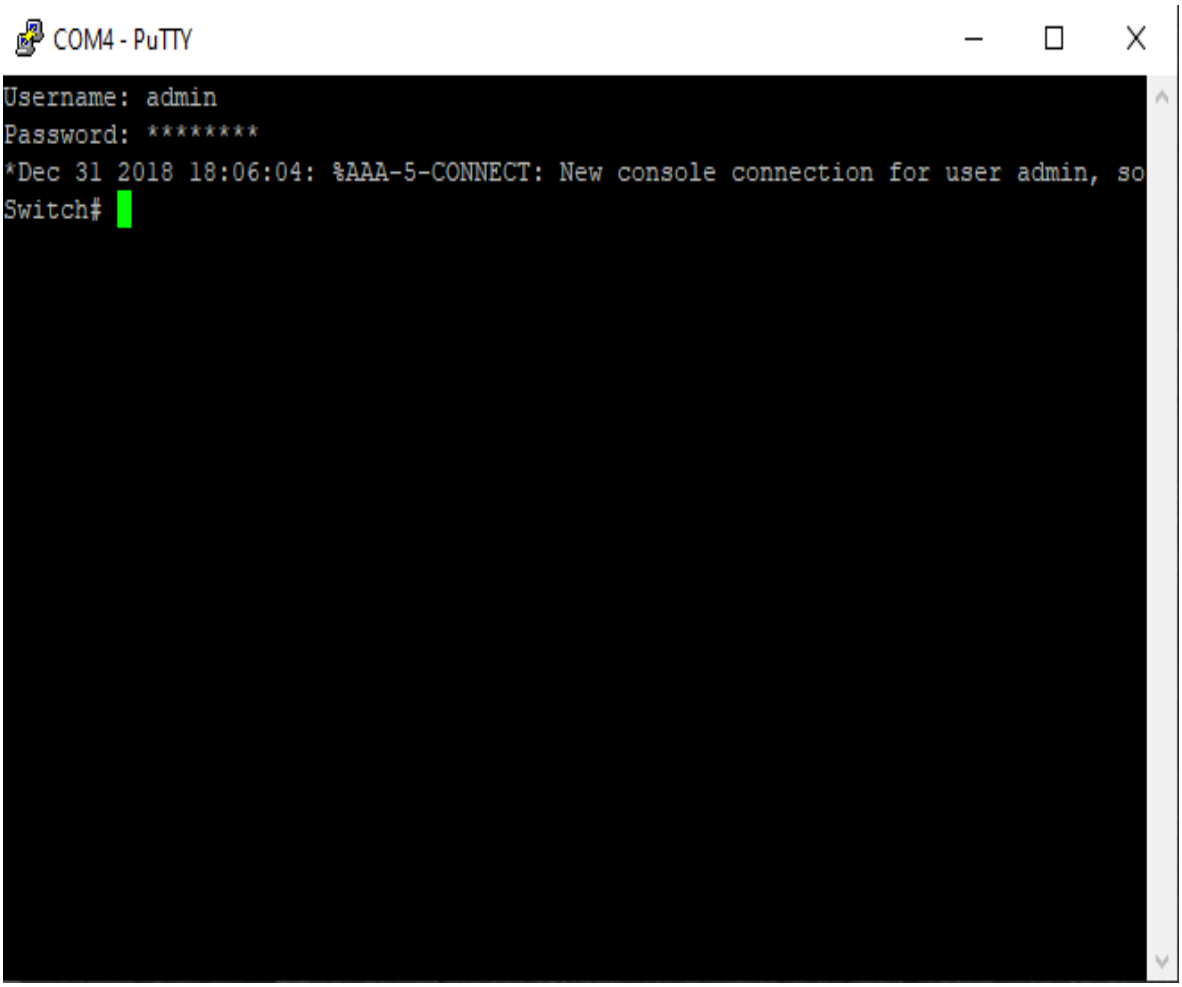


Fig-3. COMMANDO Series C2000 Switch CLI access via console port

How to Login COMMANDO Series C2000 WEBUI and Enable Telnet?

Before Accessing Command Line Interface via telnet you have to login to WEBUI of COMMANDO C2000 Switch. Connect one Ethernet port to your system with RJ45 LAN cable.

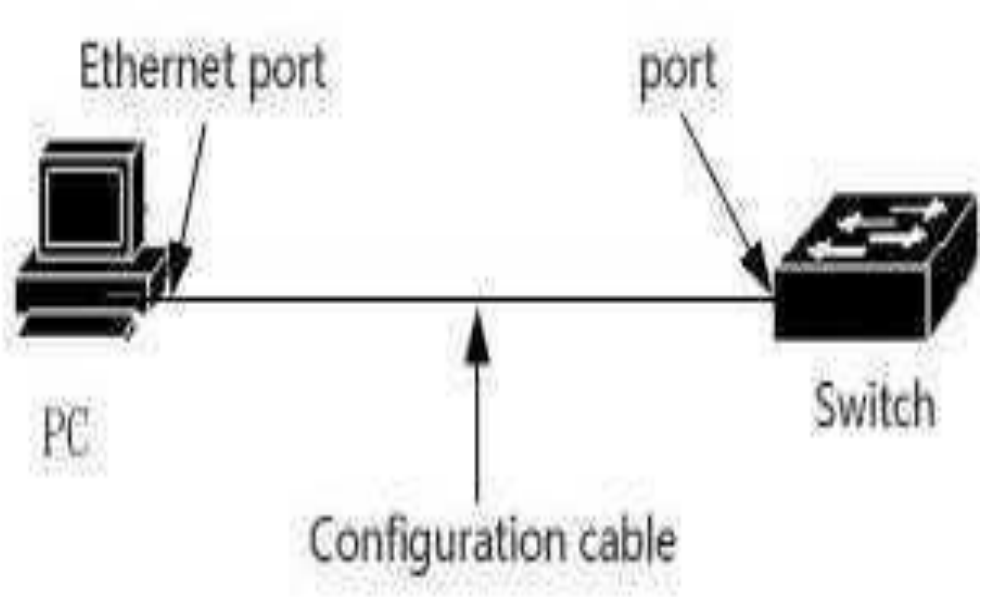


Fig-4. COMMANDO Series C2000 Switch port connected with PC via RJ45 LAN cable.

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

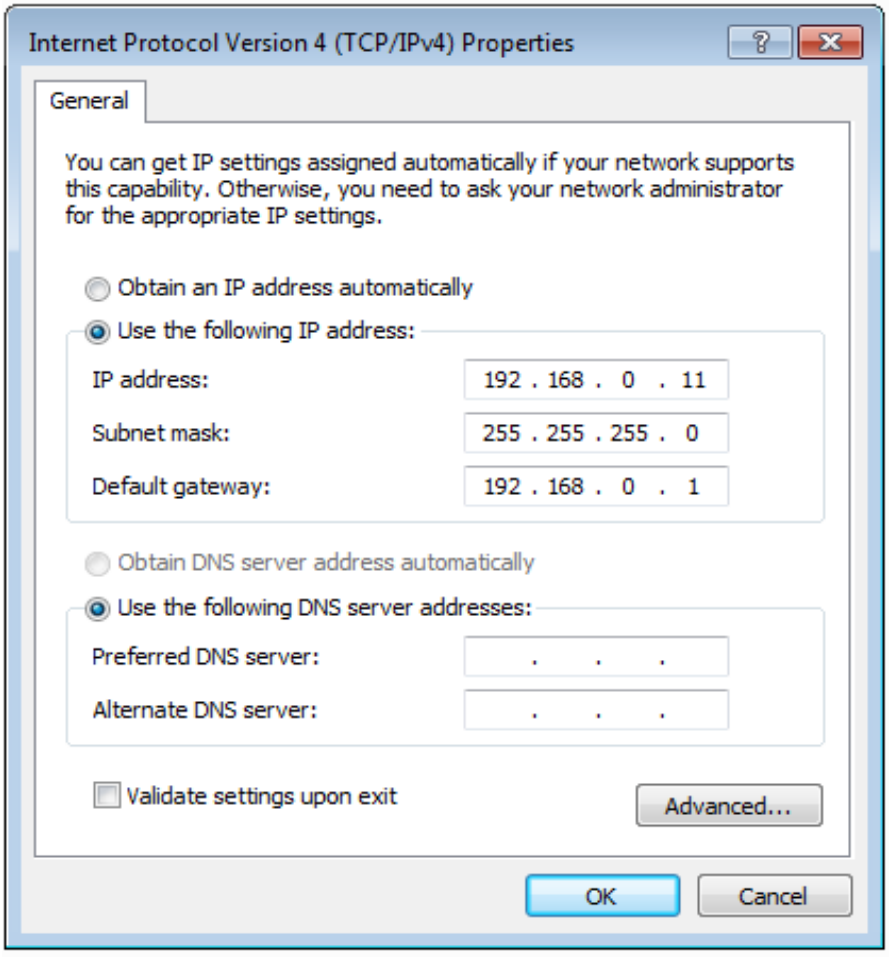


Fig-5. Local Area Connection properties for Web Interface

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 WEBUI mode,
Username: **admin**
Password: ********
(Note:- Password is mentioned on backside of device)

Enter the login button. COMMANDO C2000 series switch starting Page appears .

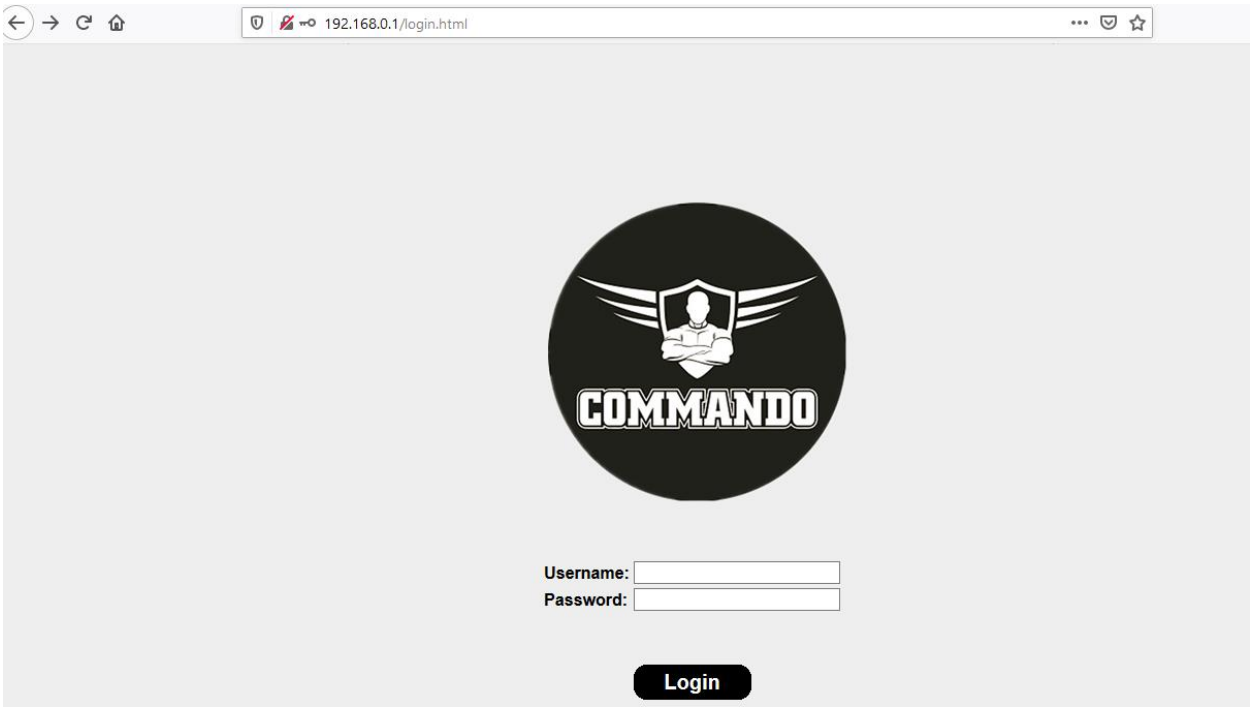


Fig-6. COMMANDO C2000 Switch WEBUI Administrator Login Page

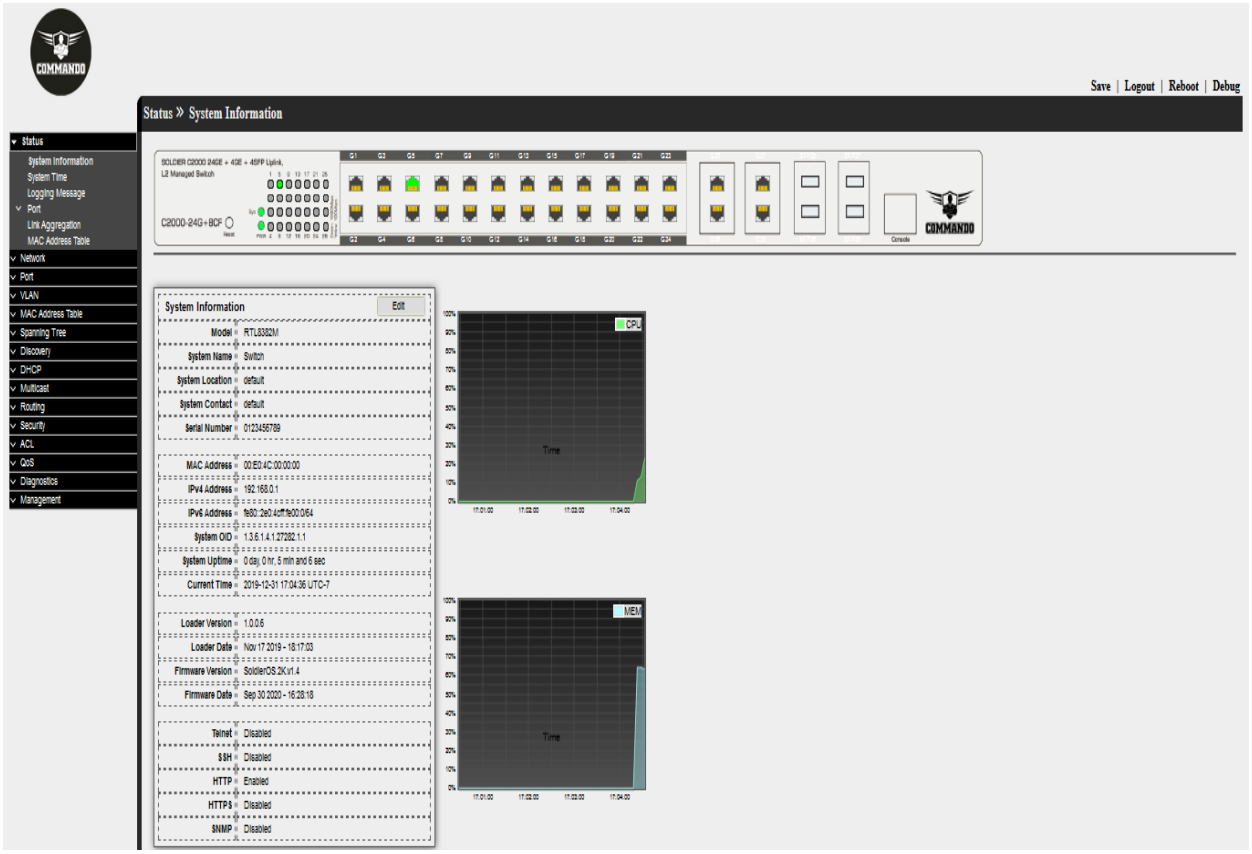


Fig-7. COMMANDO C2000 Switch WEBUI starting Page

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 C2000 Switch Command Line Interface (CLI) to enable **"Telnet".** By default **"Telnet"** service is disabled by default so you have to 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) .

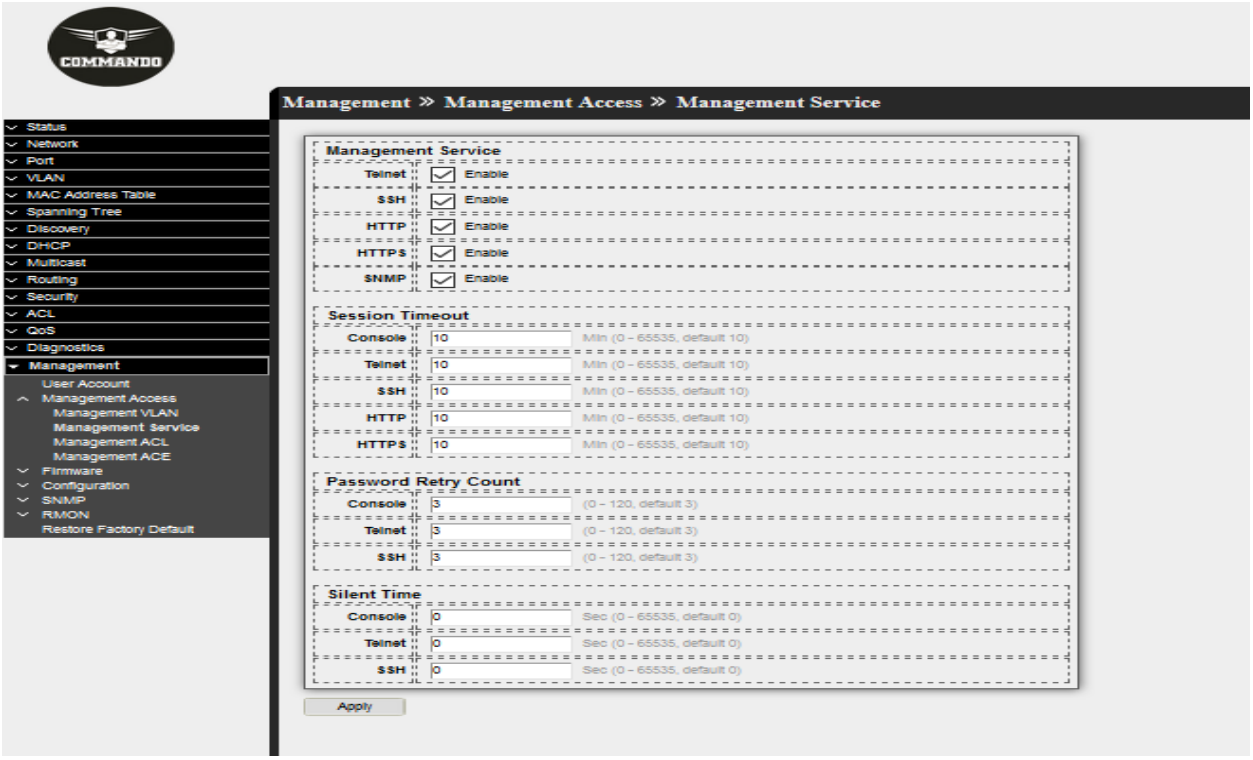


Fig-8. COMMANDO C2000 Switch Management Access service.

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**

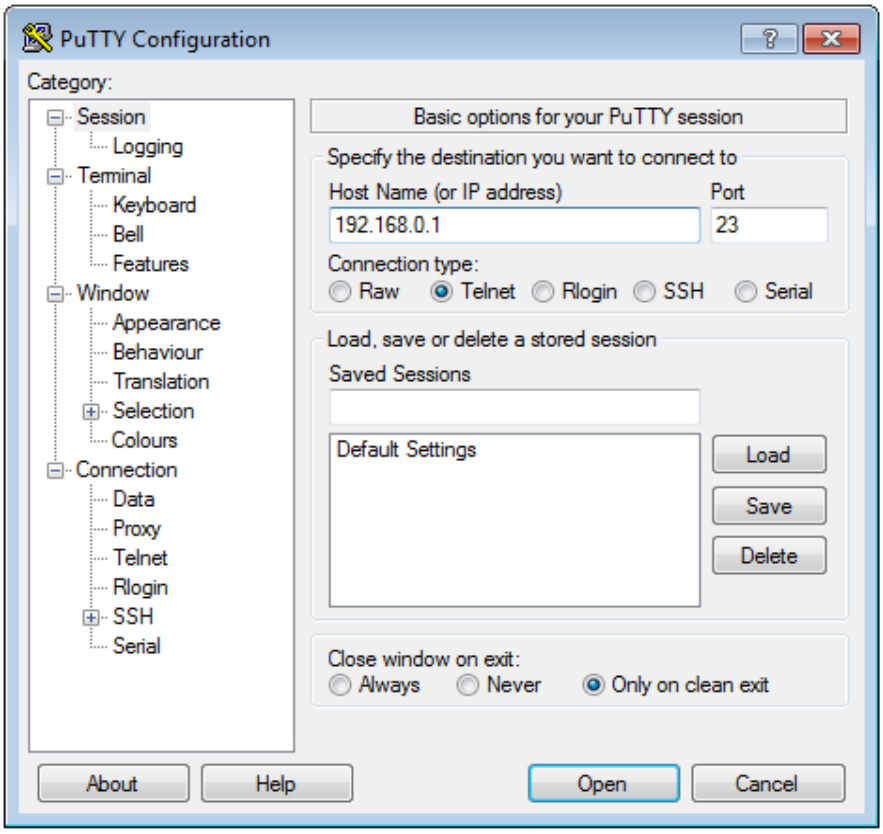


Fig-9. Putty configuration in PC for Telnet access

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

Username: **admin**

Password: ********

(Note:- Password is mentioned on backside of device)

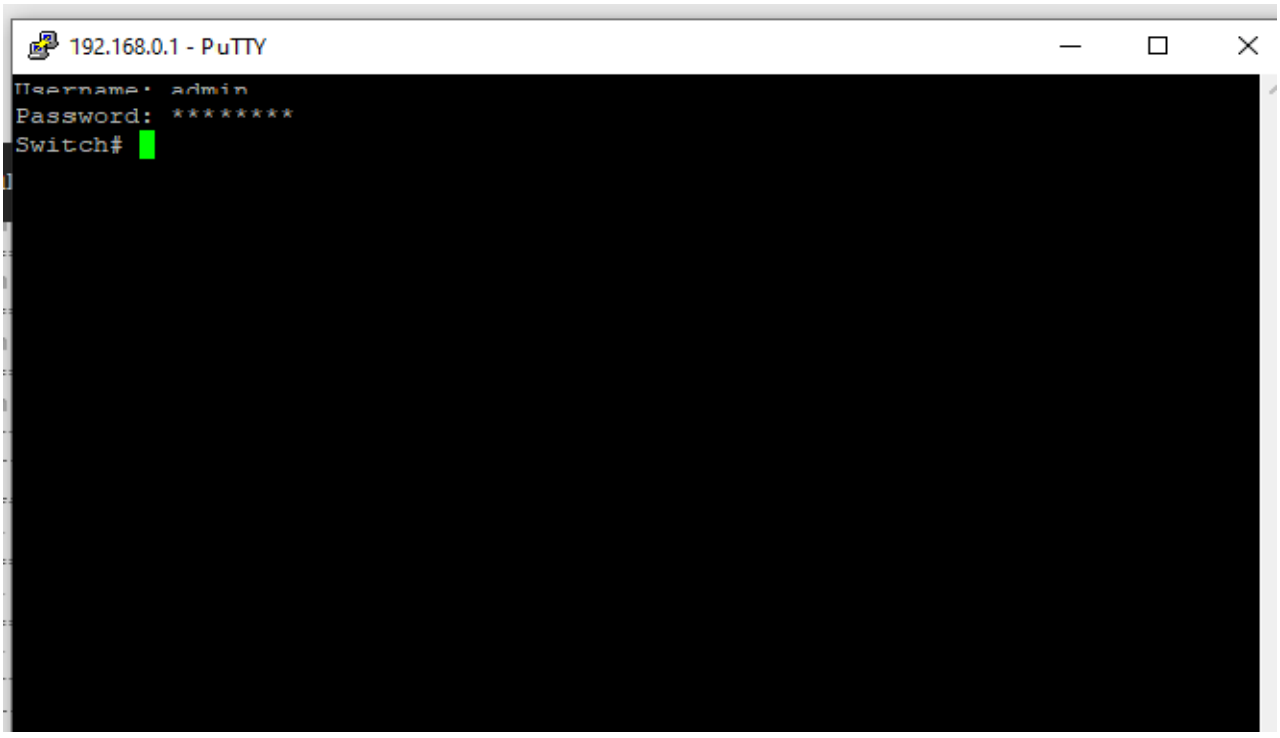


Fig-10. COMMANDO Series C2000 Switch CLI access via telnet

1.1 Web browse based graphical user interface (WEBUI) Introduction

COMMANDO C2000 Series SoliderOS had a web browser based graphical user interface (WEBUI). This is inbuilt in each COMMANDO C2000 series switches. You can use either the CLI via Console/Telnet or WEBUI for manageing C2000 Series Switches. COMMANDO Networks recommend that you use this WEBUI which can configure almost everything as you needed in simple and user friendly manner. This WEBUI 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 parmeter given above and in Web browser giving IP address 192.168.0.1 you will get the login page.

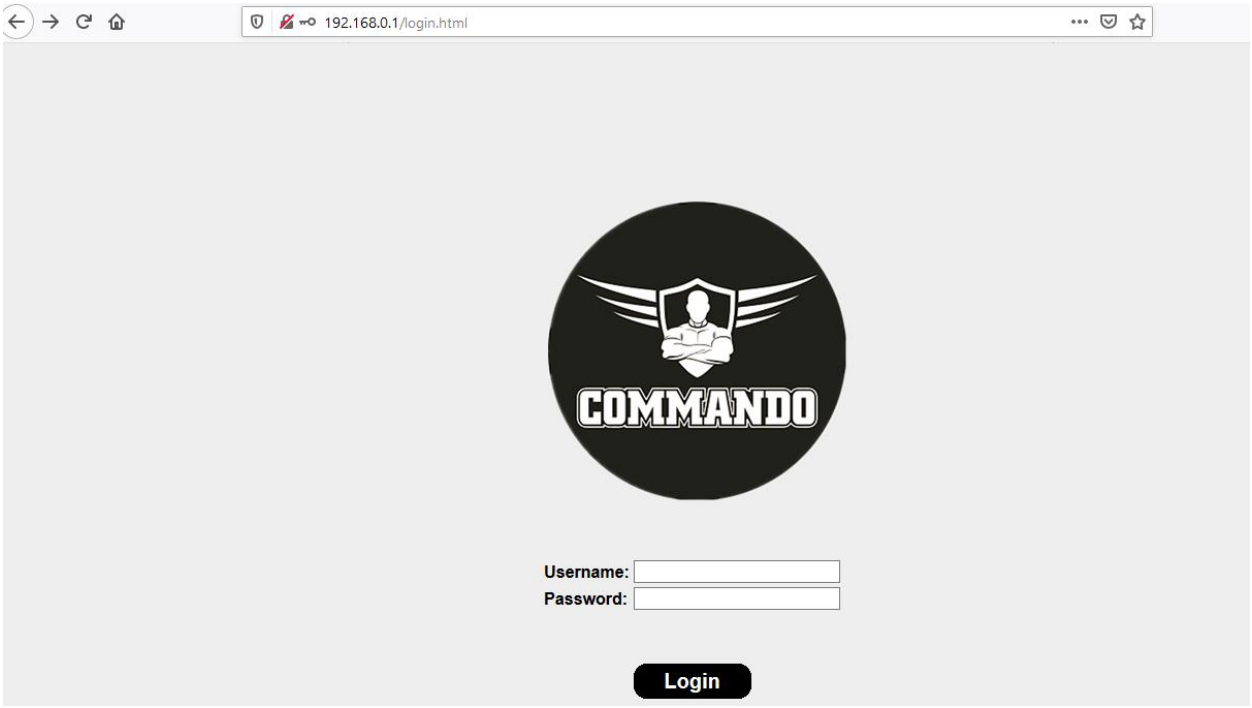


Fig 1.1 Default Login page of C2000 Series Switches

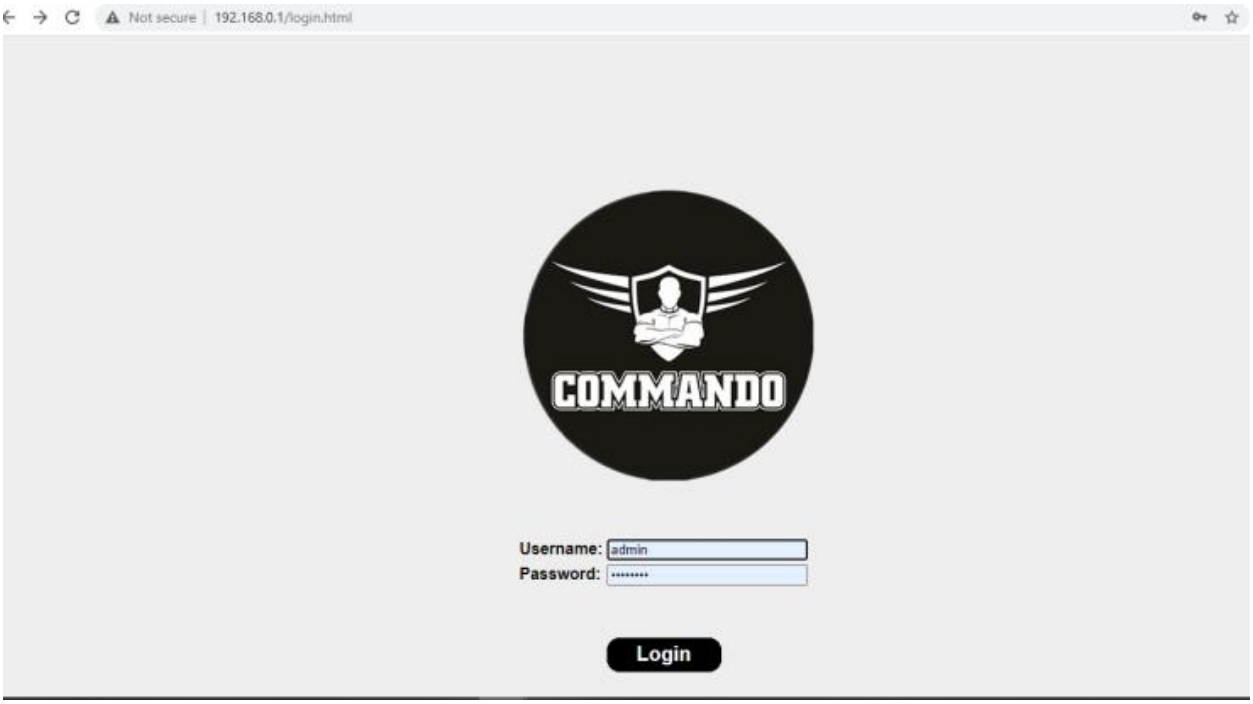


Fig 1.2 Username and Password page of C2000 Series Switches

Note:- With C2000 Web based Graphical User Interface (WEBUI)

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 C2000 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.

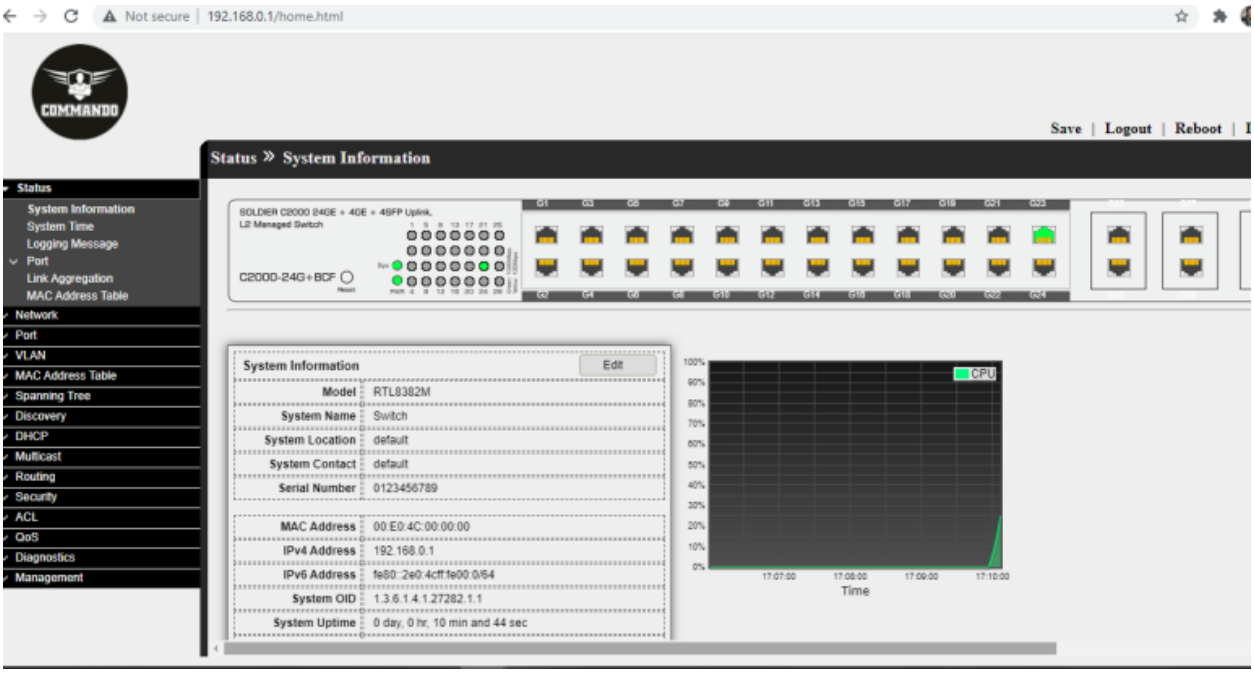


Fig 1.3 System Information page of C2000 Series Switches

1.2 Main Menu Description in WEBUI

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 downarrow key can expand group head label to get specific Web pages for Switch to configure as per requirement of users.

In C2000 Series Switches SoliderOS comes with PoE as Well as Non PoE models. COMMAMDO SoilderOS has 15 Group heads for C2000 PoE based switches and 14 Group heads for Non PoE switches. Lots of functions and protocols can be easily configured by WEBUI and very handy and easy to trobleshoot any networking issue.

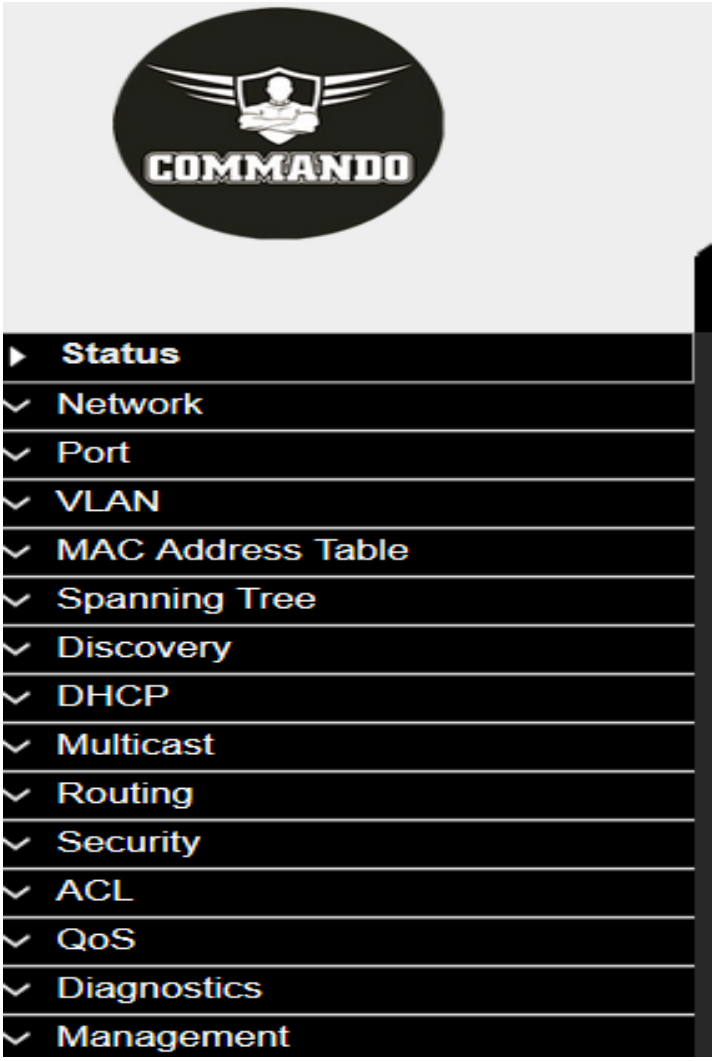


Fig 1.4 WEB Pages for C2000 Series Switches.

Quick Start Device Configuration

To simplify C2000 Series device configuration through quick navigation, the Getting Started page provides links to the most commonly used pages.

Table 1.1 C2000 Series Switches SoliderOS Web Software Frameworks.

Group head lable	Corresponding Web pages
Status	System Information System Time Logging Message Port Statistics Error Disabled Bandwidth Utilization Link Aggregation MAC Address Table
Network	IP Address DNS Hosts
Port	Port Setting Error Disabled Link Aggregation Group

	Port Setting LACP EEE Jumbo Frame Port Security Protected Port Storm Control Mirroring
POE Setting	POE Port Setting POE Port Timer Setting Note:-1. Only Avaliable in PoE/PoE+/PoE++ Switches. 2. Intellligent PoE/PoE+/PoE++ Schedular is special feature of COMMANDO C2000 Series Switches.
VLAN	VLAN Create VLAN VLAN Configuration 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 IPv6 Addresses IPv6 Routes IPv6 Neighbors
Security	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
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.

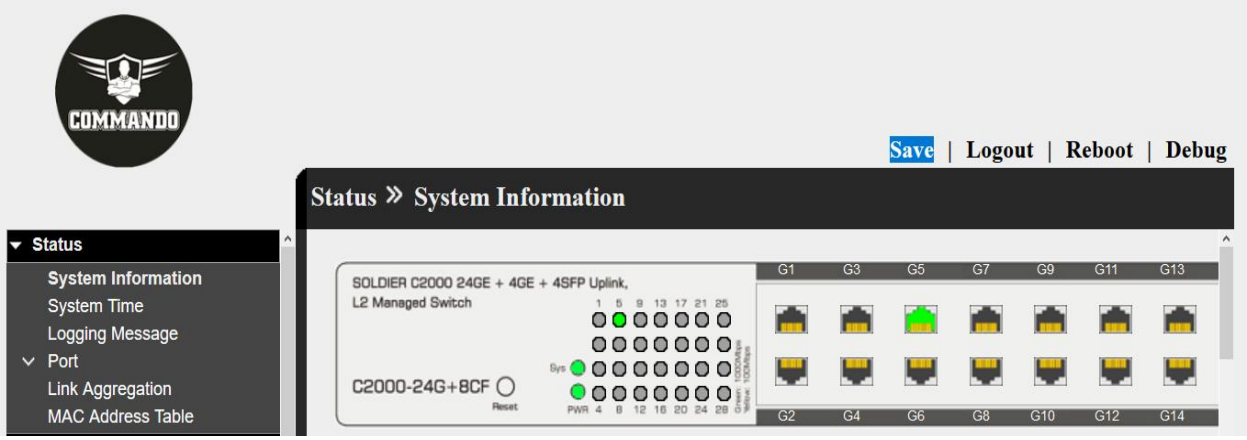


Fig 1.3.1 Save button

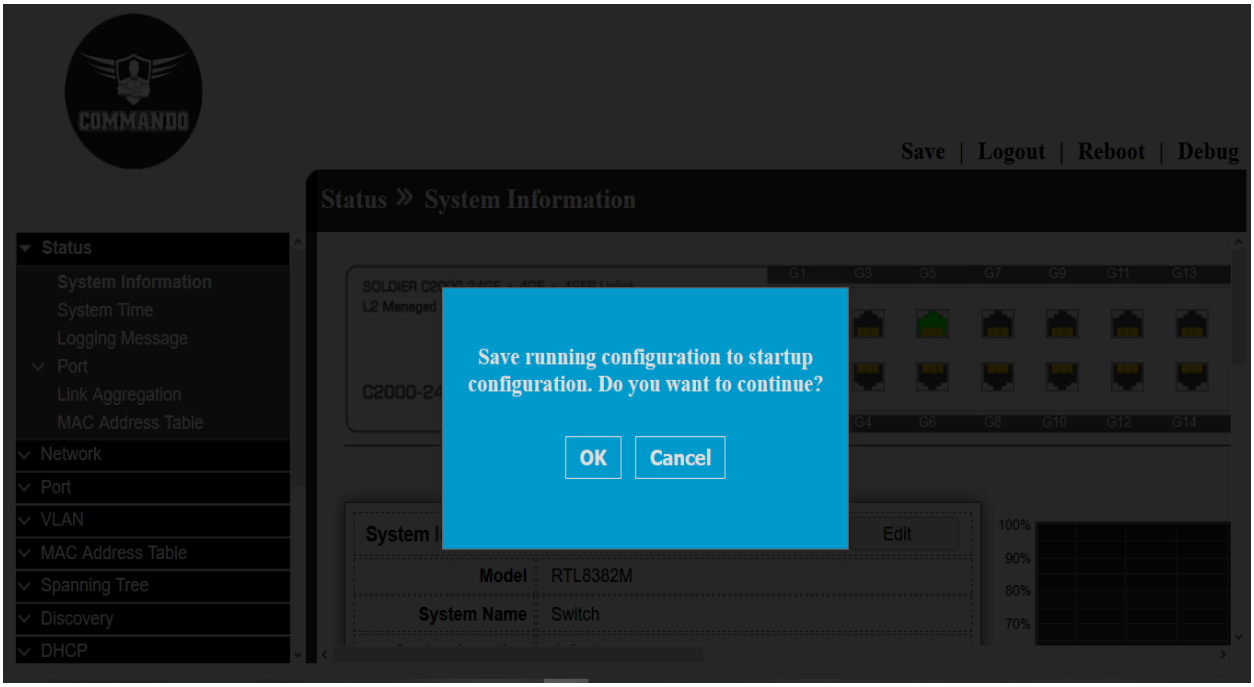


Fig 1.3.2 Applying Save button

1.3.2 Logout

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

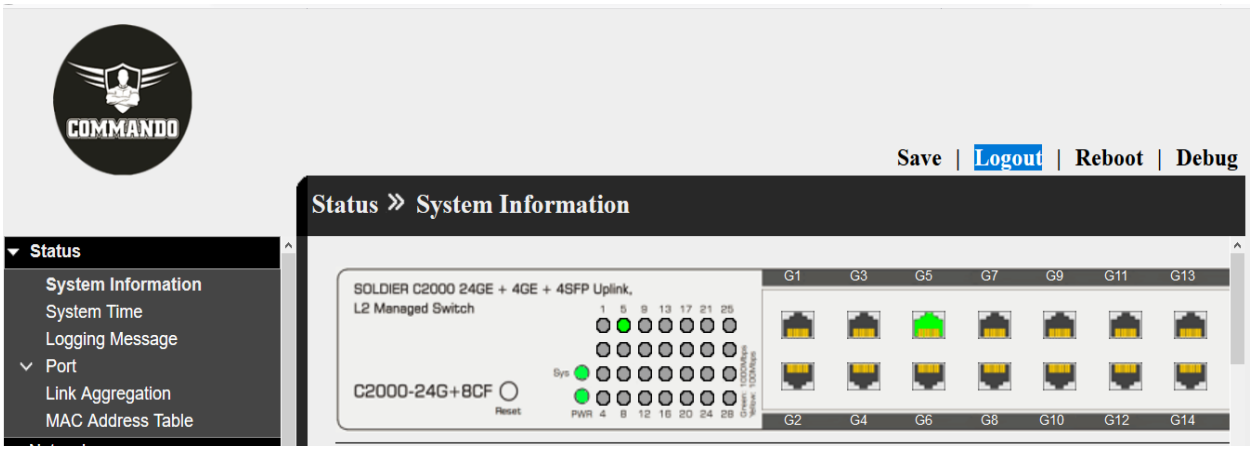


Fig 1.3.3 Logout button on WEBUI

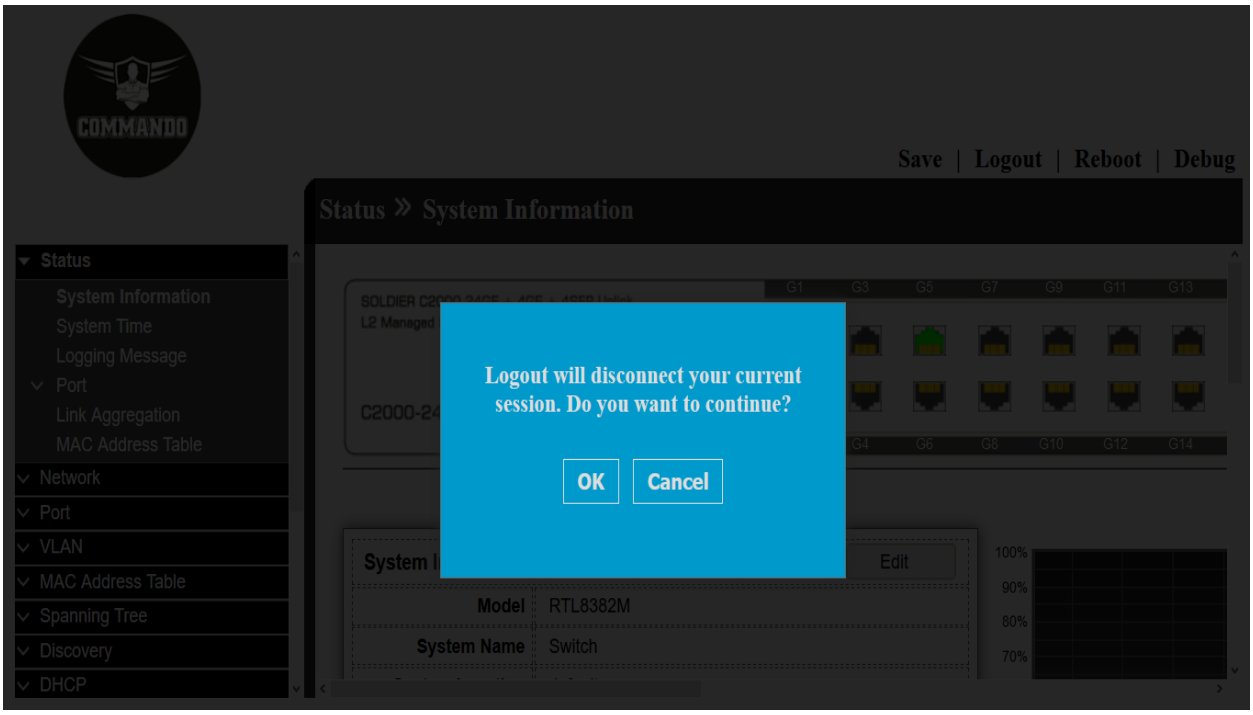


Fig 1.3.4 Applying Logout button on WEBUI

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.

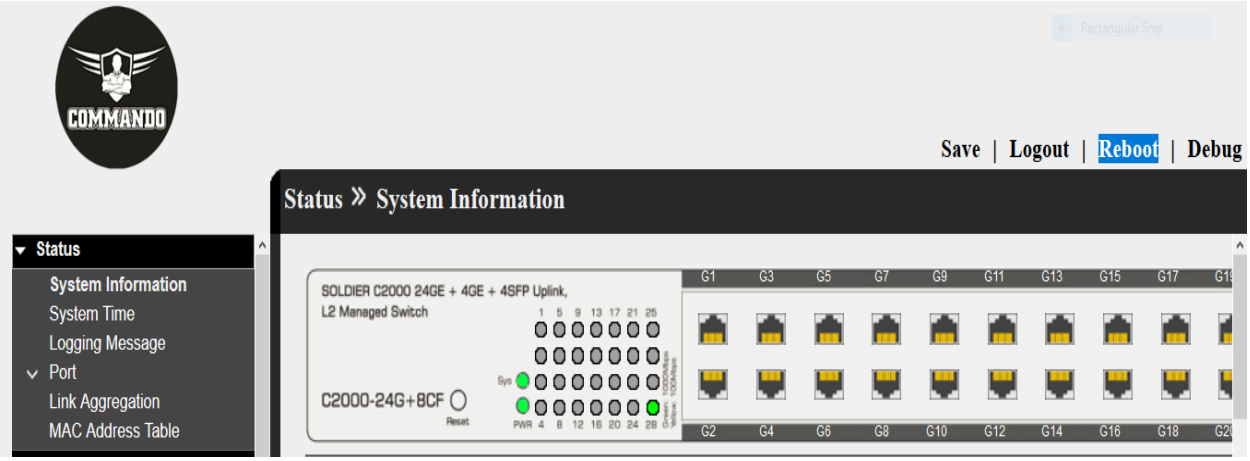


Fig 1.3.5 Reboot button on WEBUI

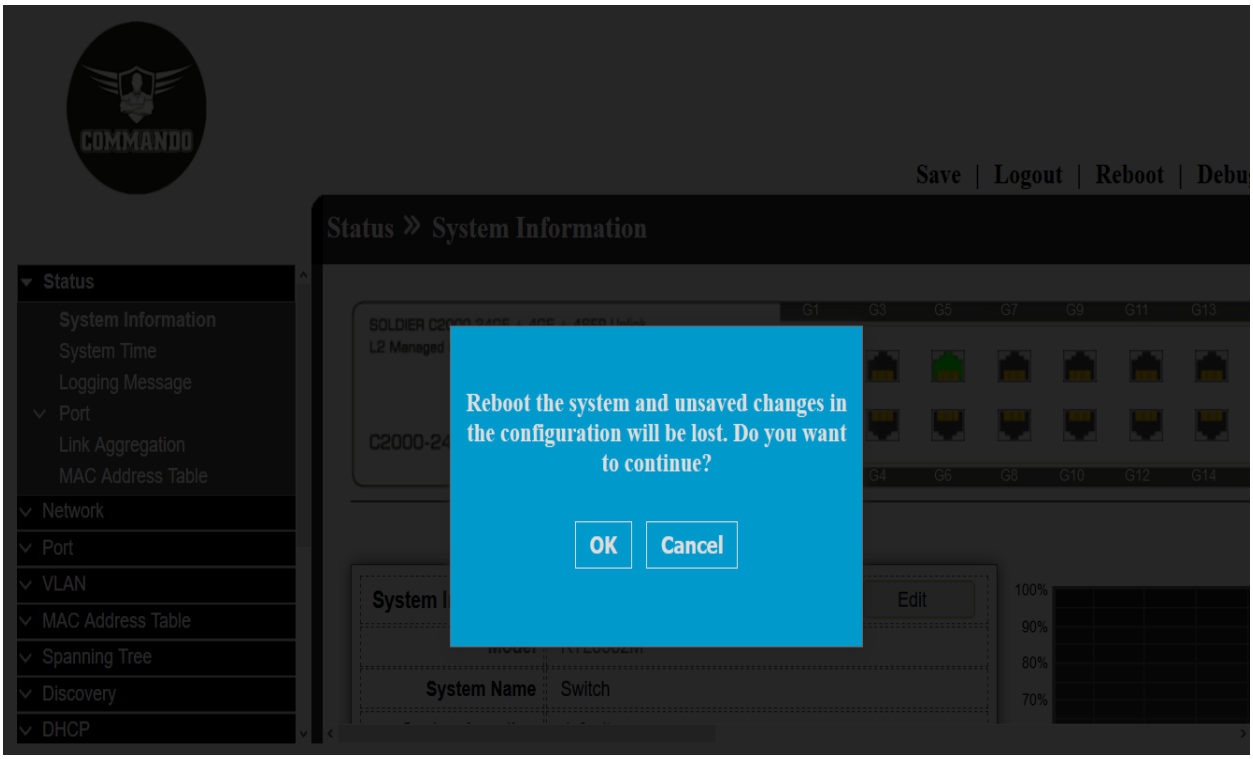


Fig 1.3.6 Applying Reboot button on WEBUI

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.

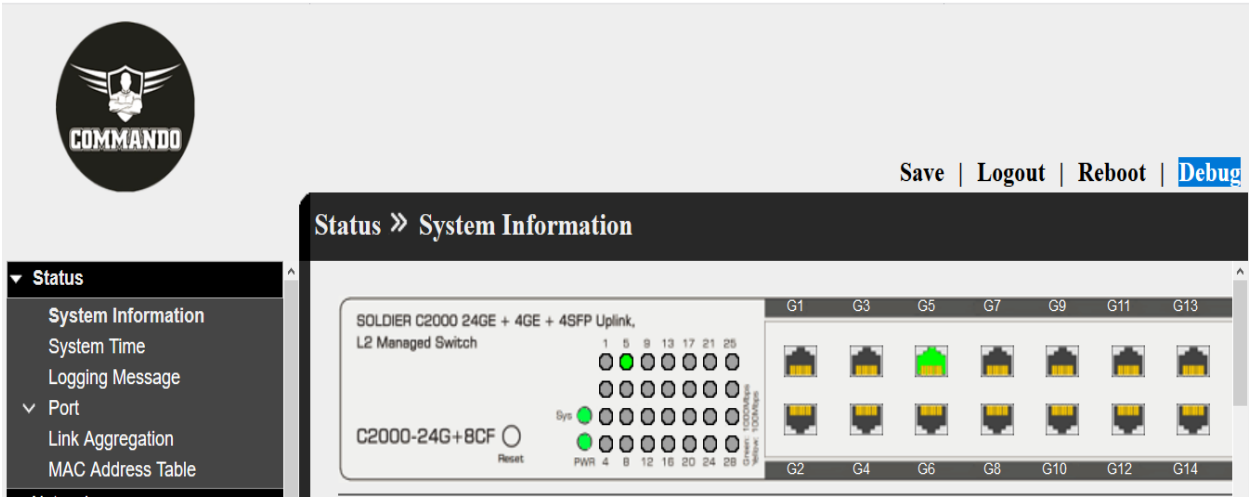


Fig 1.3.6 Debug message button on WEBUI

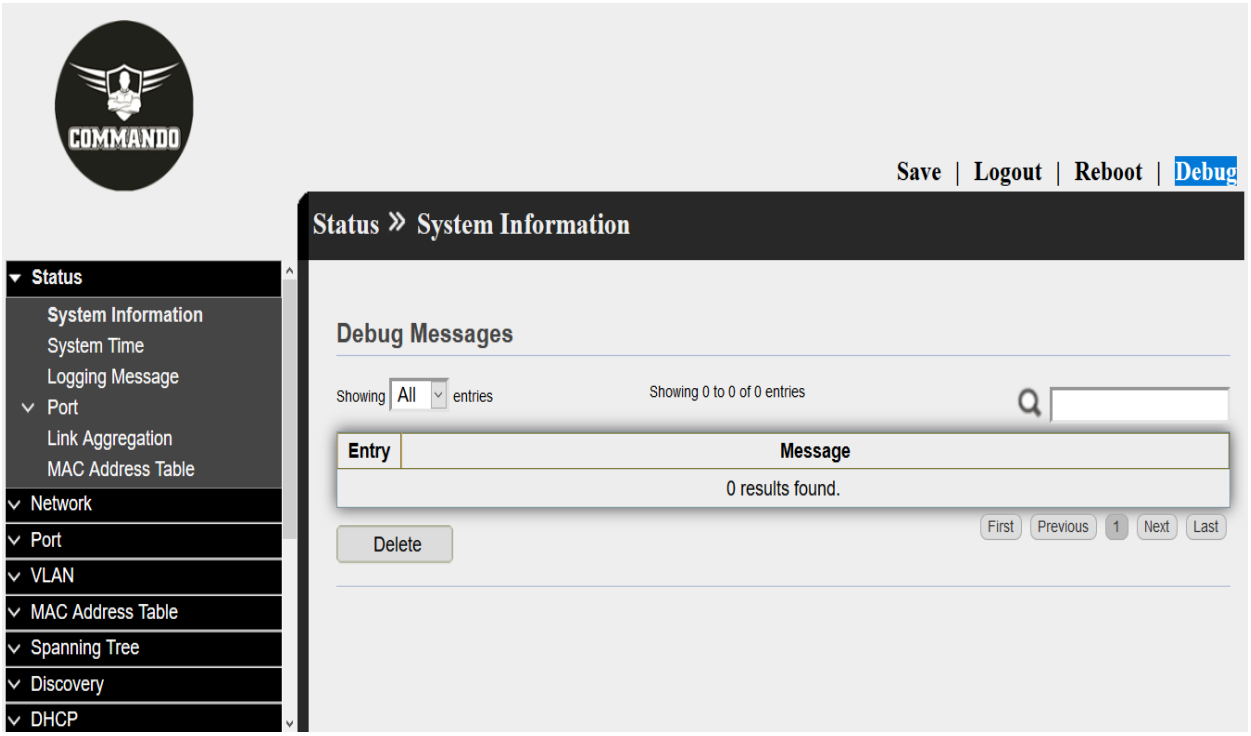


Fig 1.3.7 View Debug message on WEBUI

Chapter 2 COMMANDO C2000 SoilderOS 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. It covers also 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).

Loggin 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 C2000 SoilderOS. 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.

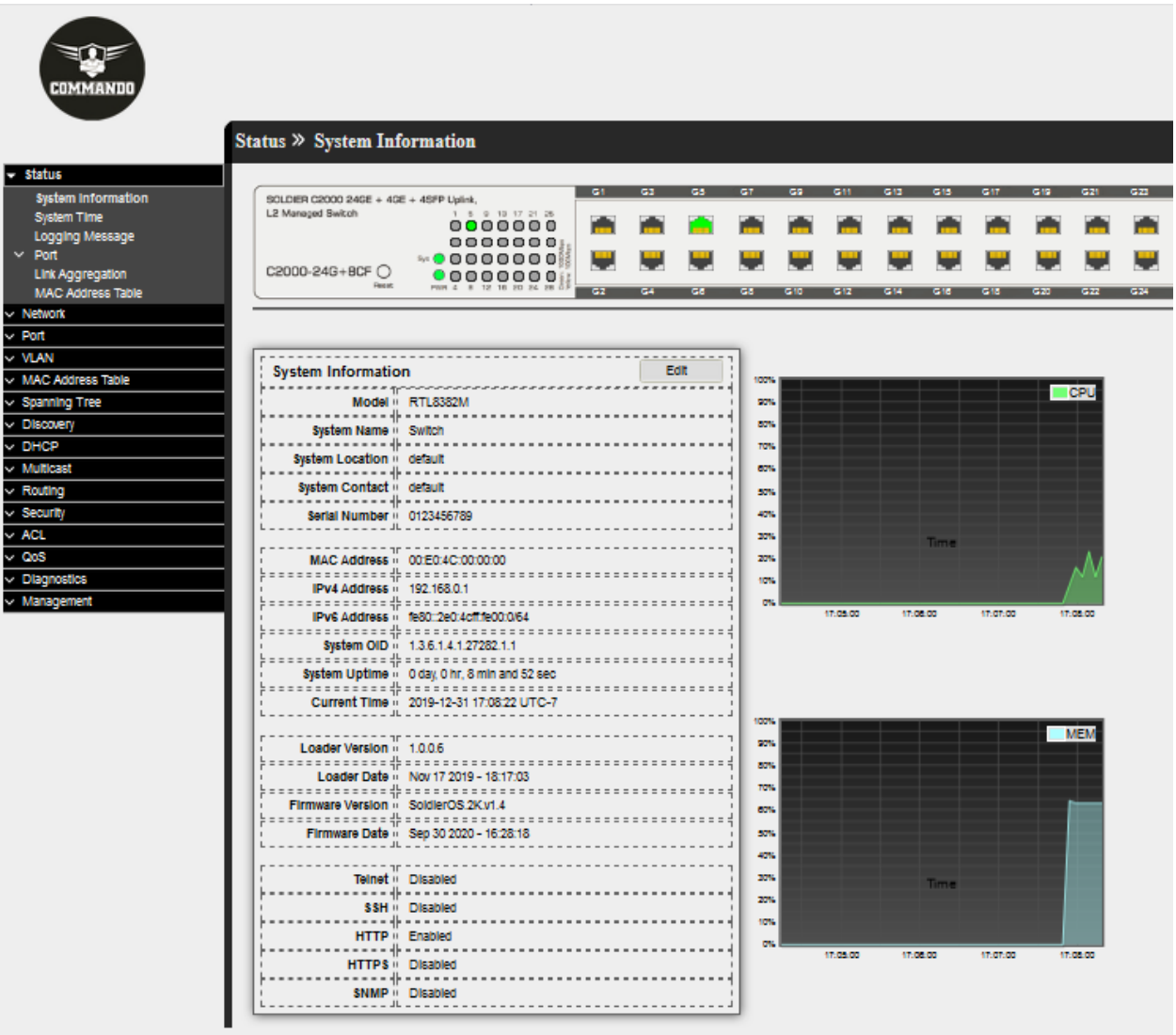


Fig 2.1 System information Web page

2.1.1 Changing the System Name, Location and Contact

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

Status>>System Information>>Edit button

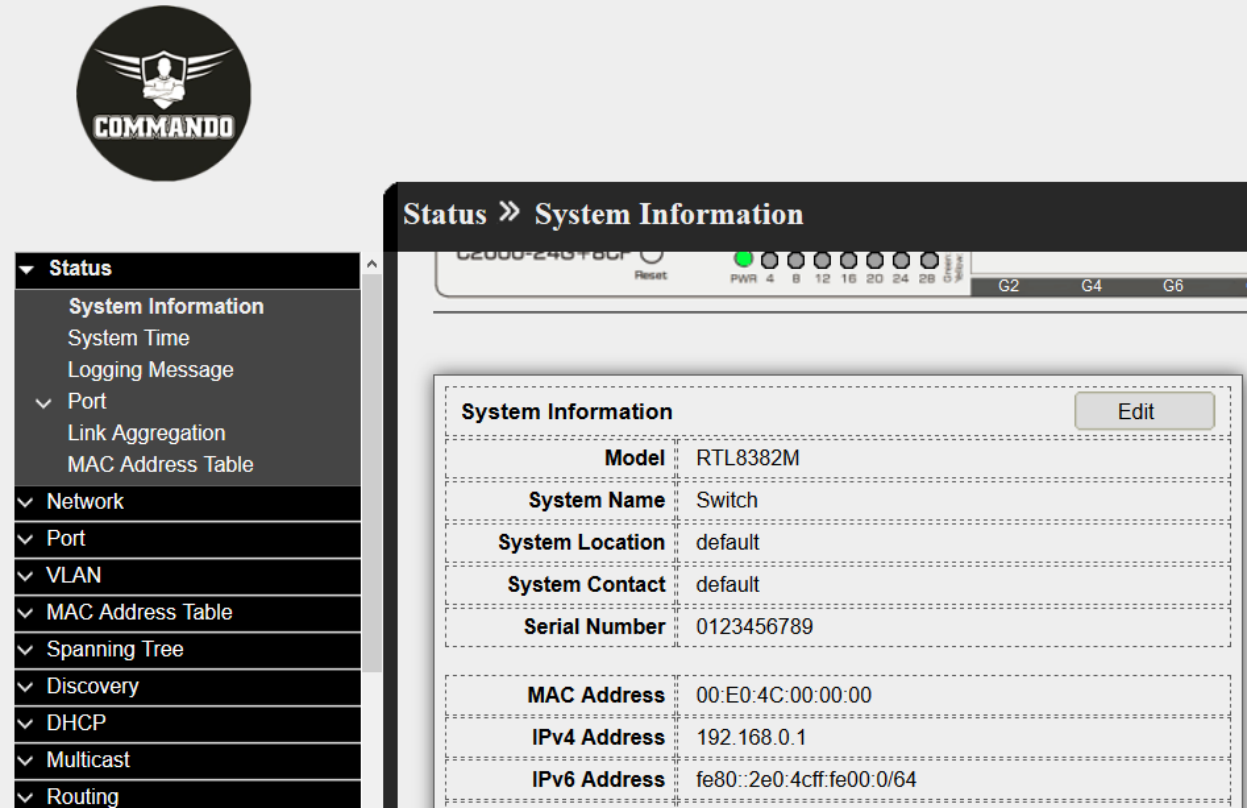


Fig 2.1.1 Changing the System Name,System Location and System Contact

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

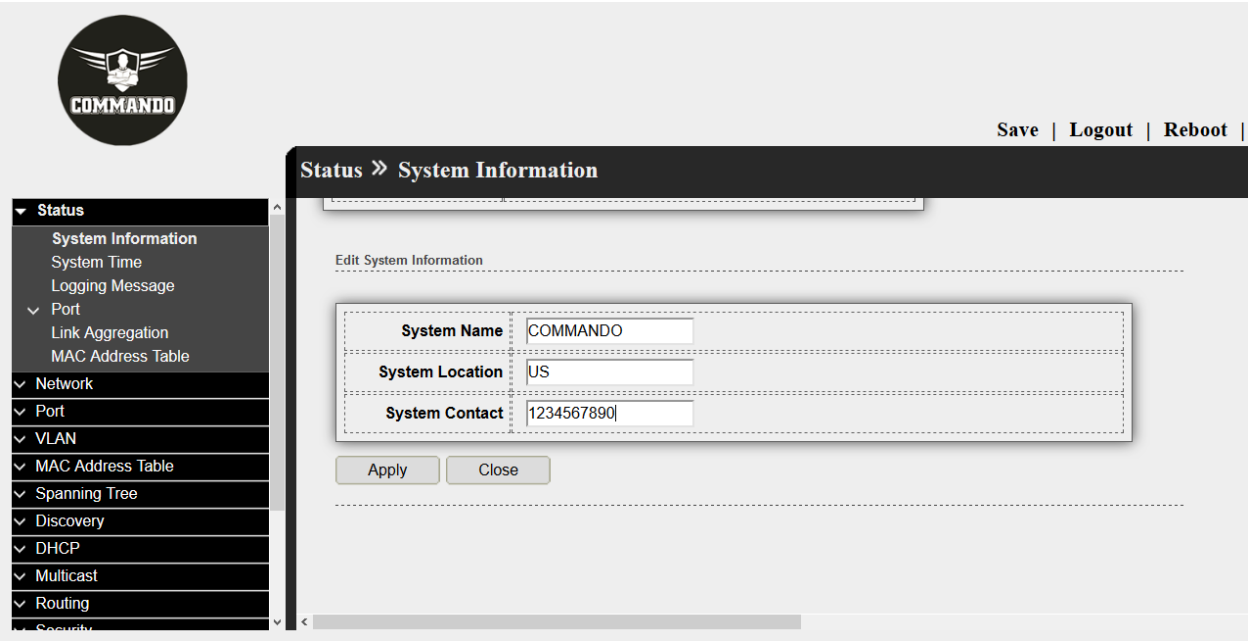


Fig 2.1.2 Changing System Name, System Location and System Contact

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.

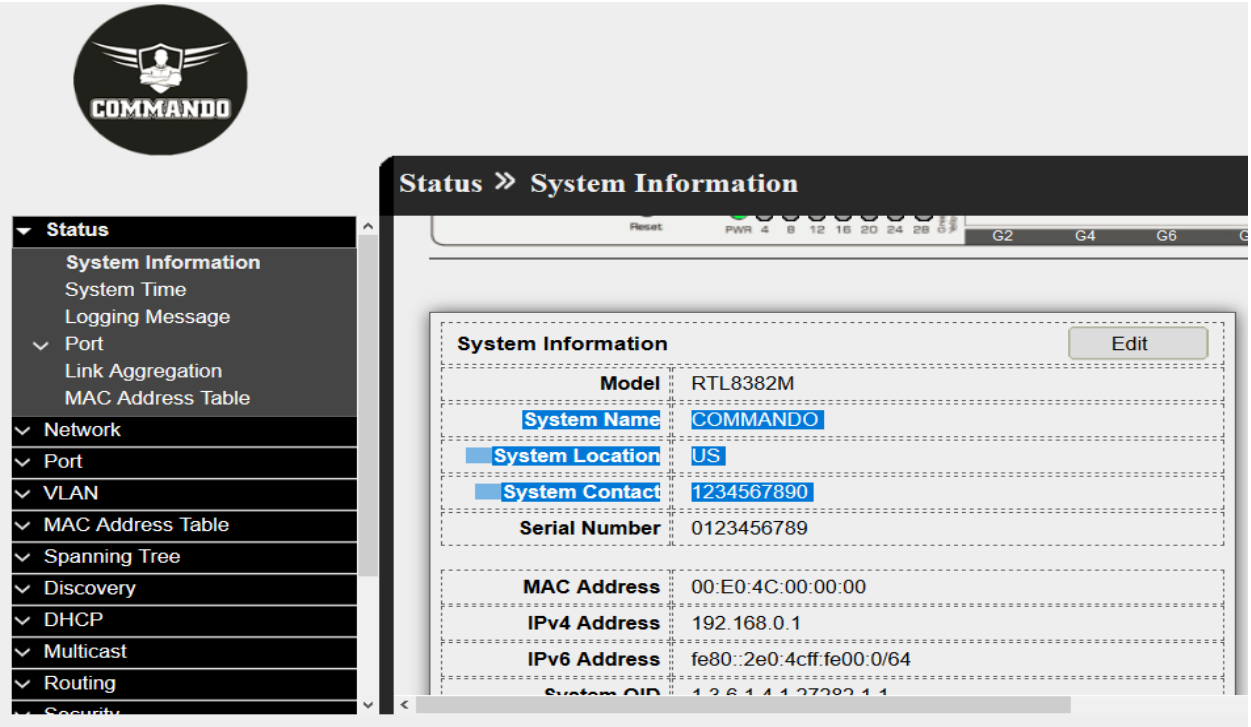


Fig 2.1.3 Viewing Changed System Name, System Location and System Contact

2.2 System Time

Synchronized system clocks 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 of 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 WEBUI. 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 WEBUI, 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 sets 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

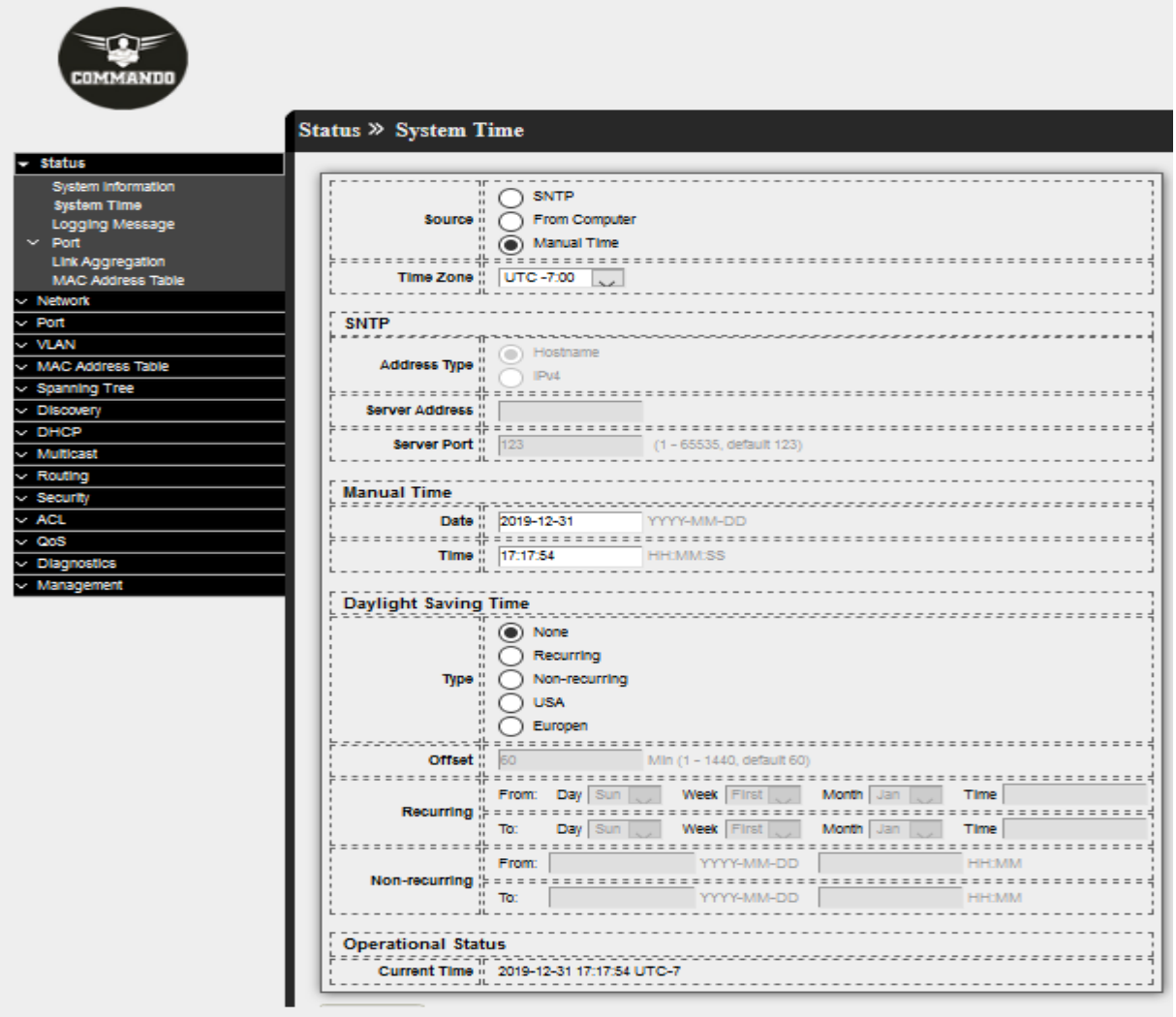


Fig 2.2.1 Default System Time configuration page

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 GMT.The main purpose of Daylight Saving Time (called "Summer Time" 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.

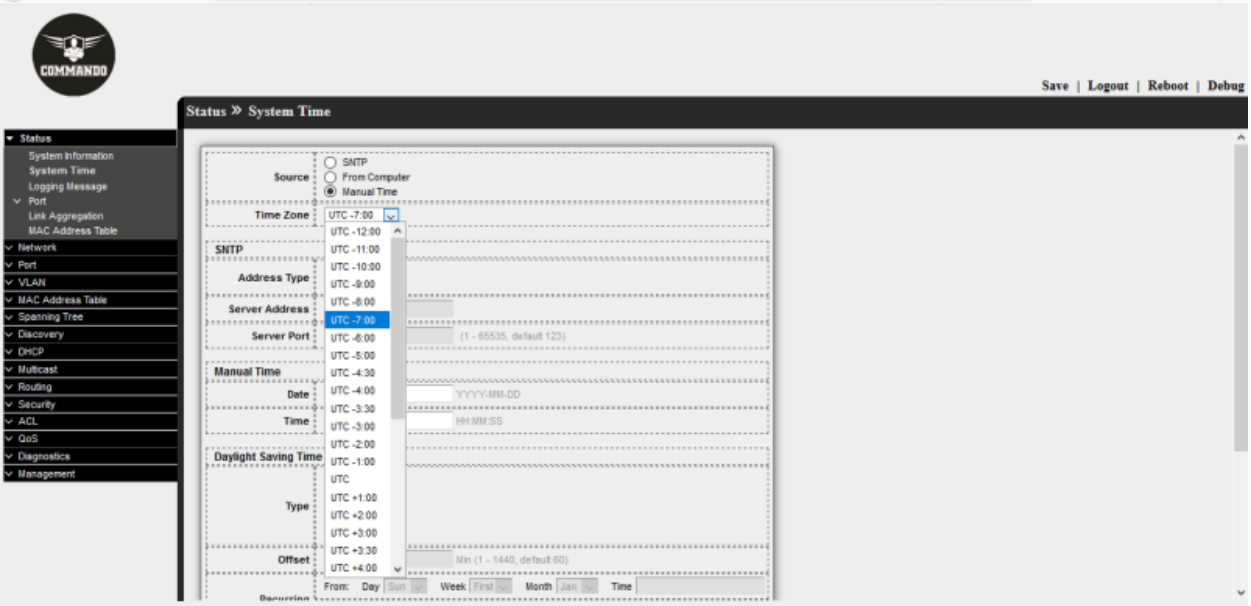


Fig 2.4.2 Timezone configuration page

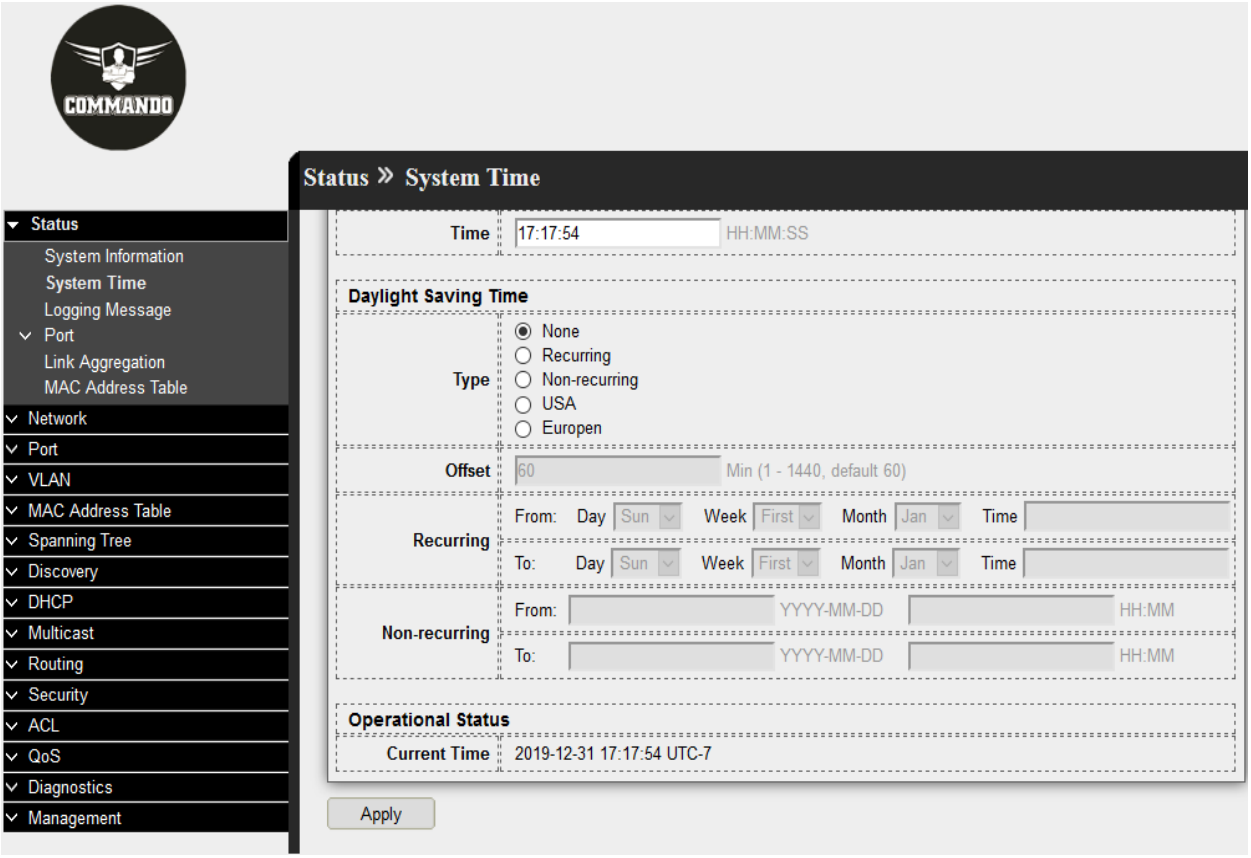


Fig 2.4.3 Daylight saving time configuration page

From Computer

This is the best way to configure the time setting in switch. C2000 Series Switches will take and sync with loggin 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.

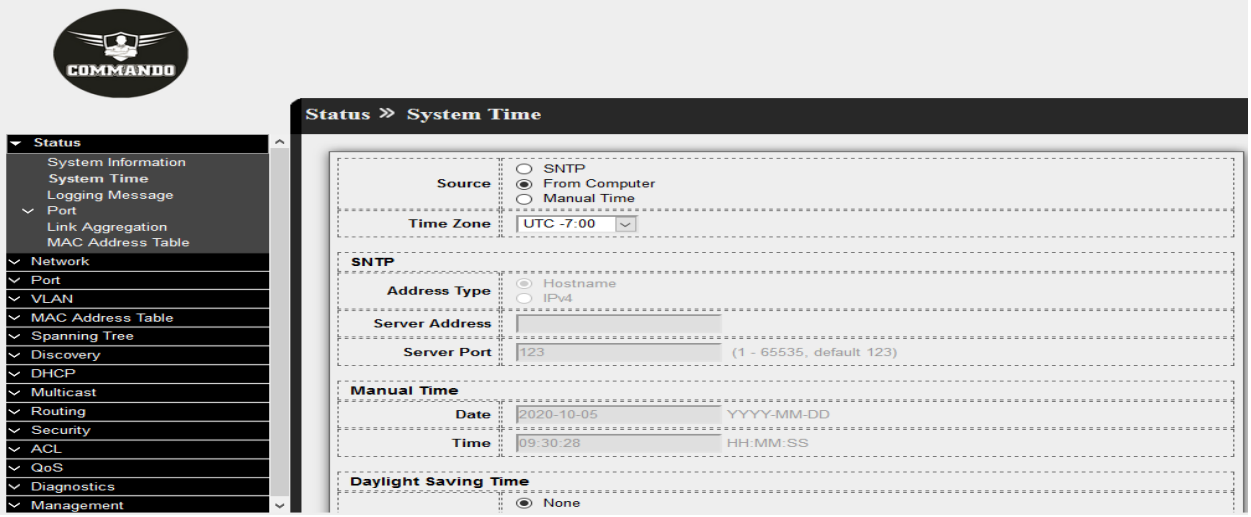


Fig 2.4.4 Time configuration from connected computer page

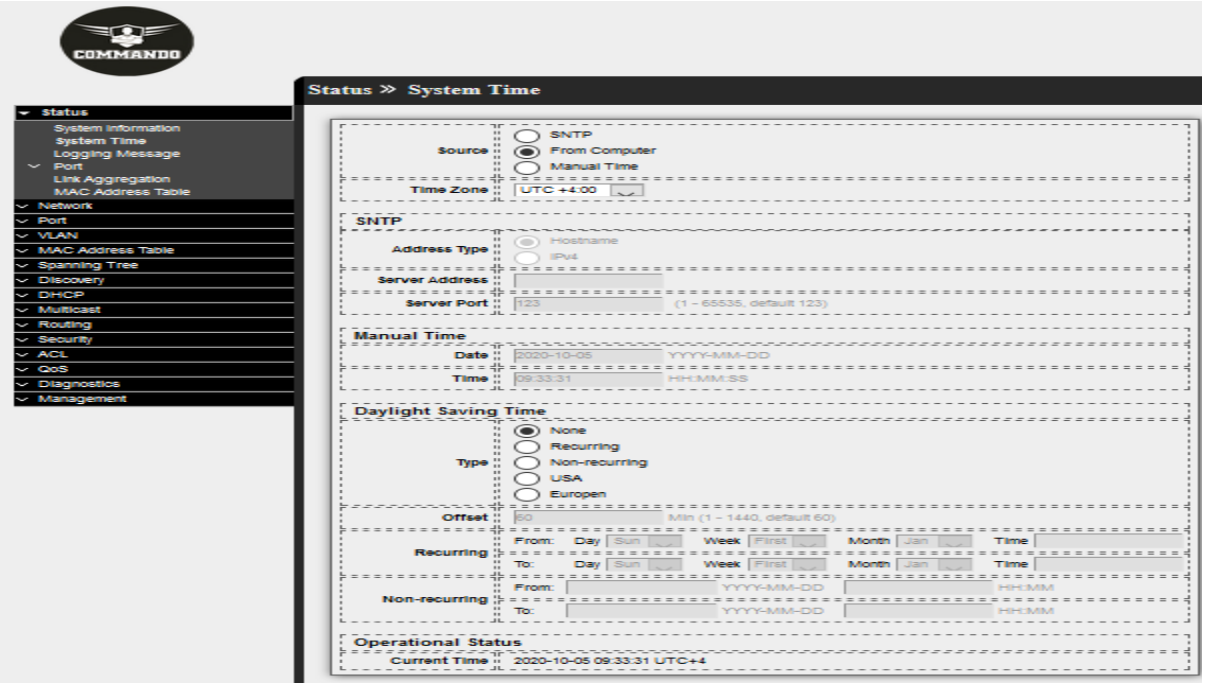


Fig 2.4.5 Time configuration from connected computer page

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.

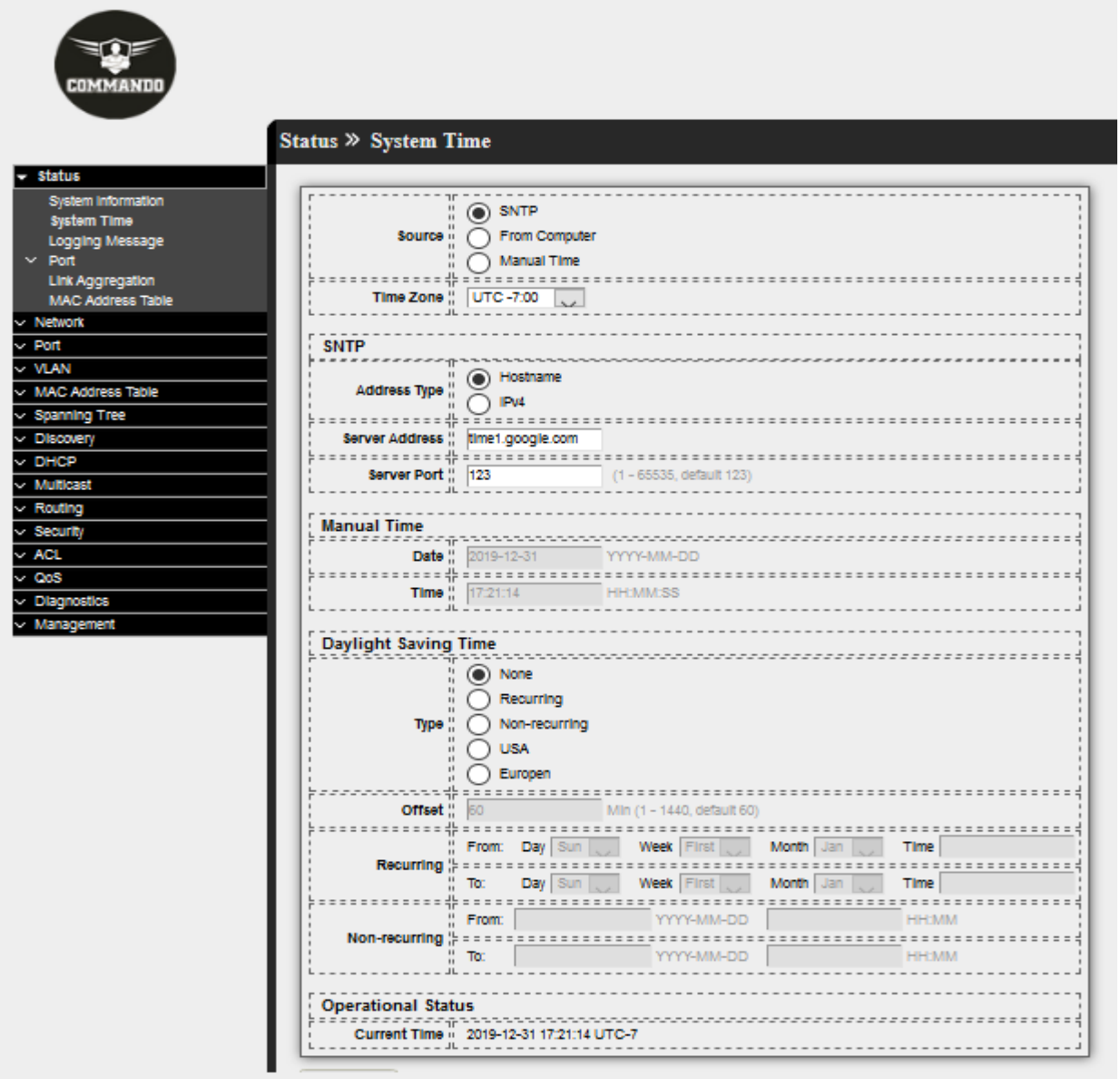


Fig 2.4.6 SNTP configuration page

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

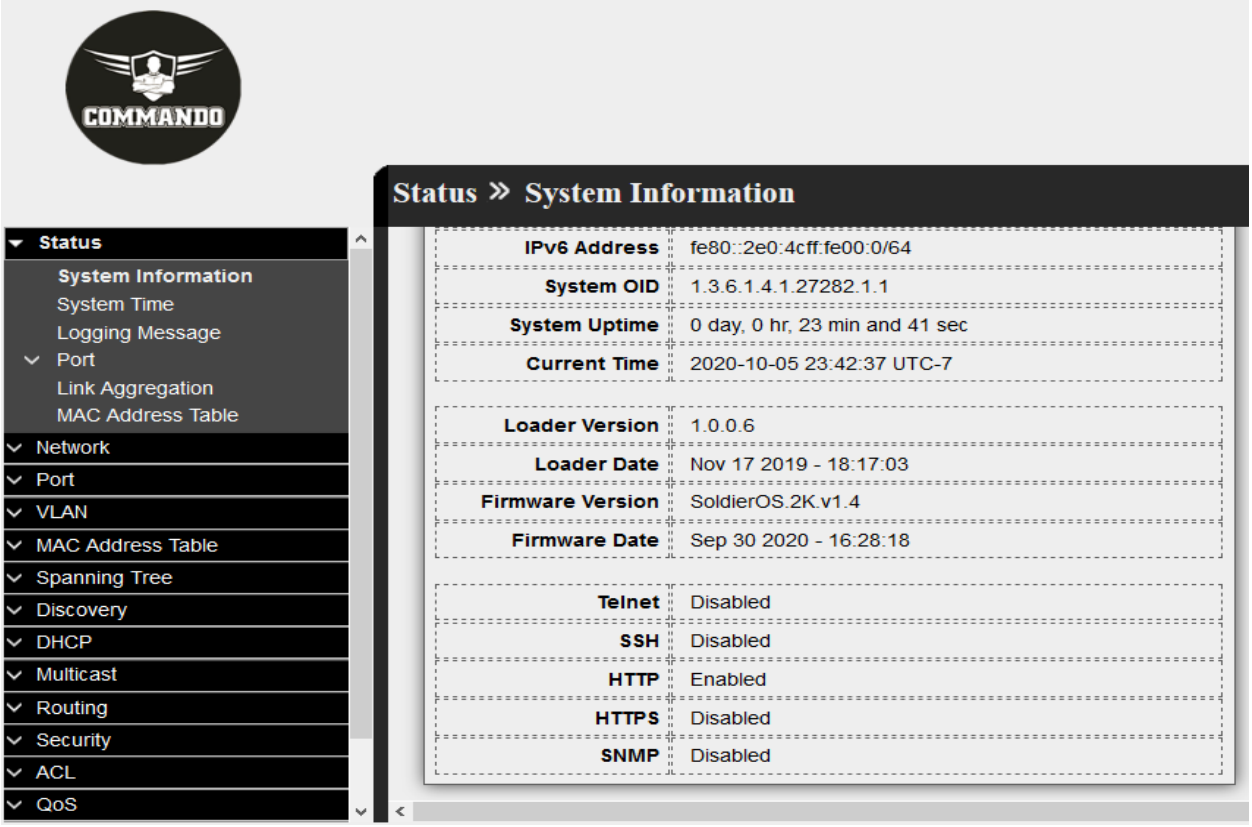


Fig 2.4.5 System Information page displaying current time.

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.

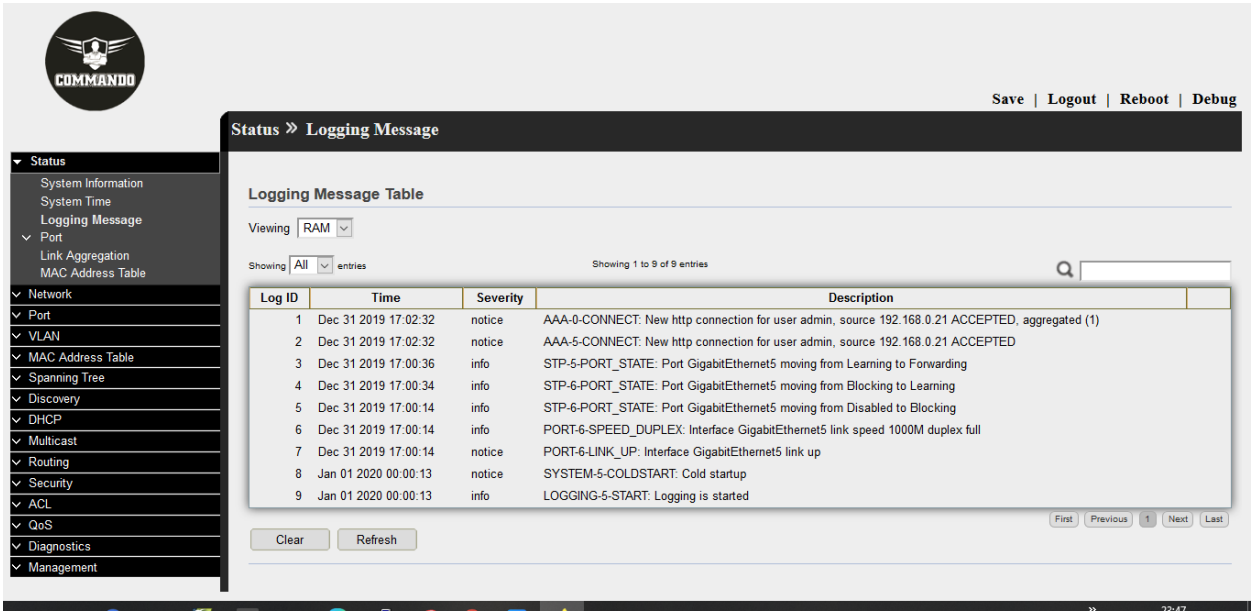


Fig 2.3.1 Logging Message Table of RAM

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

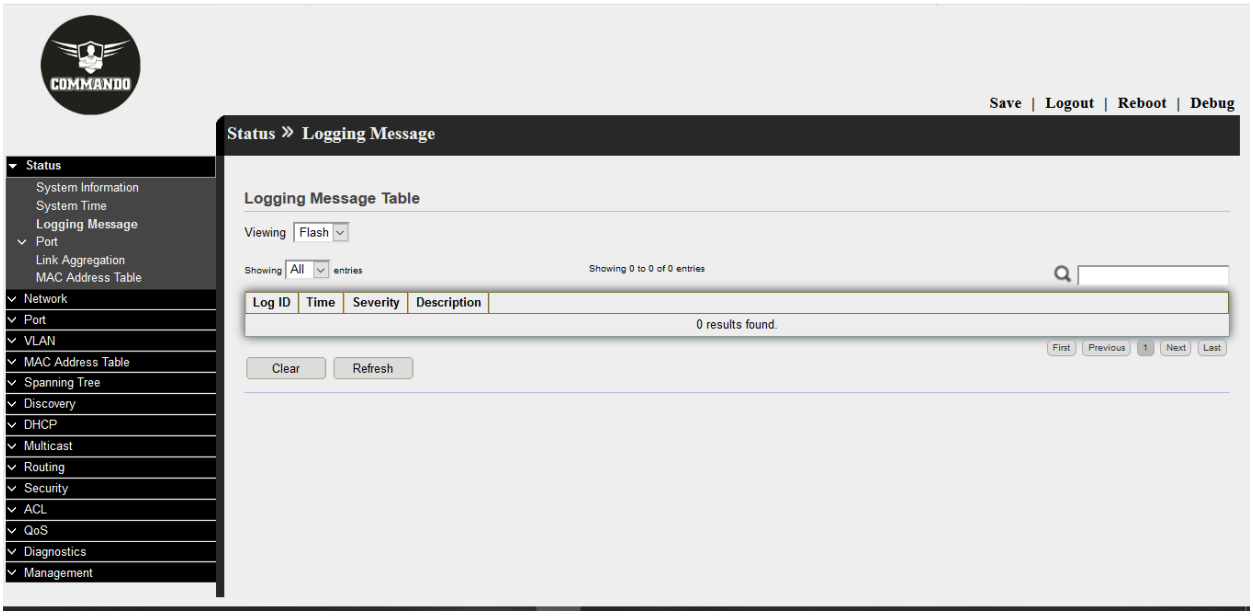


Fig 2.3.2 Logging Message Table of Flash

The number of entries to be shown for logging message table is also selectable by default All entries are shown

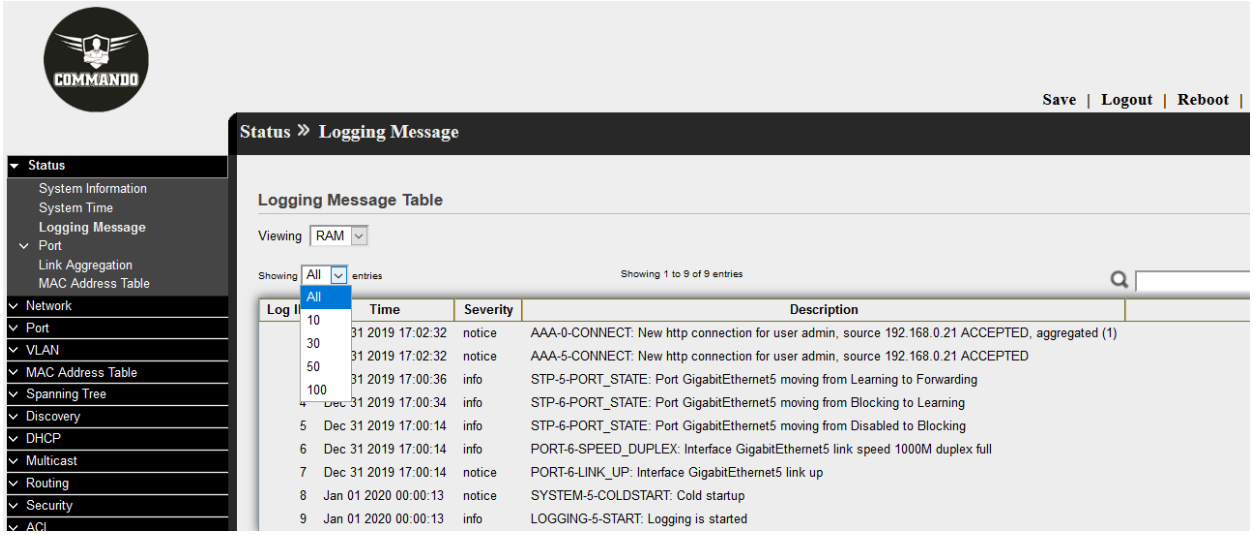


Fig 2.3.3 Logging Message Table of Entries selection

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 GigaEthernet 1 is selected and refresh rate is 10 seconds .The Port configuration page displays port summary and status information. To view perticular port status click **Status >> Port >> Statistics** and select Port.

Note:- Default selection is GE1

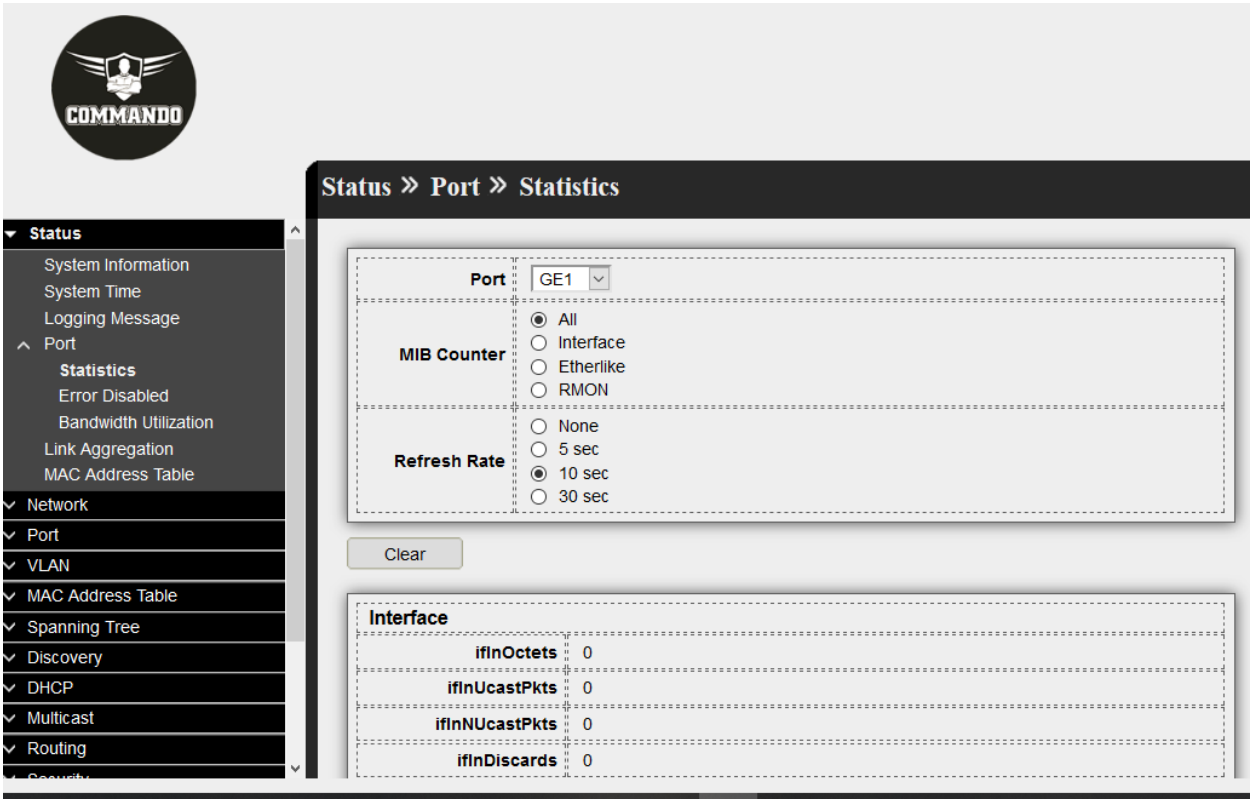


Fig 2.4.1 Port selection for MIB Counter Statistics

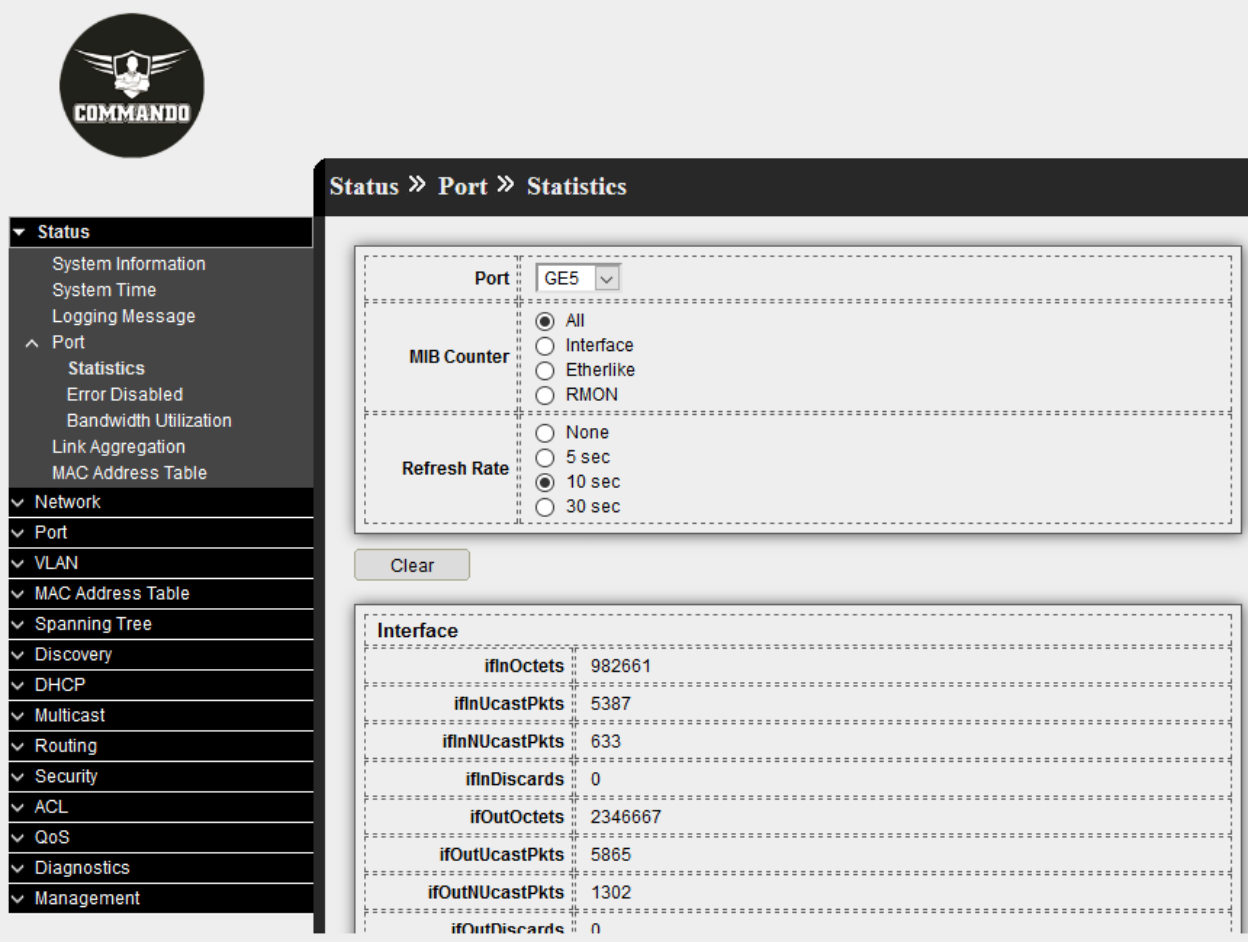


Fig 2.4.2 Giga Ethernet 5 port selection for MIB Counter Statistics

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.

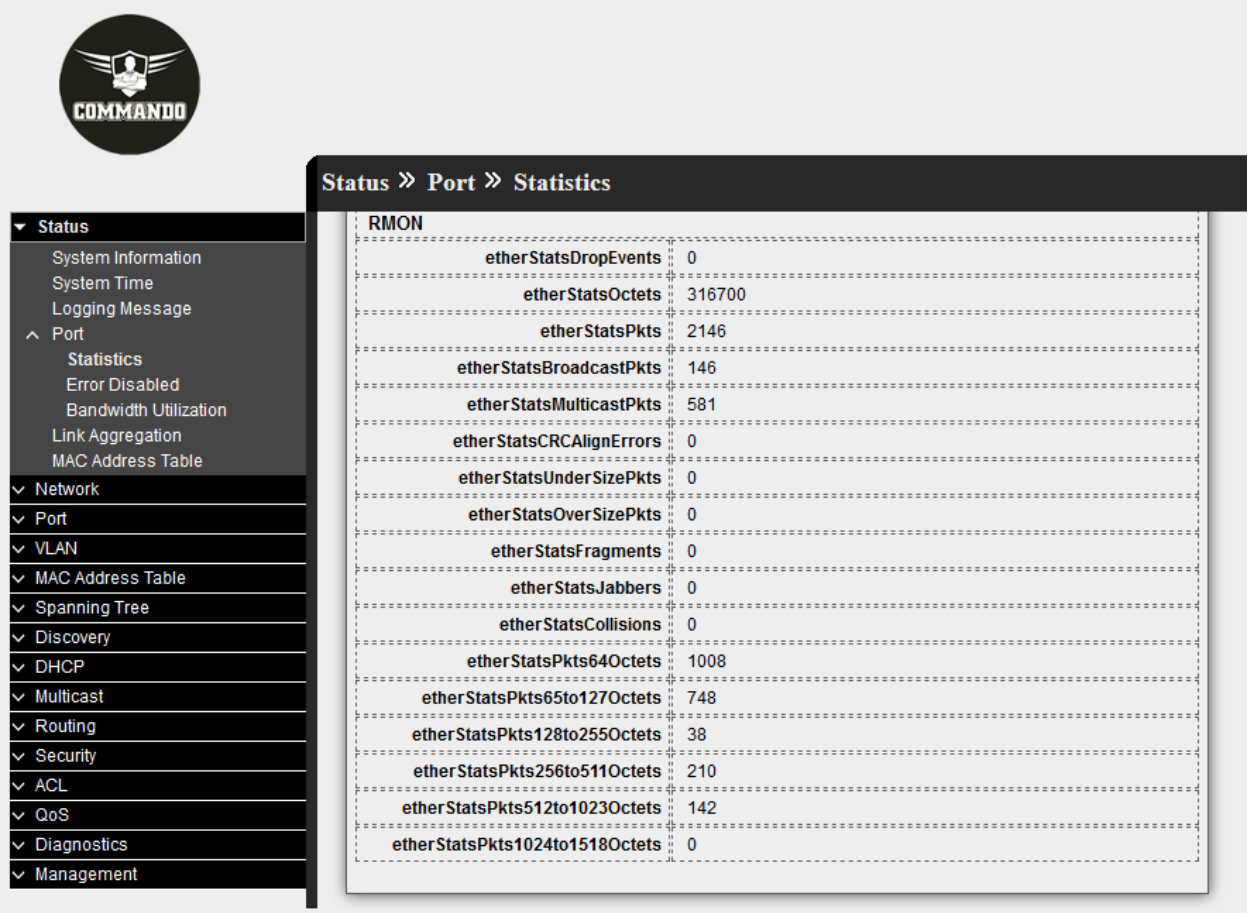


Fig 2.4.3 RMON MIB Counter Statistics

2.3.2 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 /Restict 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.**

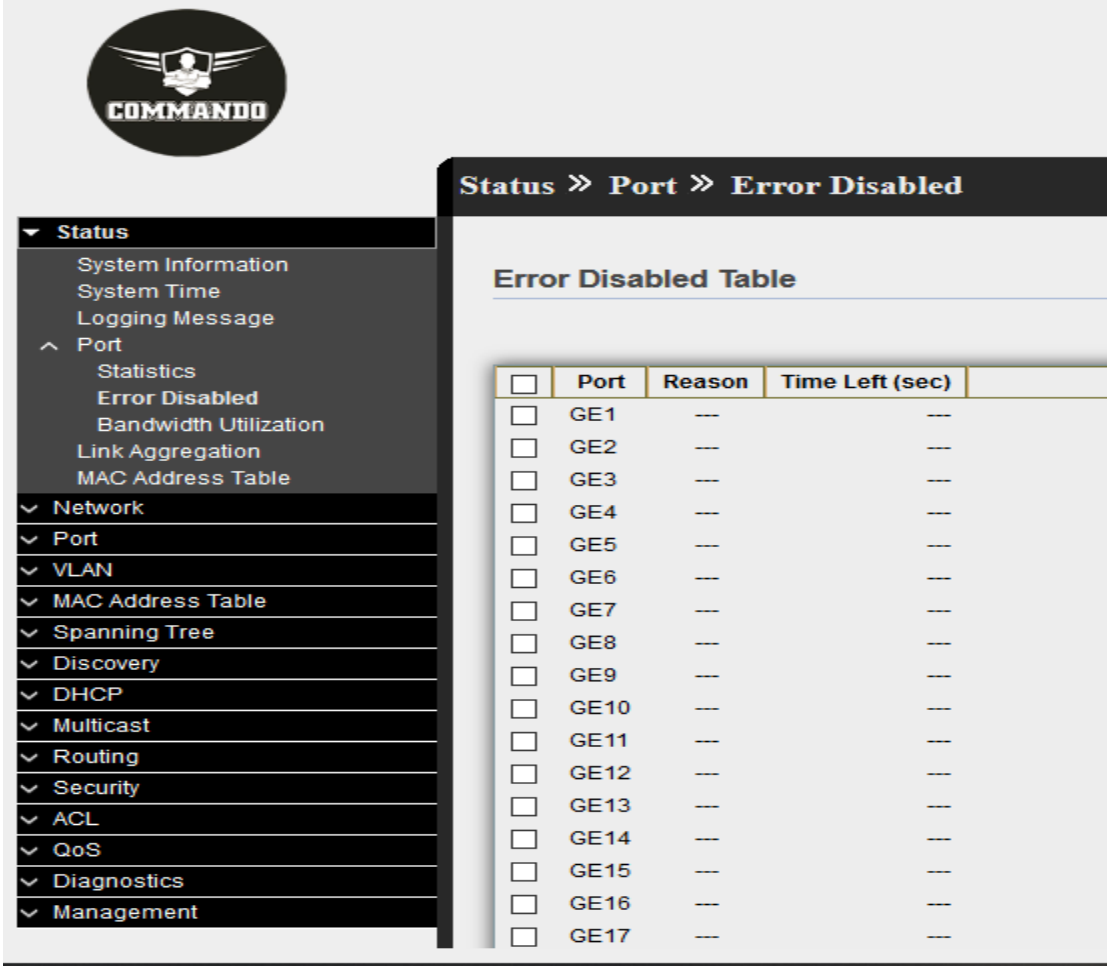


Fig 2.4.4 Default Port Error disabled Table

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 WEBUI can easily recover from error disable by selecting port and pressing recovery button.

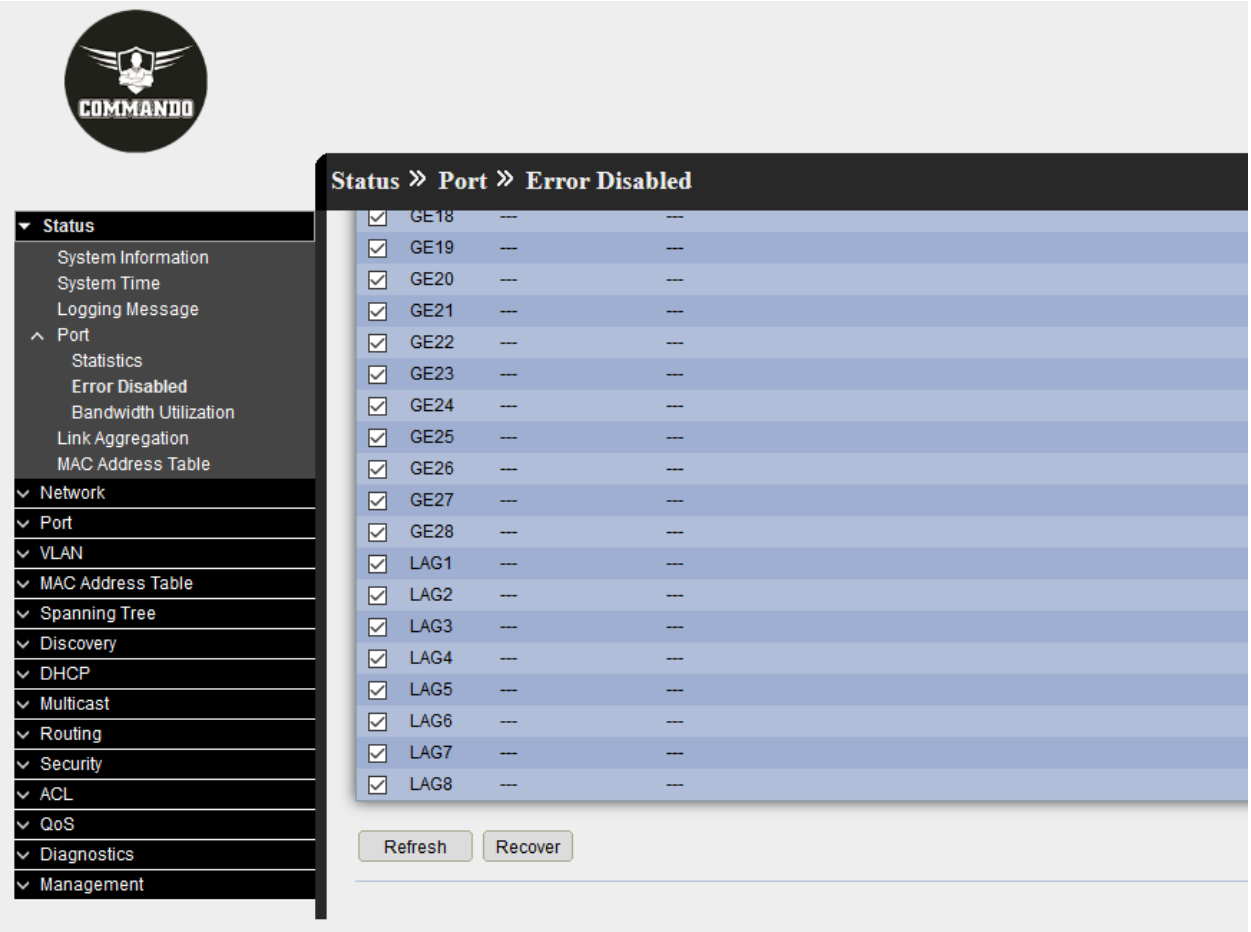


Fig 2.4.5 Recovering form error disabled state.

2.3.3 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.**

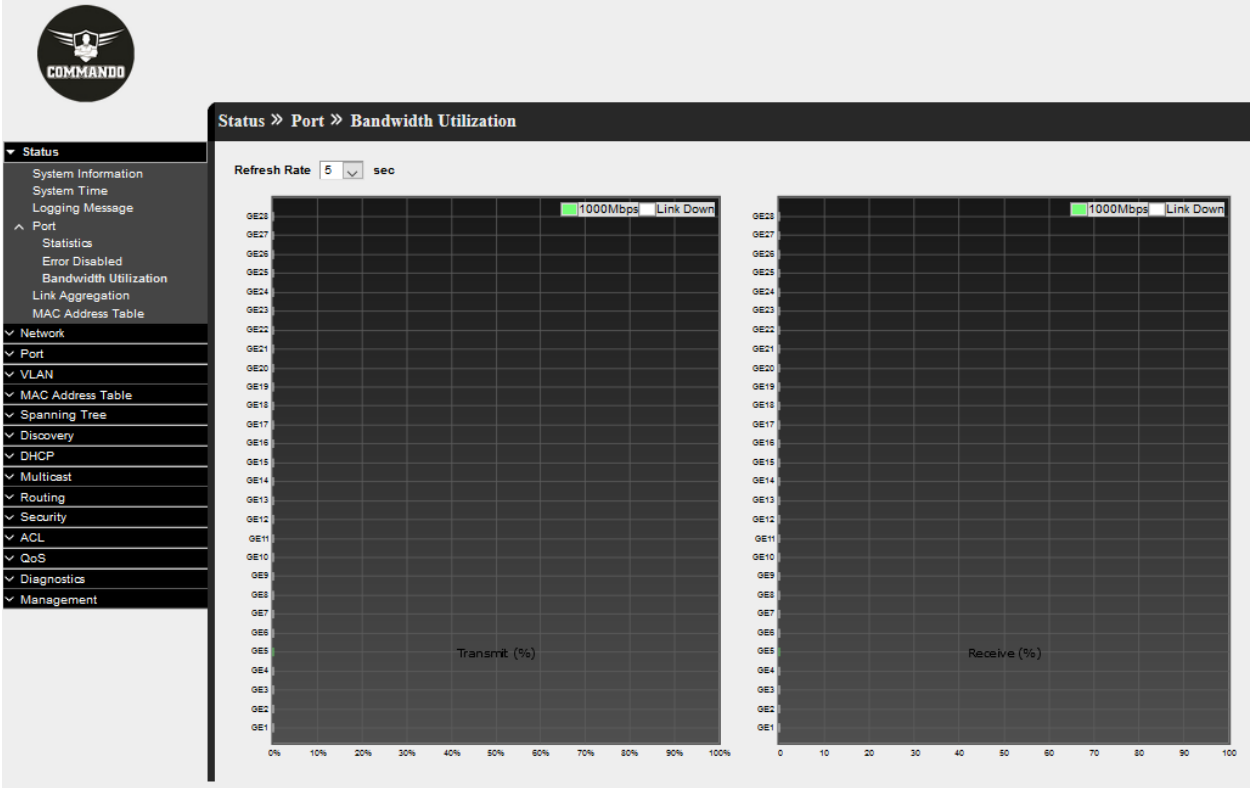


Fig 2.4.6 Bandwidth utilization and refresh rate

2.5 Link Aggregation

Link aggregation is a way of bundling a bunch of individual Ethernet/ Fast Ethernet/ Gigabitethernet 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.

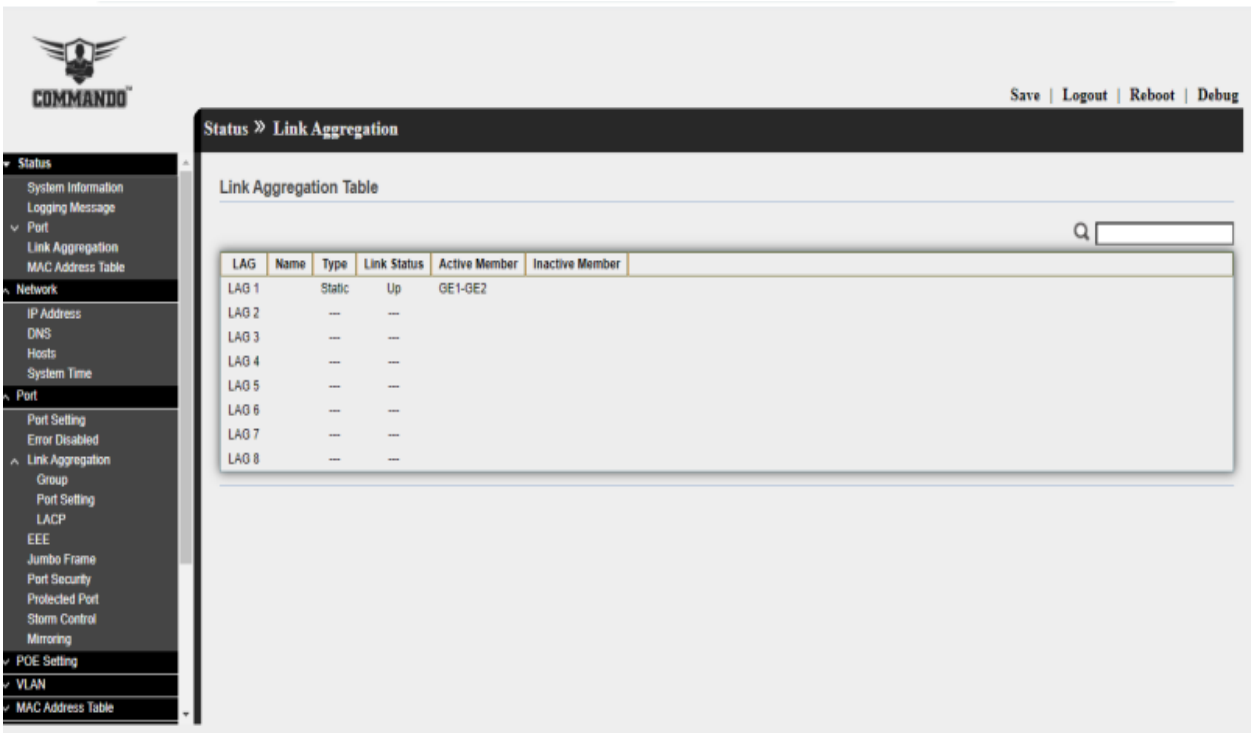


Fig 2.5.1 Link Aggregation table information.

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.**

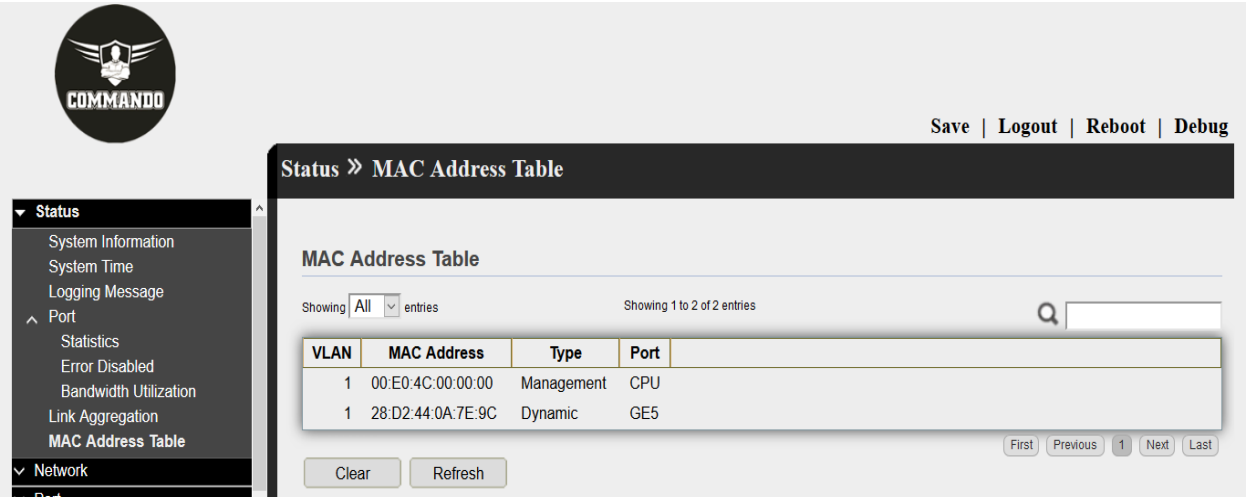


Fig 2.6.1 Mac Address Table information

Chapter 3 Network

IP Address :--> The management IP address in the context of a switch is the address that the switch itself (192.168.0.1 By default) can be reached at via CLI, telnet, SSH, WEBUI (or via monitoring requests such as SNMP traffic). You can assign the management IP address to an arbitrary value that works for your network, as long as the switch would be reachable at that address.

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 through the use of 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 IP Address

This page allows to configure and view very important information about IPv4 & IPv6 address, Subnet Mask & Default Gateway. When we try to use Console, TELNET, SSH, HTTP, HTTPS, SNMP to connect to the Switch, we need to use IP address **192.168.0.1** by default to access Switch.

How to change the Access IP address 192.168.0.1 of Switch?

Following page allows you to edit the IP address, Netmask, Gateway and DNS server of the switch. To configure and view the IP Address menu, navigate to **Network >> IP Address** and change the IP address as well as gateway (Optional) as per your choice.

Note:- 1) If all Switch Access IP (Management IP) in network not changed from default i.e.192.168.0.1 having more than one C2000 switch in same LAN. Then, It can create confusion for access in network via Console, TELNET, SSH, HTTP, HTTPS, SNMP.
2) If you are using more than one C2000 Series switches in LAN or Network then it is recommended to change the default IP address from 192.168.0.1 to desired IP address as per user requirement.

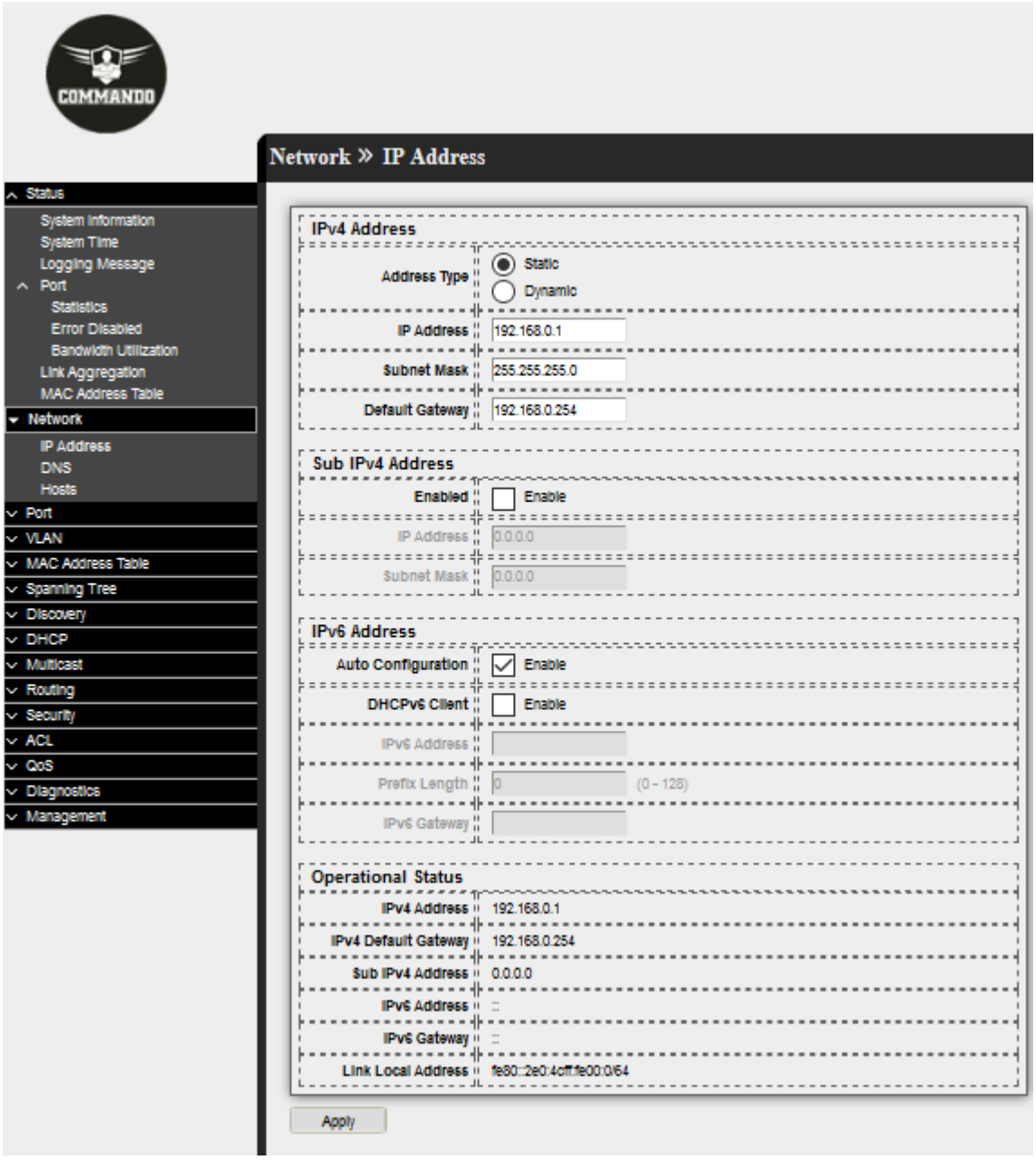


Fig 3.1.1 Default Management IP address showing 192.168.0.1 page

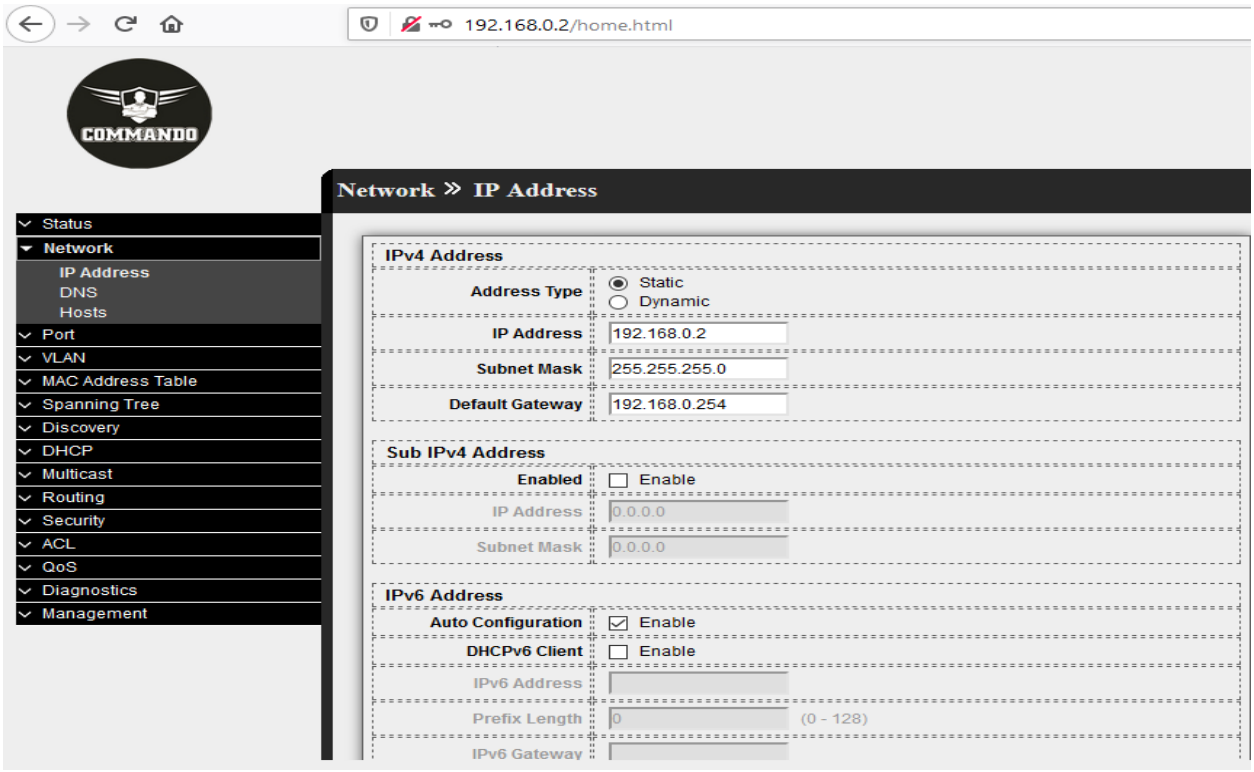


Fig 3.1.2 Changing Management IP address page

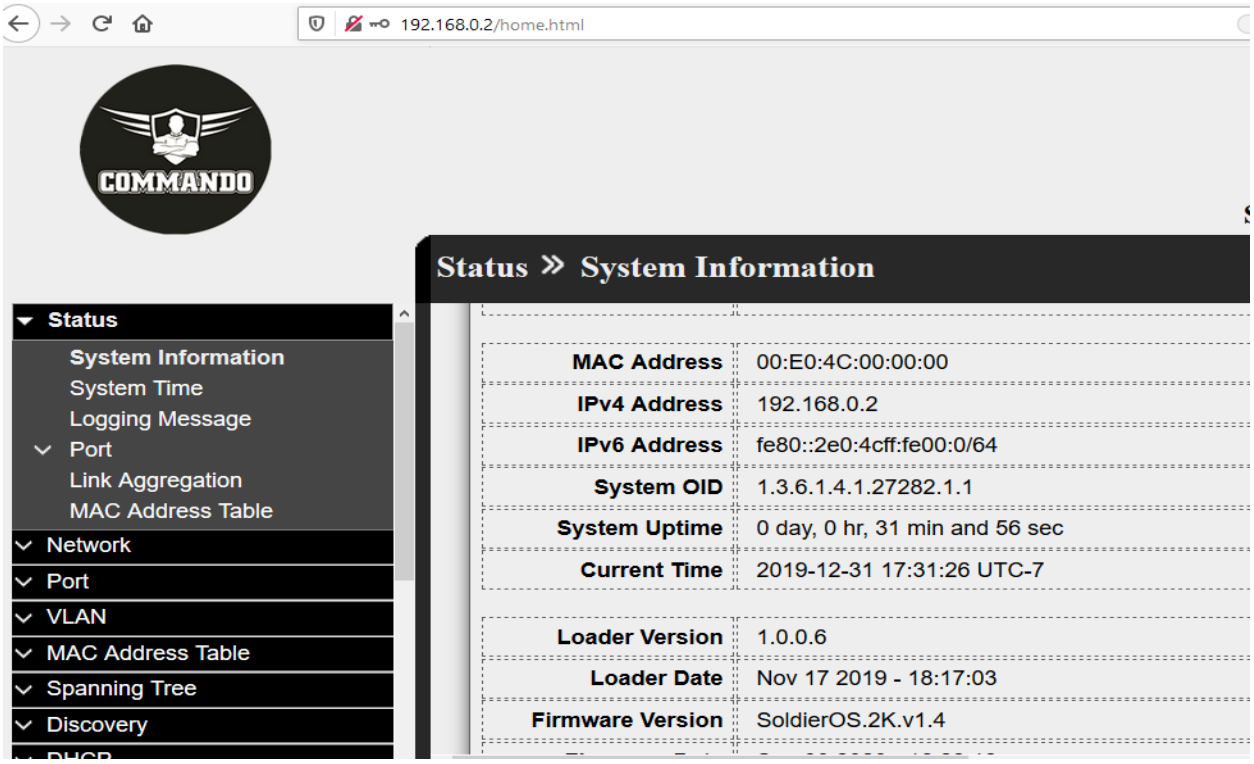


Fig 3.1.3 Verification of Changed Management IP address page

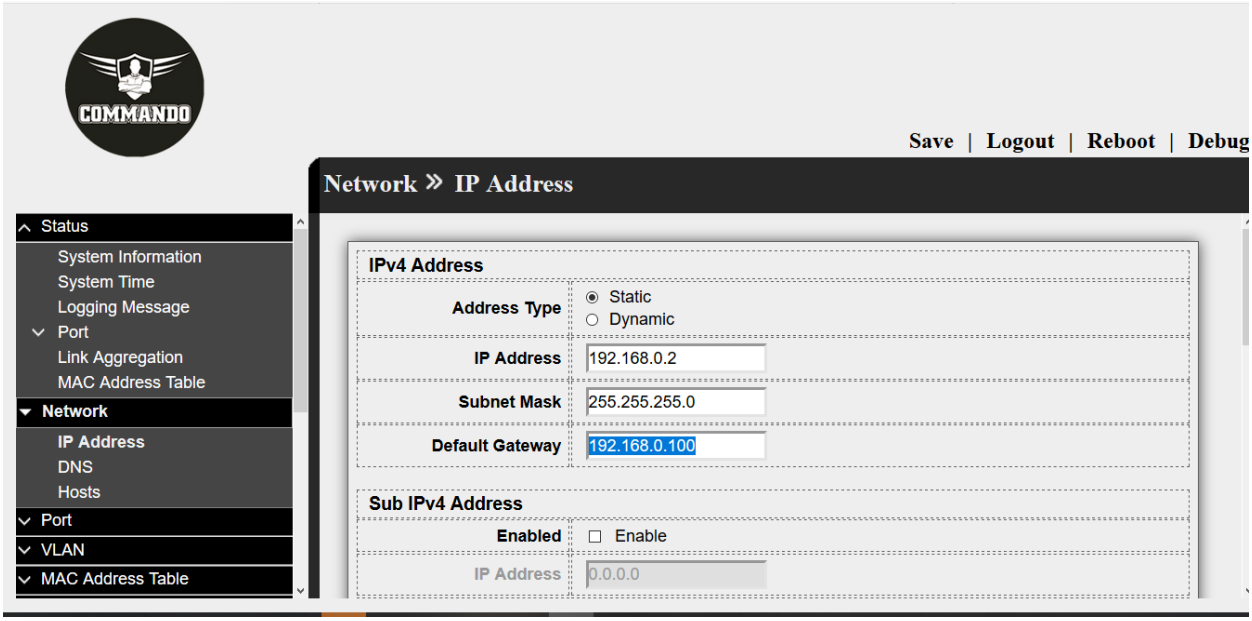


Fig 3.1.4 Setting Default Gateway page

3.2 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 through the use of one or more configured DNS servers.

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

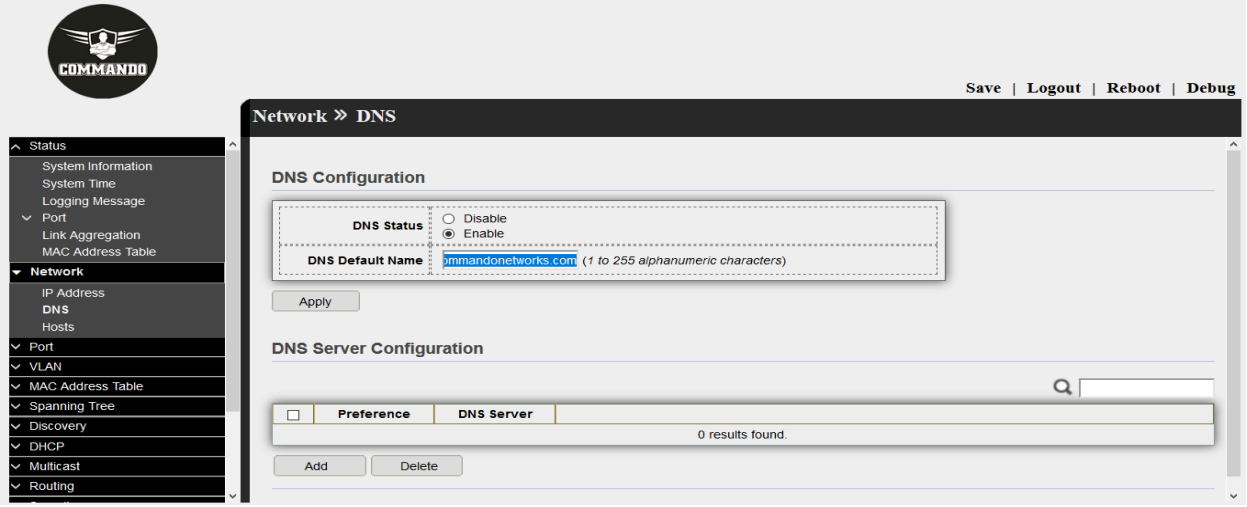


Fig 3.2.1 DNS configuration page

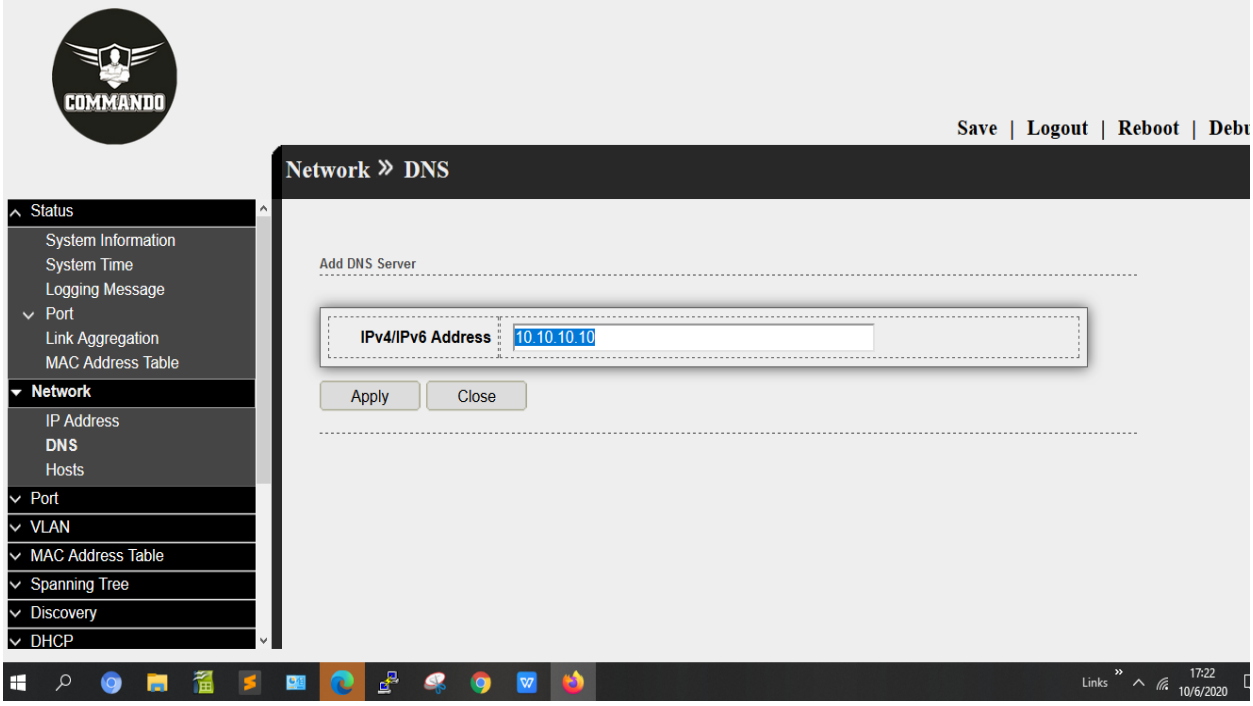


Fig 3.2.2 Add DNS Server page

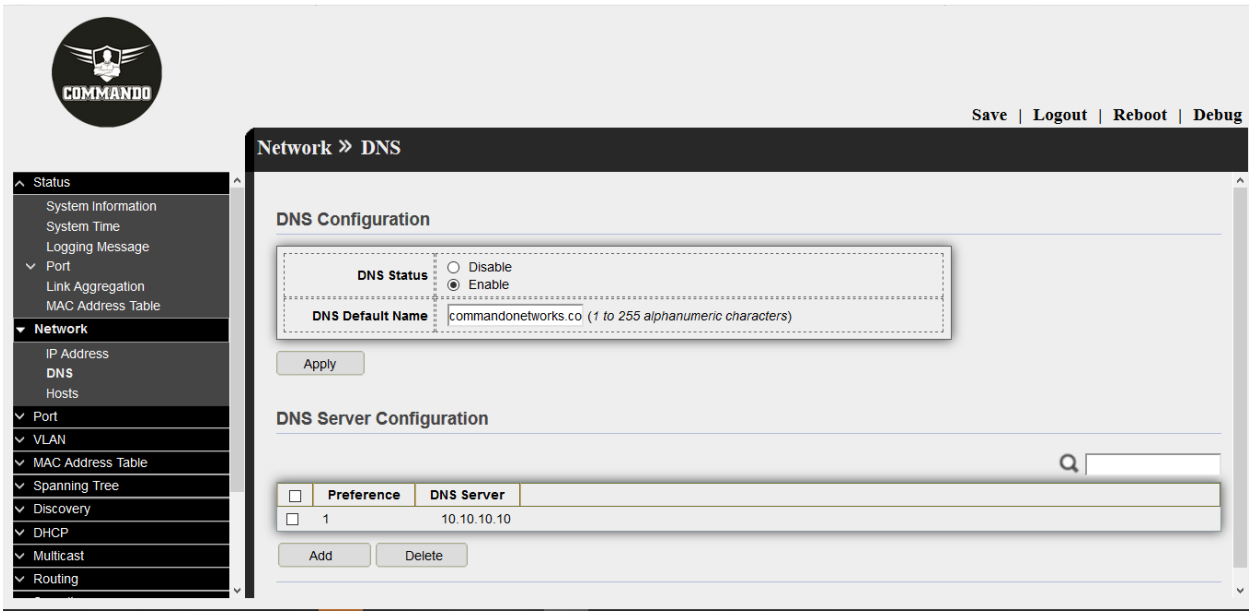


Fig 3.2.2 DNS Server configuration page

3.3 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 configuartion, click **Network >>Hosts**

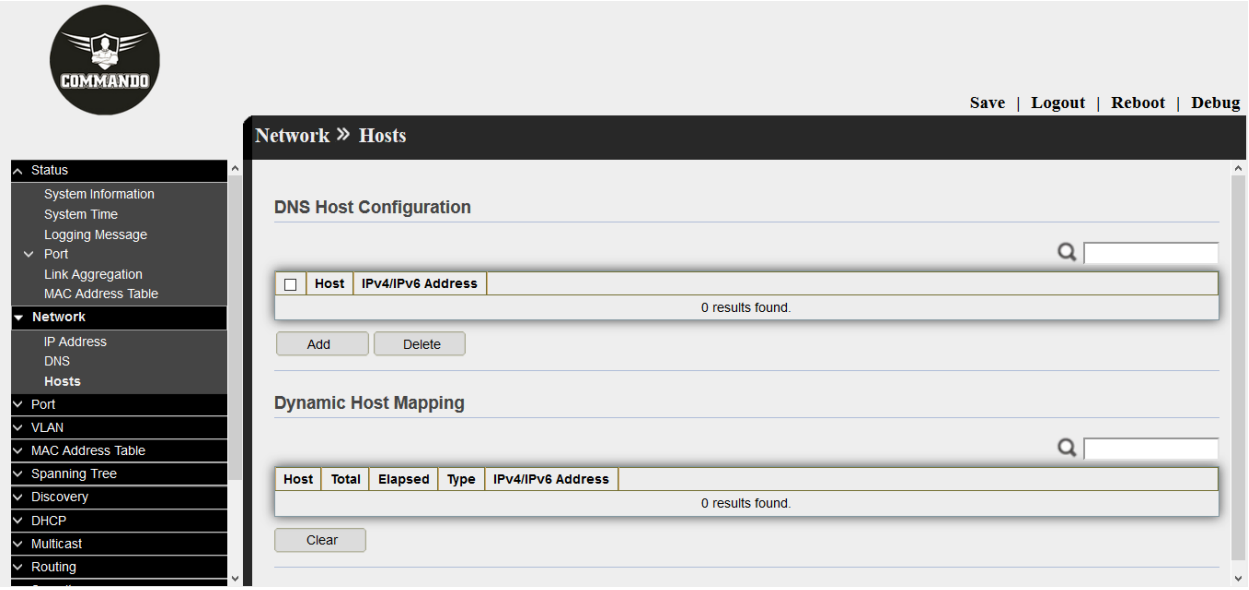


Fig 3.3.1 DNS Host blank configuration page

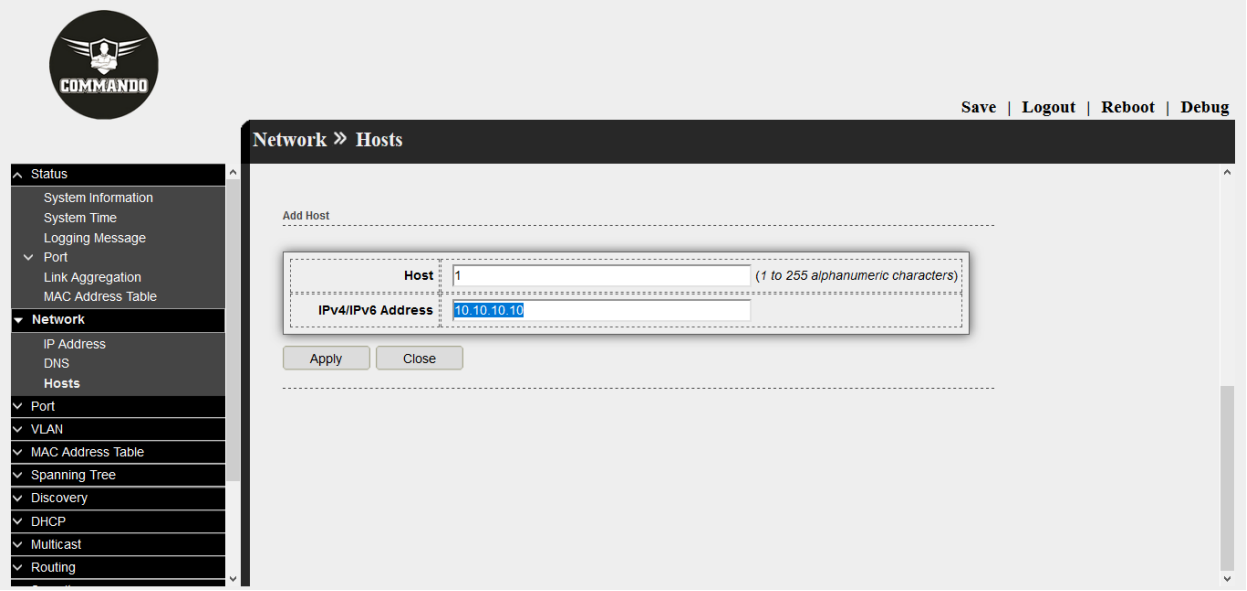


Fig 3.3.2 Add DNS Host and IP address configuration page

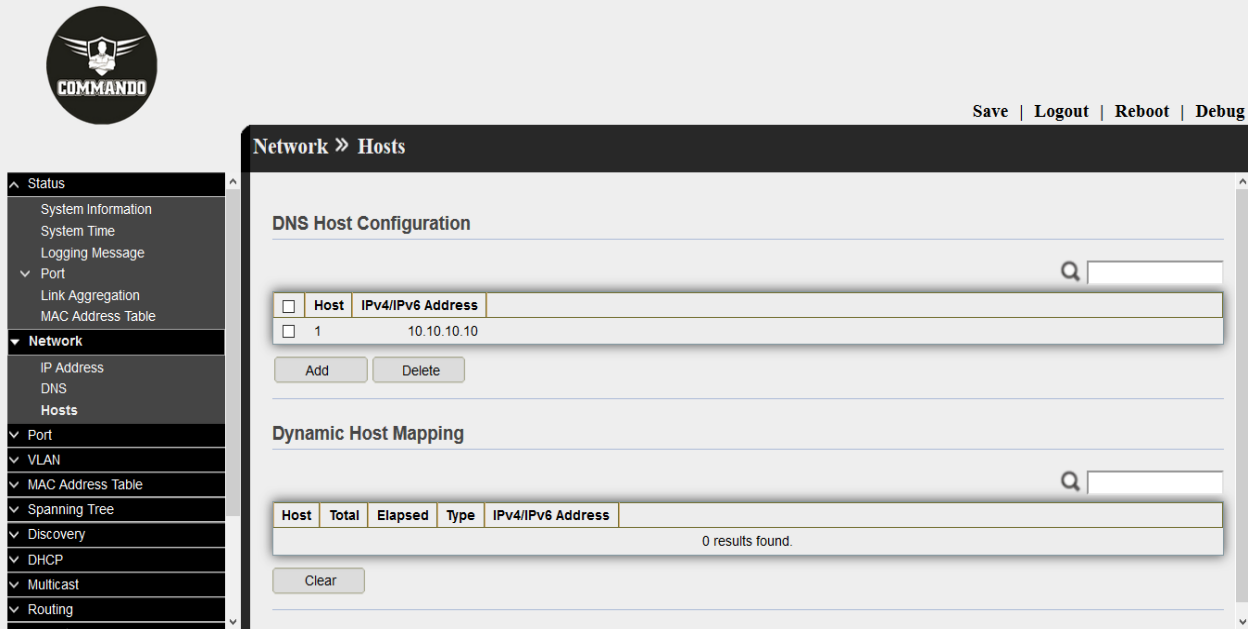


Fig 3.3.2 DNS Host configuration page

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 also 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**

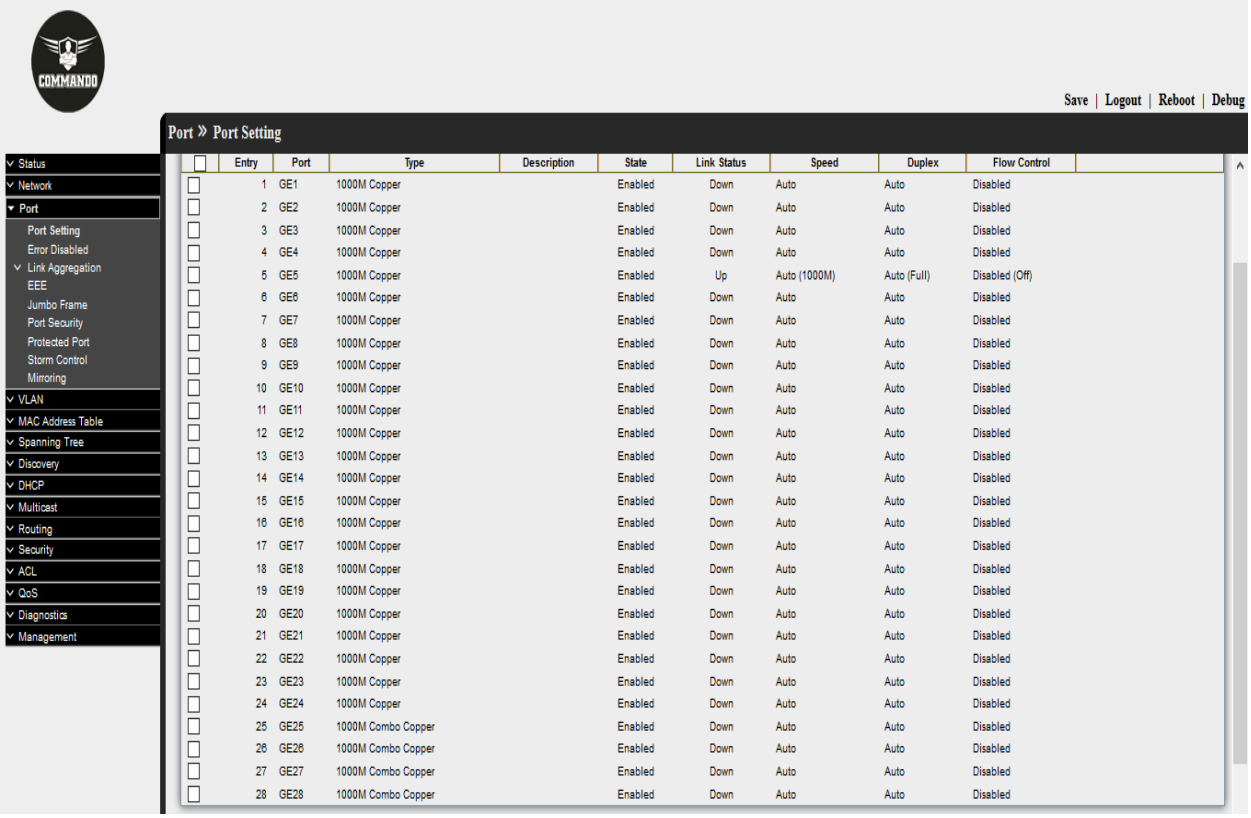


Fig 4.1.1 Port setting table page

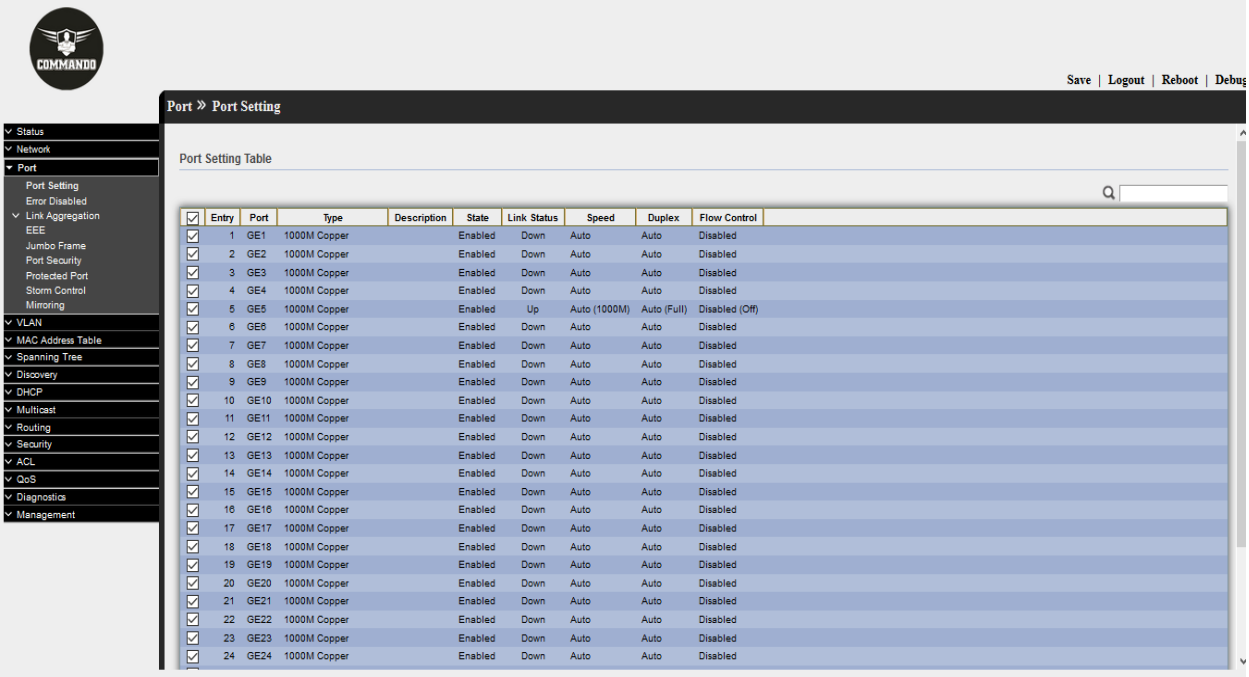


Fig 4.1.2 Port setting multiple ports selection page.

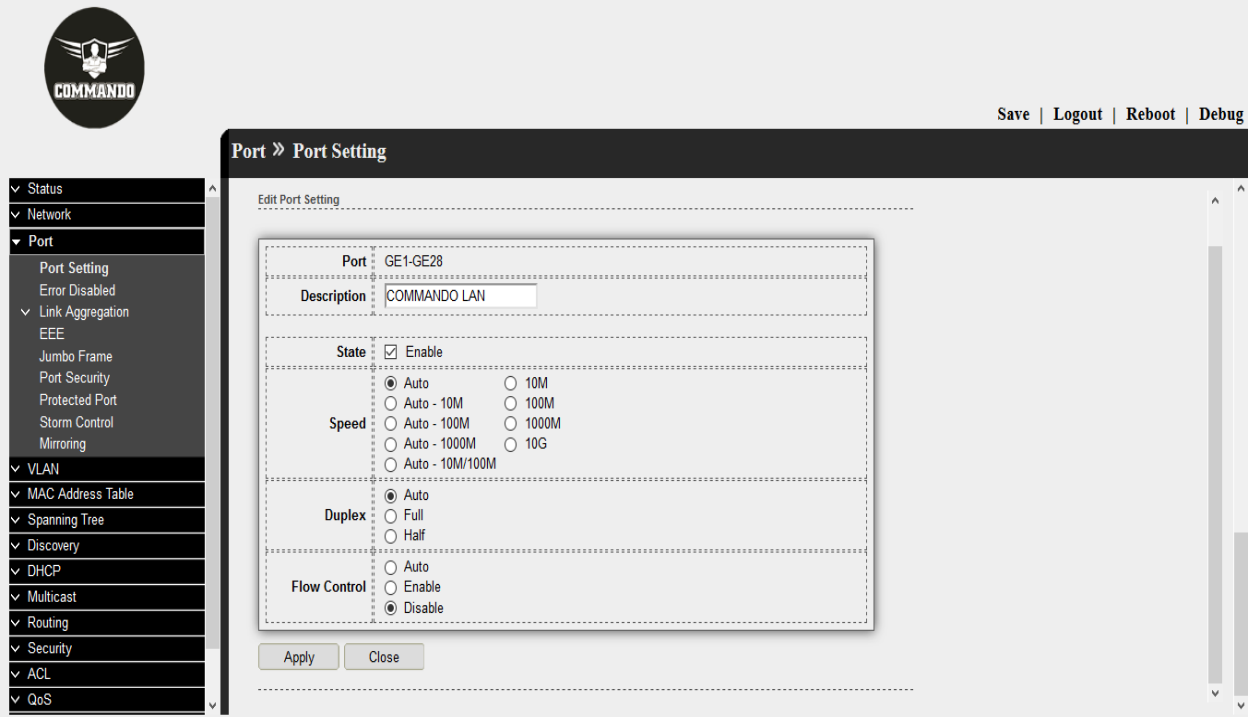


Fig 4.1.3 Port setting multiple ports Description, status, speed, duplex, flow control selection page.

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 defult 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 of time 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**

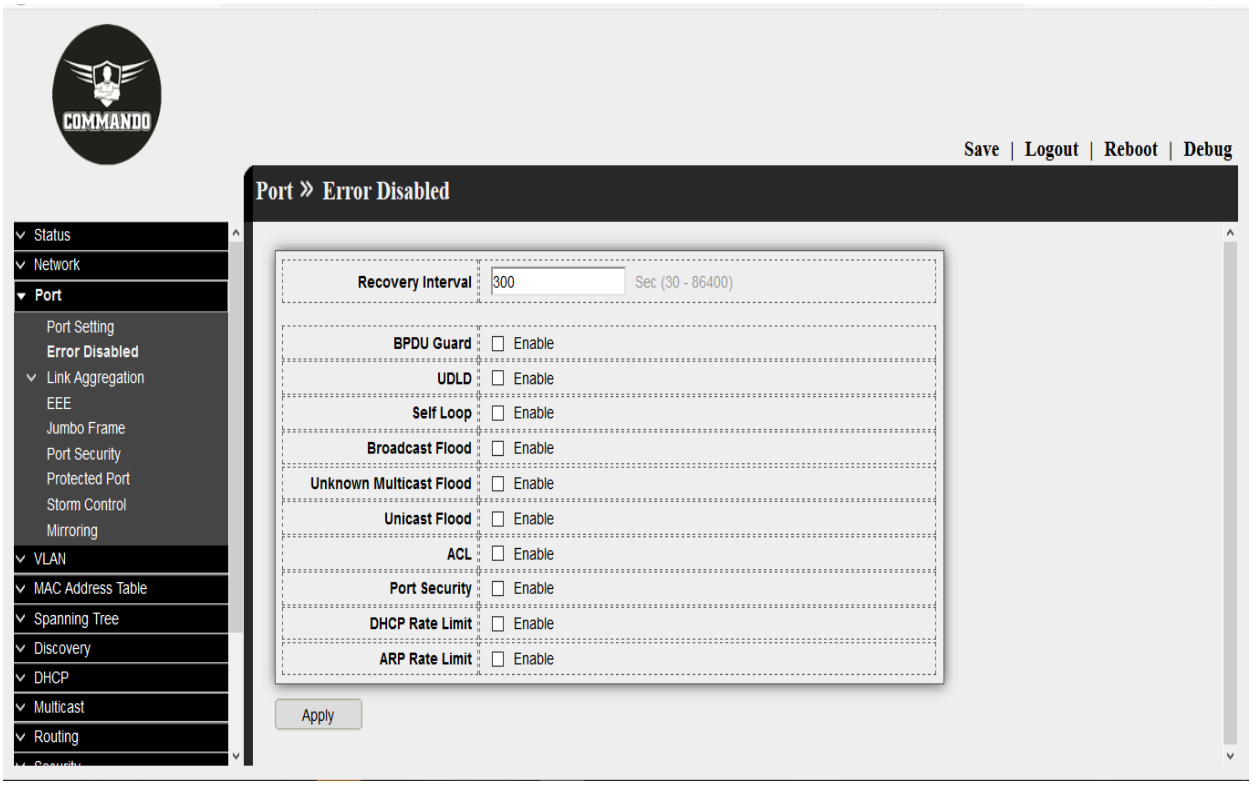


Fig 4.2.1 Error disabled selection page.

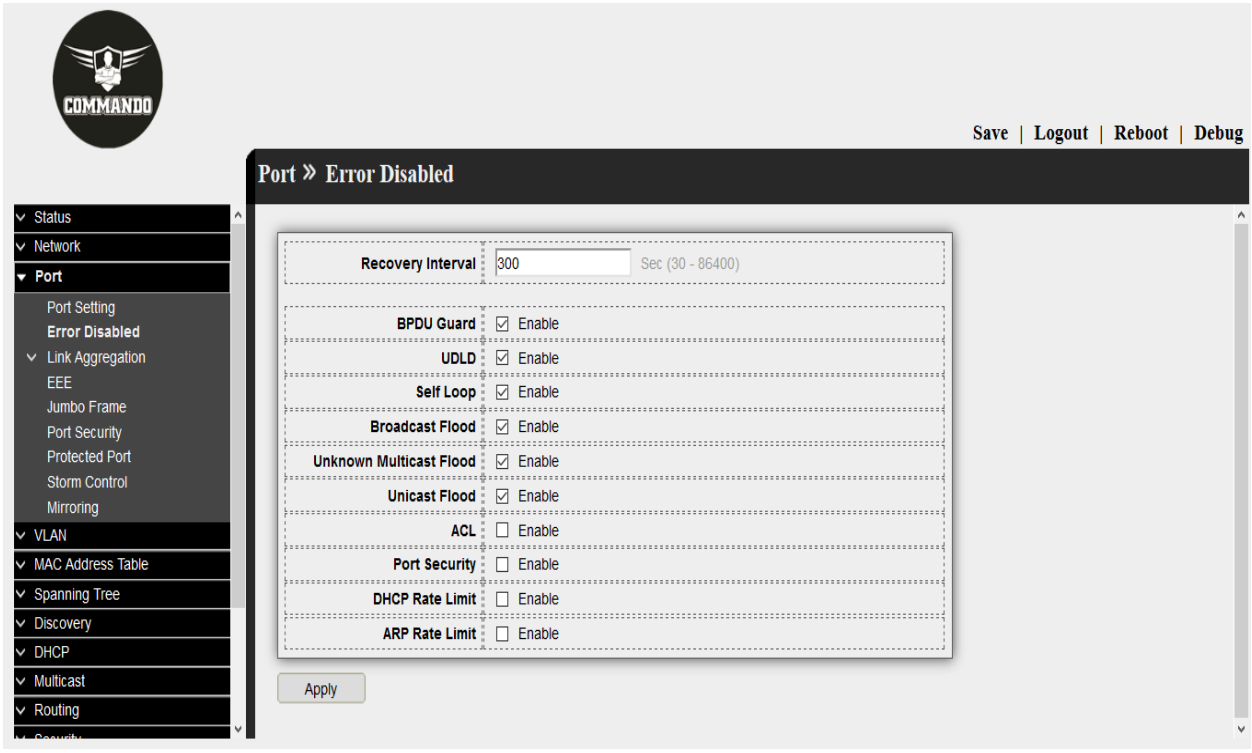


Fig 4.2.2 Enableing various parameters in Error disabled selection page.

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 & upto 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.**

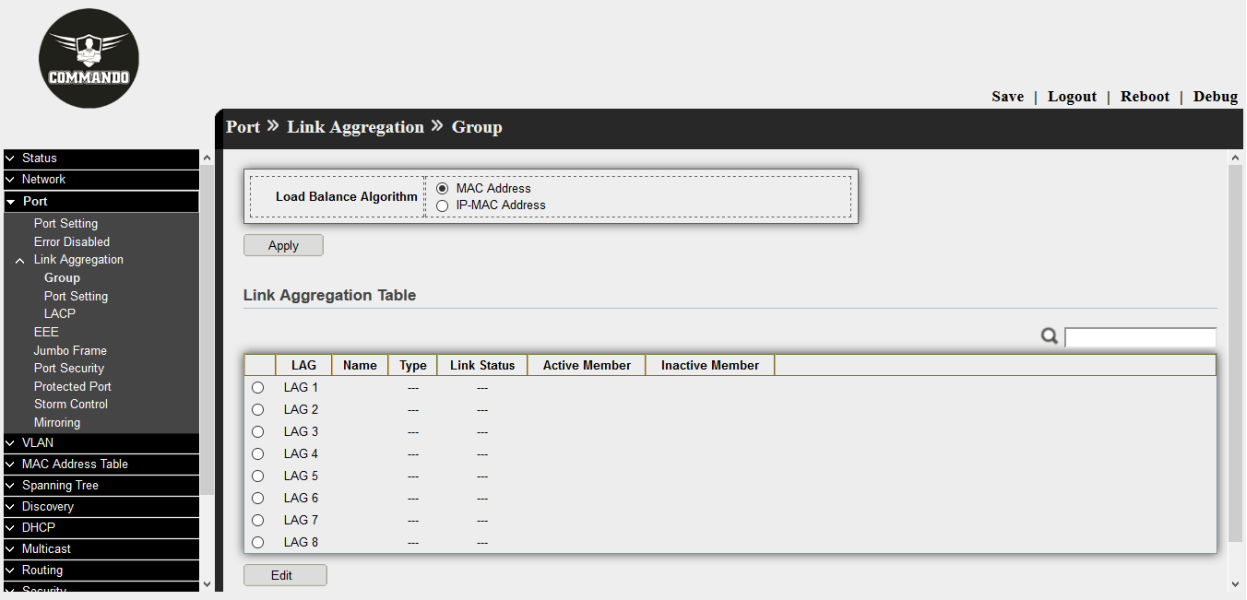


Fig 4.3.1 Link Aggregation group selection page.

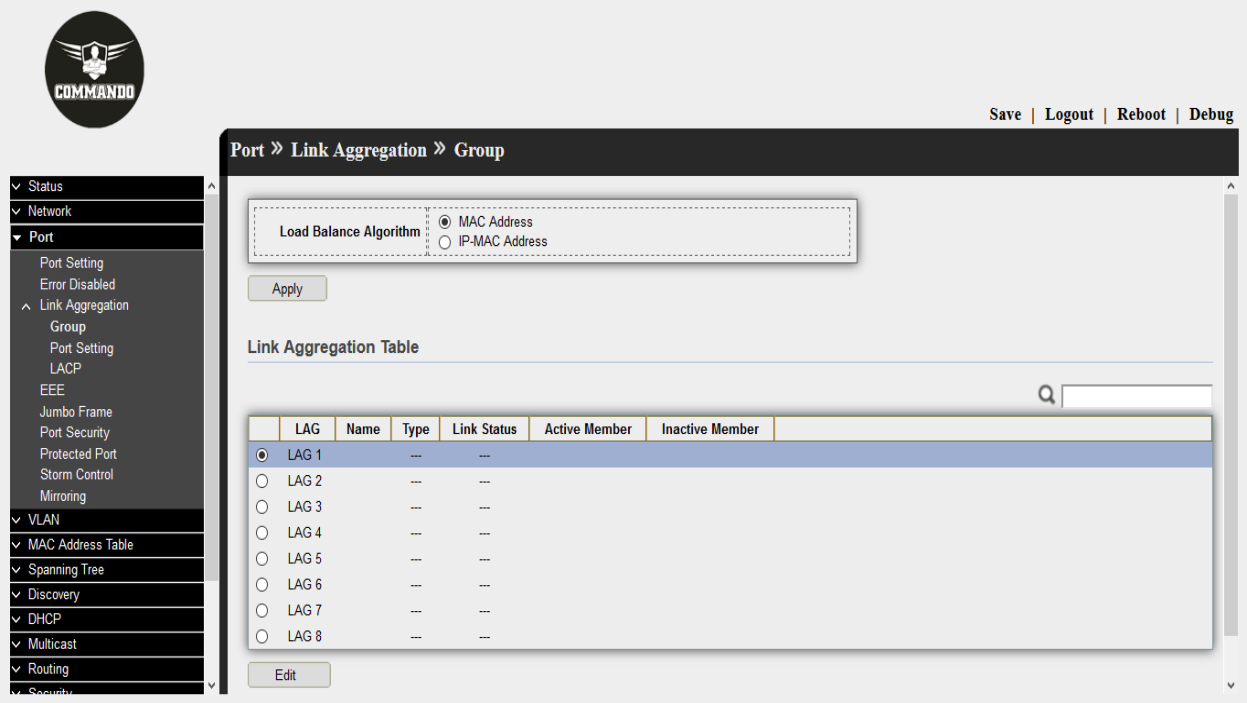


Fig 4.3.2 Link Aggregation LAG selection for editing page.

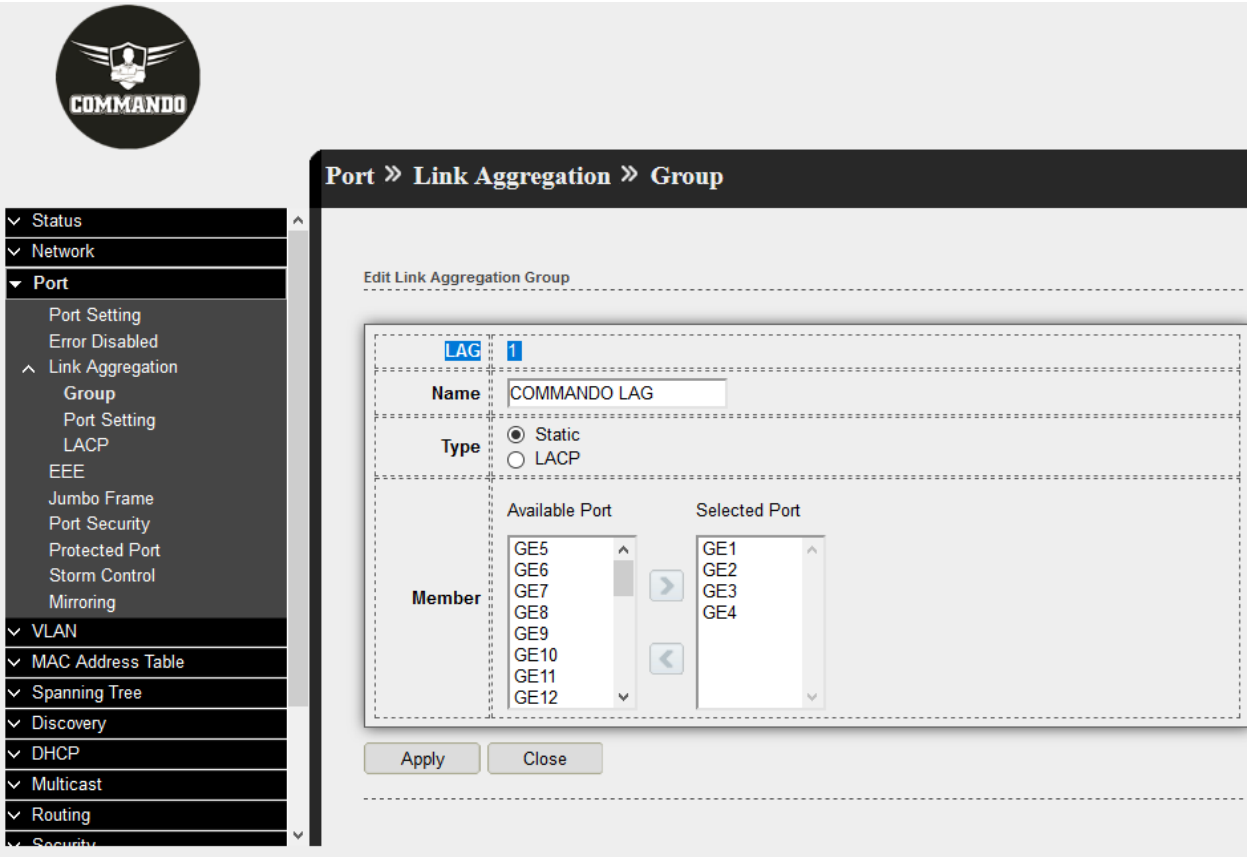


Fig 4.3.3 Link Aggregation Edit LAG page.

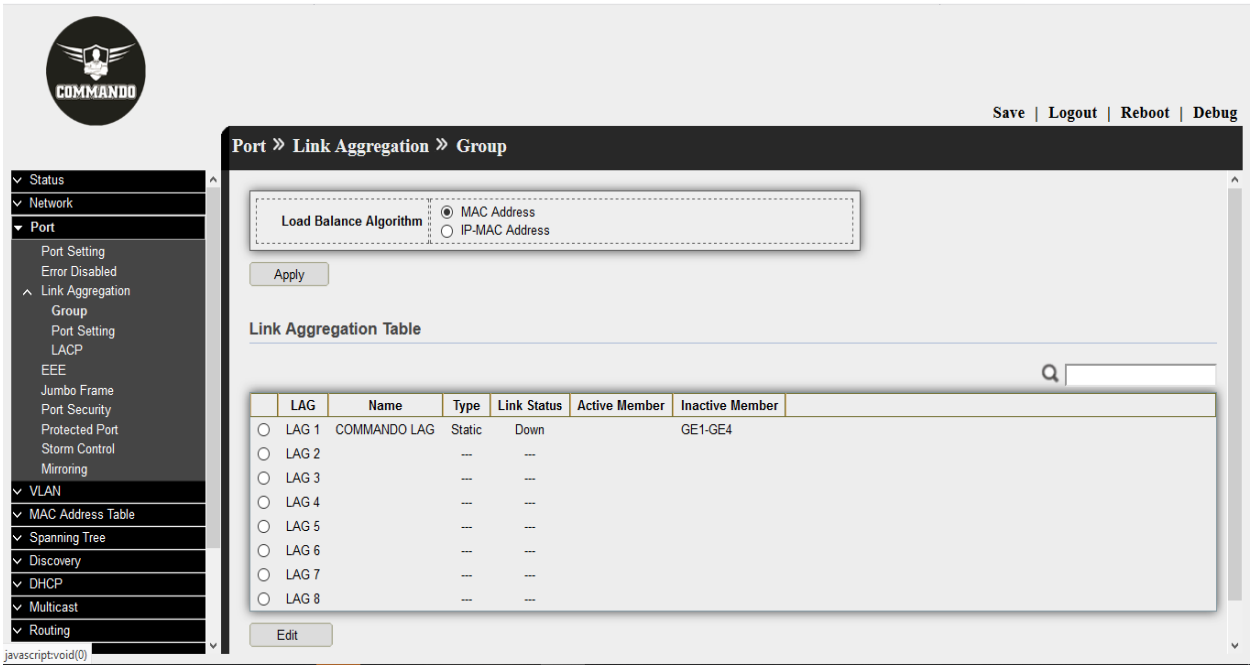


Fig 4.3.4 Link Aggregation Table page.

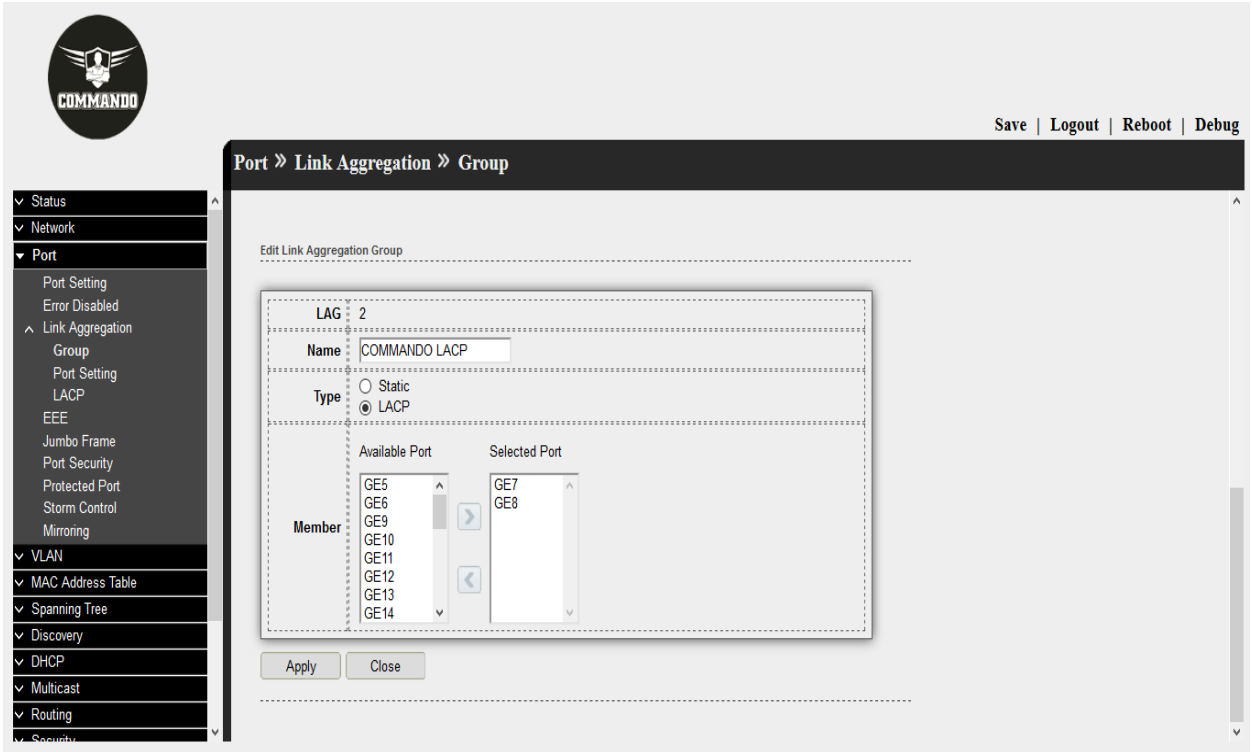


Fig 4.3.5 LACP Edit LAG page.

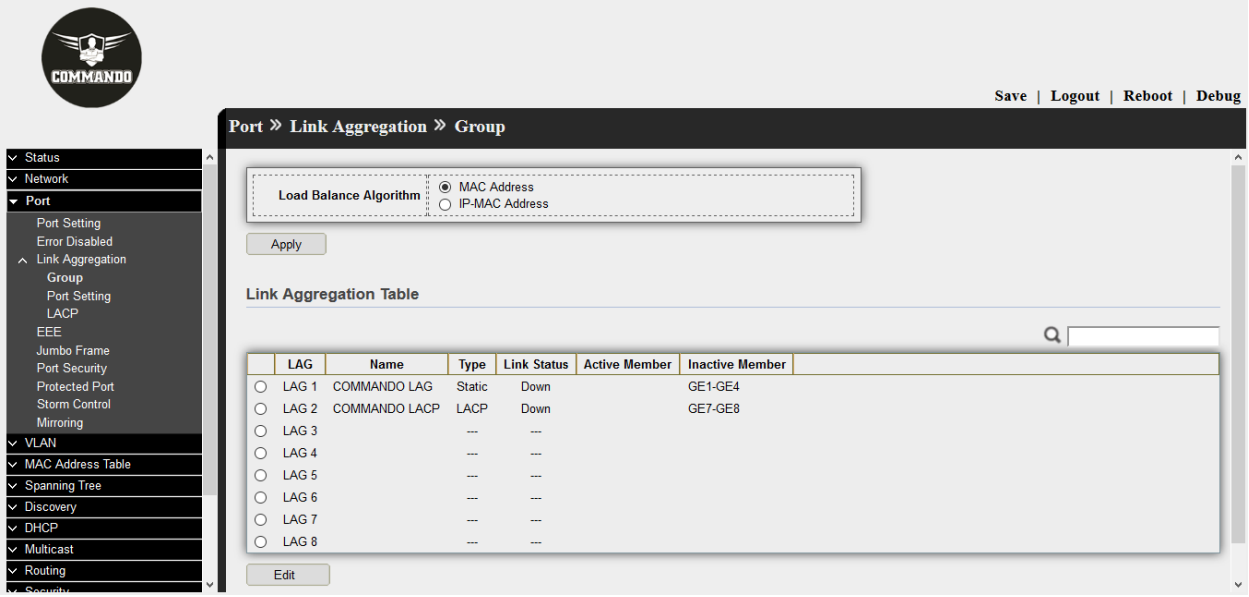


Fig 4.3.6 Link Aggregation group configuration page

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.**

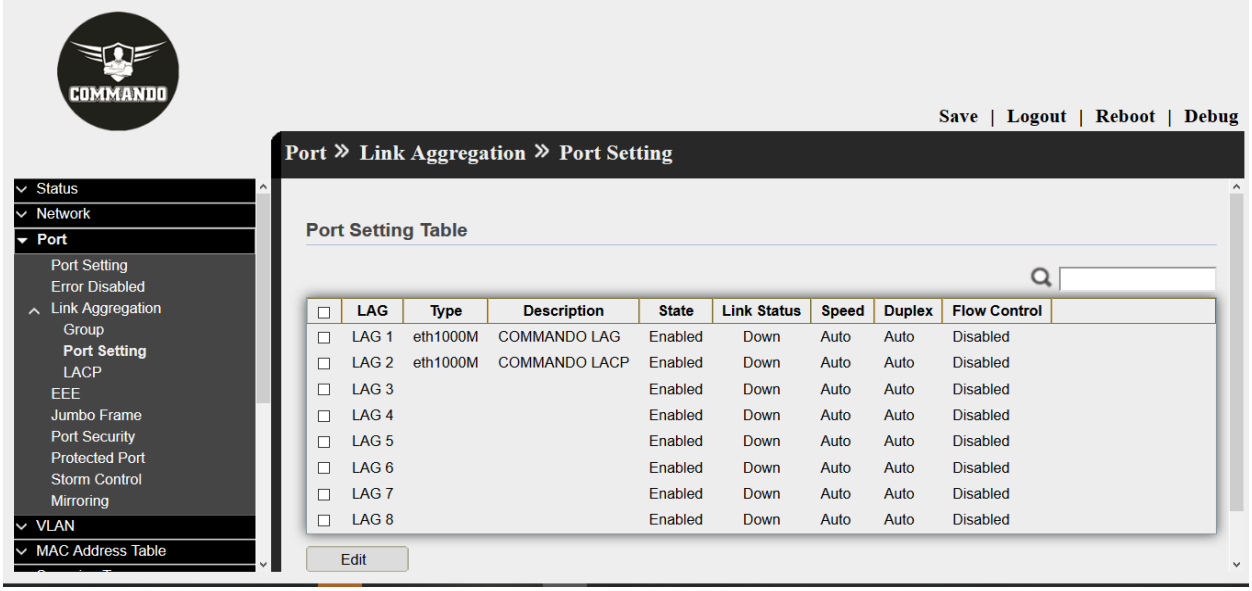


Fig 4.3.7 Link Aggregation port setting table page

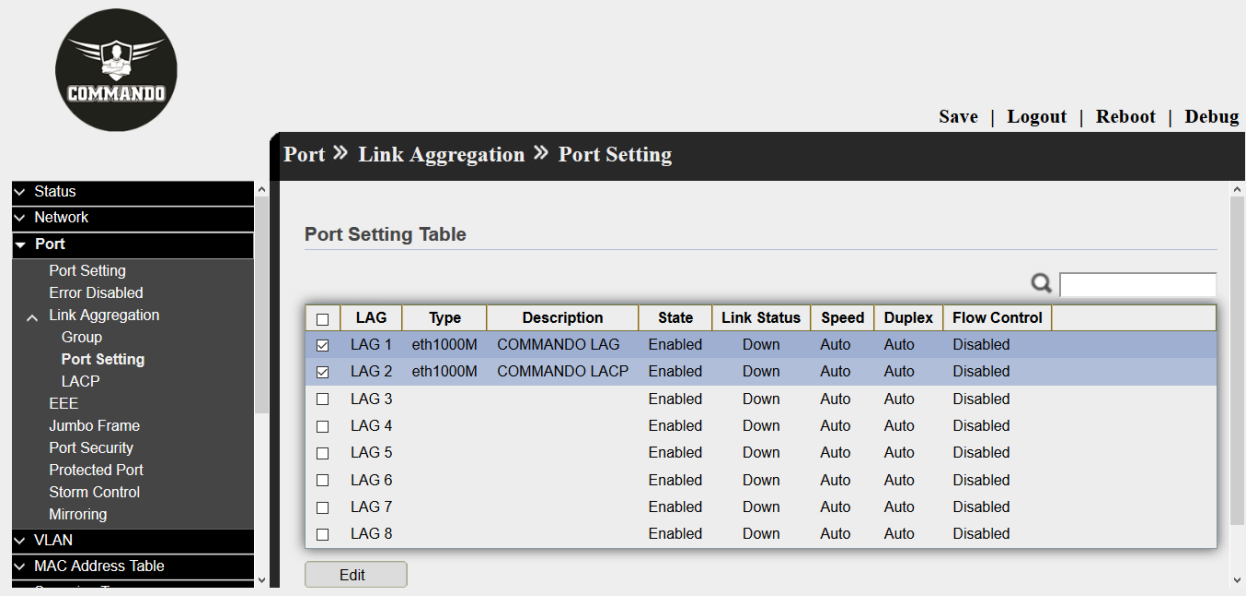


Fig 4.3.8 Link Aggregation selecting port page

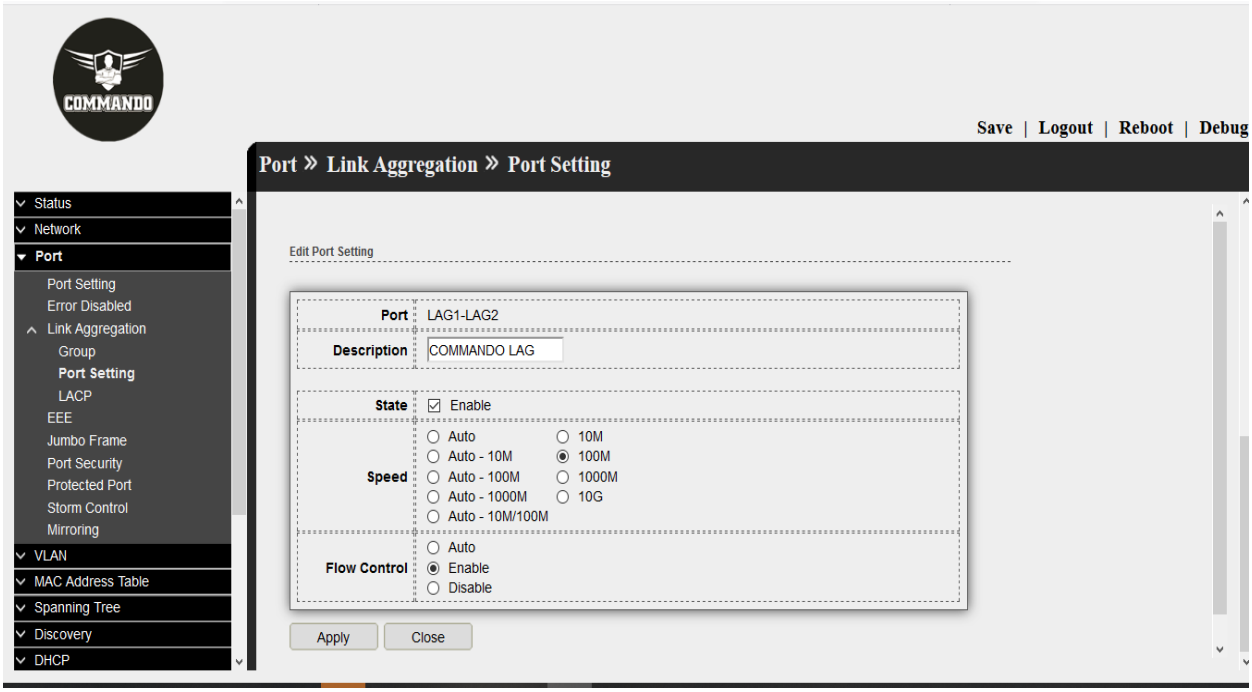


Fig 4.3.9 Link Aggregation port setting for LAG1-LAG2 speed to 100M and flow control page

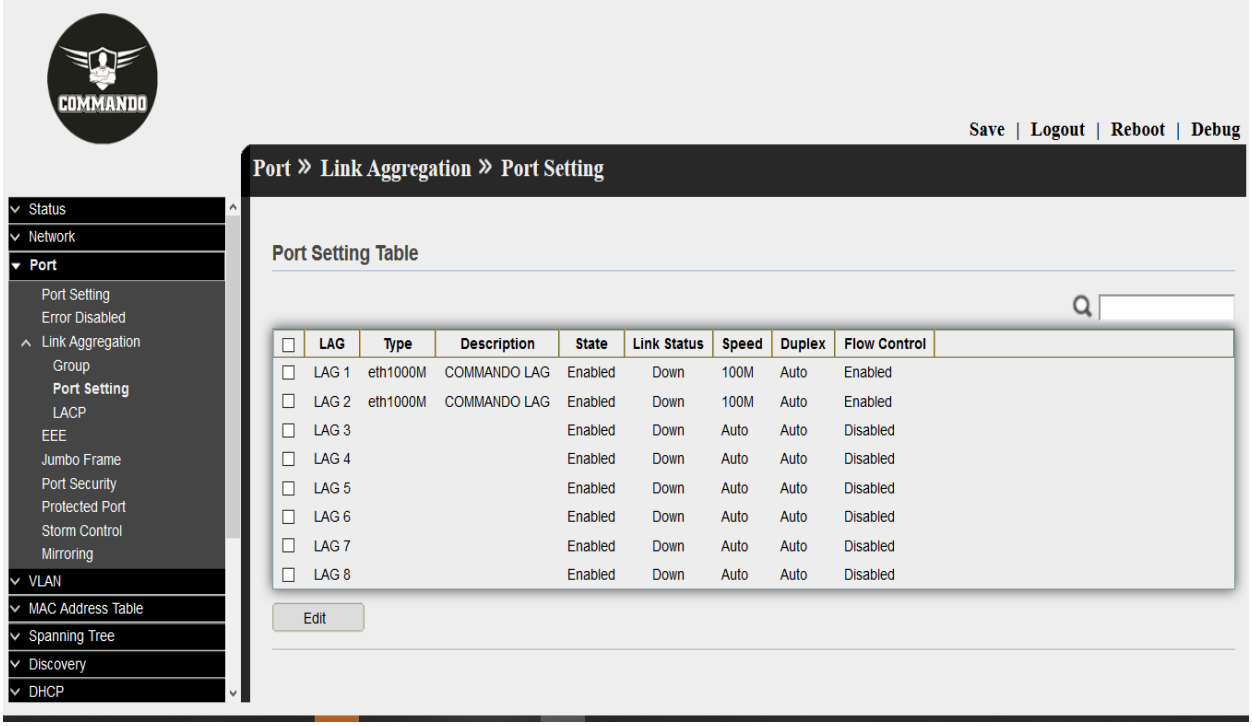


Fig 4.3.10 Link Aggregation port setting table for LAG1-LAG2 page

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 similar to 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.**

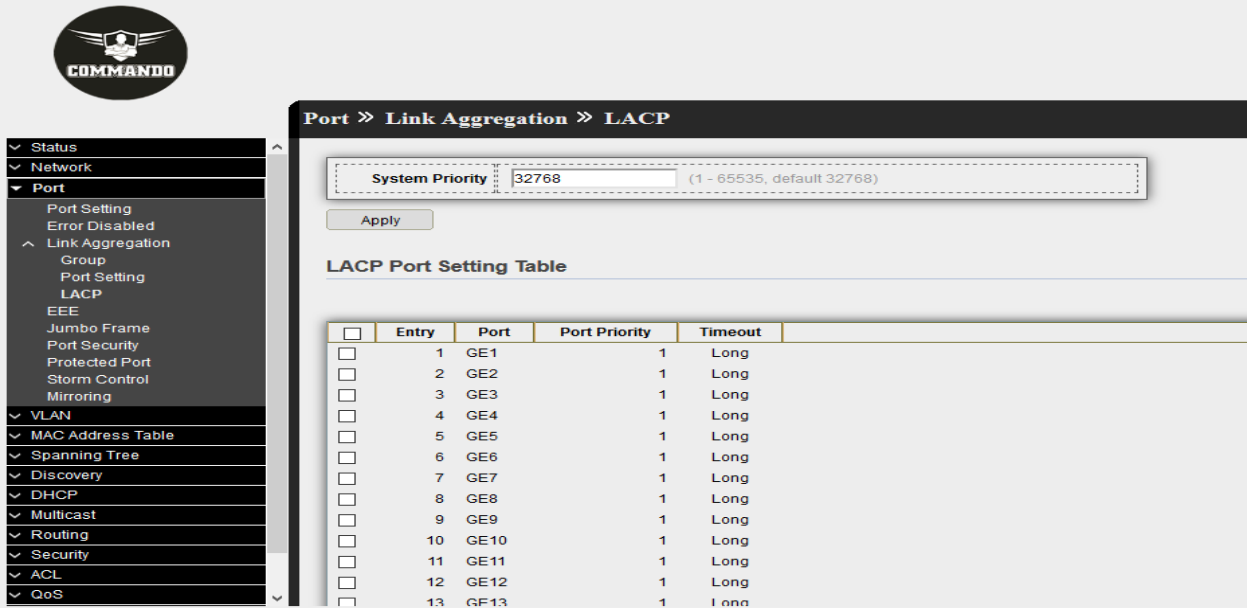


Fig 4.3.6 Link Aggregation LACP Port Setting Table page

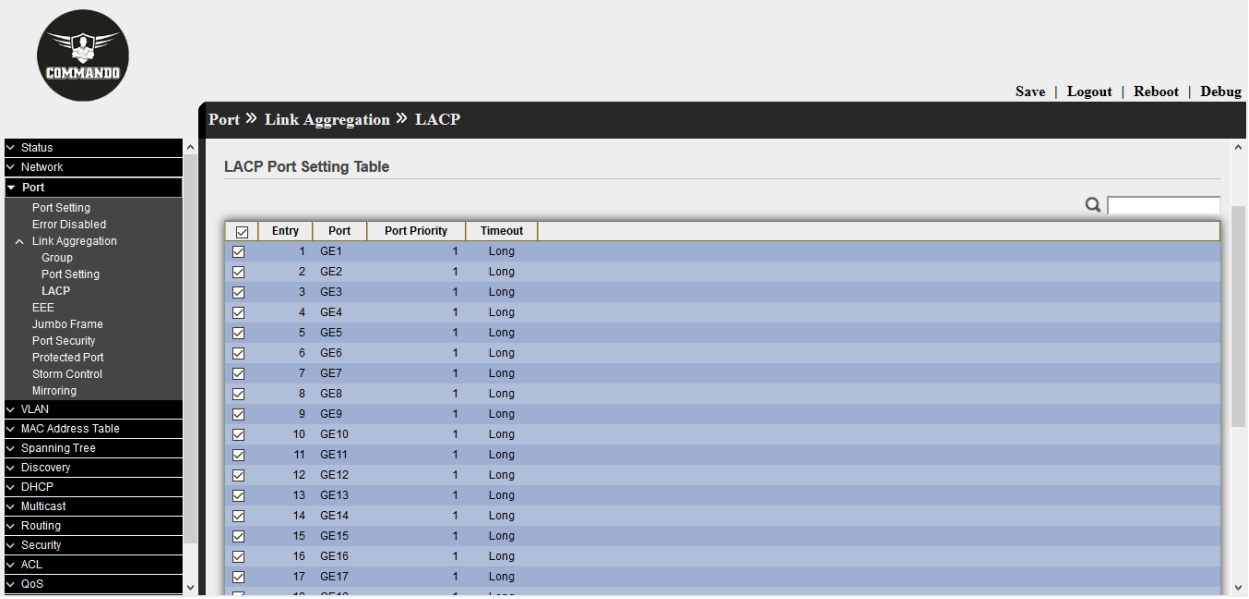


Fig 4.3.7 Link Aggregation LACP Port Setting port selection page

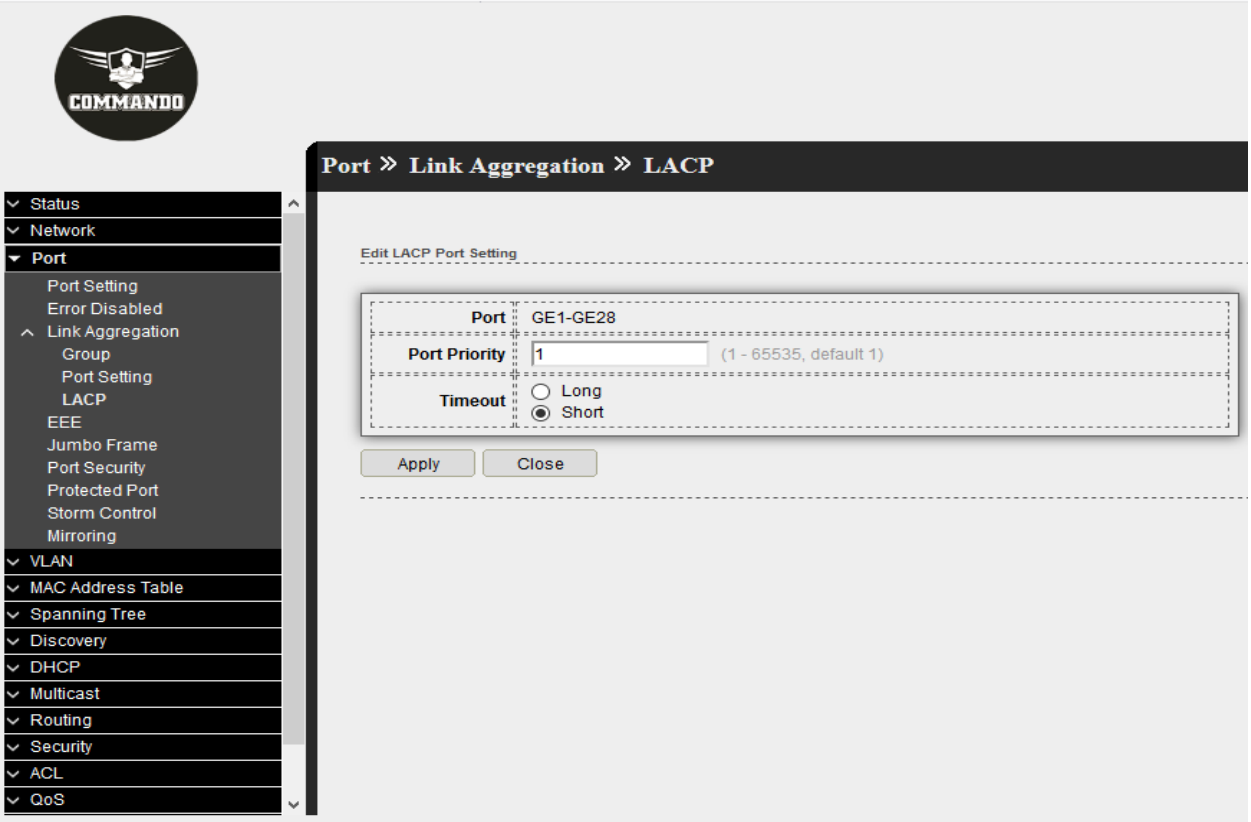


Fig 4.3.8 Edit LACP Port Setting page

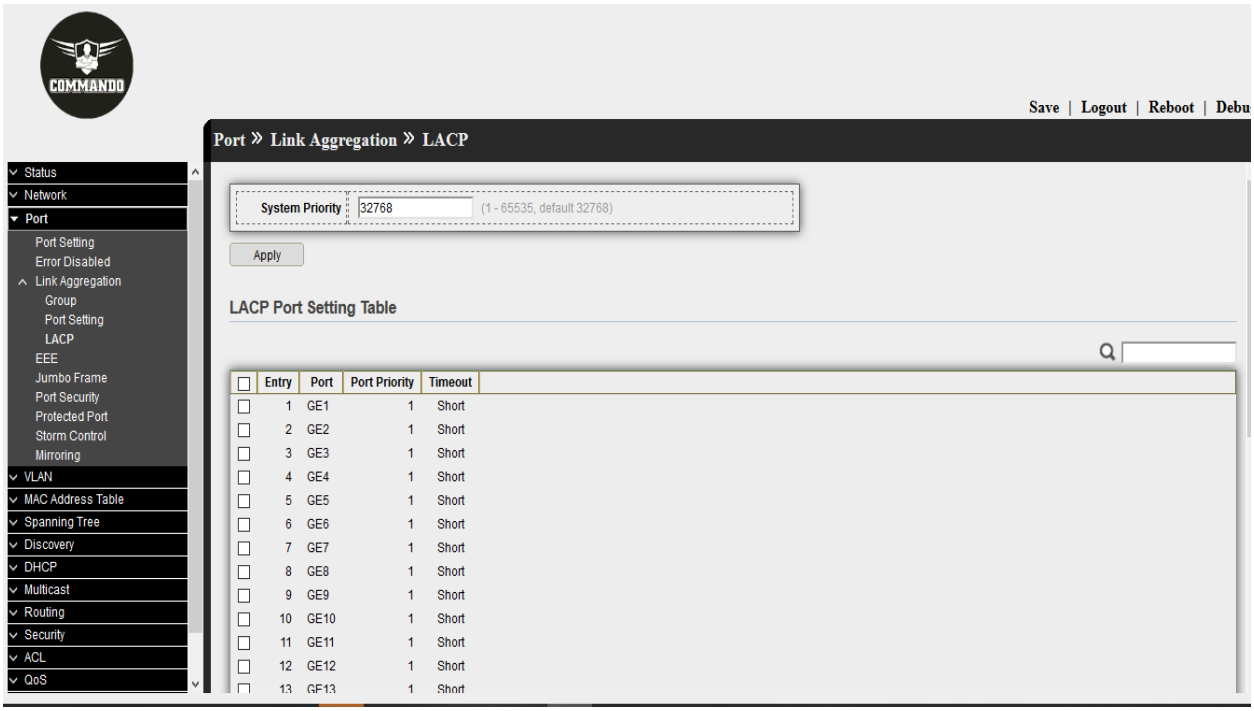


Fig 4.3.9 LACP Port Setting Table page

4.4 EEE

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 diabled on C2000 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.**

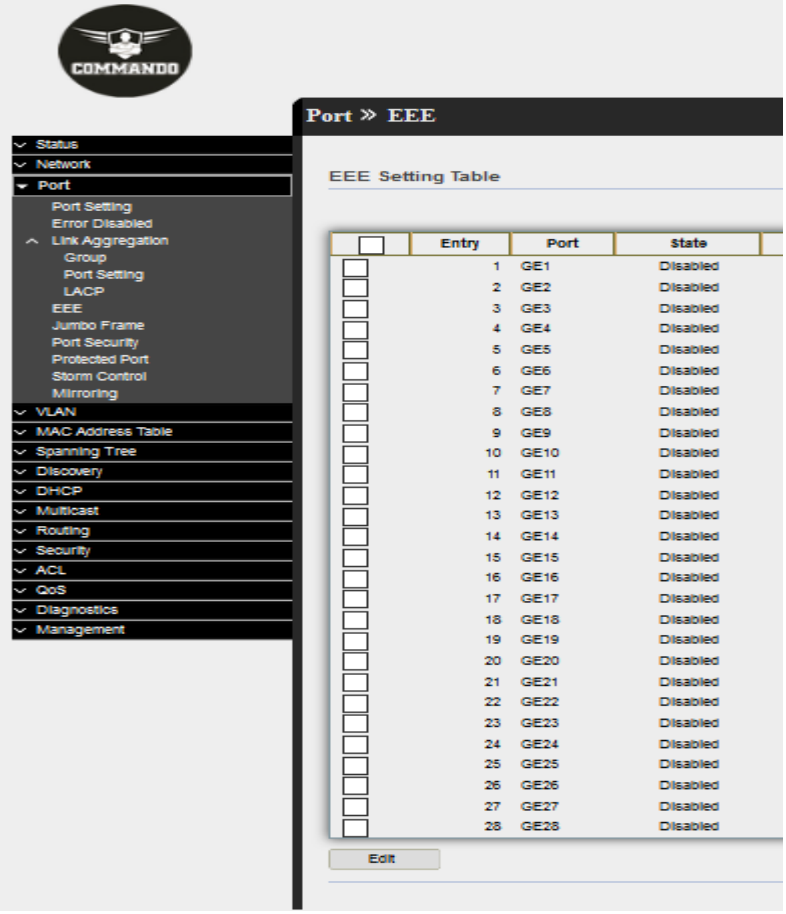


Fig 4.4.1 Port EEE Setting Table port selection page

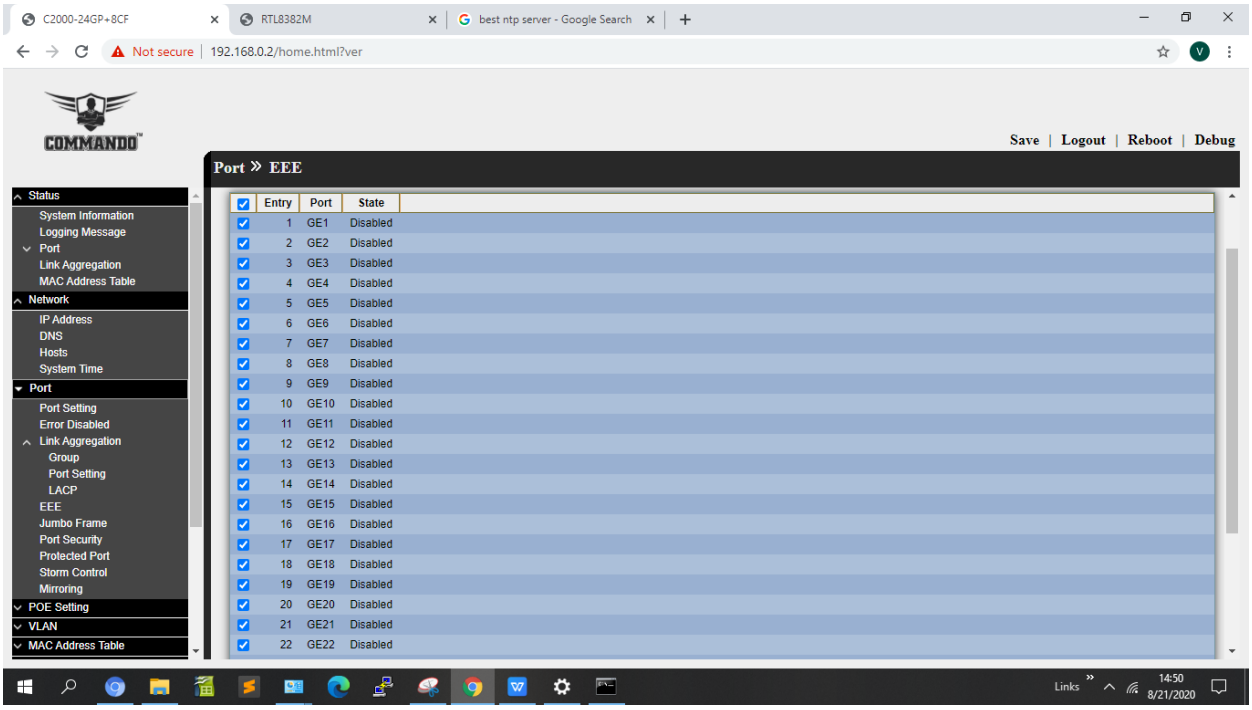


Fig 4.4.2 Port EEE Setting Table all ports selection page

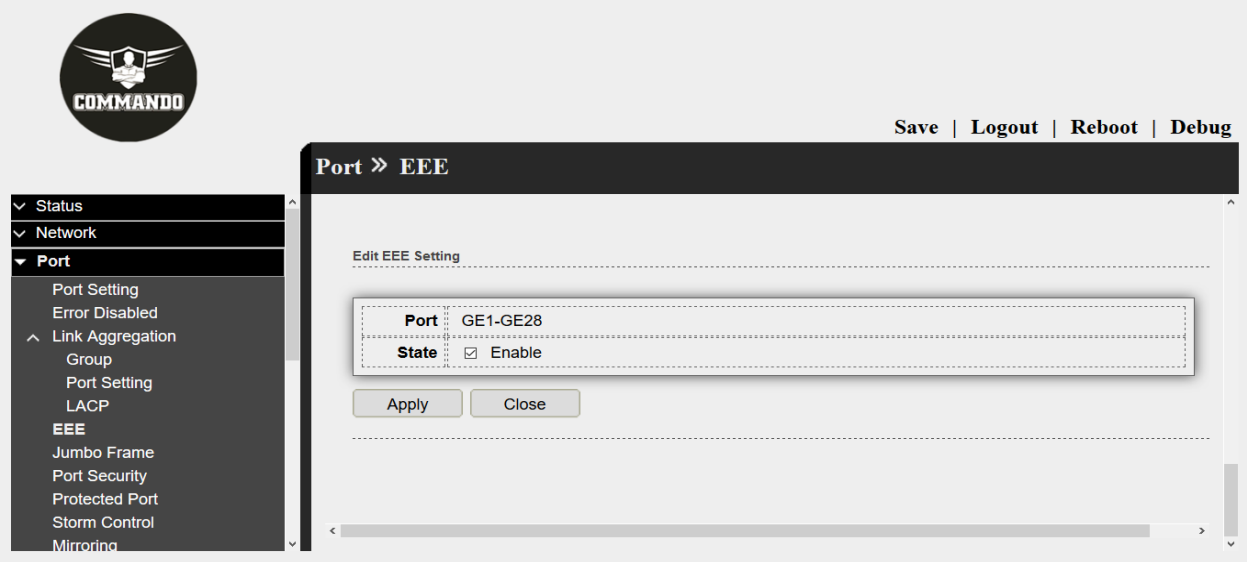


Fig 4.4.3 Port EEE Setting port application page

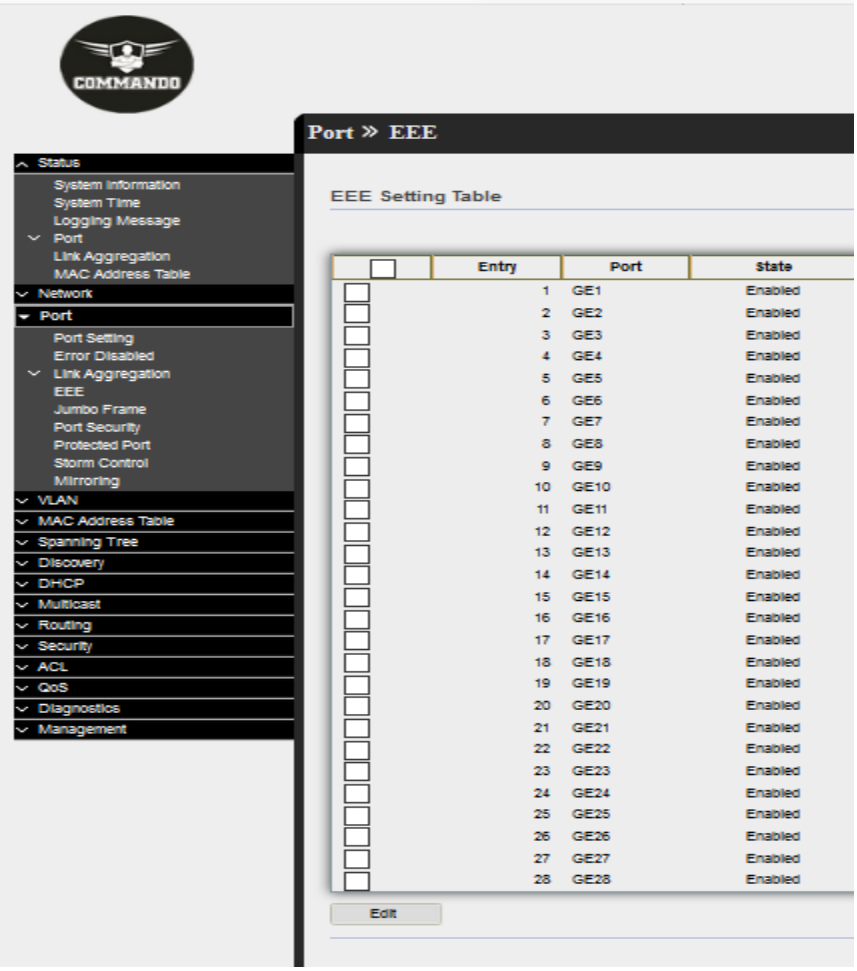


Fig 4.4.4 Port EEE Setting Table after Enabled Port page

Note:- It will take 2 minutes to update the EEE on all ports.

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

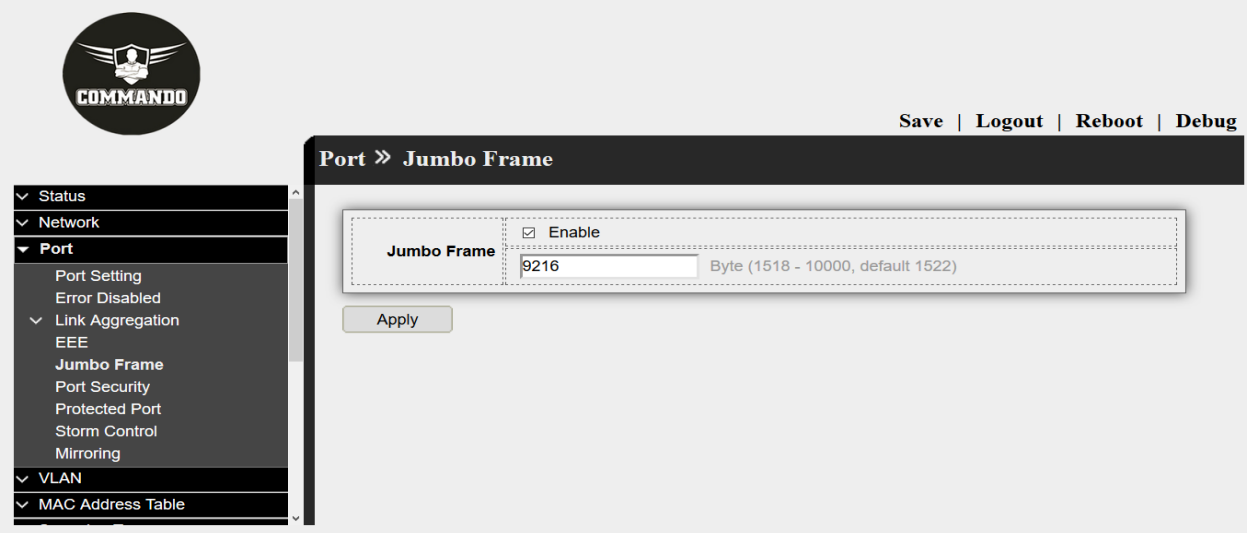


Fig 4.5.2 Jumbo Frame Enable for 9216 bytes page

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 performas per limitation.

To Configure Port Security , click **Port>> Port Security**

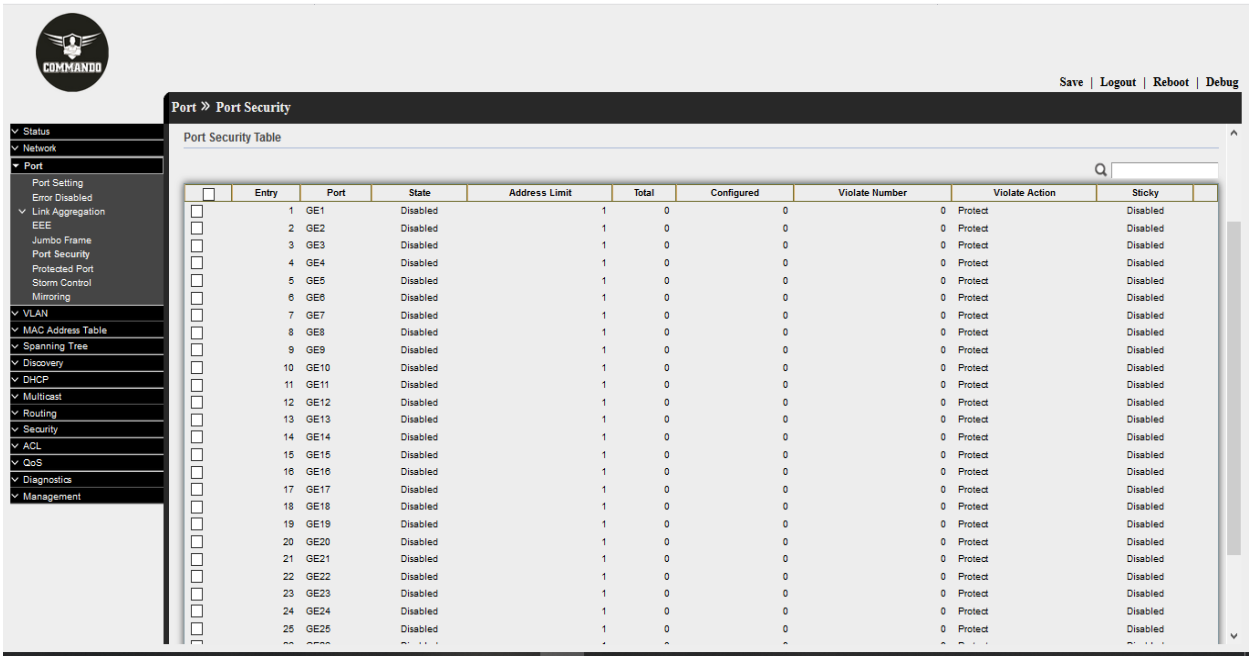


Fig 4.6.1 Default Port Security Table page

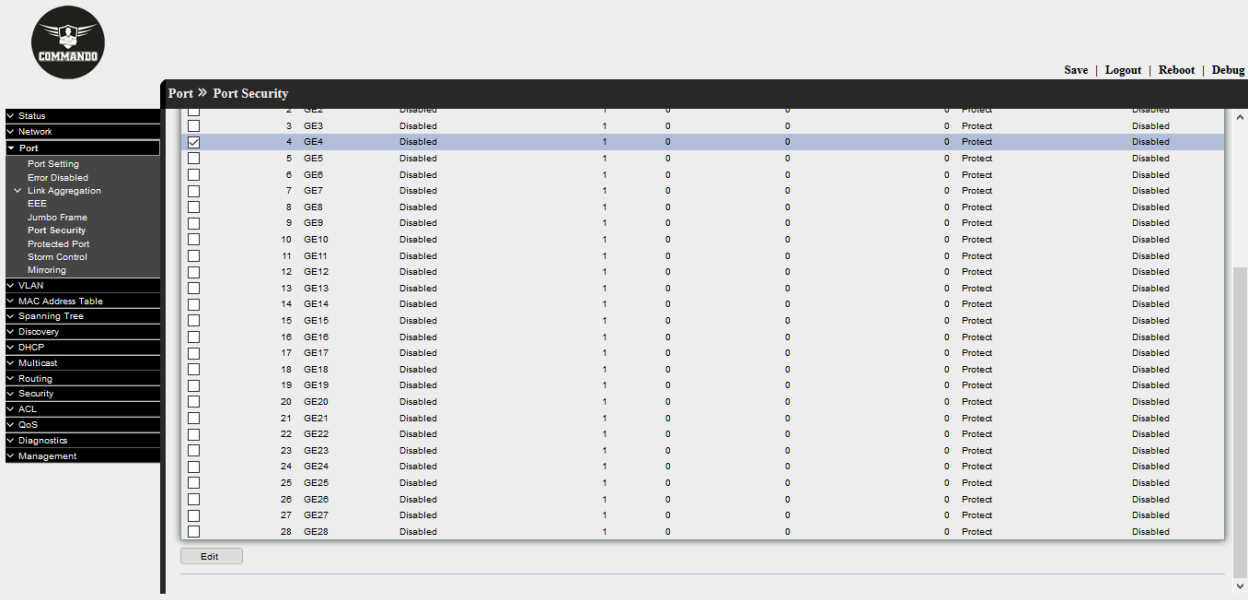


Fig 4.6.2 Selecting Port Security GE4 page

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 Violet Action “Protect or Restrict or Shutdown”, Select\Deselect “Sticky” option & Click on “Apply”.

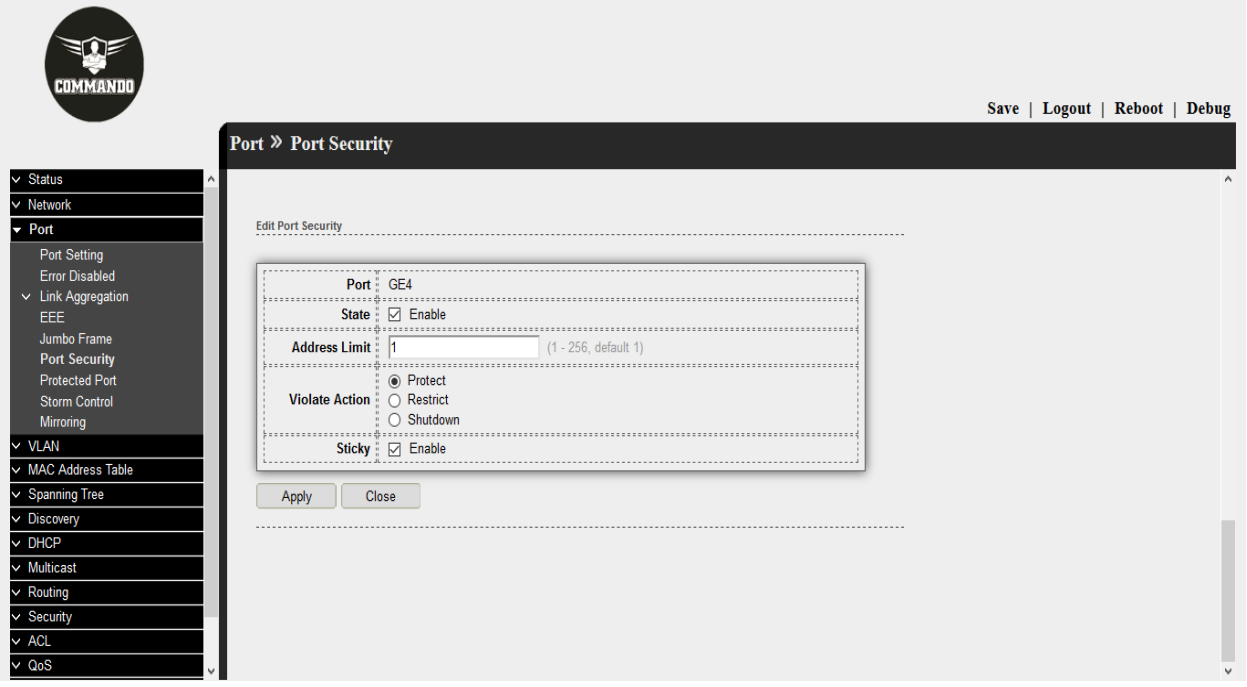


Fig 4.6.3 Edit Port security for GE4 interface page

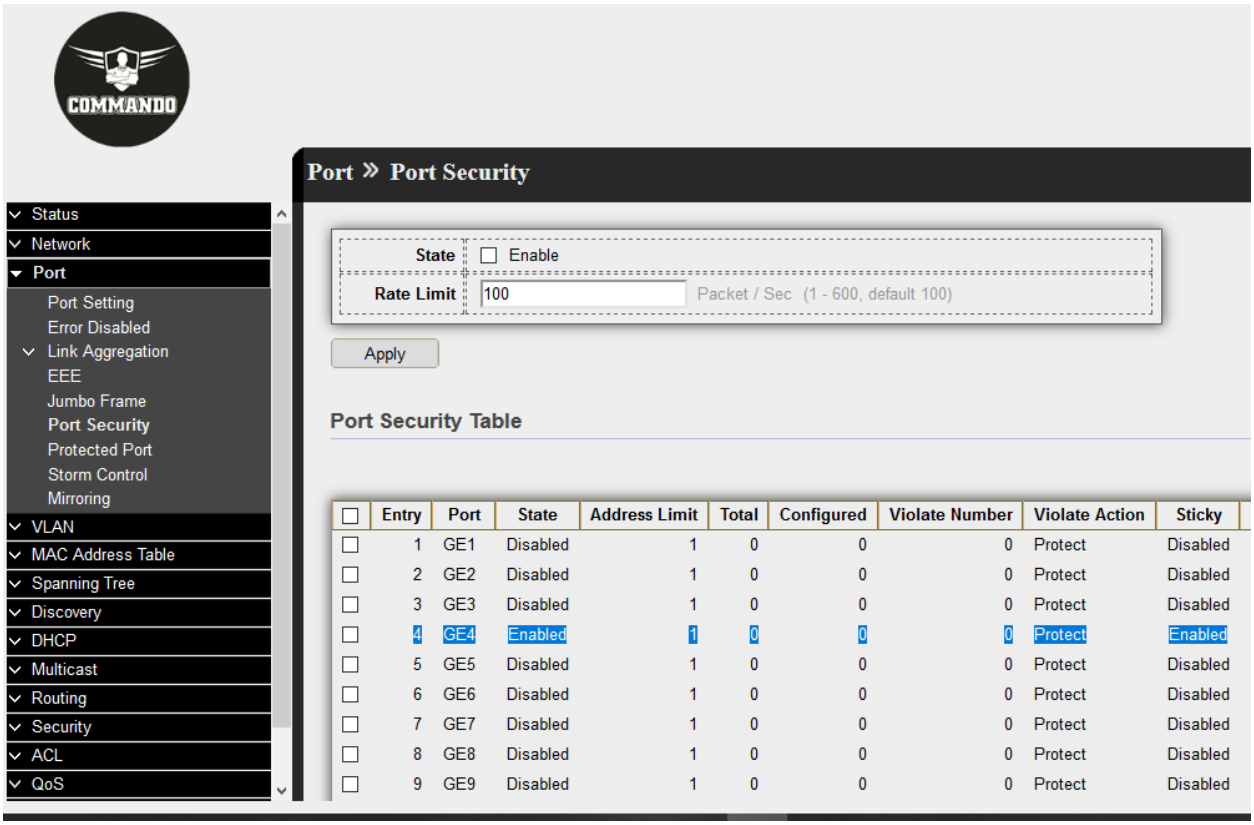


Fig 4.6.4 Edit Port security for GE1-GE28 ports interface page

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.**

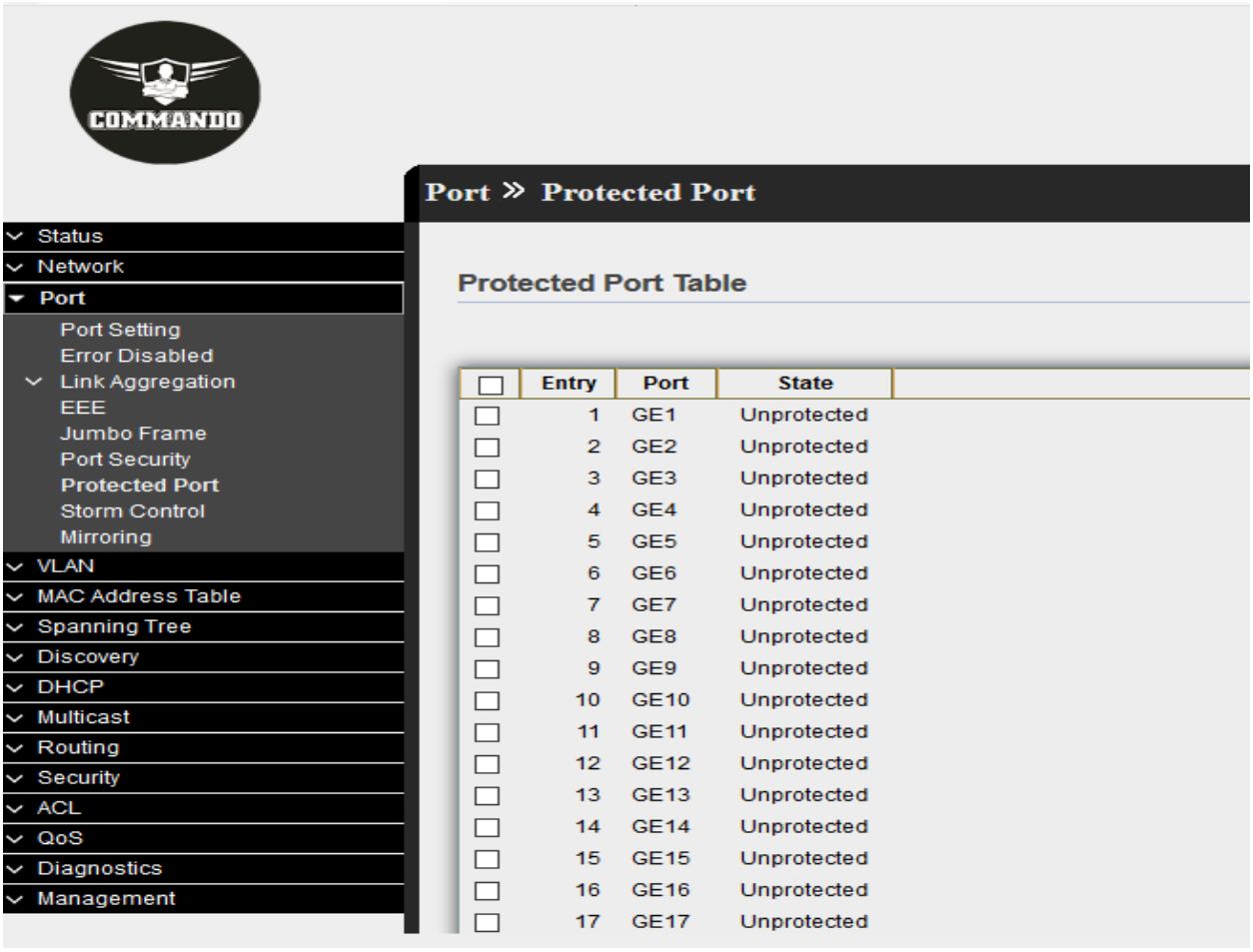


Fig 4.7.1 Protected Port Table page

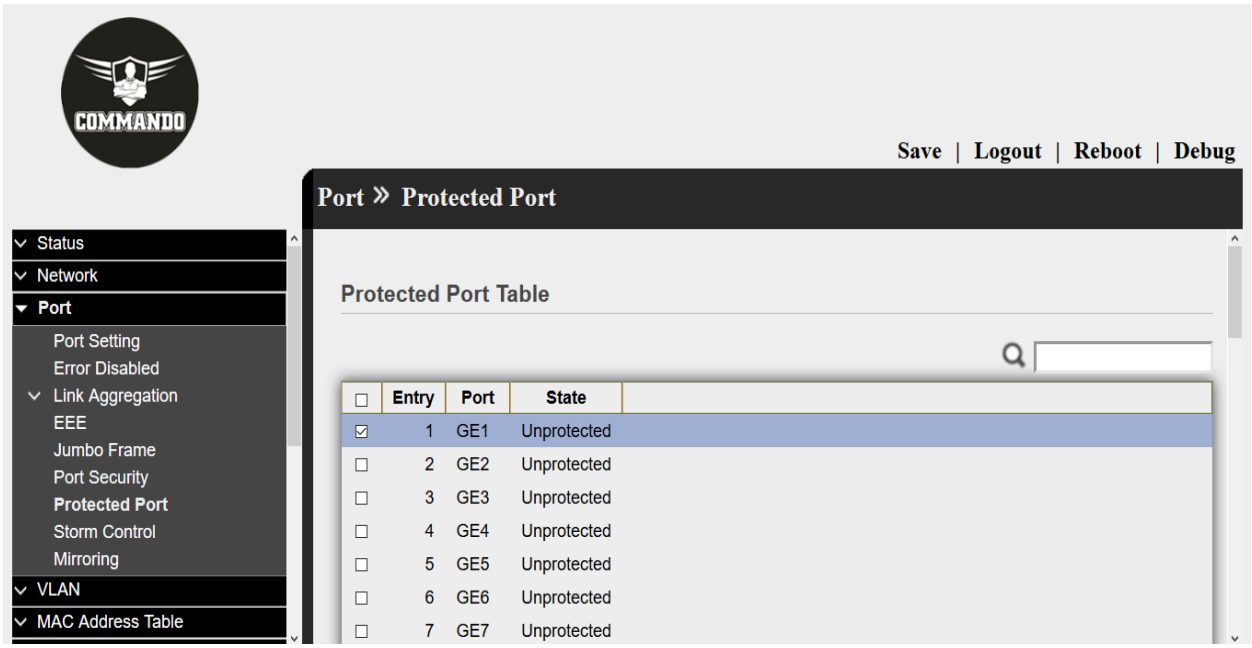


Fig 4.7.2 Selection of GE1 port for Protected page

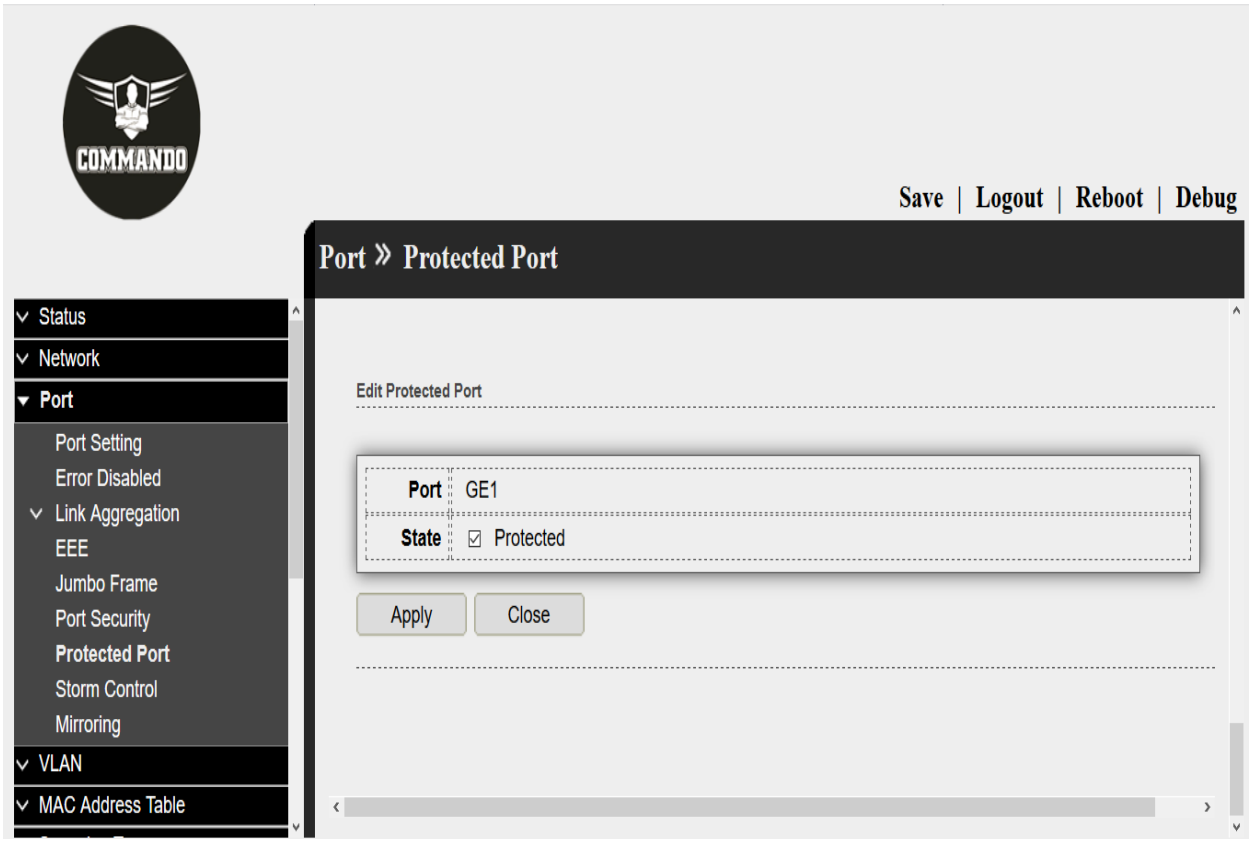


Fig 4.7.3 Enableing GE1 port for Protected Port configuration page

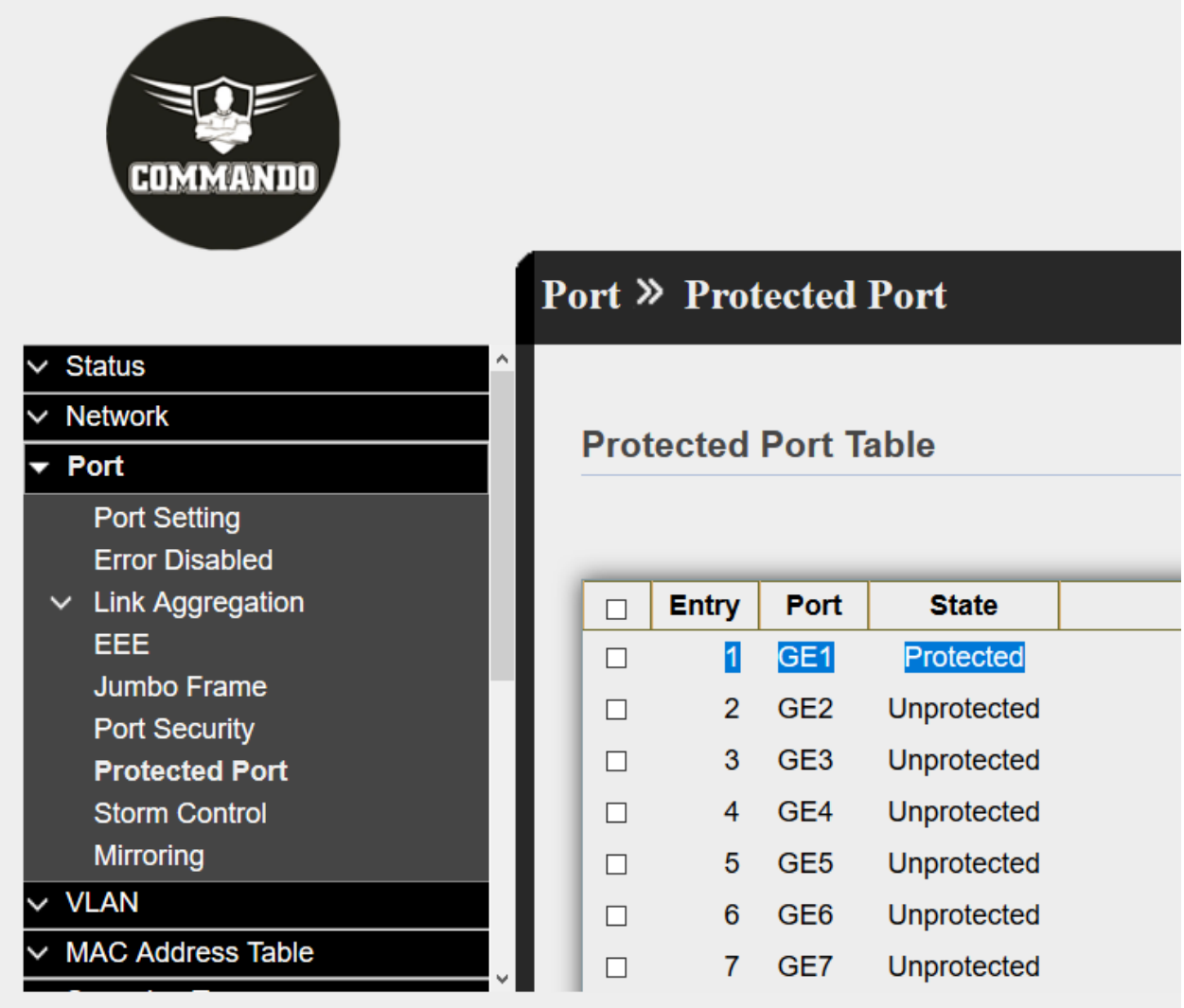


Fig 4.7.4 Protected Port Table after enabling GE1 page

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.**

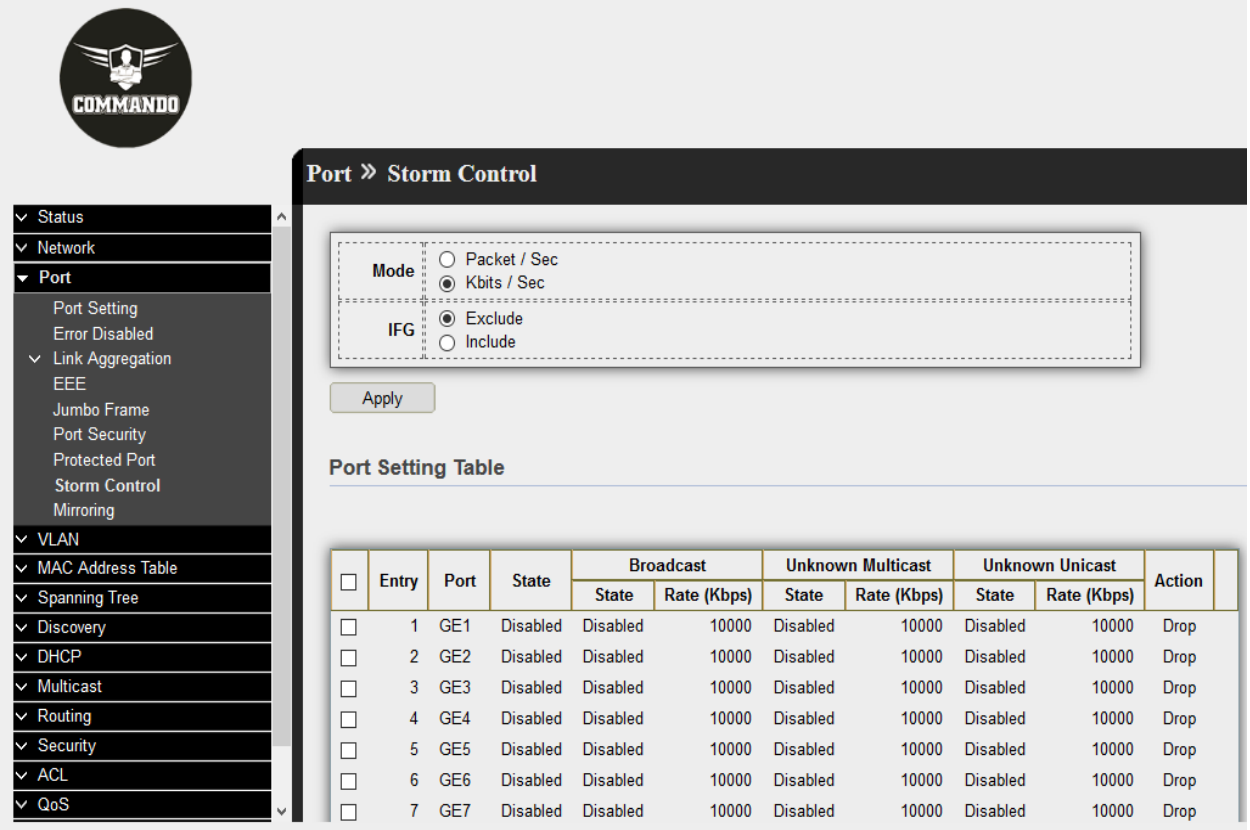


Fig 4.8.1 Default Storm control port setting table page

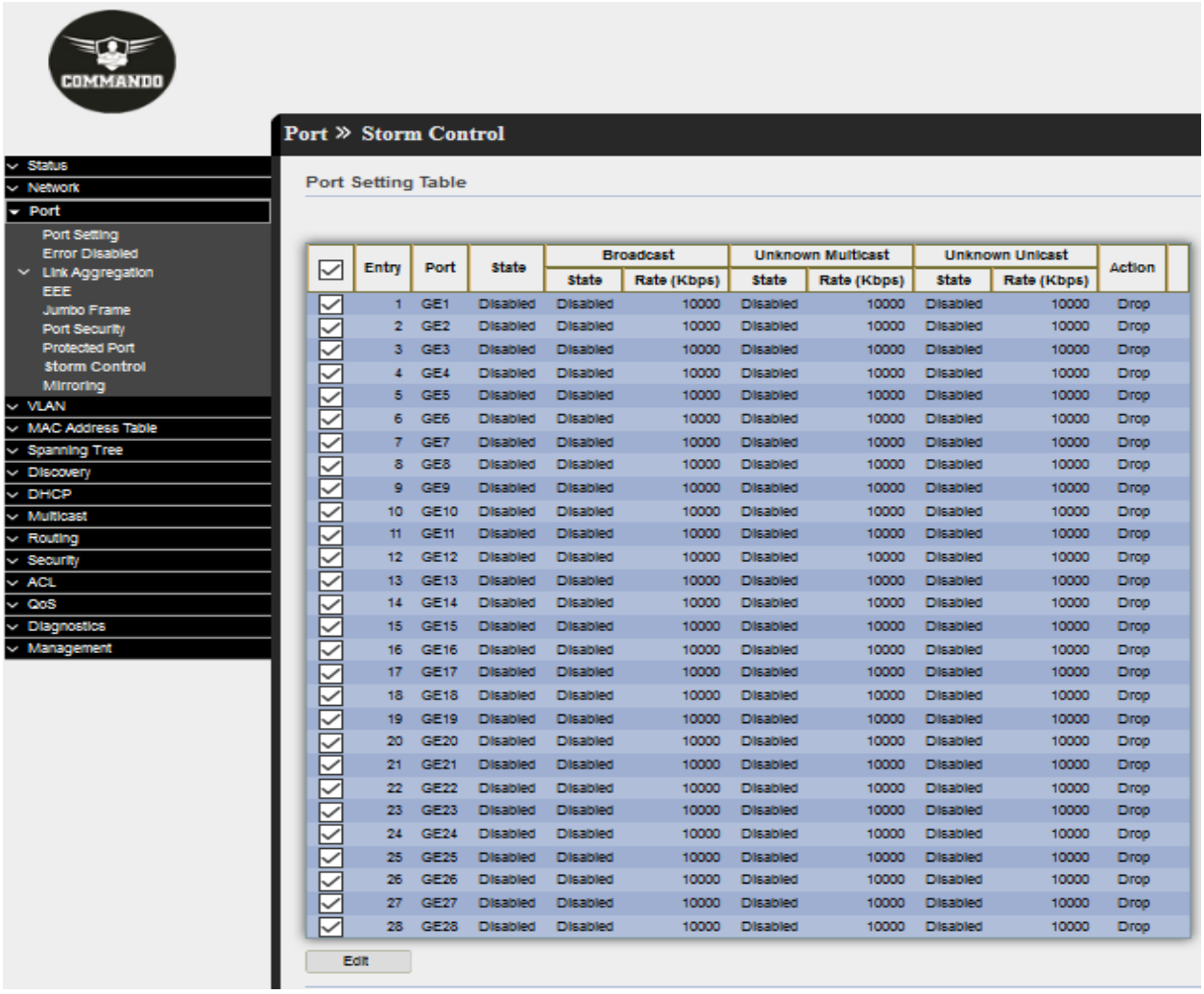


Fig 4.8.2 Storm control Selecting port setting page

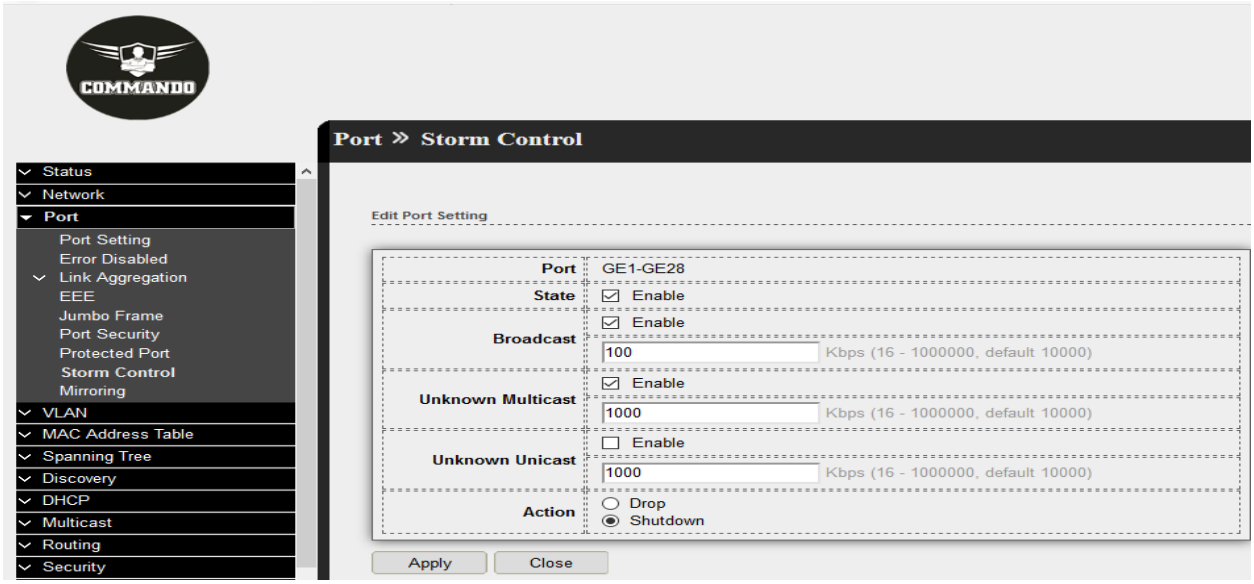


Fig 4.8.3 Storm control Edit port setting page

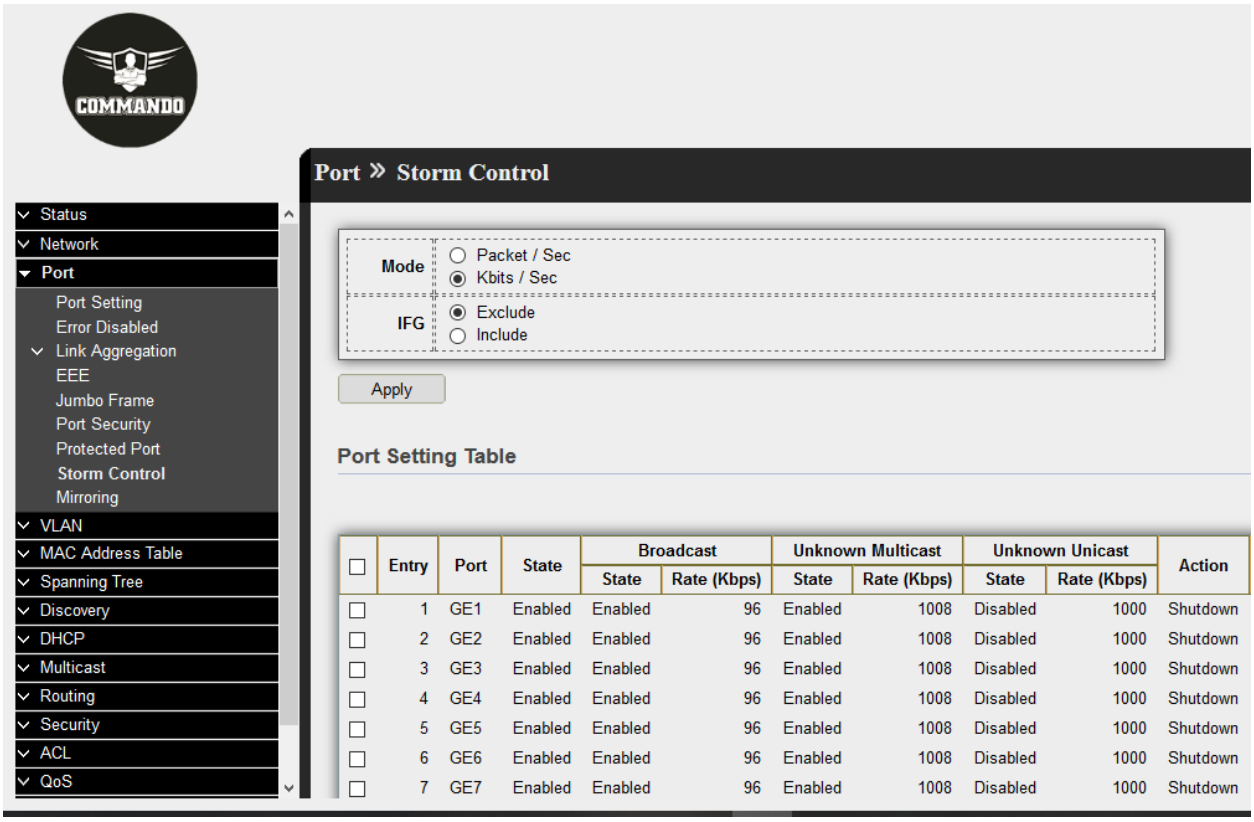


Fig 4.8.4 Storm control port setting selection page

4.9 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.**

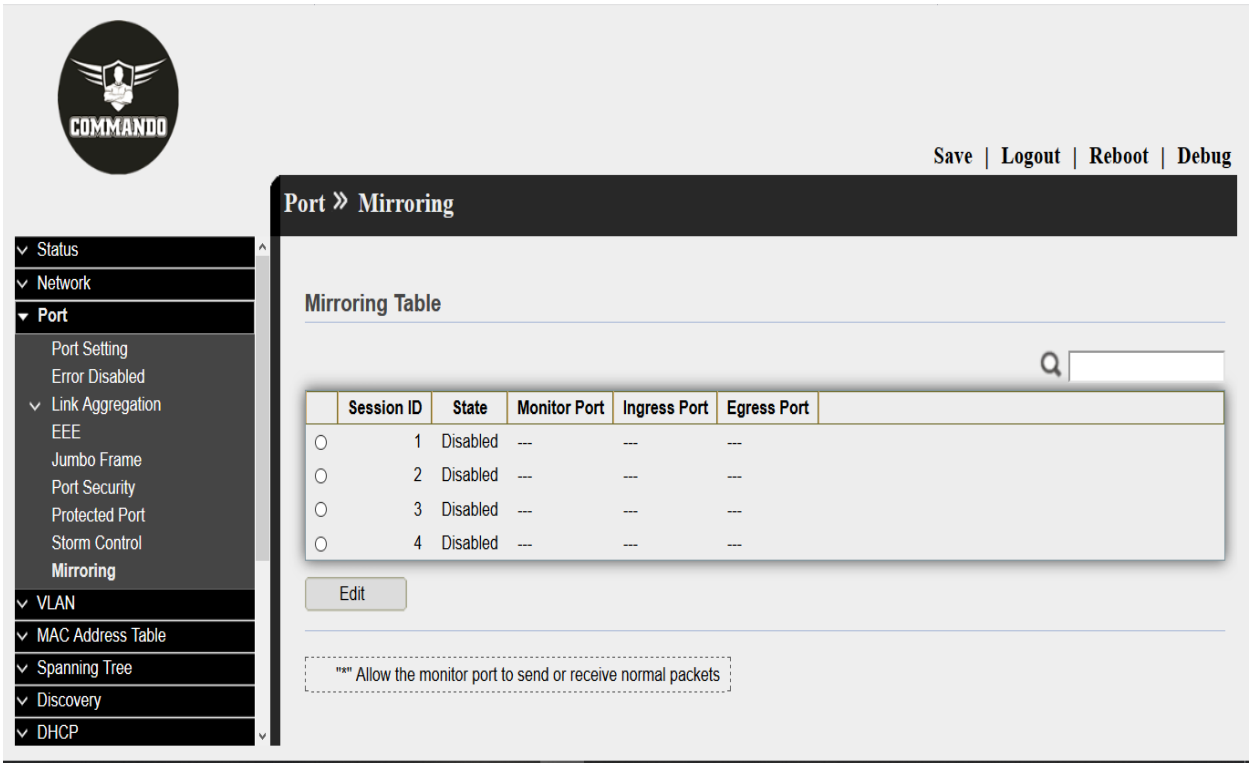


Fig 4.9.1 Mirroring Table page

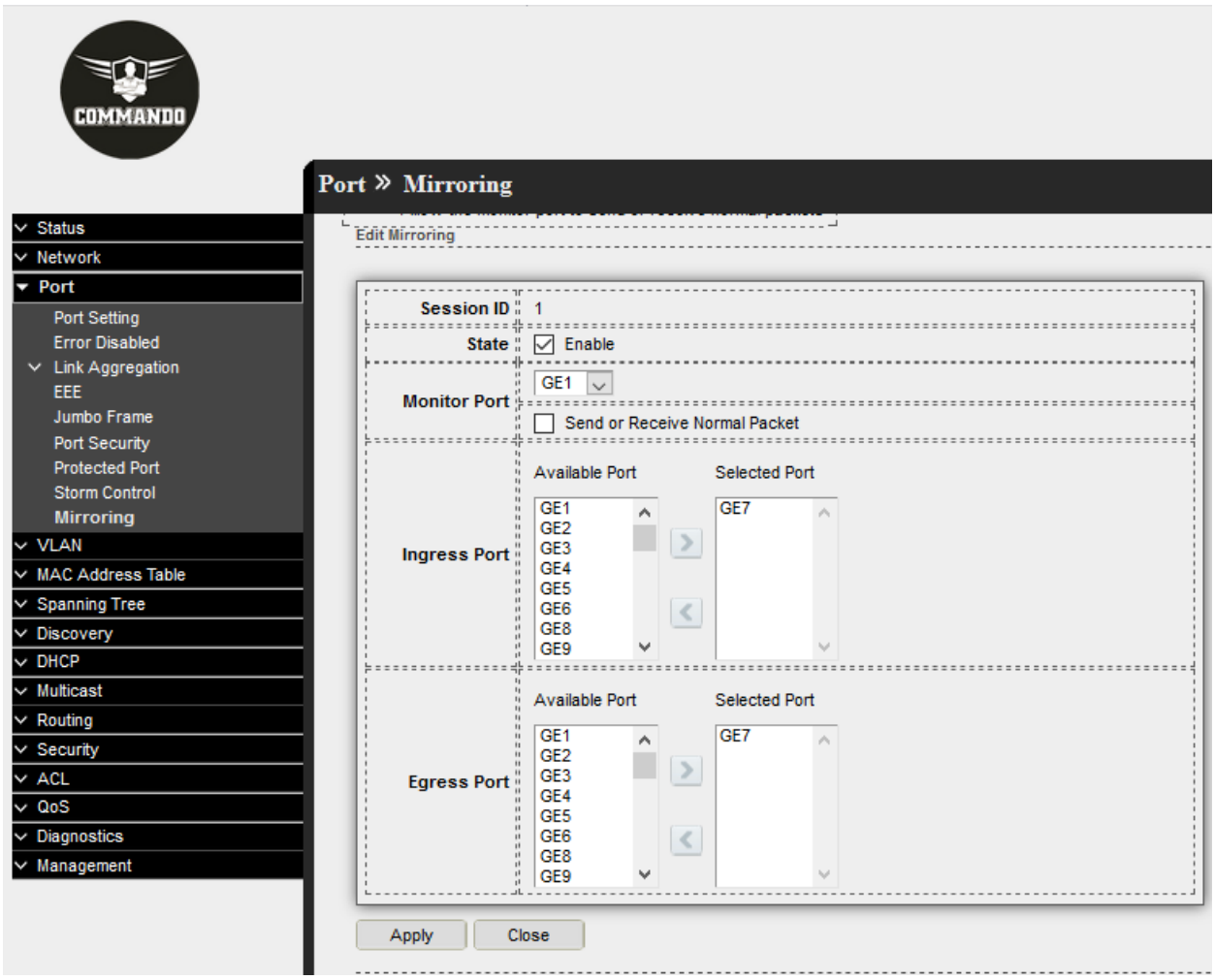


Fig 4.9.2 Edit Port Mirroring page

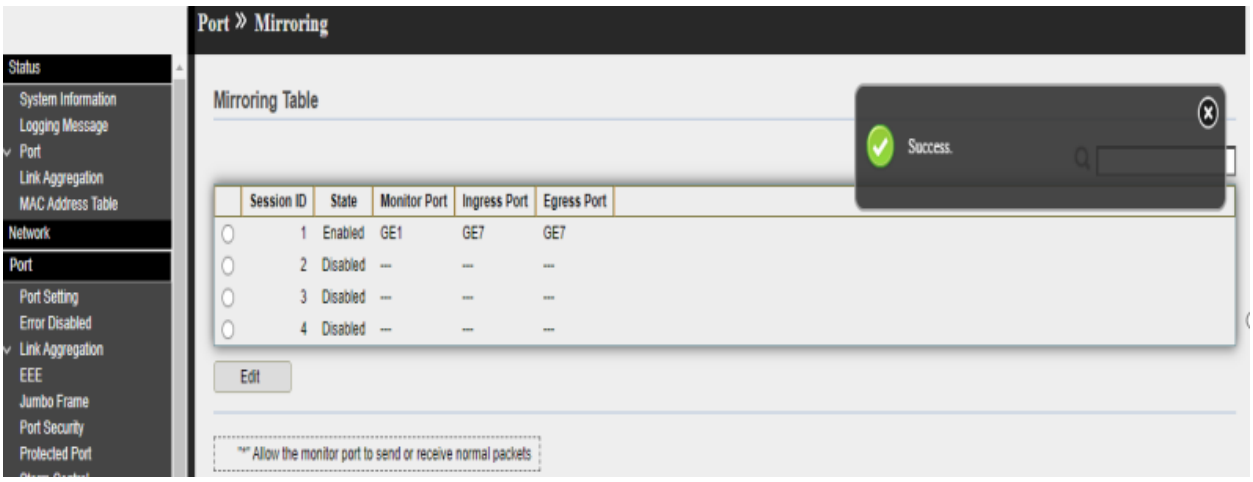


Fig 4.9.3 Mirroring Table after configuring GE1 as monitor port page

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 also 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 perticular 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 C2000 series Switches.

Property -->VLAN configuration for CCTV is very important to protect the IP cameras against unauthorized access and also 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**

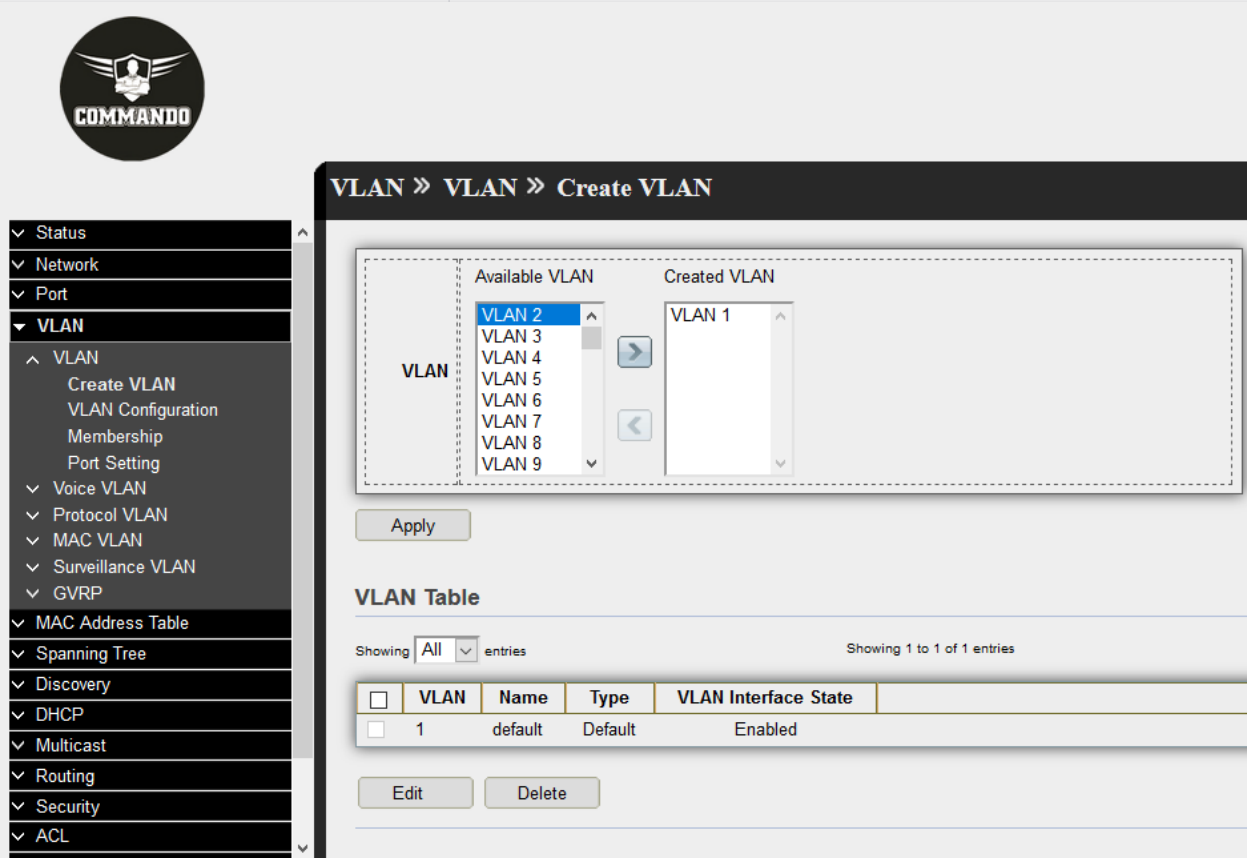


Fig 5.1.1 Create VLAN Default Page

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”.

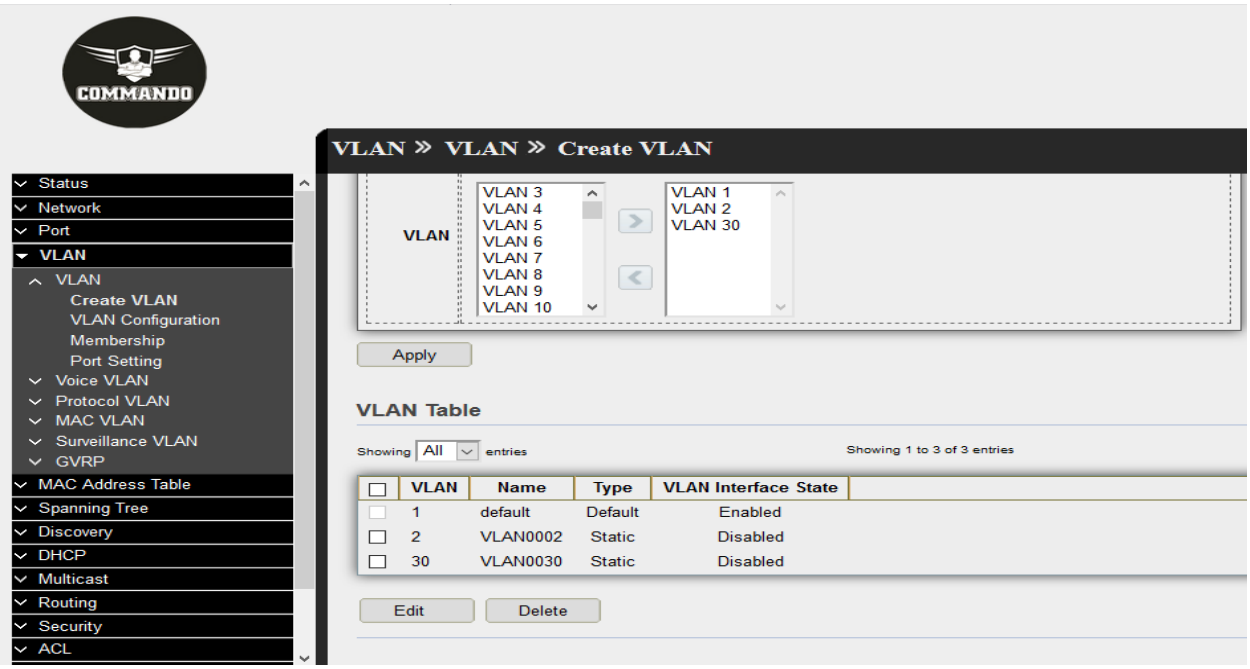


Fig 5.1.2 VLAN Page after VLAN creation

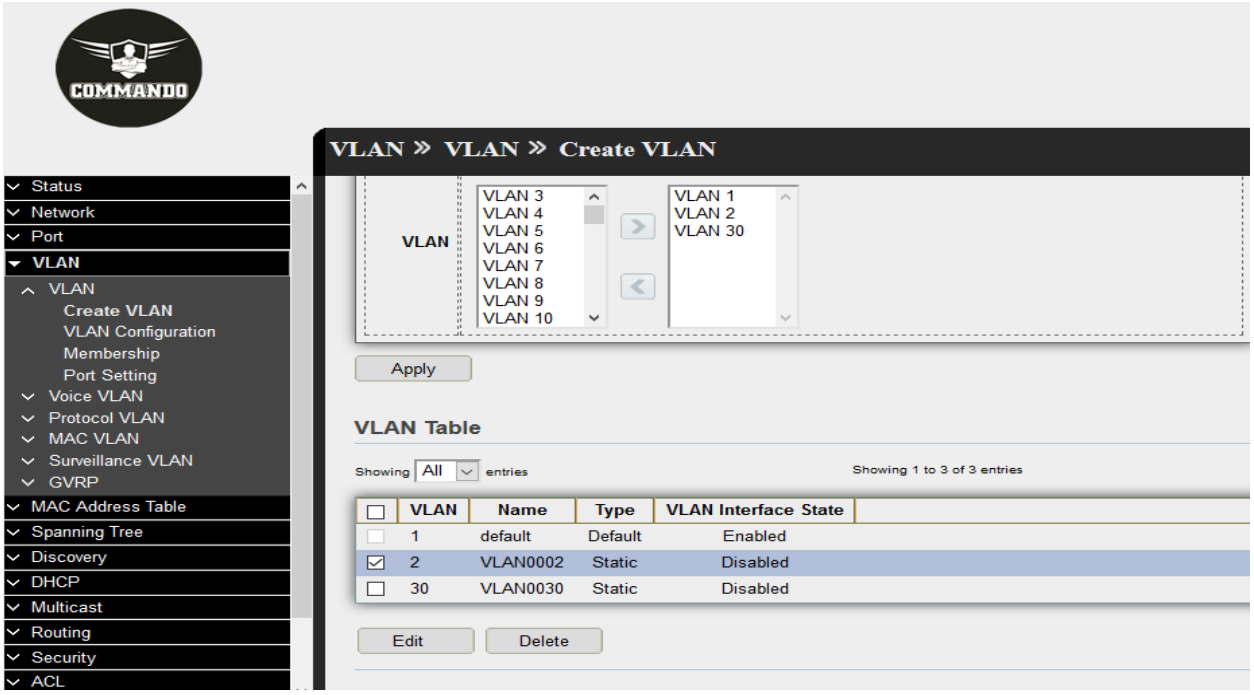


Fig 5.1.3 VLAN Default name after VLAN creation

Fig 5.1.4 Edit VLAN name after VLAN creation

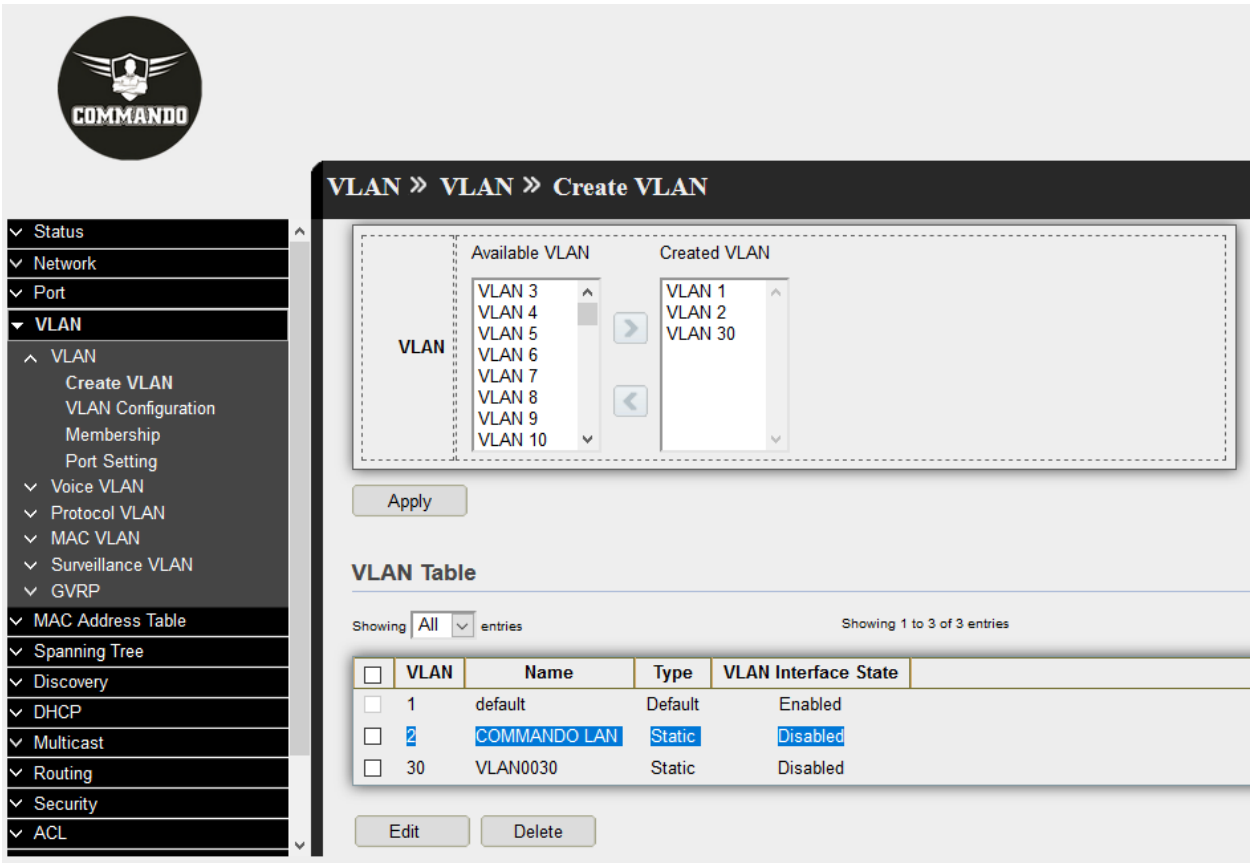


Fig 5.1.5 Vlan Table after VLAN name change page

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”.

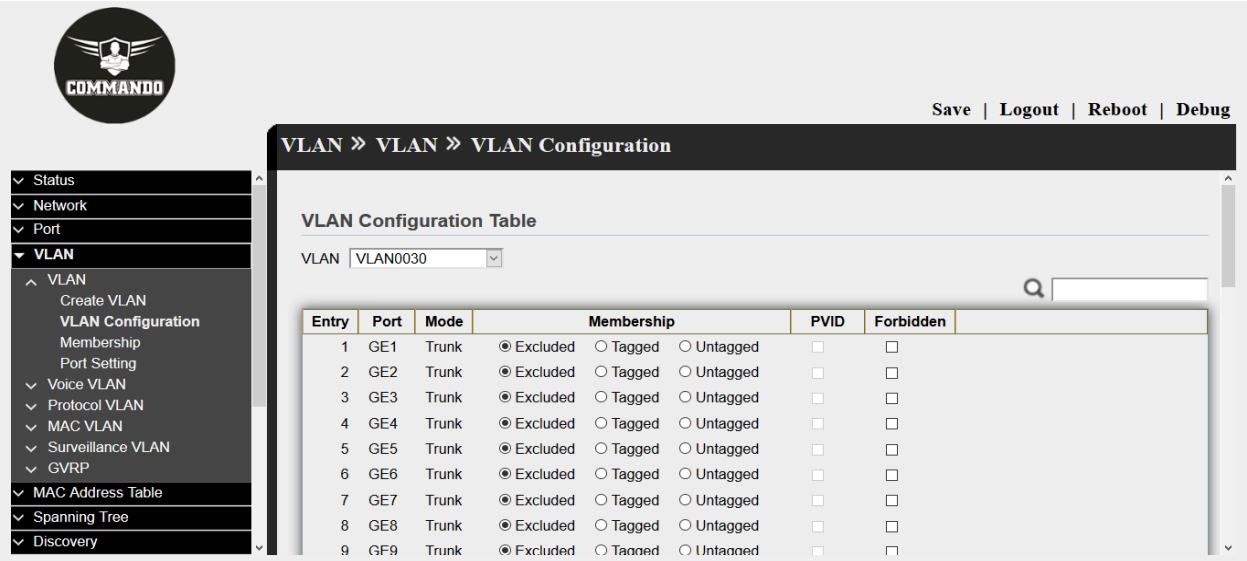


Fig 5.1.6 VLAN configuration table page

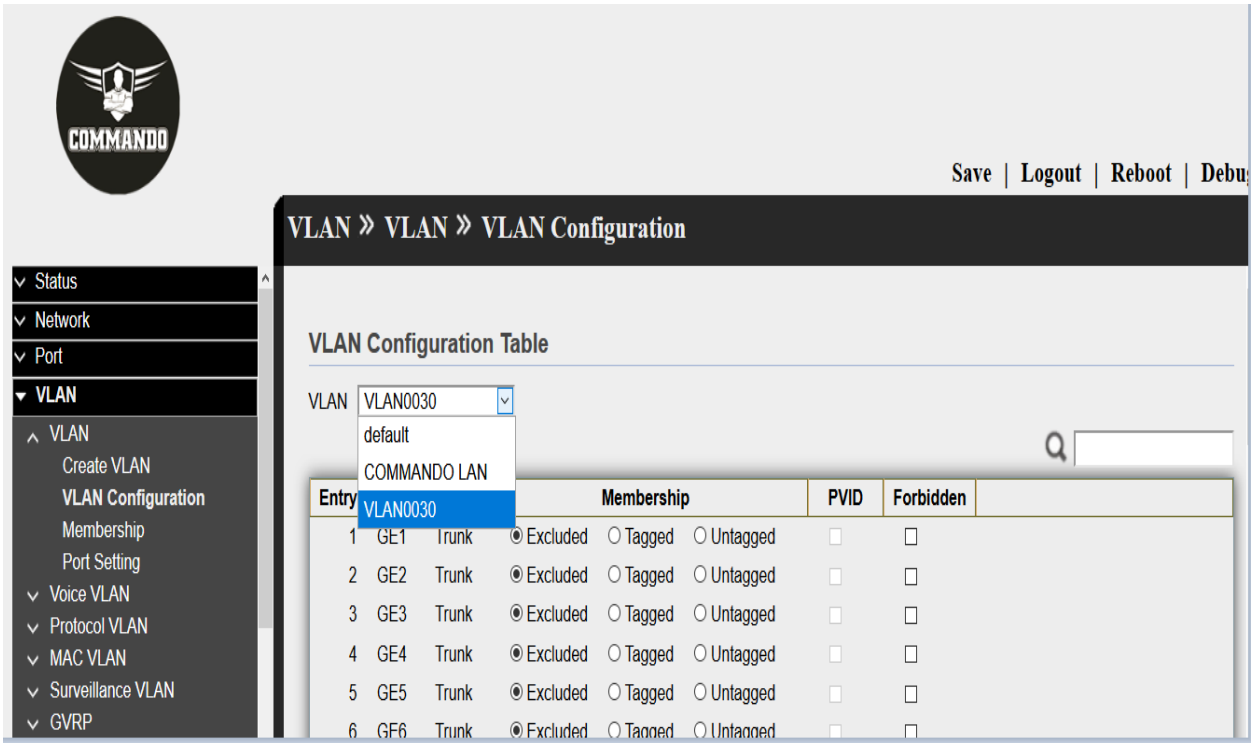


Fig 5.1.8 VLAN Selection tap on VLAN configuration table page

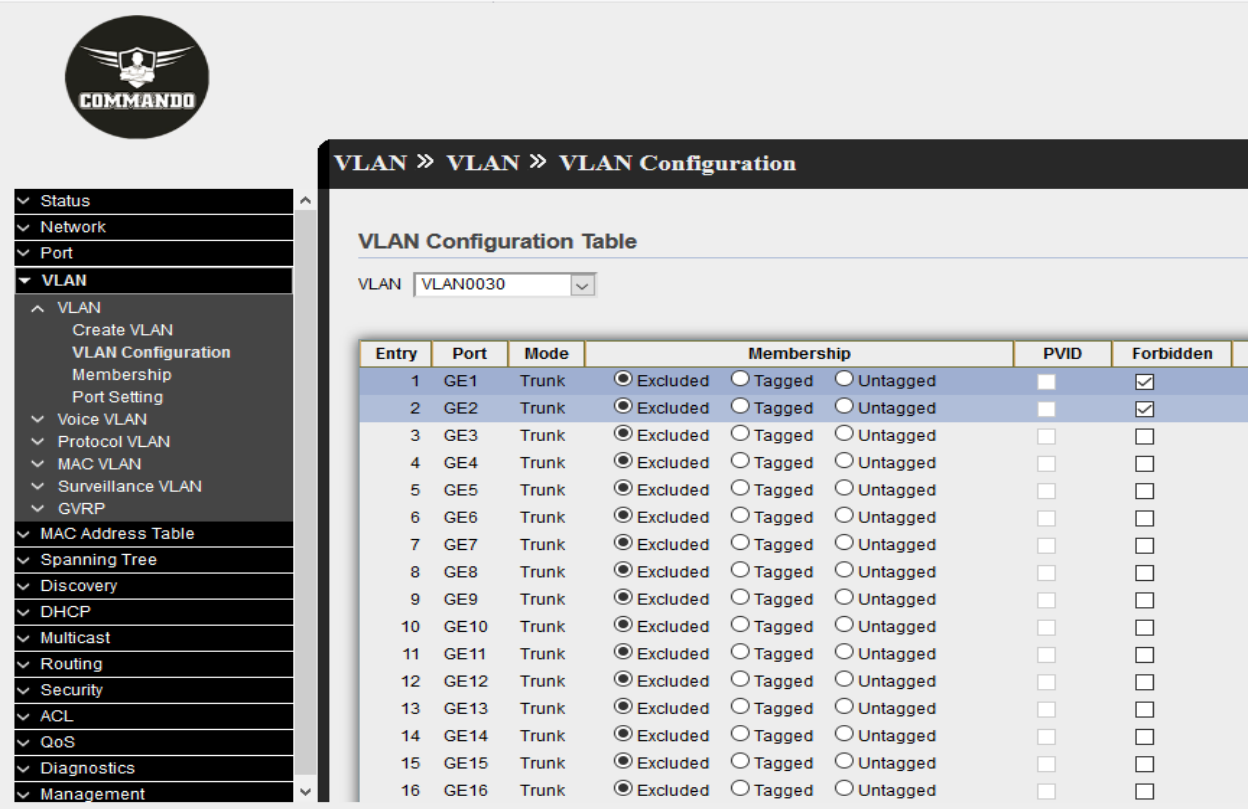


Fig 5.1.9 VLAN configuration for Ports selection page

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**

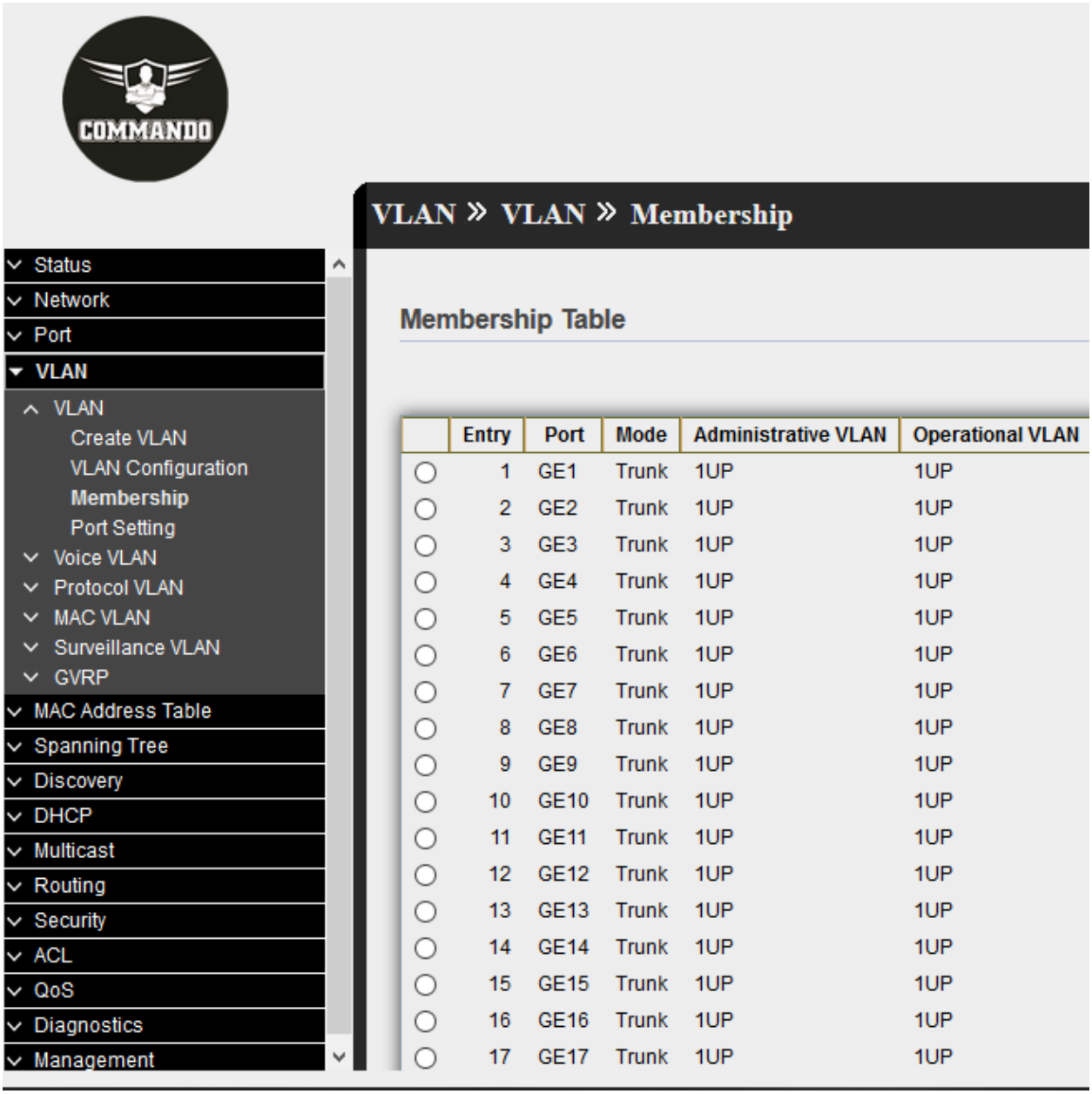


Fig 5.1.10 Default VLAN Membership table showing all having members of Vlan 1 page

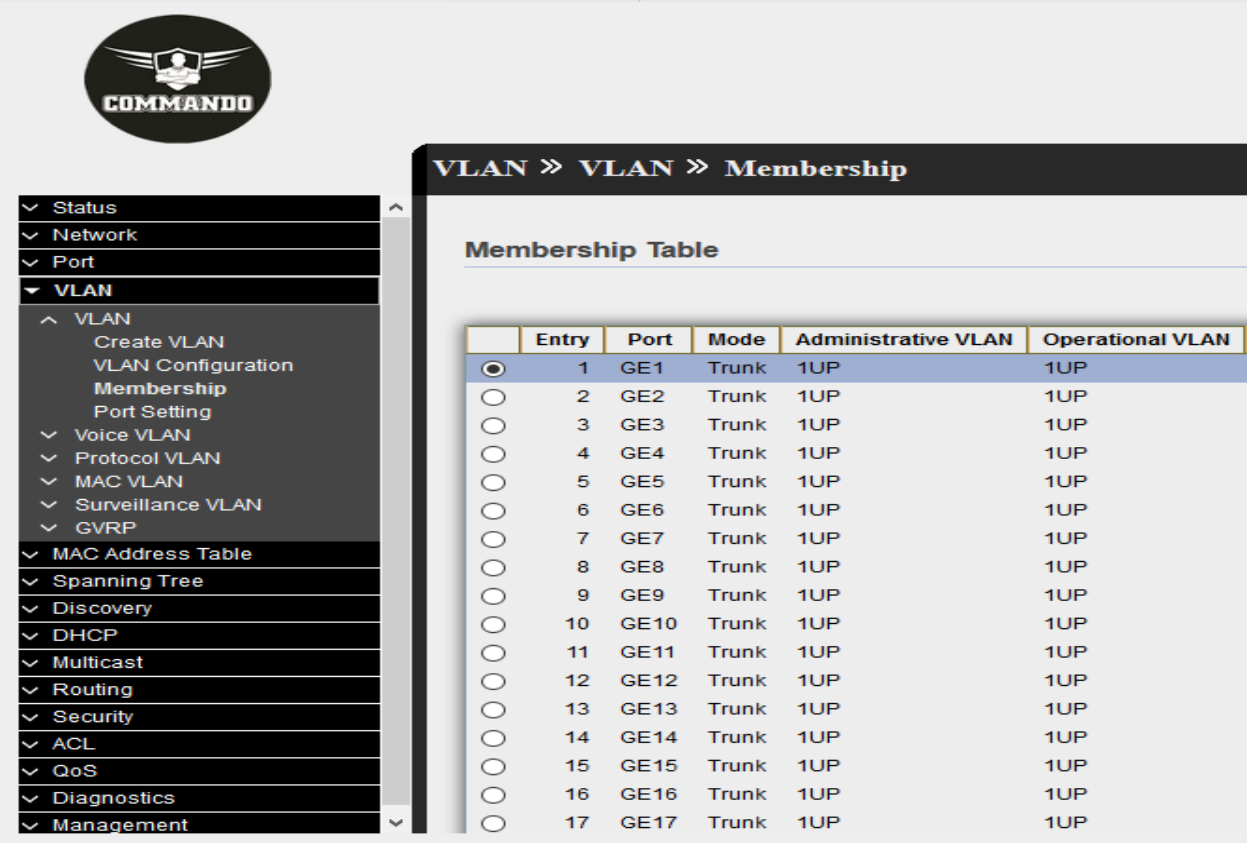


Fig 5.1.11 VLAN membership to be changed for selected port GE1 page

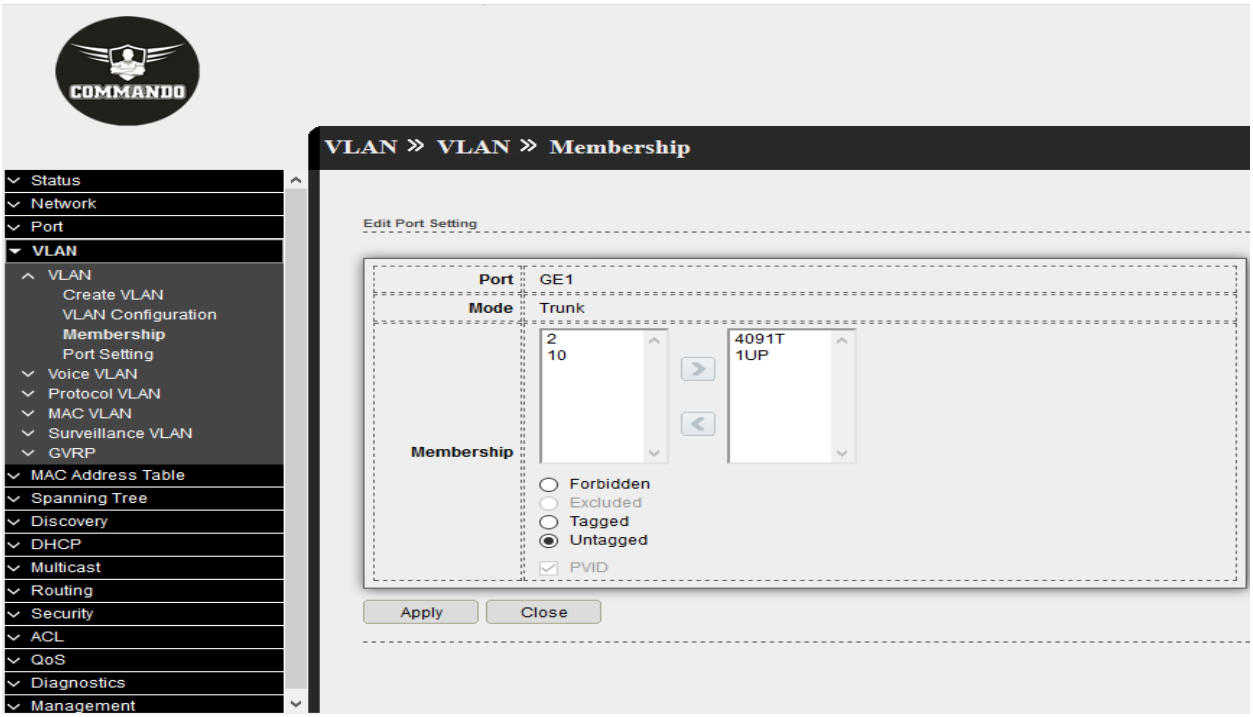


Fig 5.1.12 Edit VLAN membership for slected port GE1 page

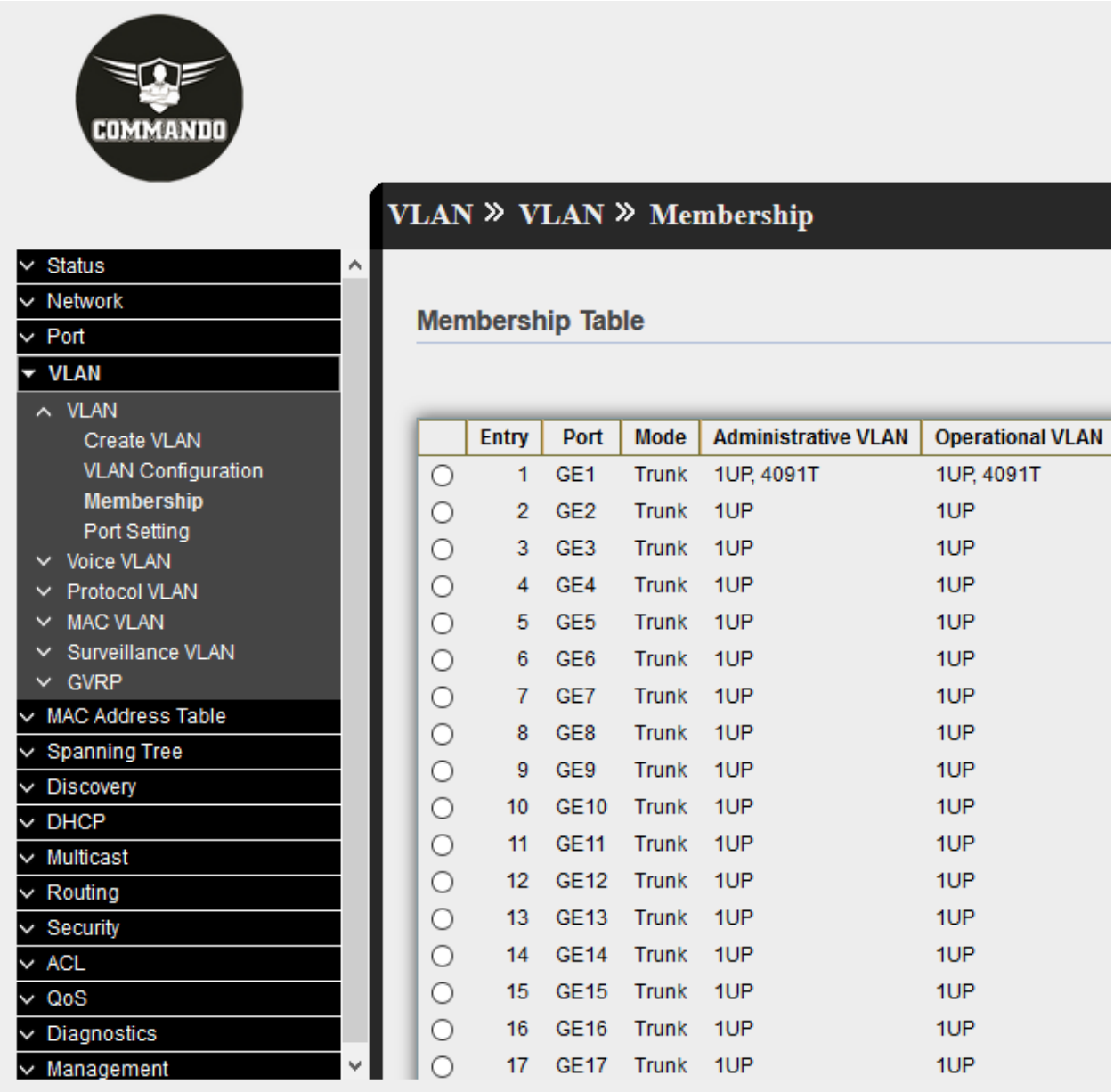


Fig 5.1.13 VLAN 4091 membership for Port GE1 table page

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**

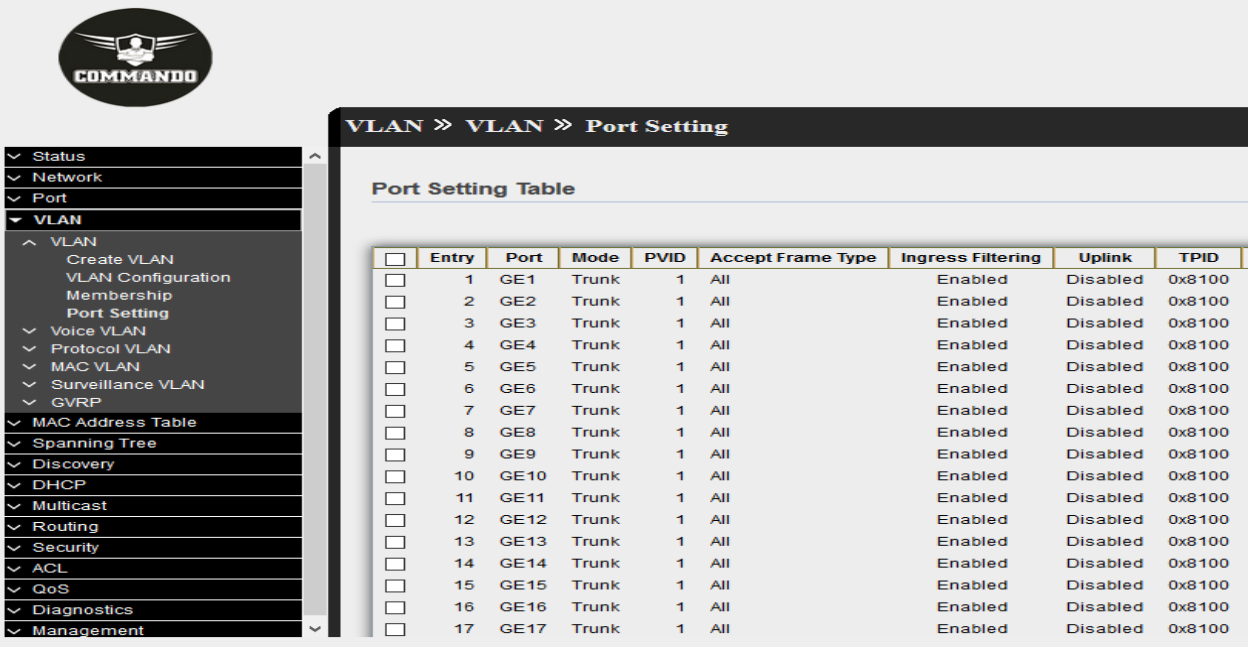


Fig 5.1.14 VLAN port setting table page

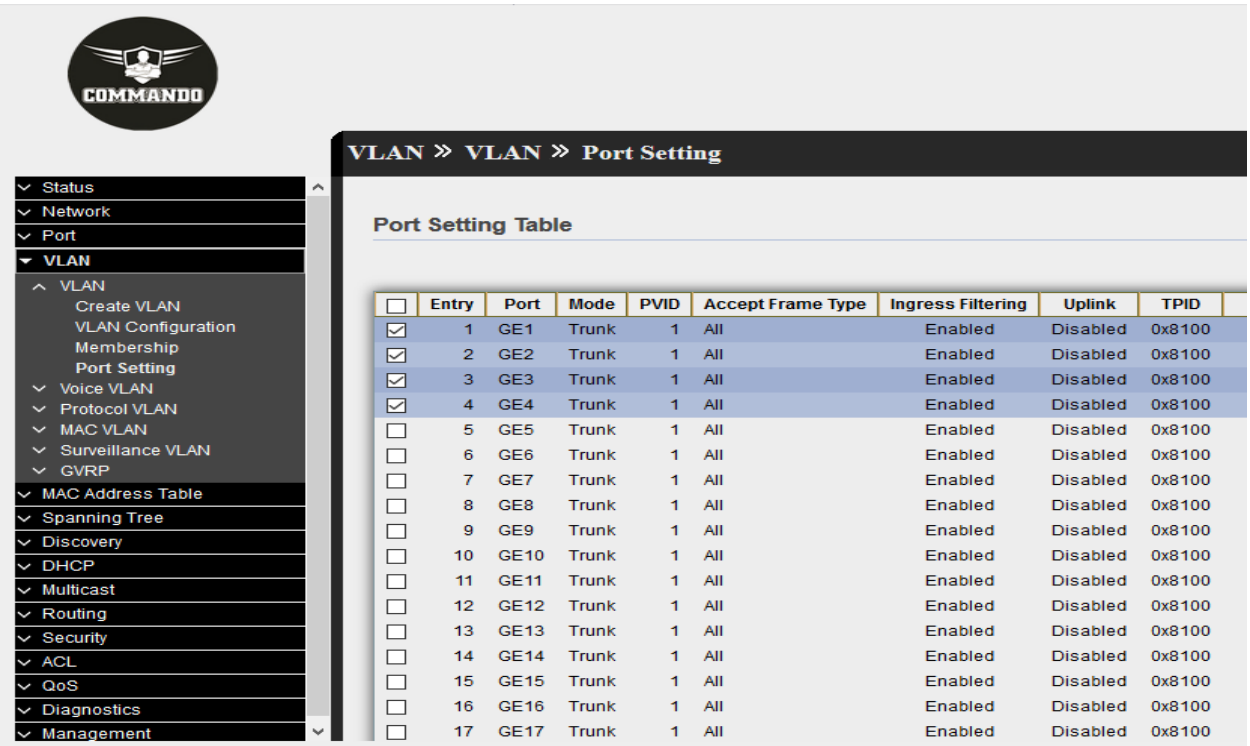


Fig 5.1.15 VLAN port setting for selected port page

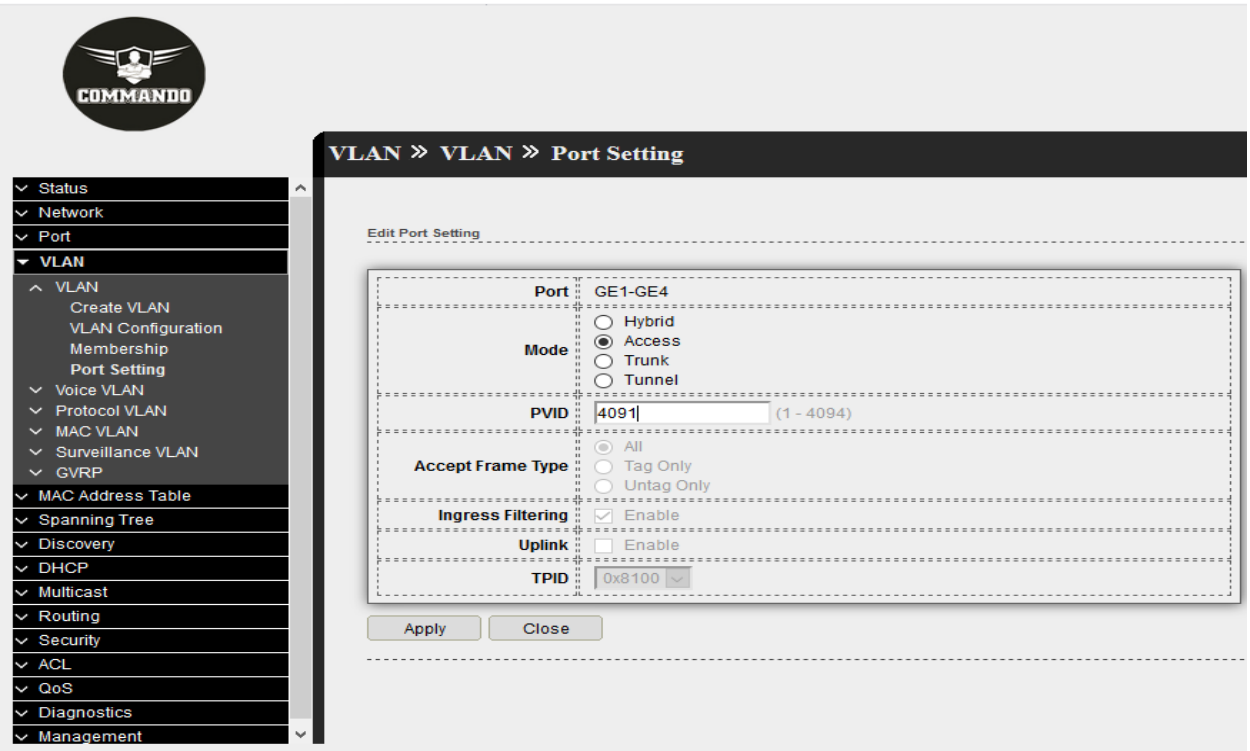


Fig 5.1.16 Edit port setting for selected ports page

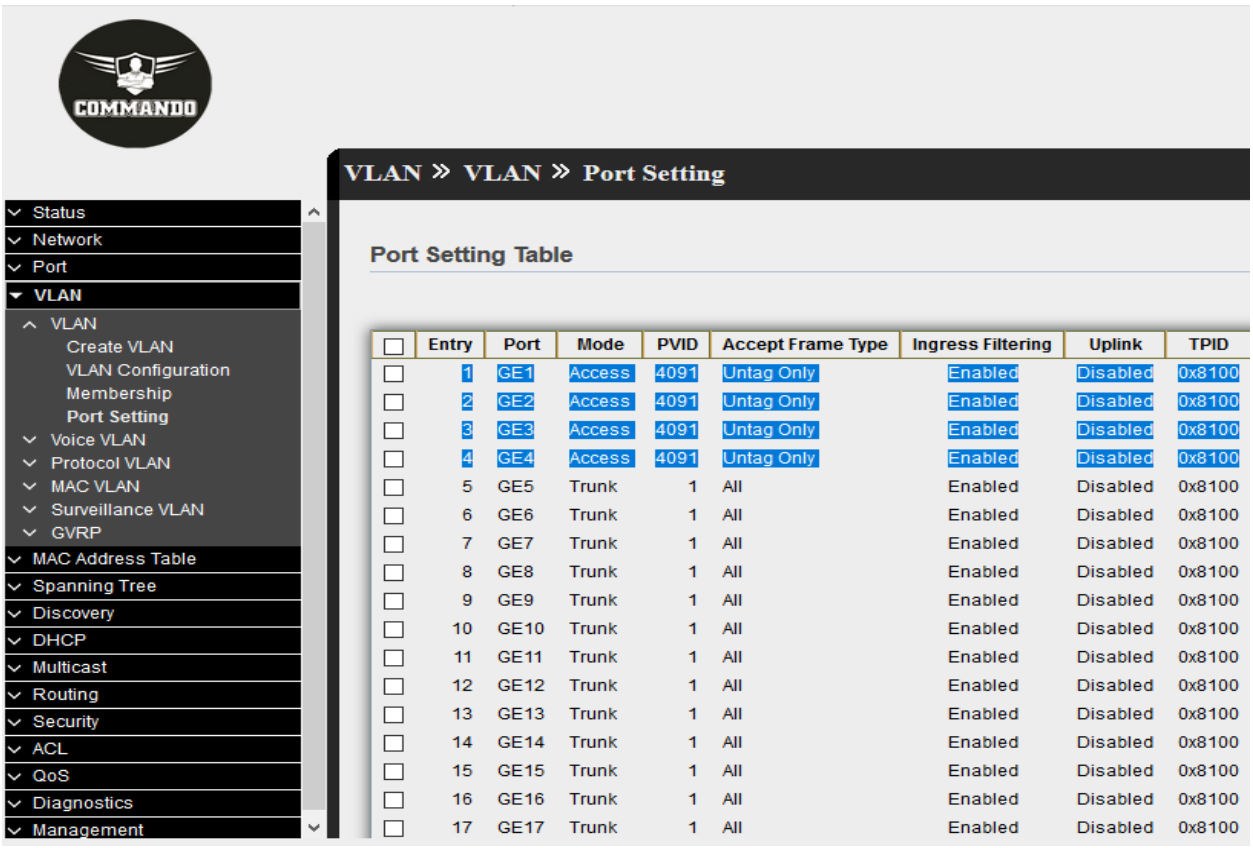


Fig 5.1.17 After Editing port setting for selected ports page

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 response 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.

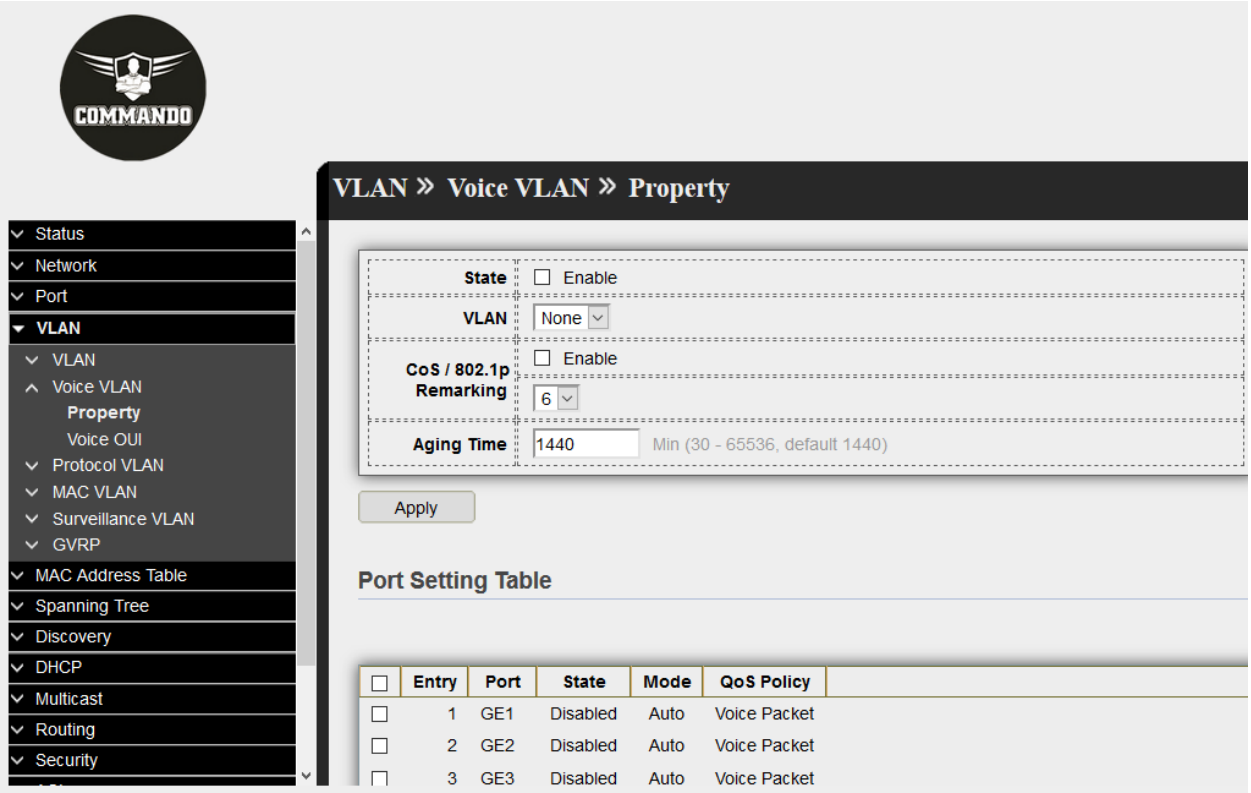


Fig 5.2.1 Default Voice VLAN state setting table page

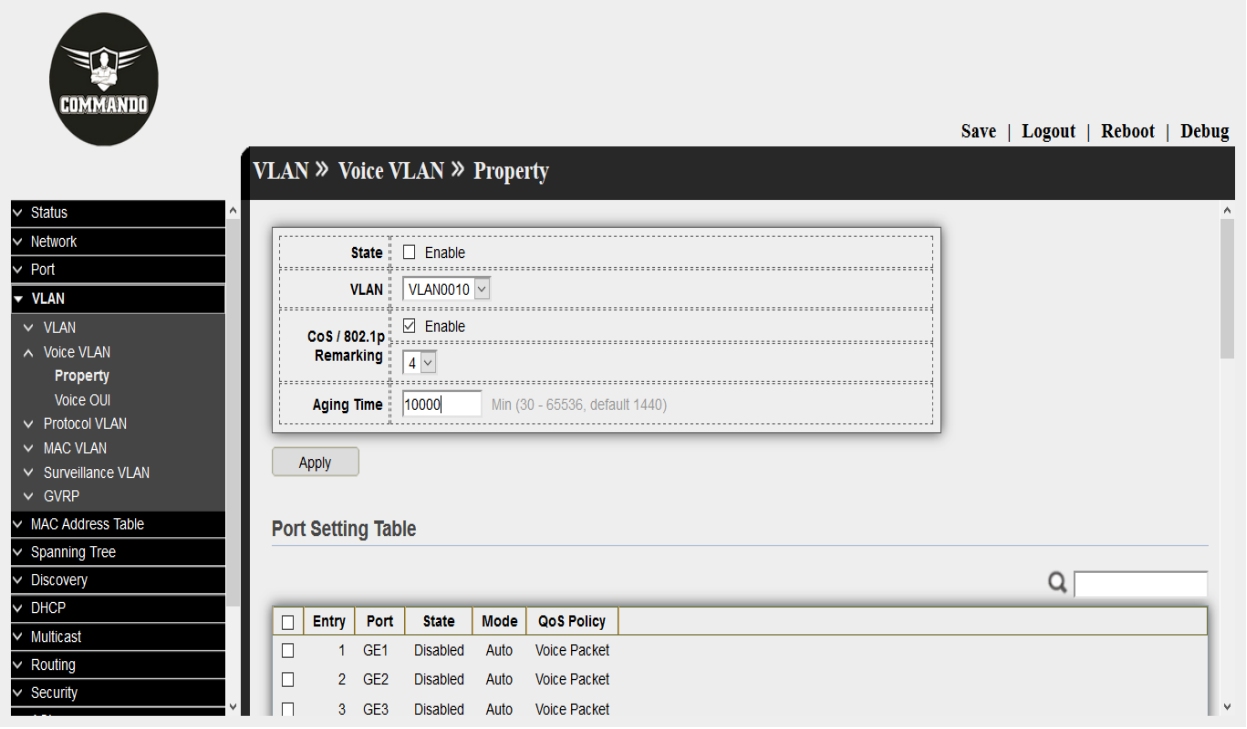


Fig 5.2.2 Changeing Voice VLAN setting CoS/802.1p Remarking page

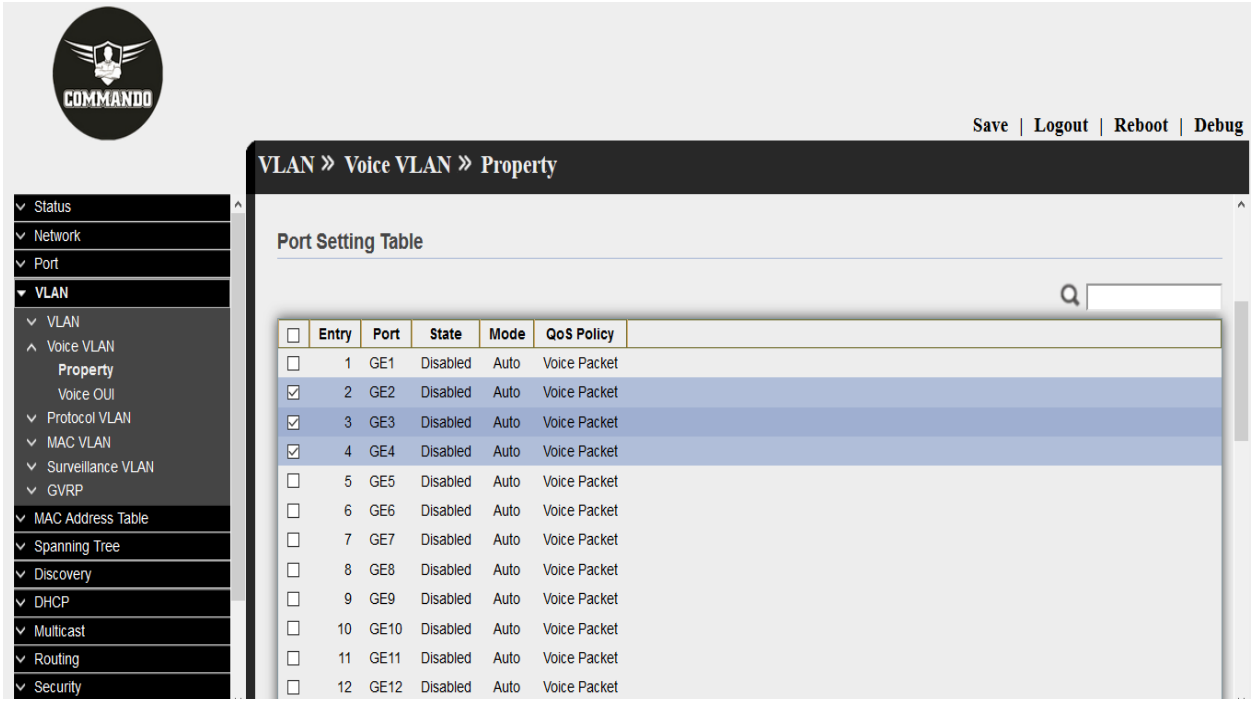


Fig 5.2.3 Voice VLAN setting CoS/802.1p Remarking page

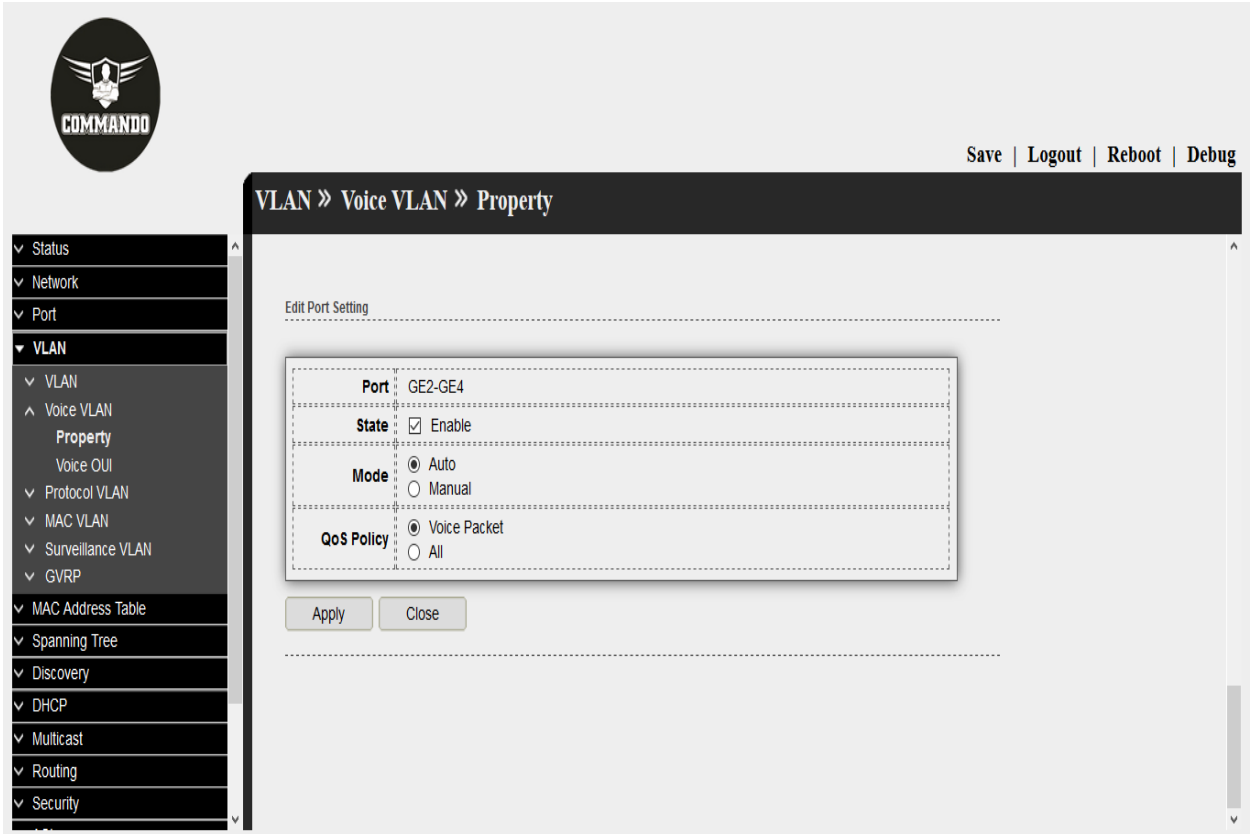


Fig 5.2.4 Voice VLAN Edit port setting page

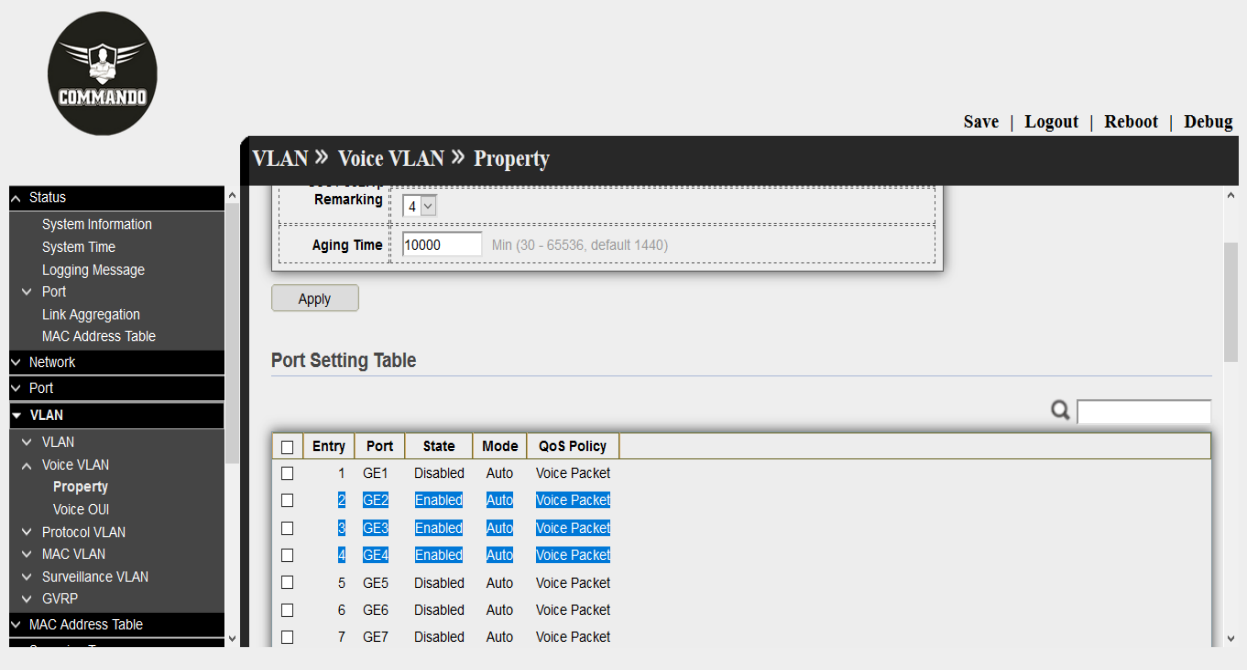


Fig 5.2.5 Voice VLAN Port setting table page

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 smartport to dynamically add the ports to the voice VLAN.

This page allow user to add, edit or delete OUI MAC addresses. Default has 8 pre□defined 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.**

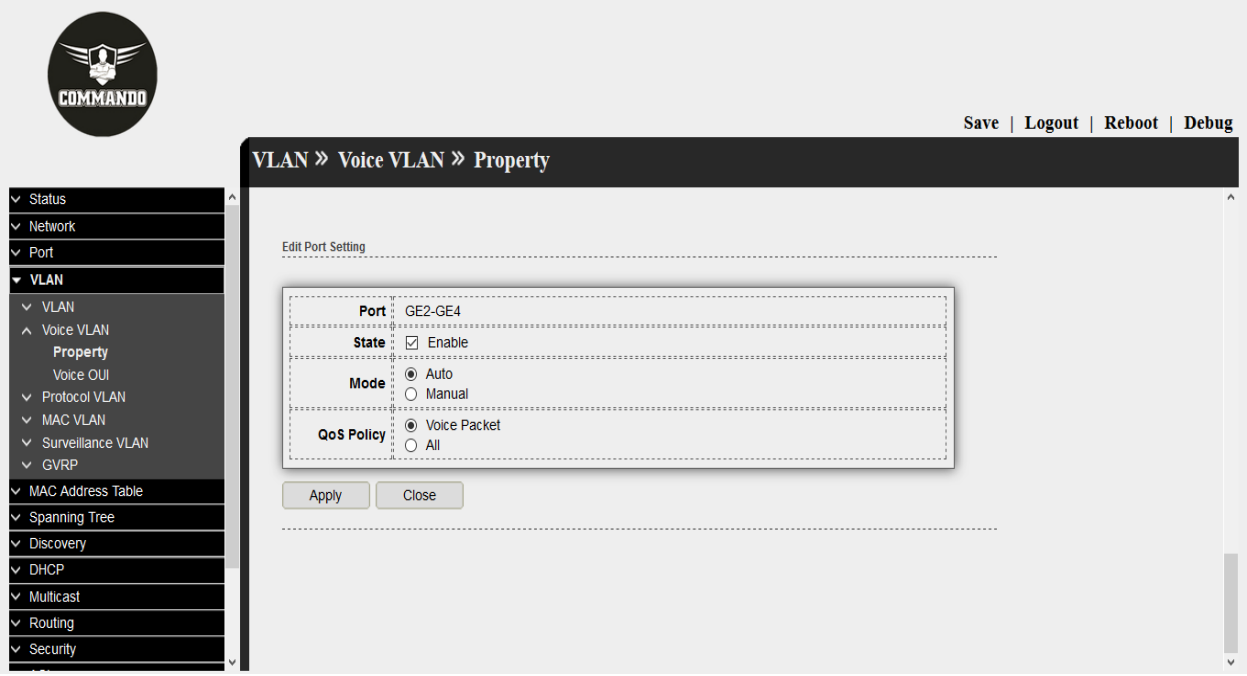


Fig 5.2.6 Voice VLAN Voice OUI Table page

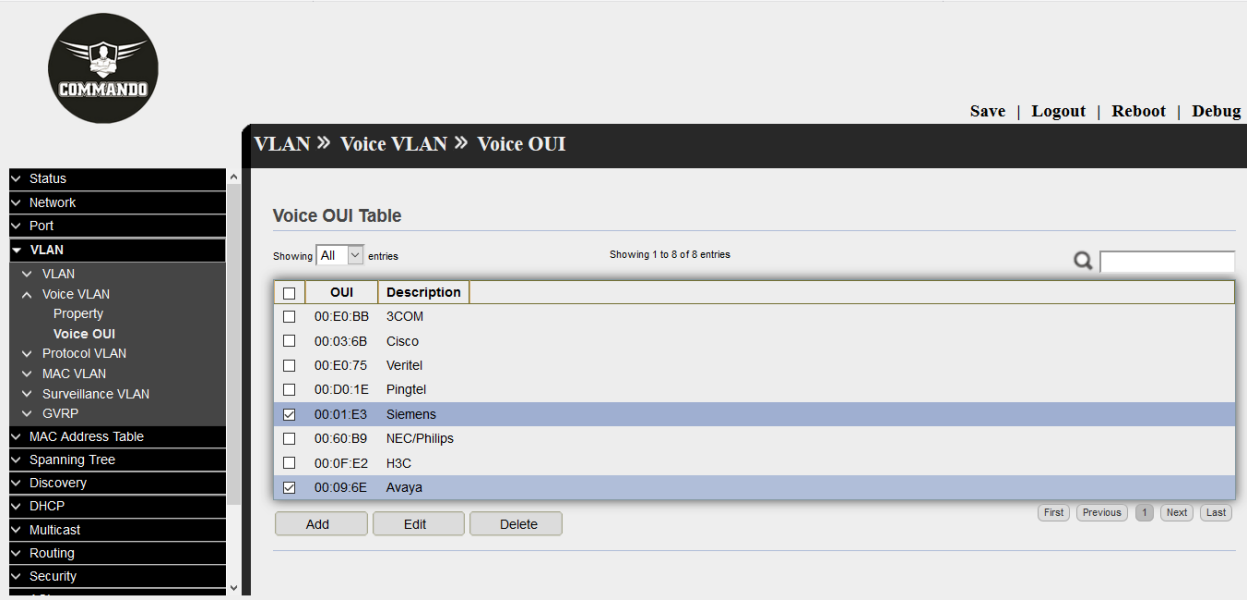


Fig 5.2.7 Selecting Voice VLAN Voice OUI page

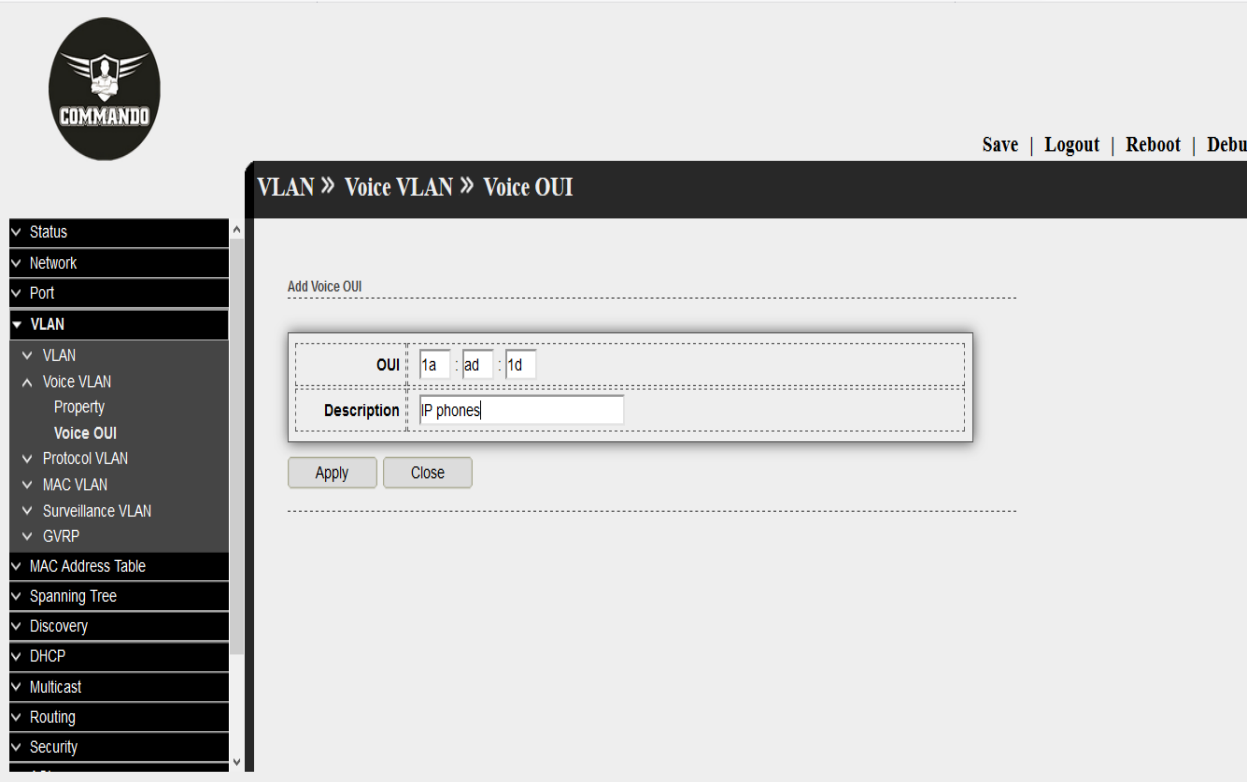


Fig 5.2.8 Voice VLAN Add Voice OUI page

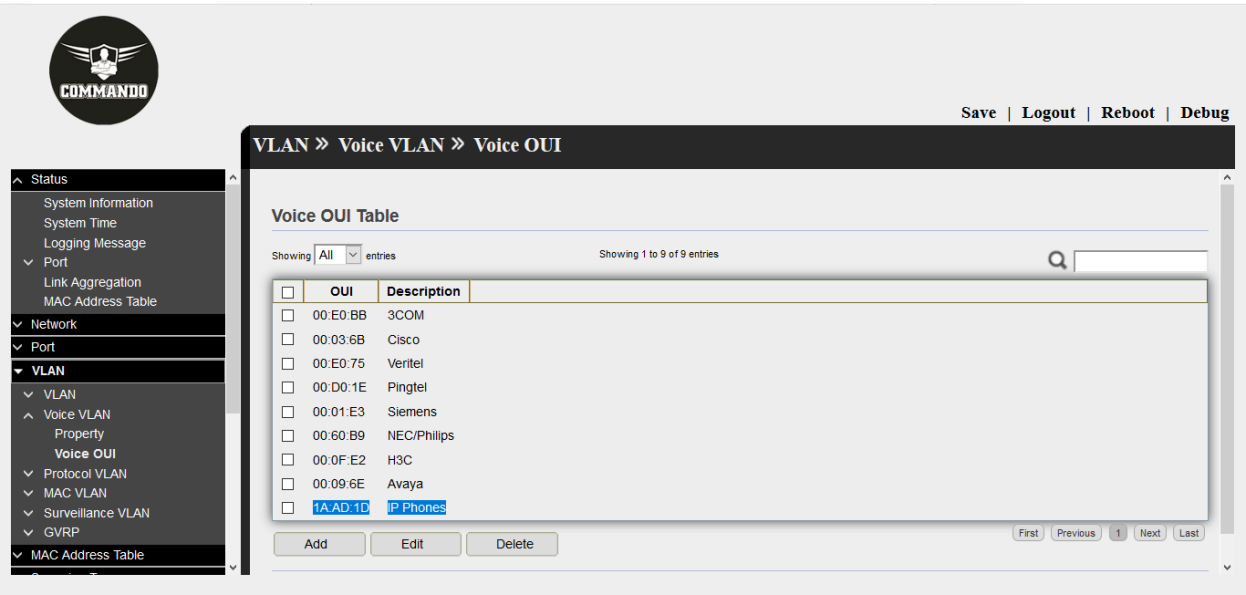


Fig 5.2.9 Voice VLAN Voice OUI Table page

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.**

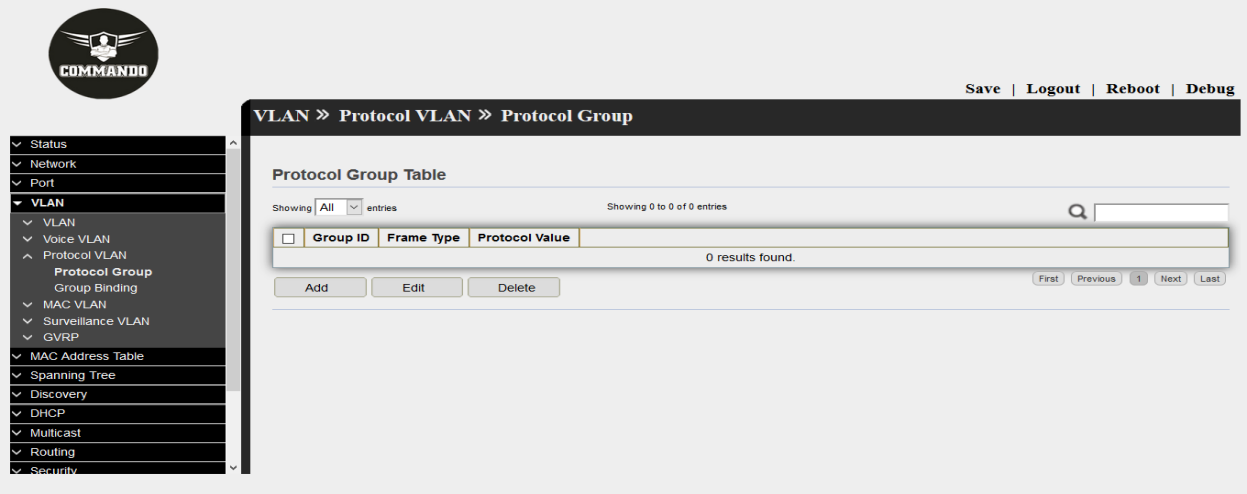


Fig 5.3.1 Default Protocol VLAN Protocol Group Table page

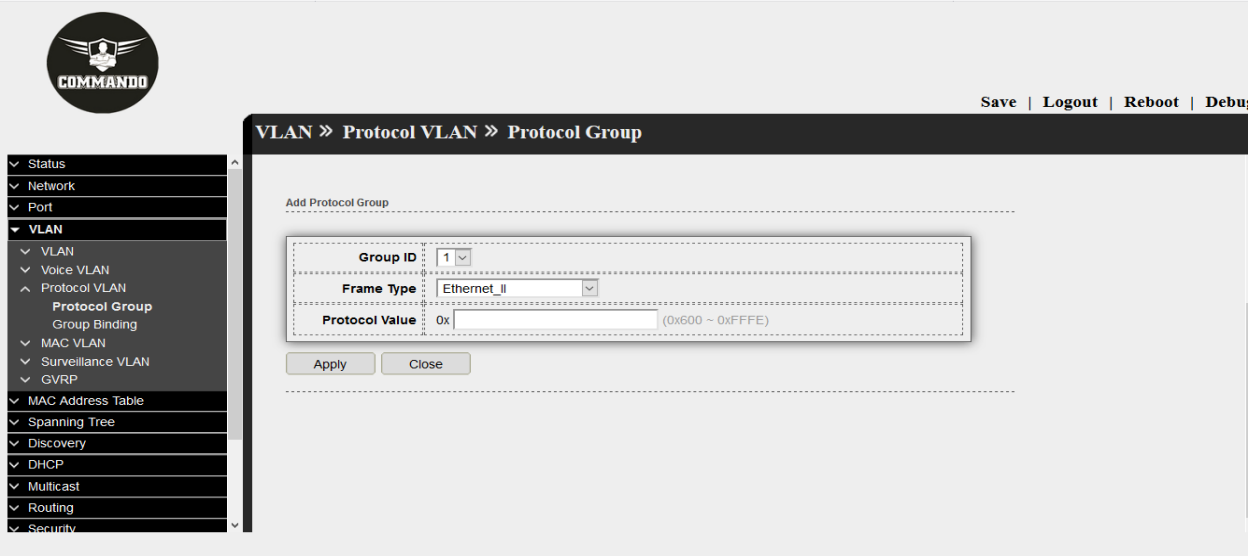


Fig 5.3.2 Add Protocol group page

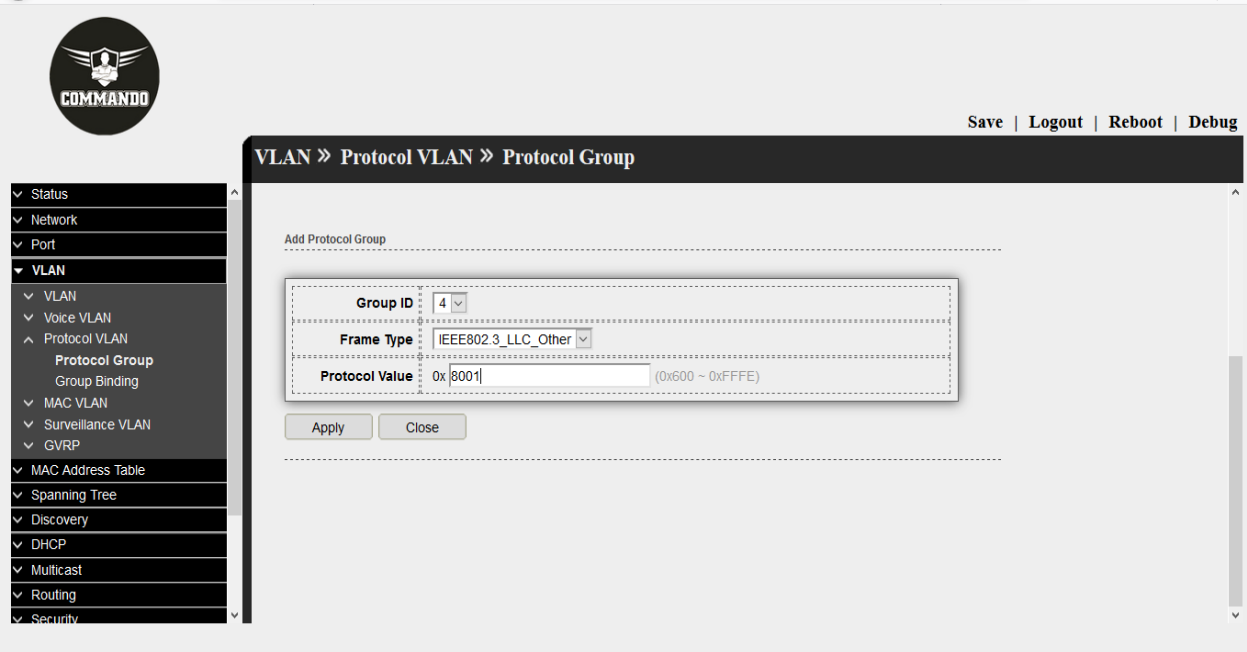


Fig 5.3.3 Protocol Group Table page

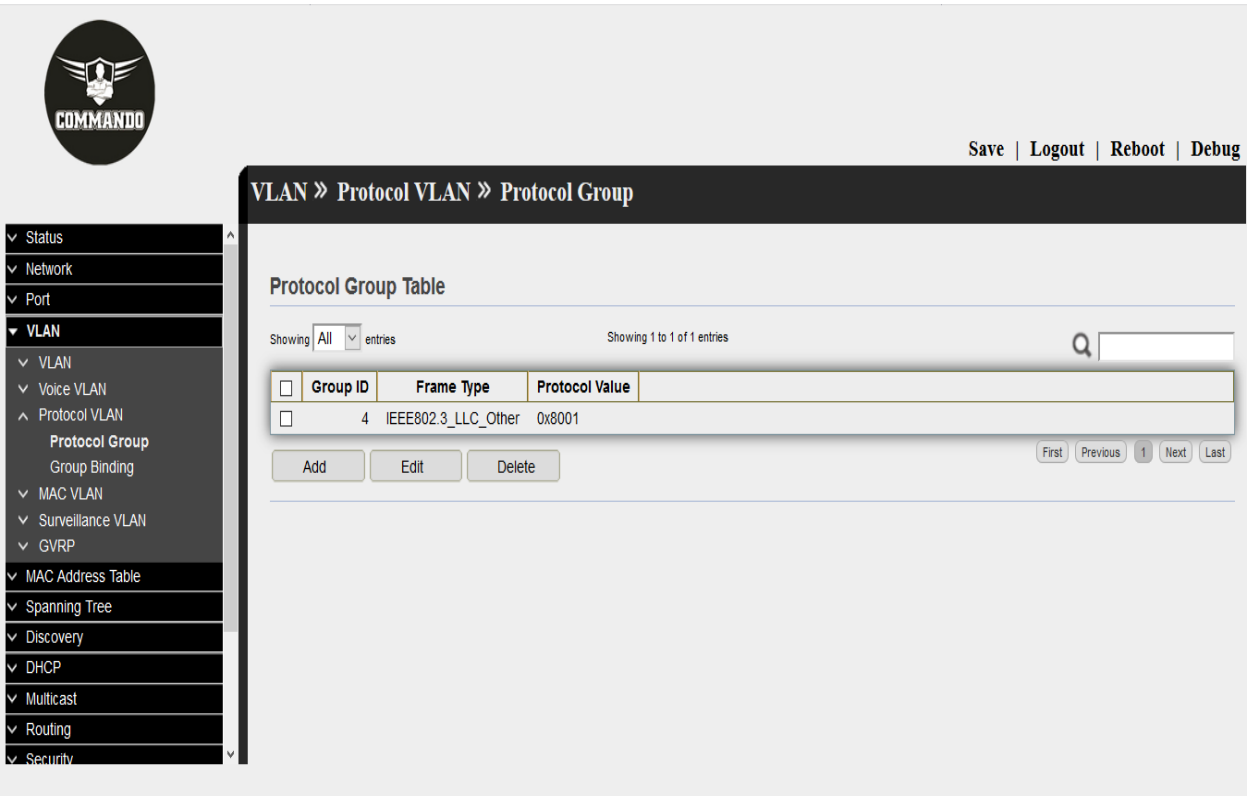


Fig 5.3.4 Protocol group table page

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.**

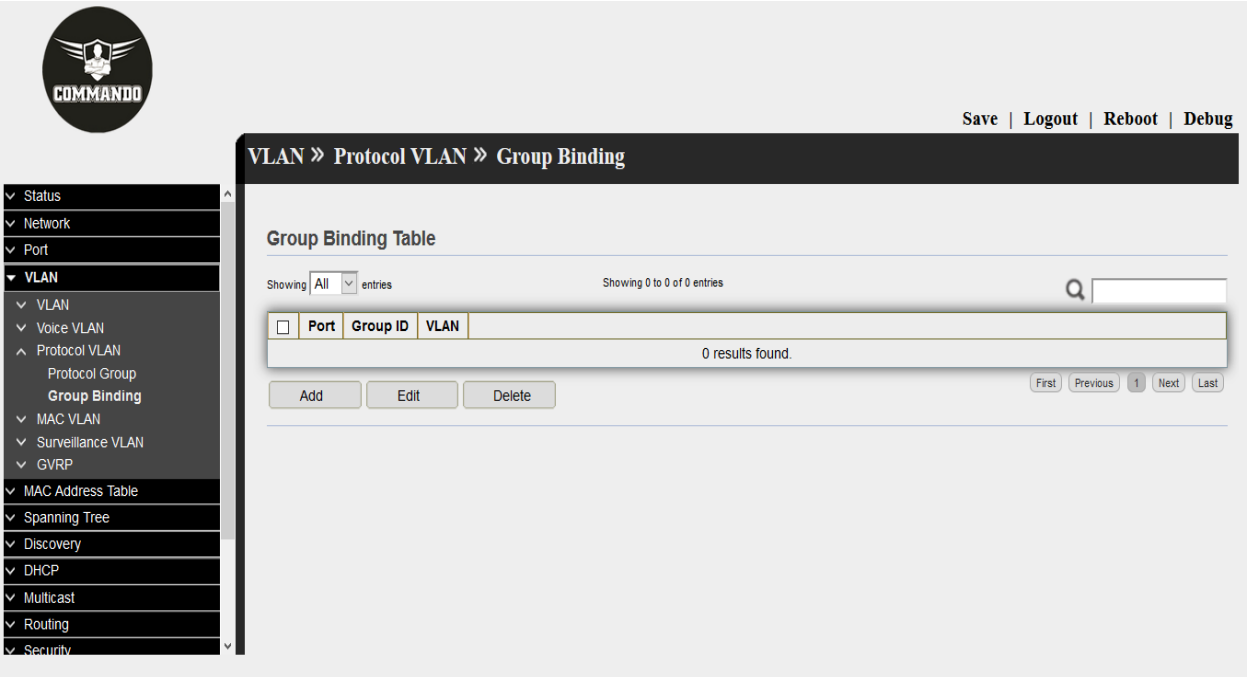


Fig 5.3.5 Default Group Binding Table page

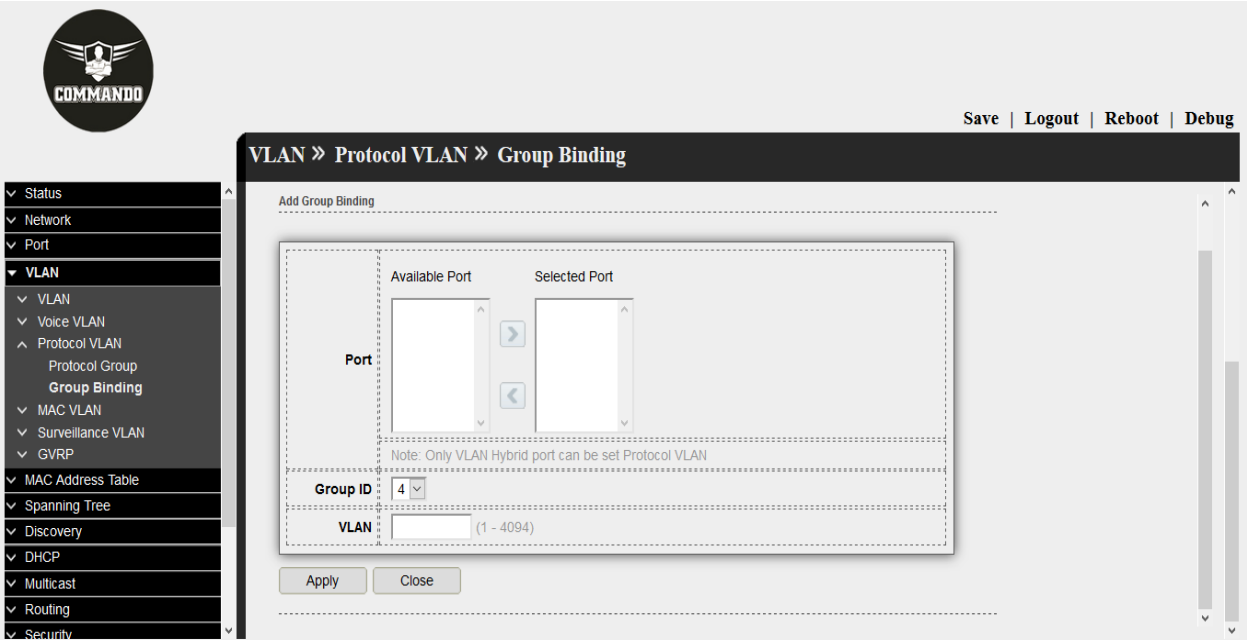


Fig 5.3.5 Add Group Binding page

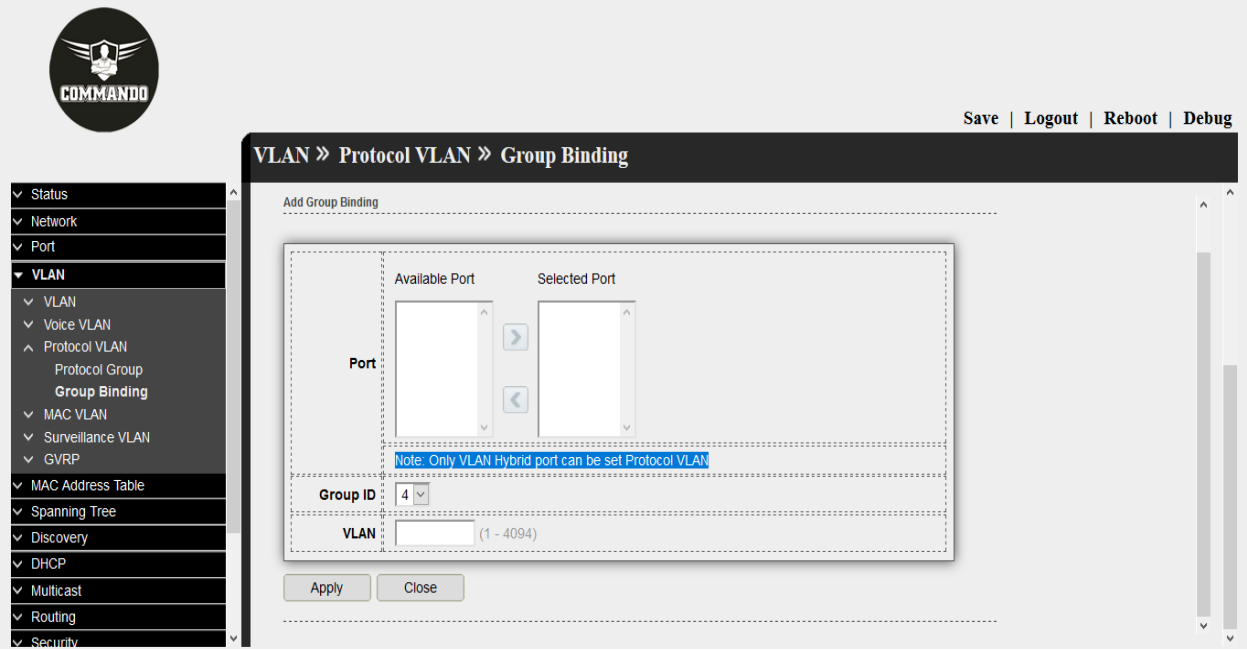


Fig 5.3.7 Group Binding for hybrid port page

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.

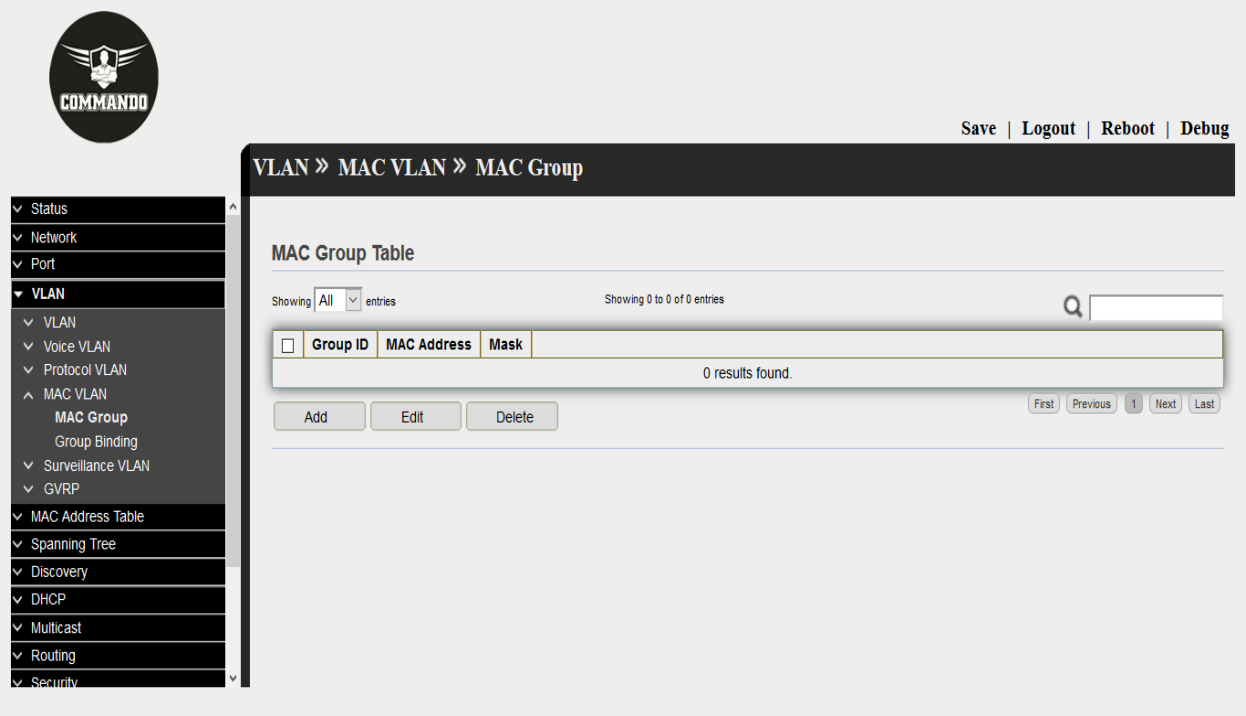


Fig 5.4.1 Default MAC Group Table page

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

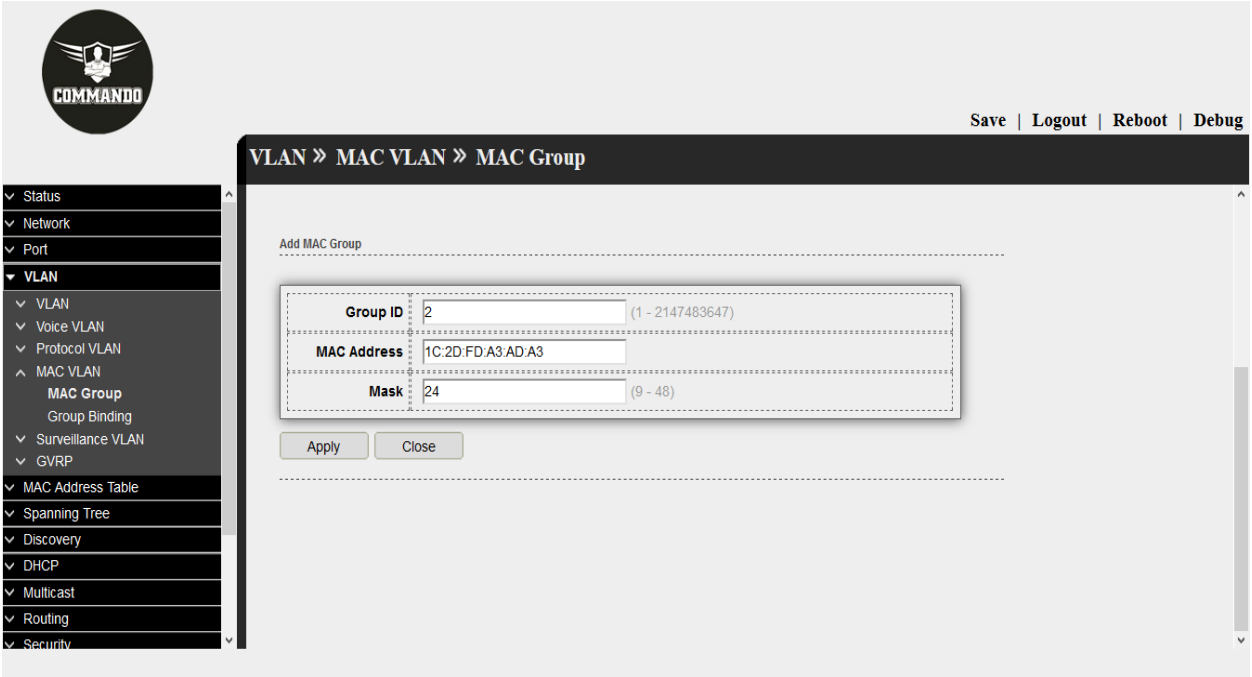


Fig 5.4.2 Add MAC Group ID page

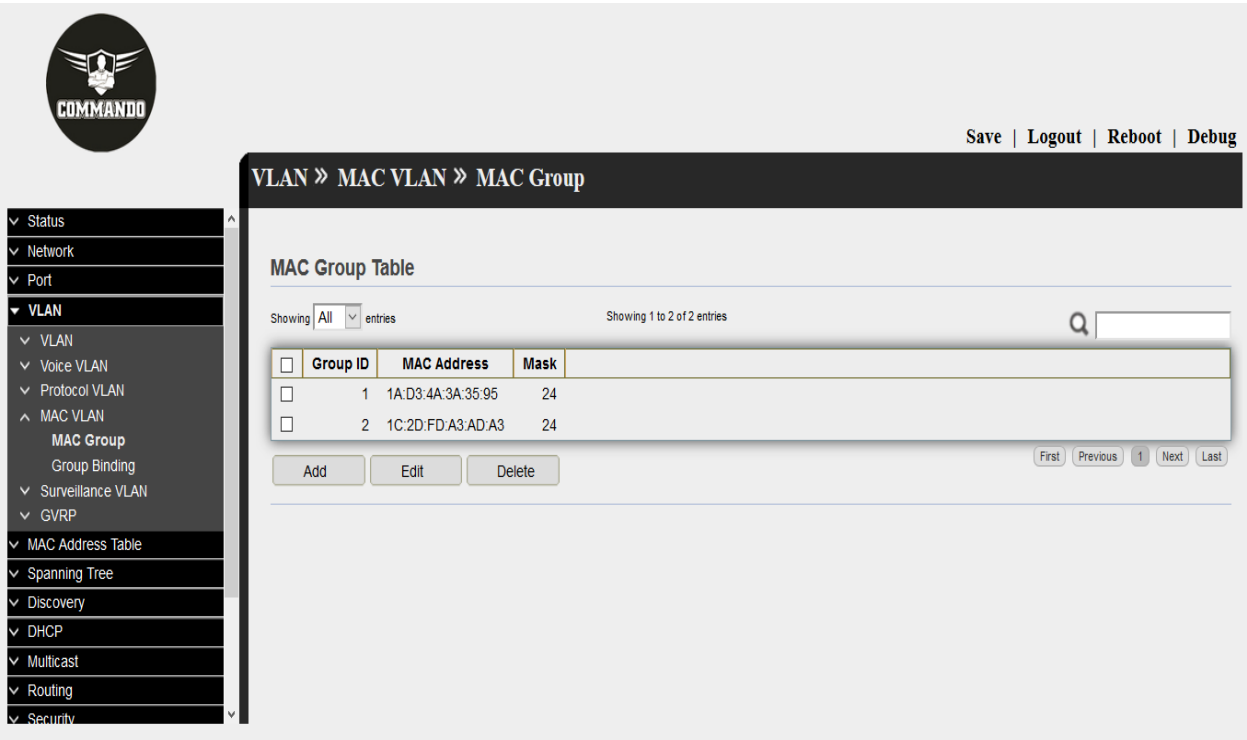


Fig 5.4.3 Mac Group table page

5.4.2 Group Binding

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

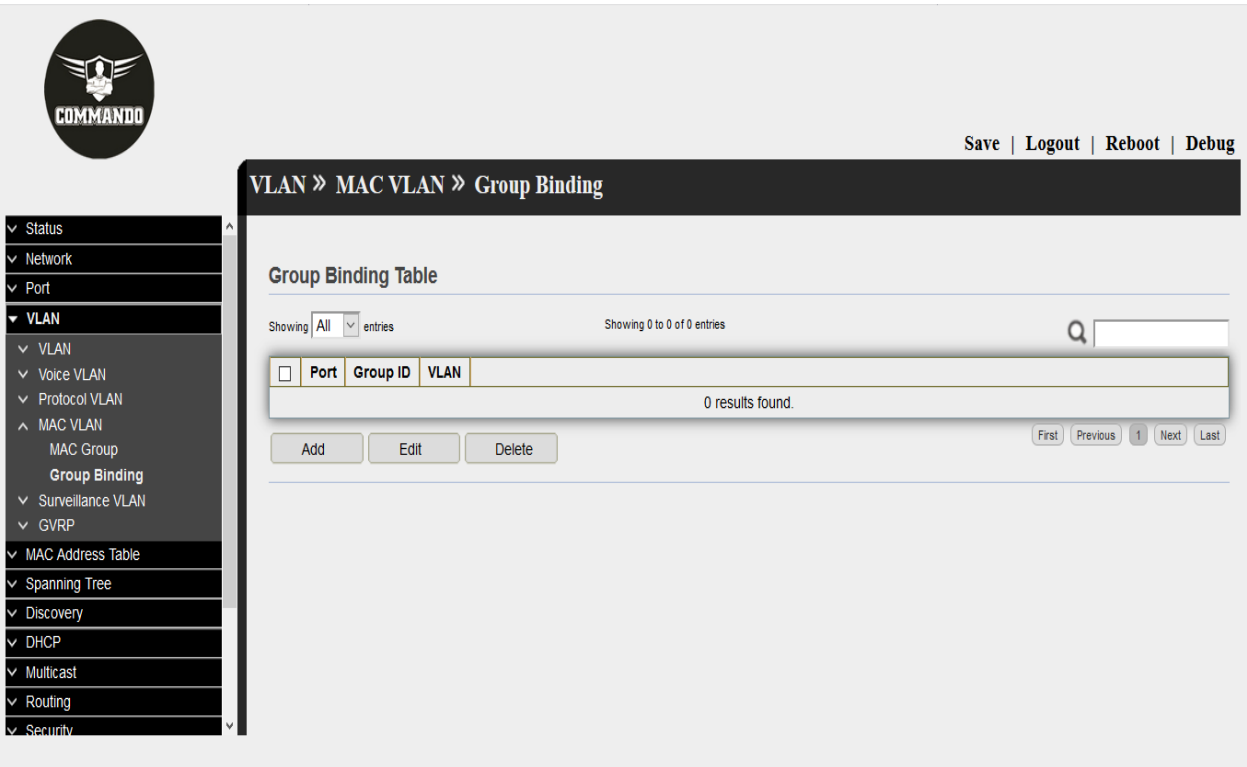


Fig 5.4.5 Blank Group binding table page

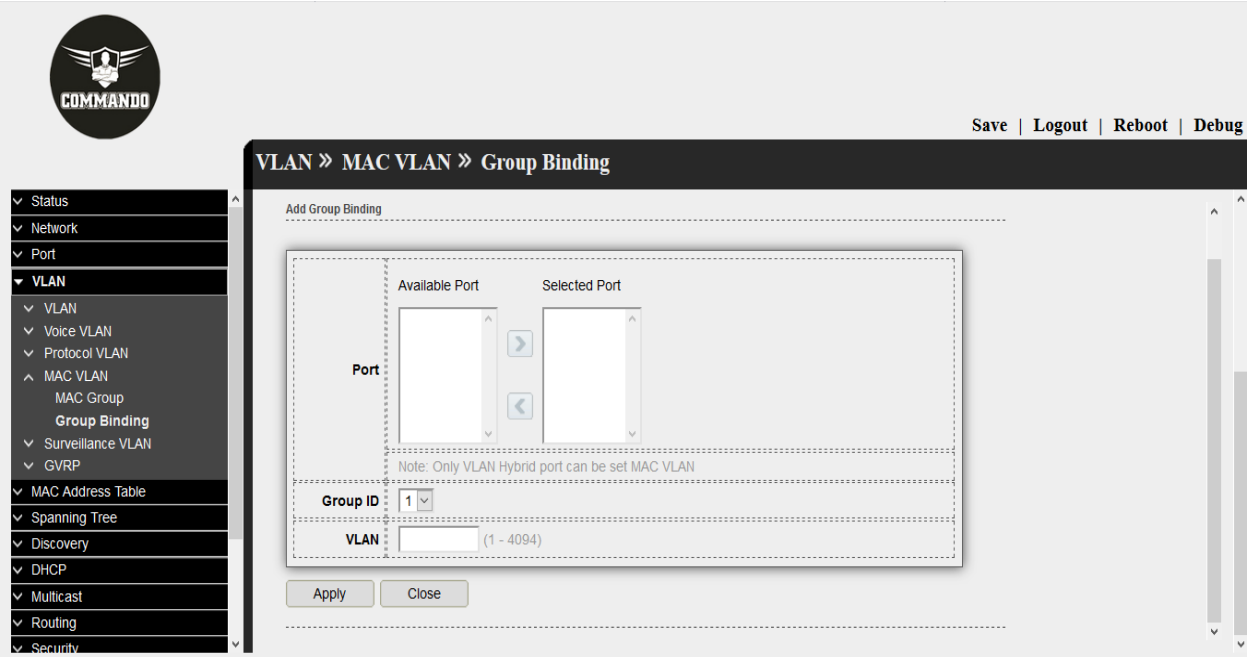


Fig 5.4.5 Blank Group binding for hybrid ports page

5.5 Surveillance VLAN

Surveillance VLAN is a feature that allows you to automatically place the video traffic from IP cameras to an 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 camaras are very important to protect the IP cameras against unauthorized access and also to separate the security camera system from other computers and devices that are connected to the IP network. C2000 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. The 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 deafult 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.**

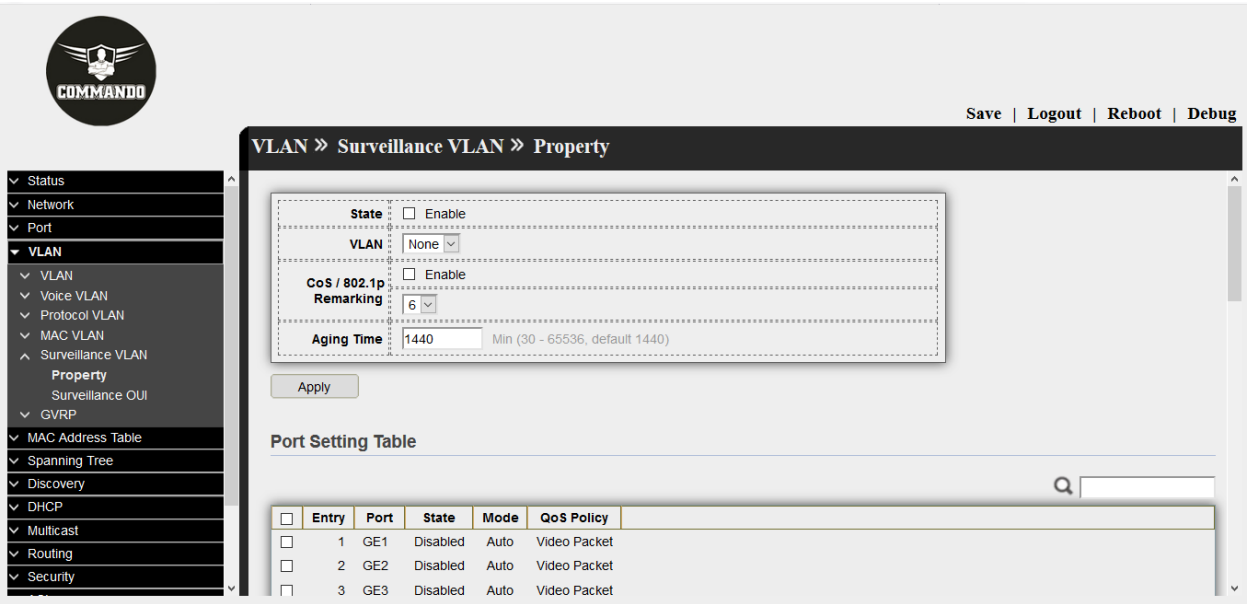


Fig 5.5.1 Surveillance VLAN Property page

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.

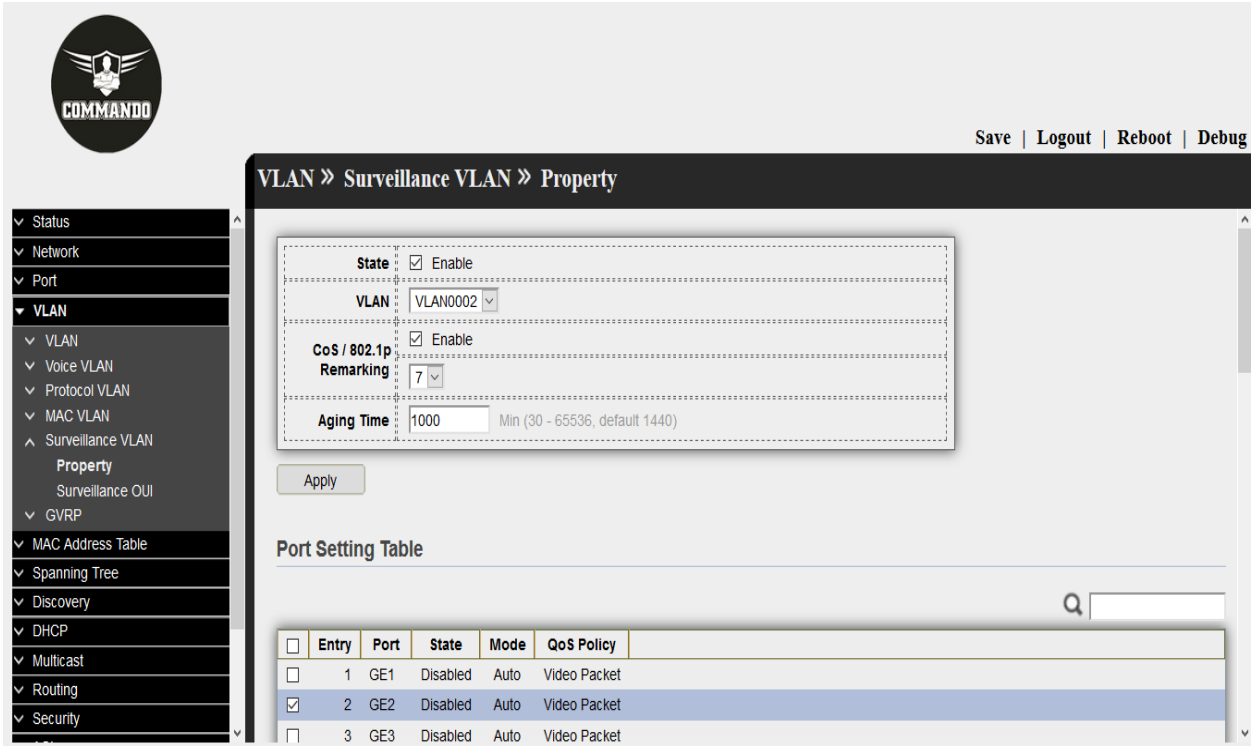


Fig 5.5.2 Surveillance VLAN port setting page for selected GE2 port

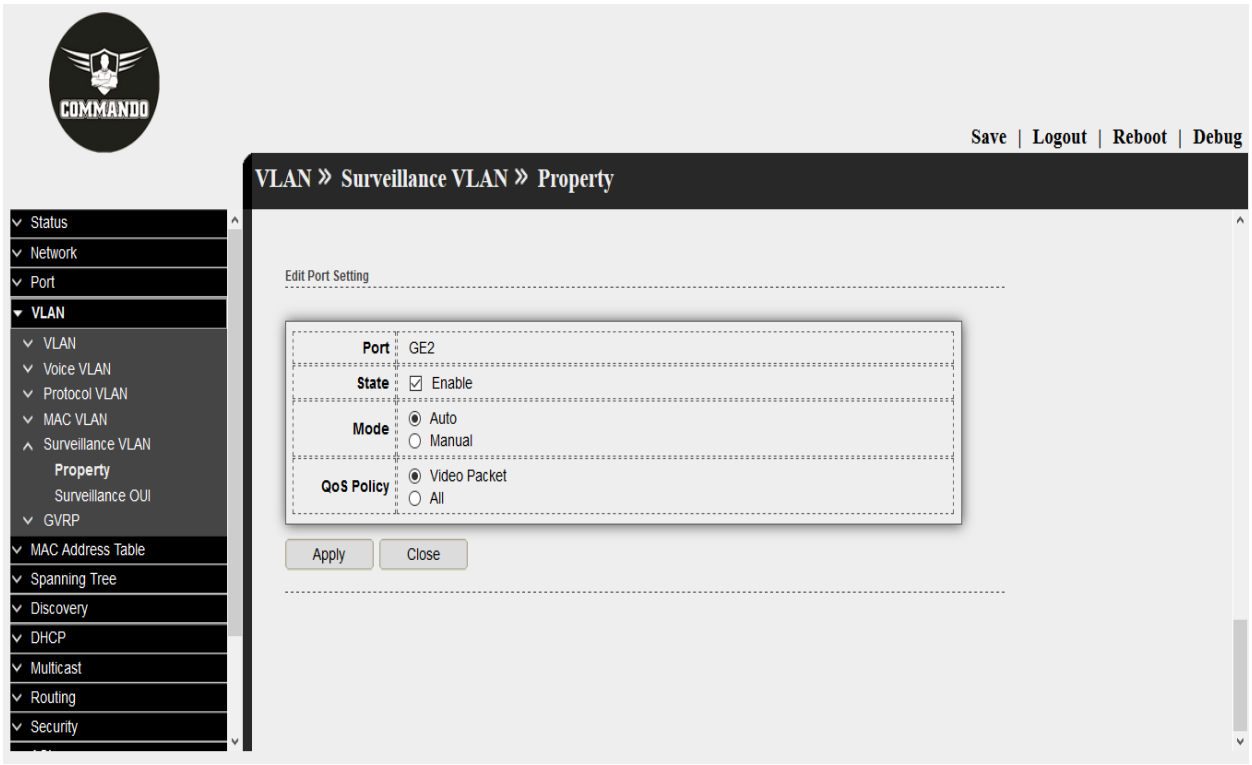


Fig 5.5.3 Surveillance VLAN Edit port setting for GE2 port page

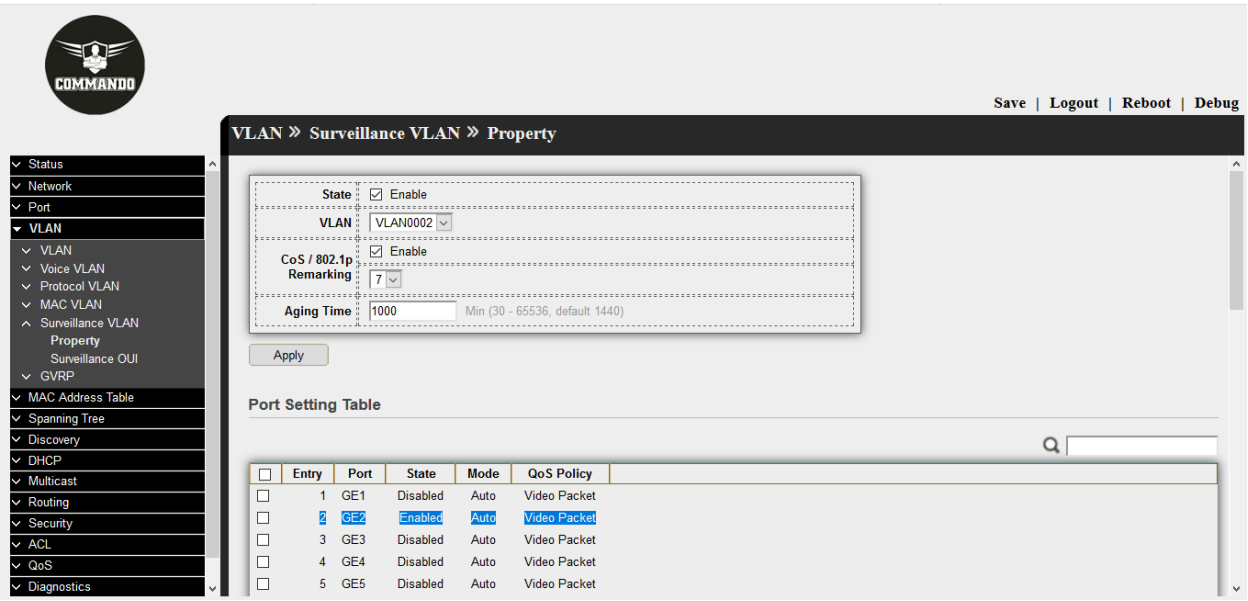


Fig 5.5.4 Surveillance VLAN Port setting table GE4 port enabled for Video packet

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 cameras 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.

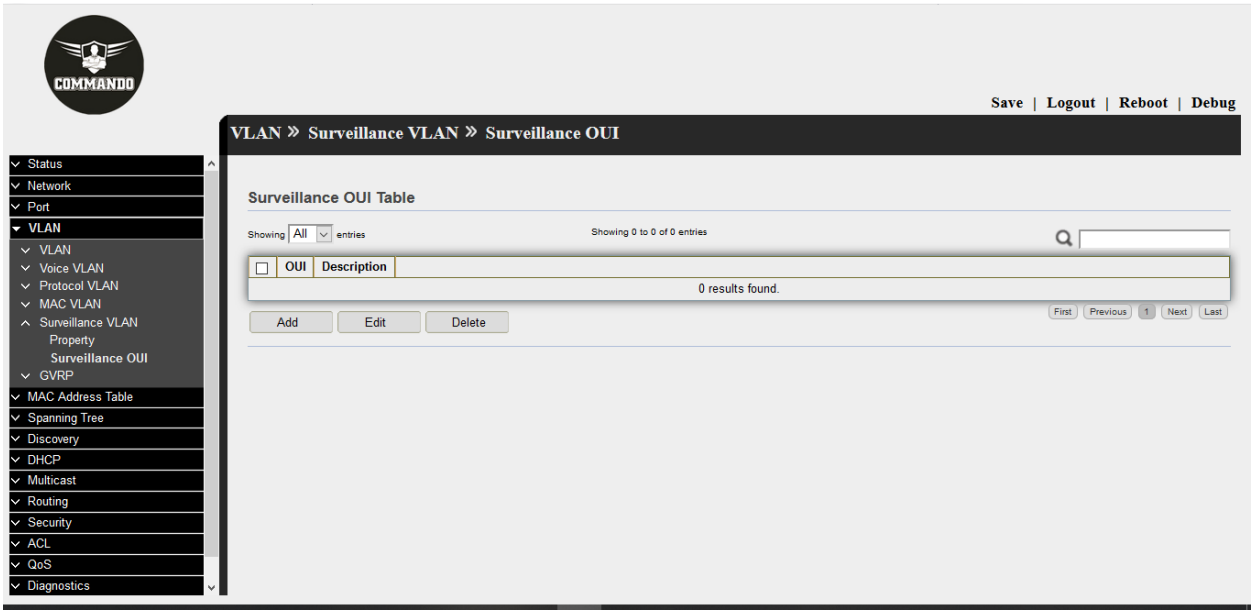


Fig 5.5.5 Surveillance OUI Table page

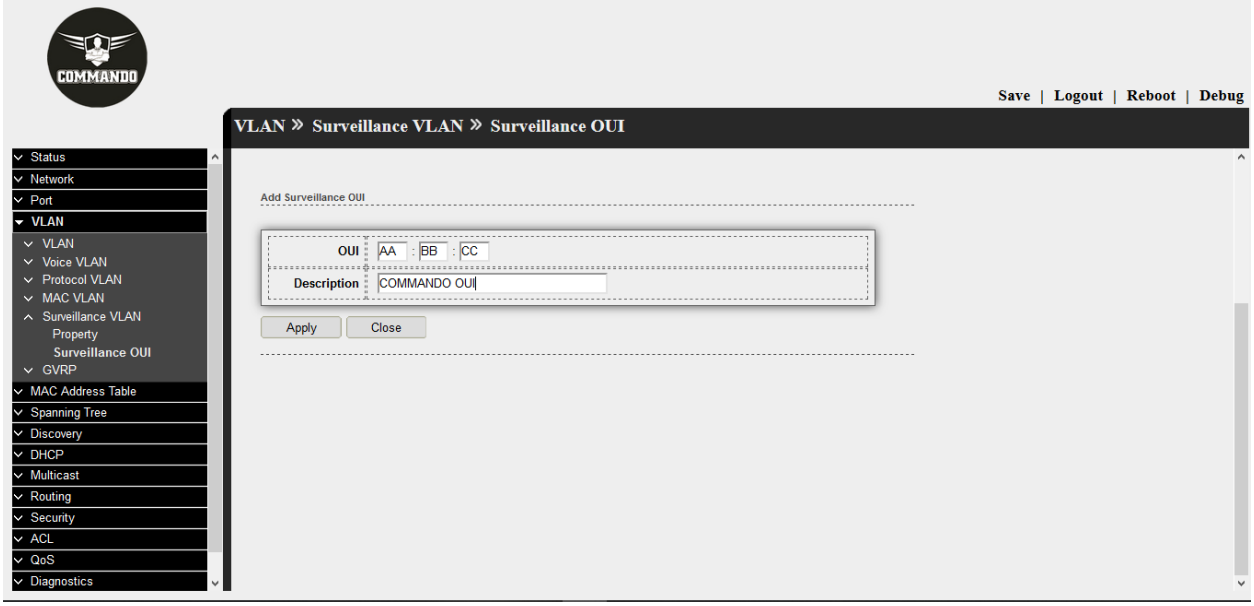


Fig 5.5.6 Add Surveillance OUI page

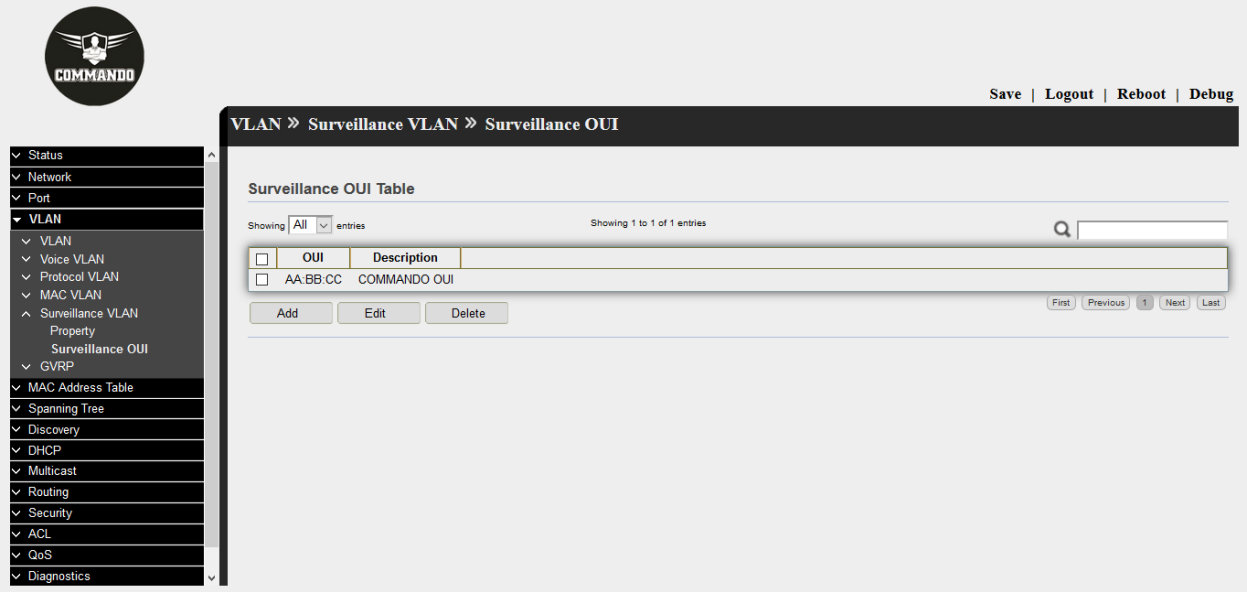


Fig 5.5.7 Surveillance OUI Table page

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.**

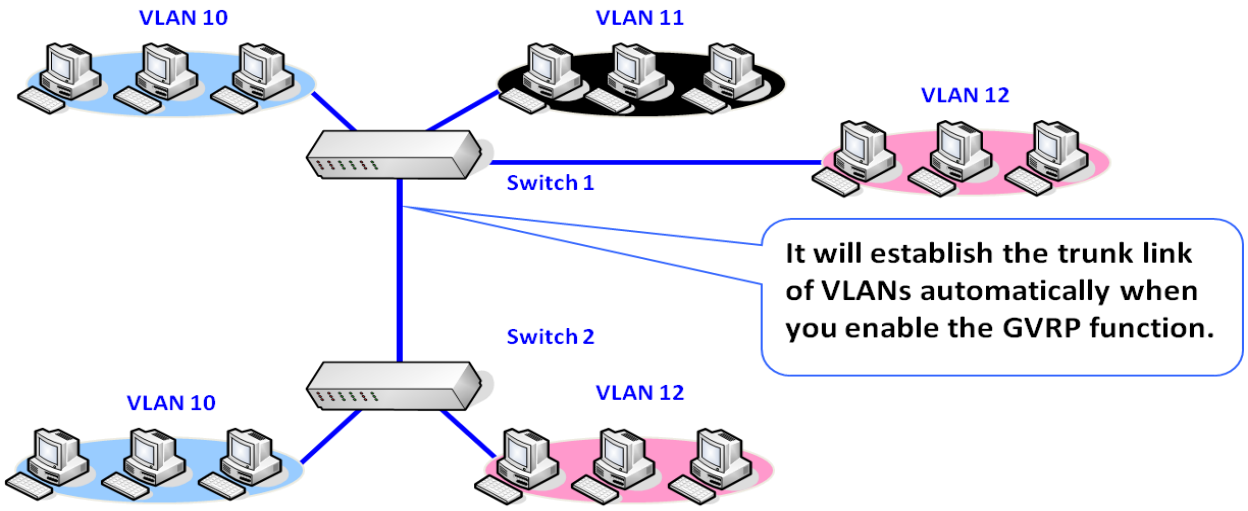


Fig 5.6.1 GVRP Function.

5.6.1 Property

By default GVRP is disabled in COMMANDO C2000 Series Switches. To Enable, configure GVRP Property and view GVRP Port setting, click **VLAN>>GVRP>>Property.**

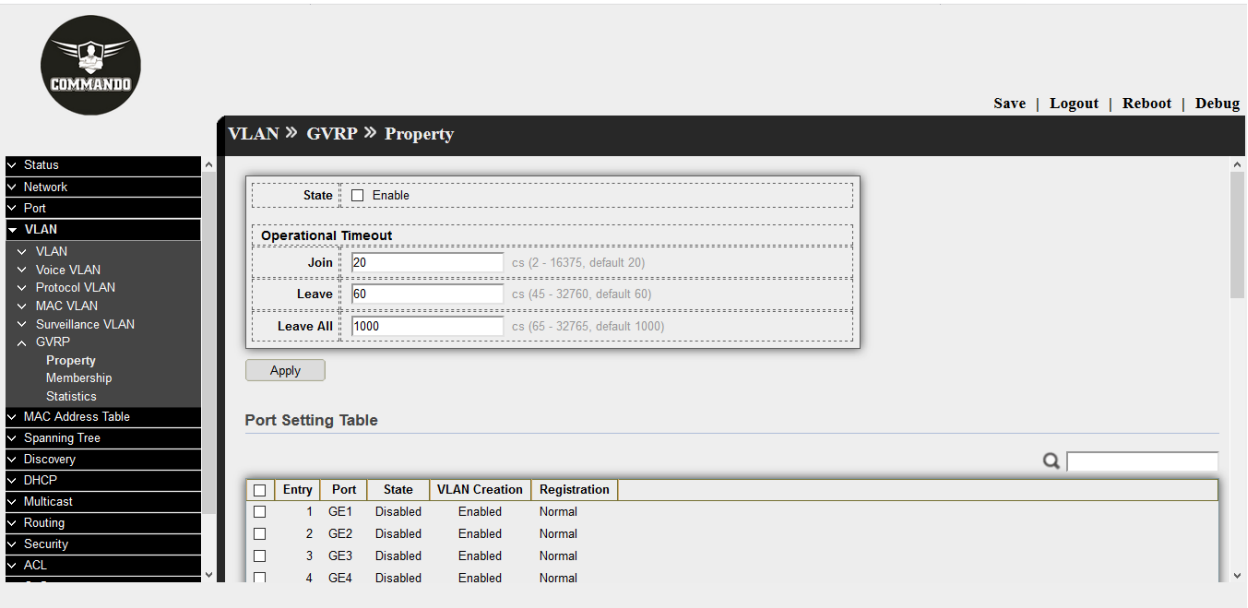


Fig 5.6.1 Default GVRP Property page

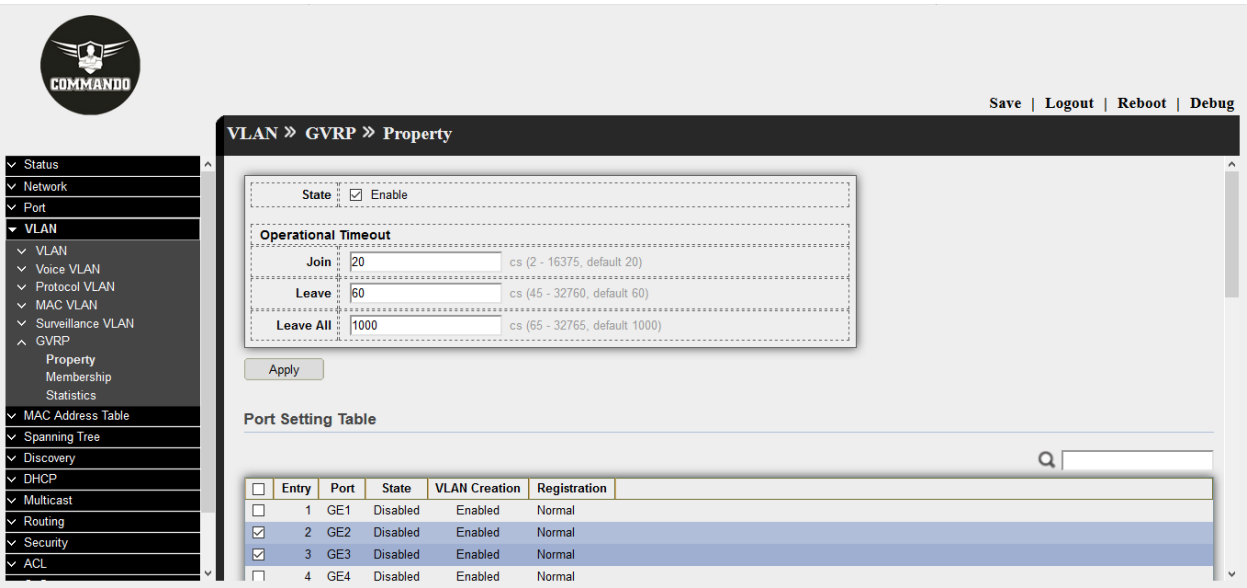


Fig 5.6.2 GVRP Property Port setting table selecting GE2 and GE3 ports page

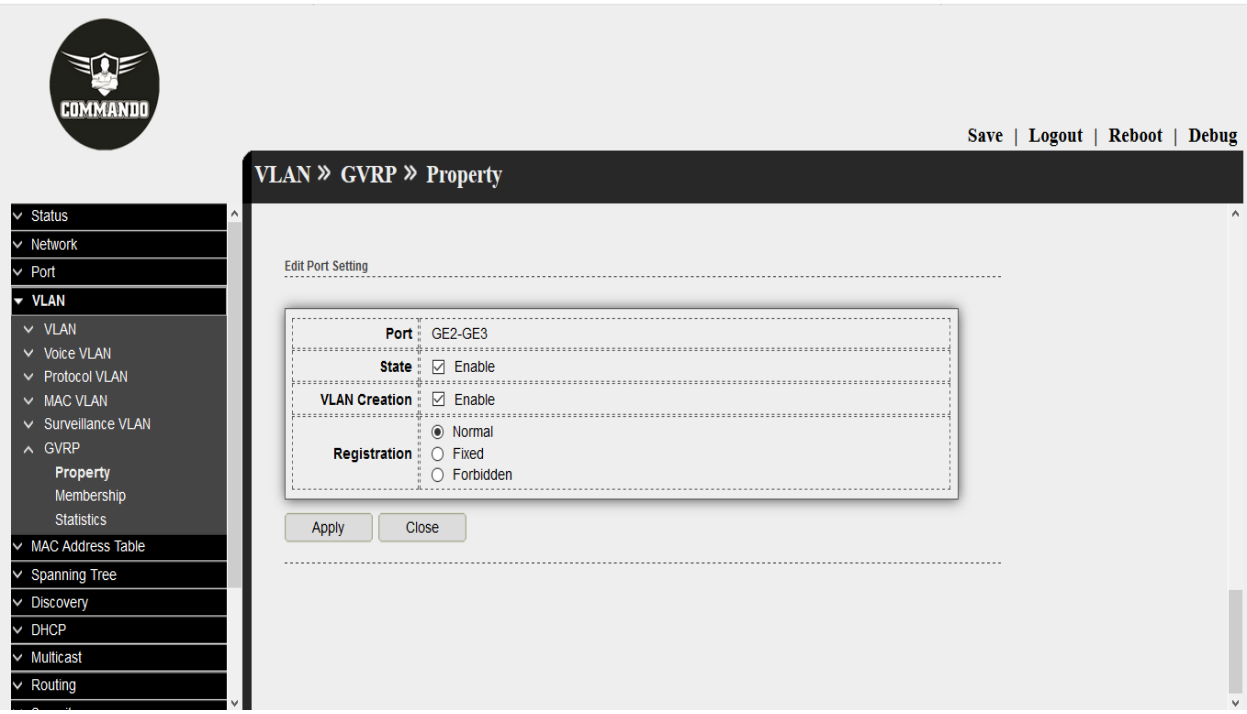


Fig 5.6.3 GVRP Property Edit Port setting for GE1 and GE2 ports page

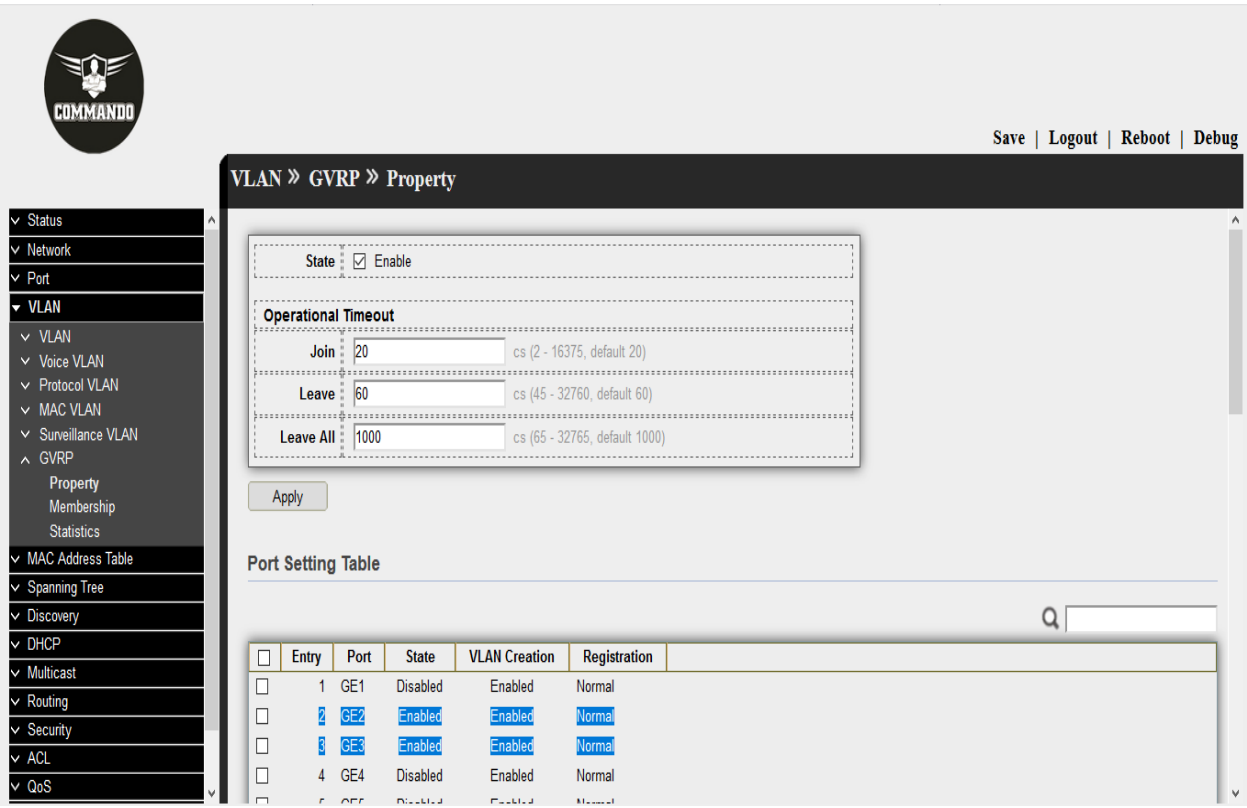


Fig 5.6.4 GVRP Property Port setting table after enableing GE1 and GE2 ports page

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.**

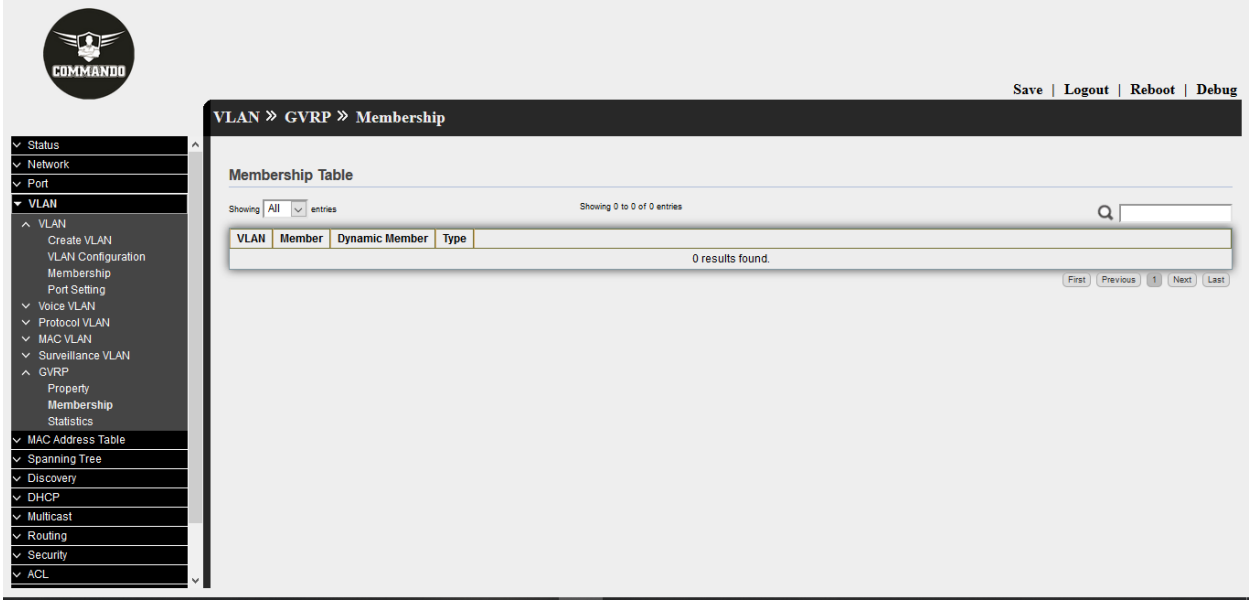


Fig 5.6.5 GVRP Membership Default page

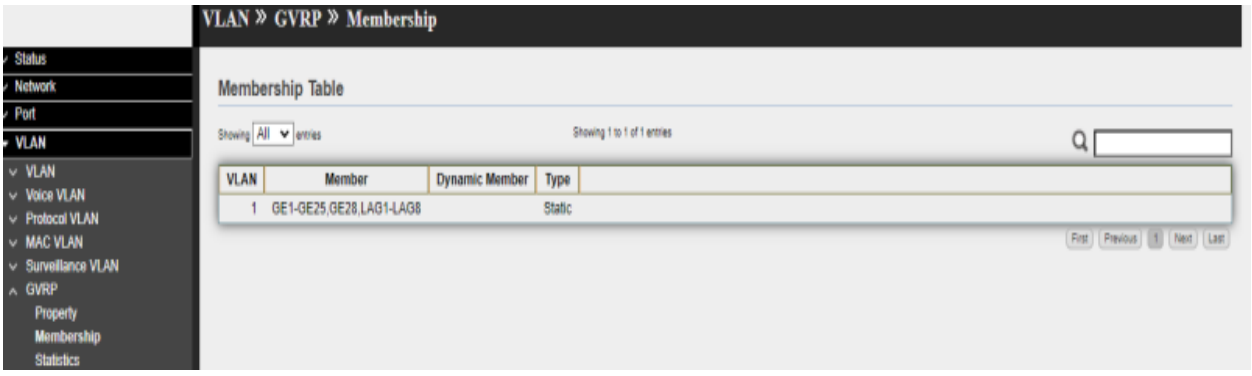


Fig 5.6.6 GVRP Membership after adding members page

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.**

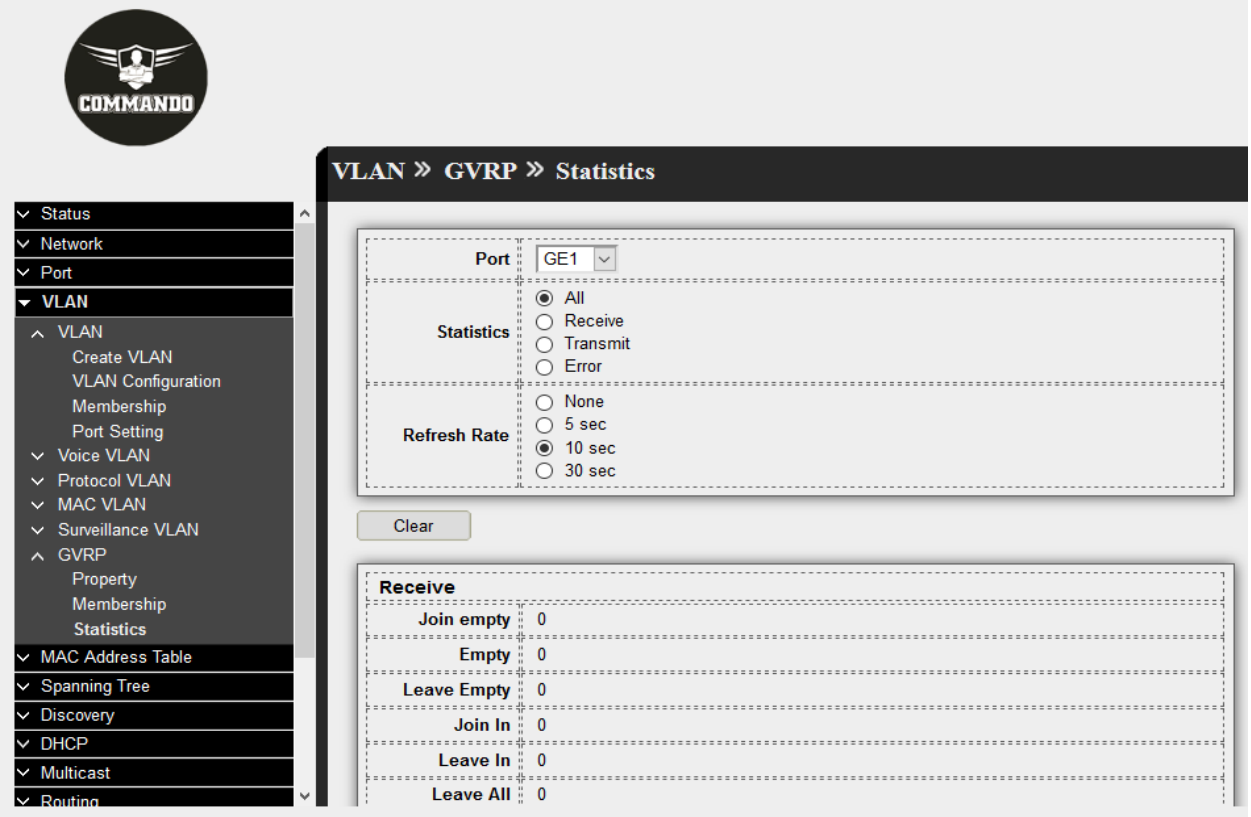


Fig 5.6.7 Default GVRP statistics page

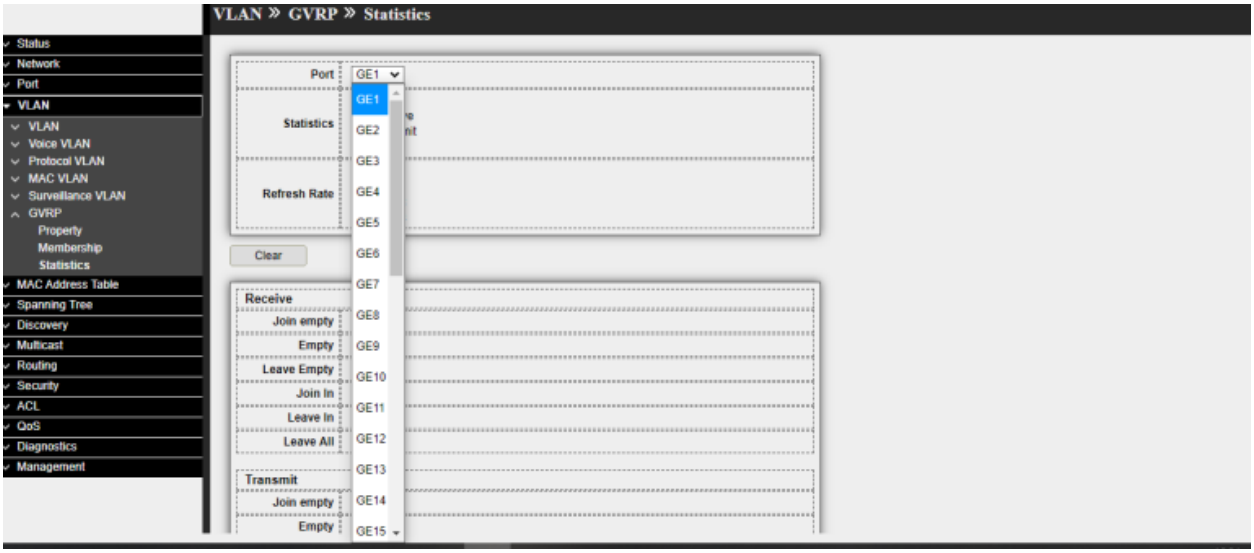


Fig 5.6.8 GVRP statistics for perticular port page

Chapter 6 MAC Address Table

Dynamic Address :--> In C2000 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.**

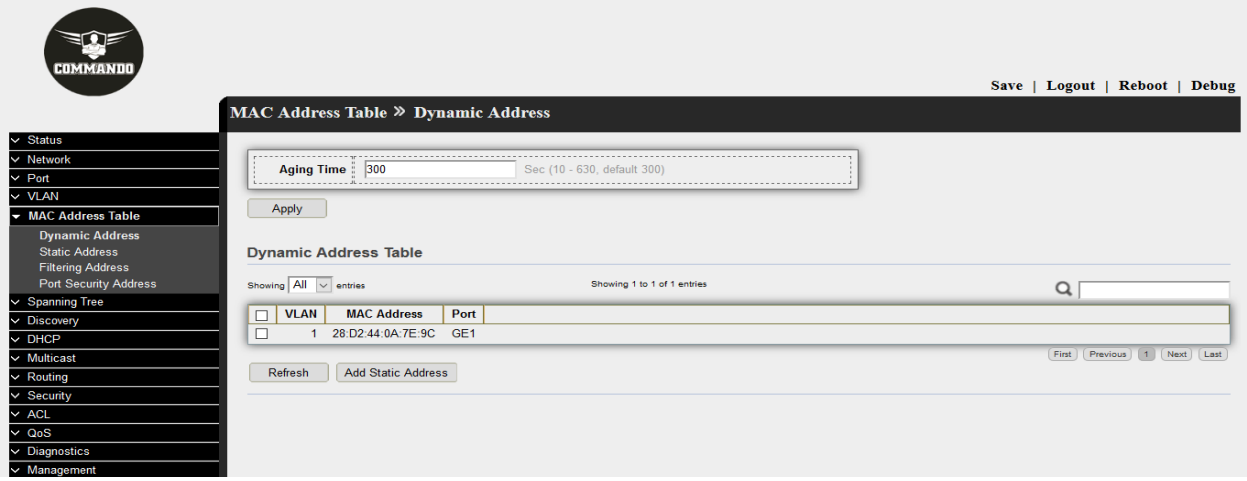


Fig 6.1.1 Dynamic MAC address table page

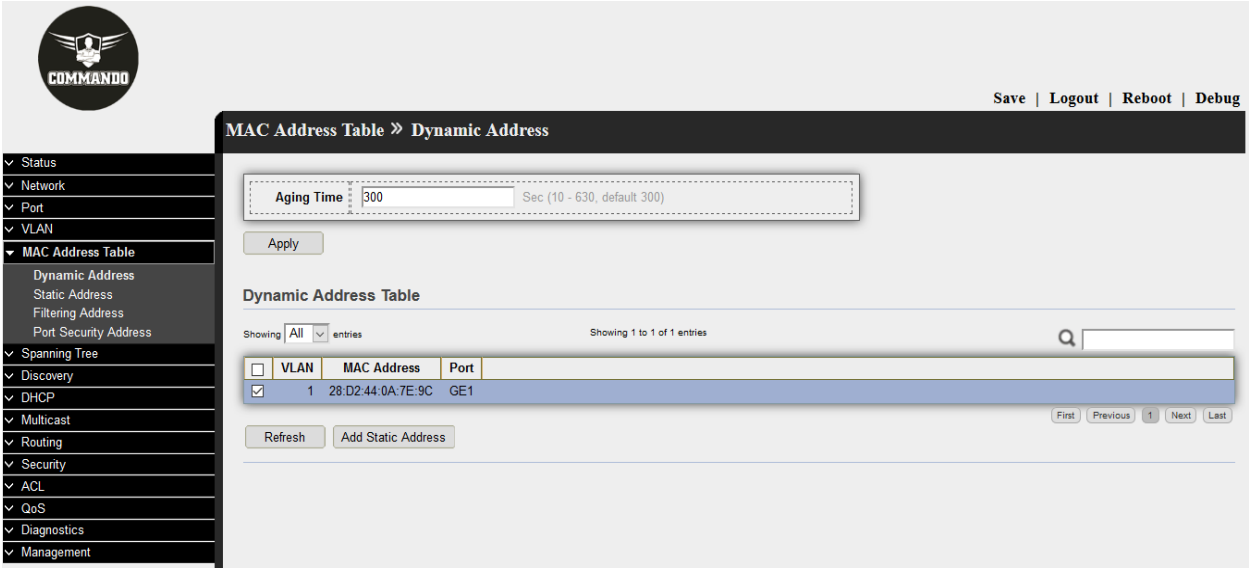


Fig 6.1.2 Add Static address from Dynamic MAC address table page

6.2 Static Address

Static MAC addresses are created manually. C2000 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.**

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

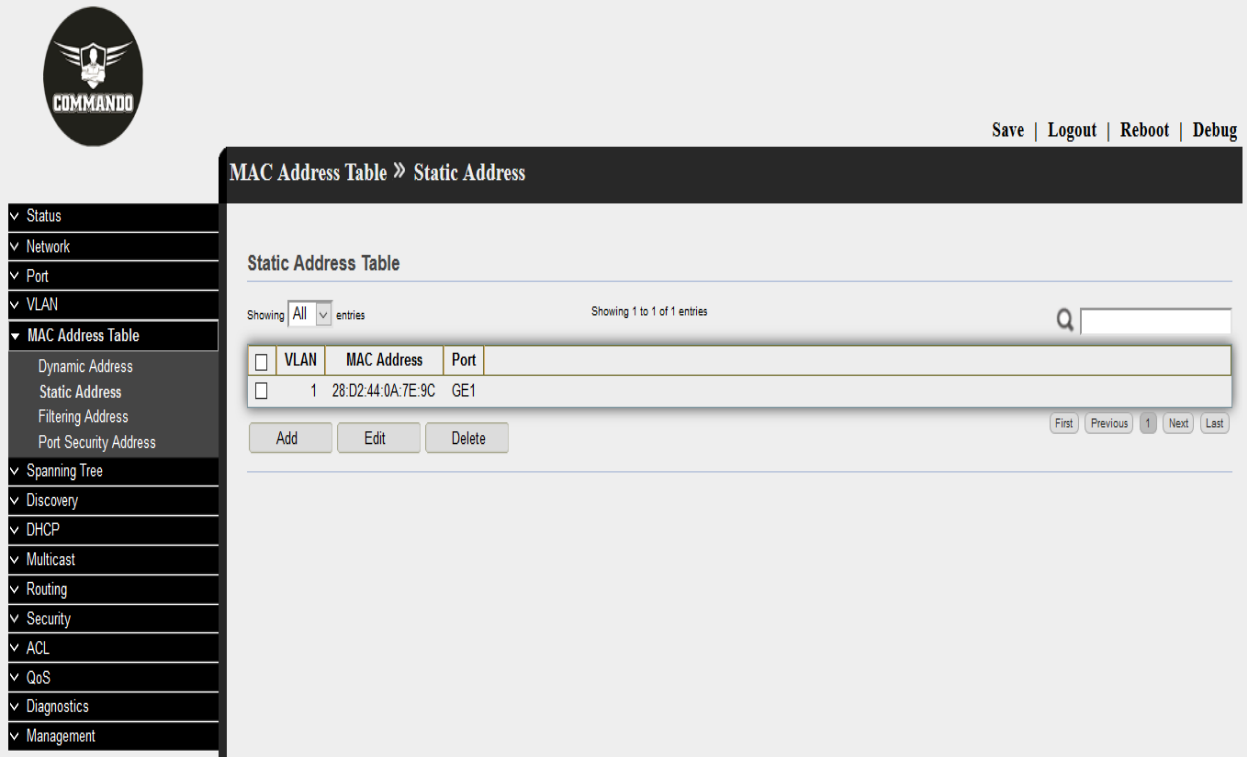


Fig 6.2.3 Static MAC address table After adding MAC address page

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

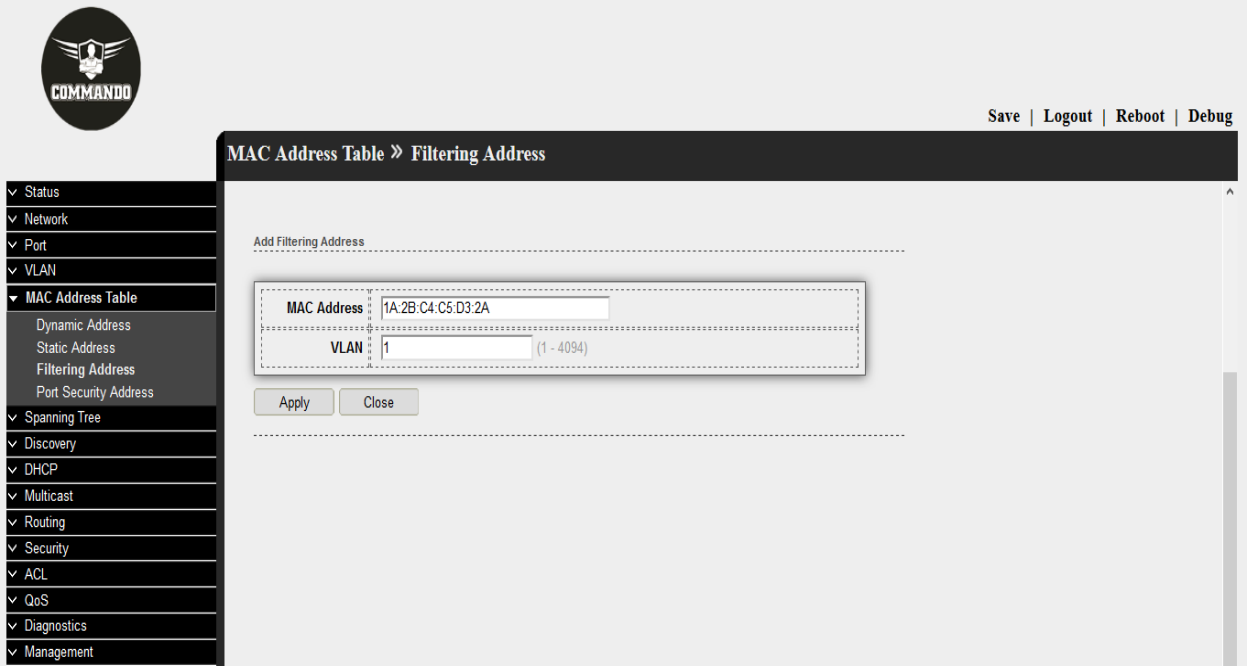


Fig 6.3.2 Add Filtering mac address to Specified VLAN page

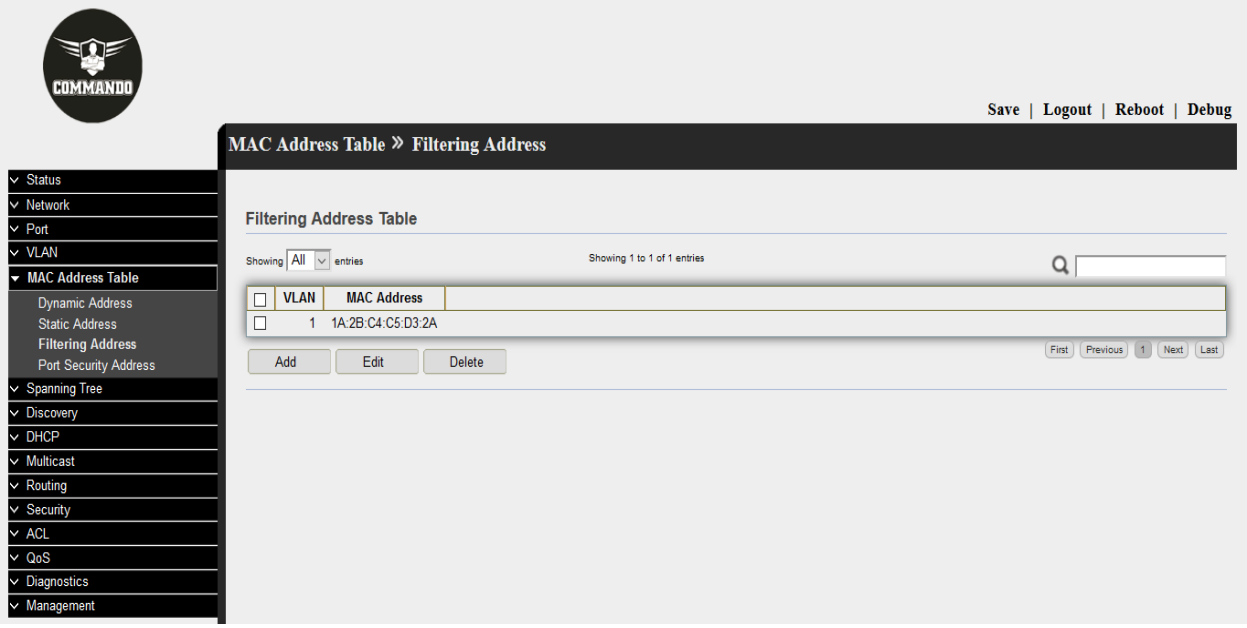


Fig 6.3.3 Filtering address table after adding MAC entry page

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.**

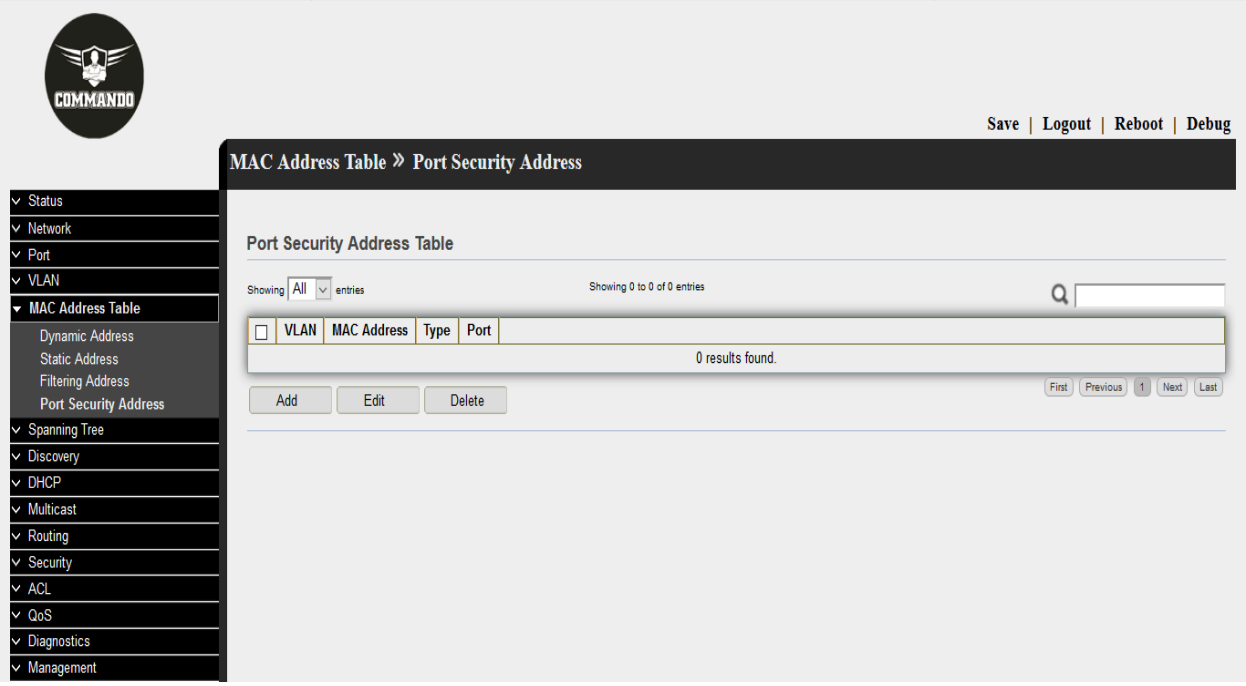


Fig 6.4.1 Port Security address table default page

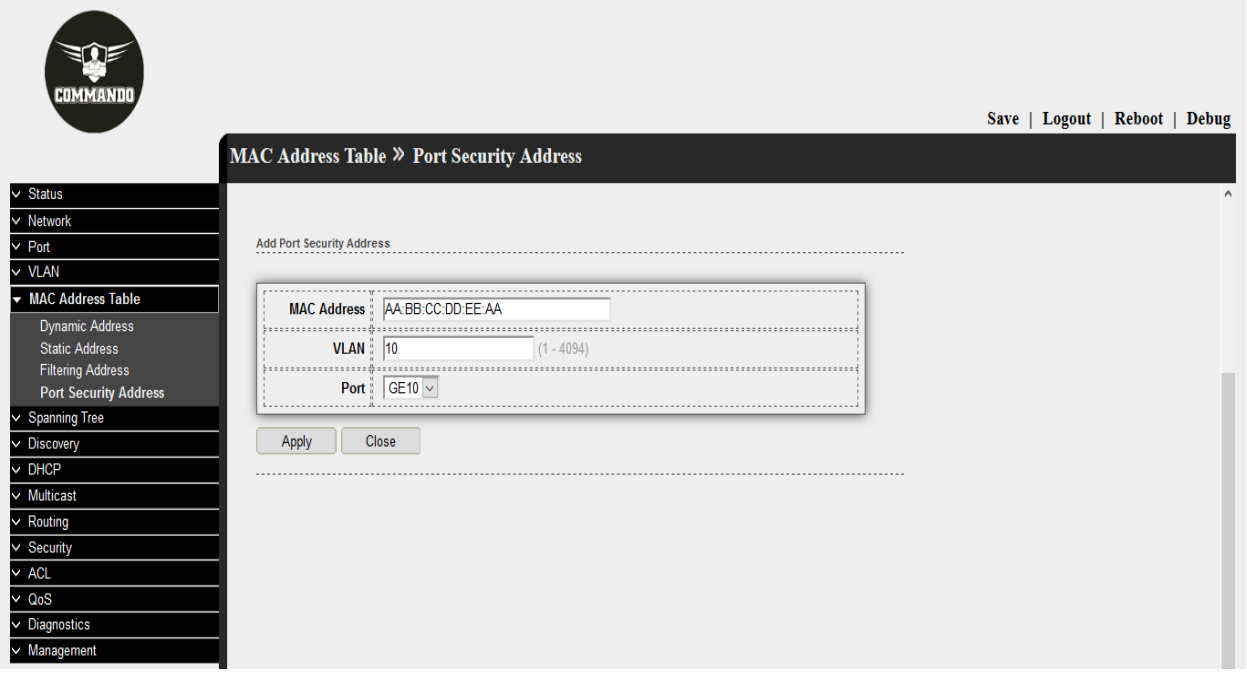


Fig 6.4.2 Add Port Security MAC address page

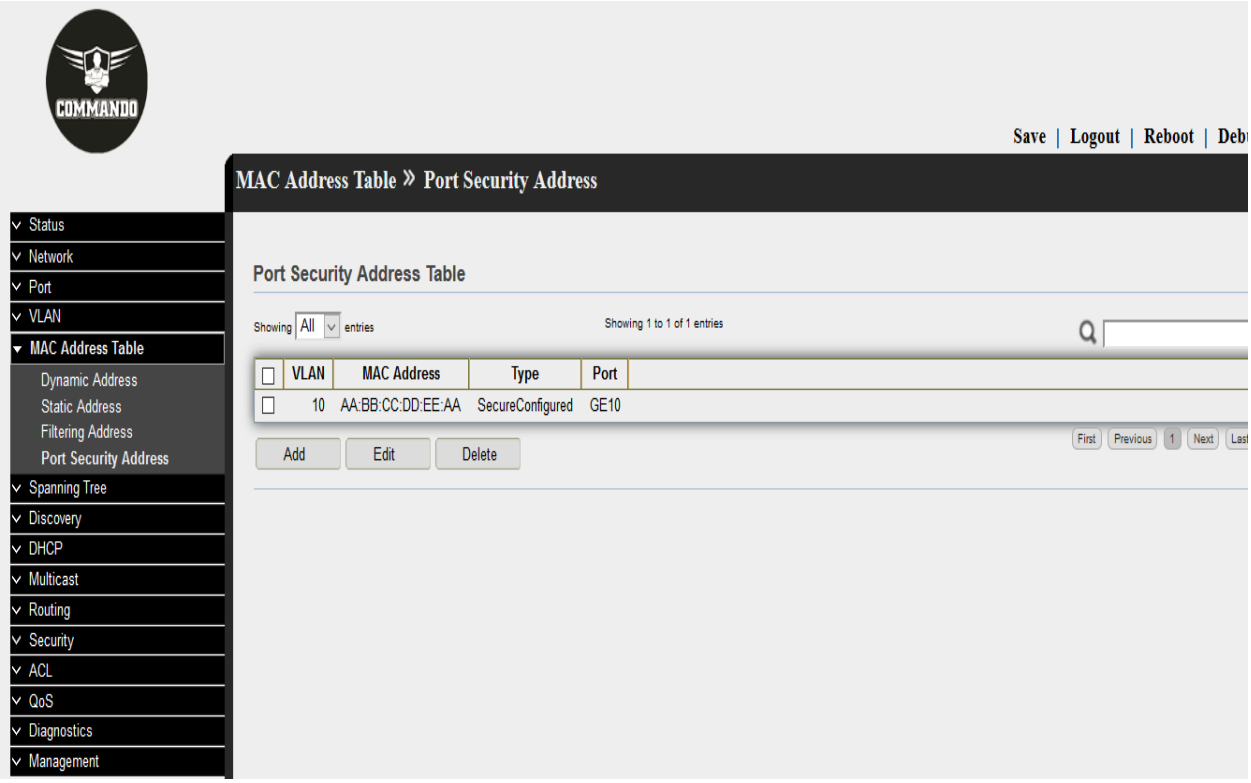


Fig 6.4.3 Port Security address table after adding entry page

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. 50 sec required to apply STP/RSTP/MSTP to learn the topology of network and apllication on switch default Spanning tree setting in C2000 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 of these 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 redundent 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 topologies 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 C2000 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 C2000 Series switch.

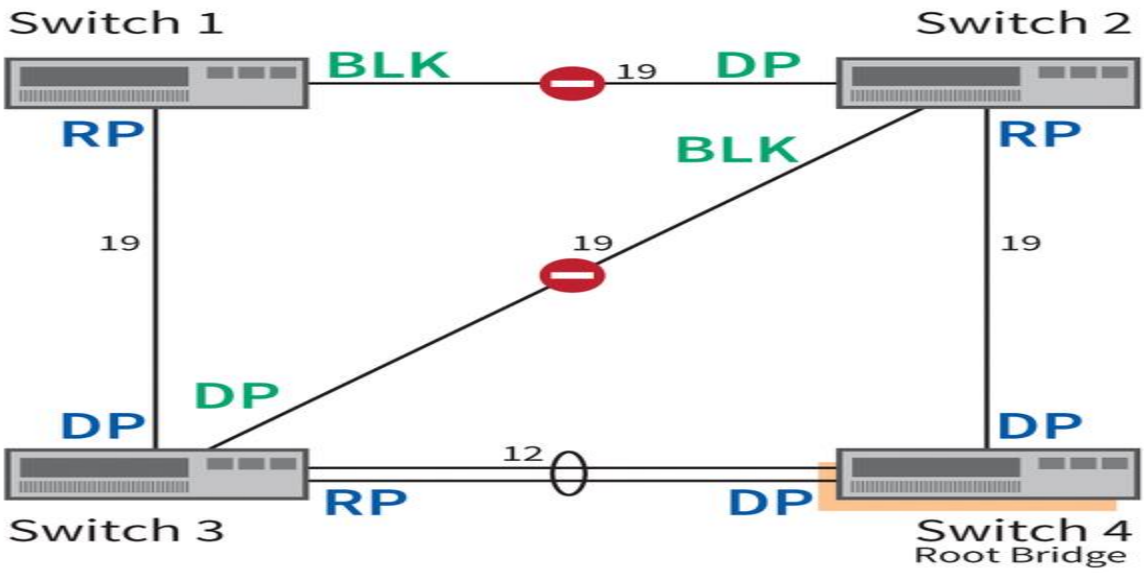


Fig 7.1.1 Spanning Tree enabled network Changed topology .

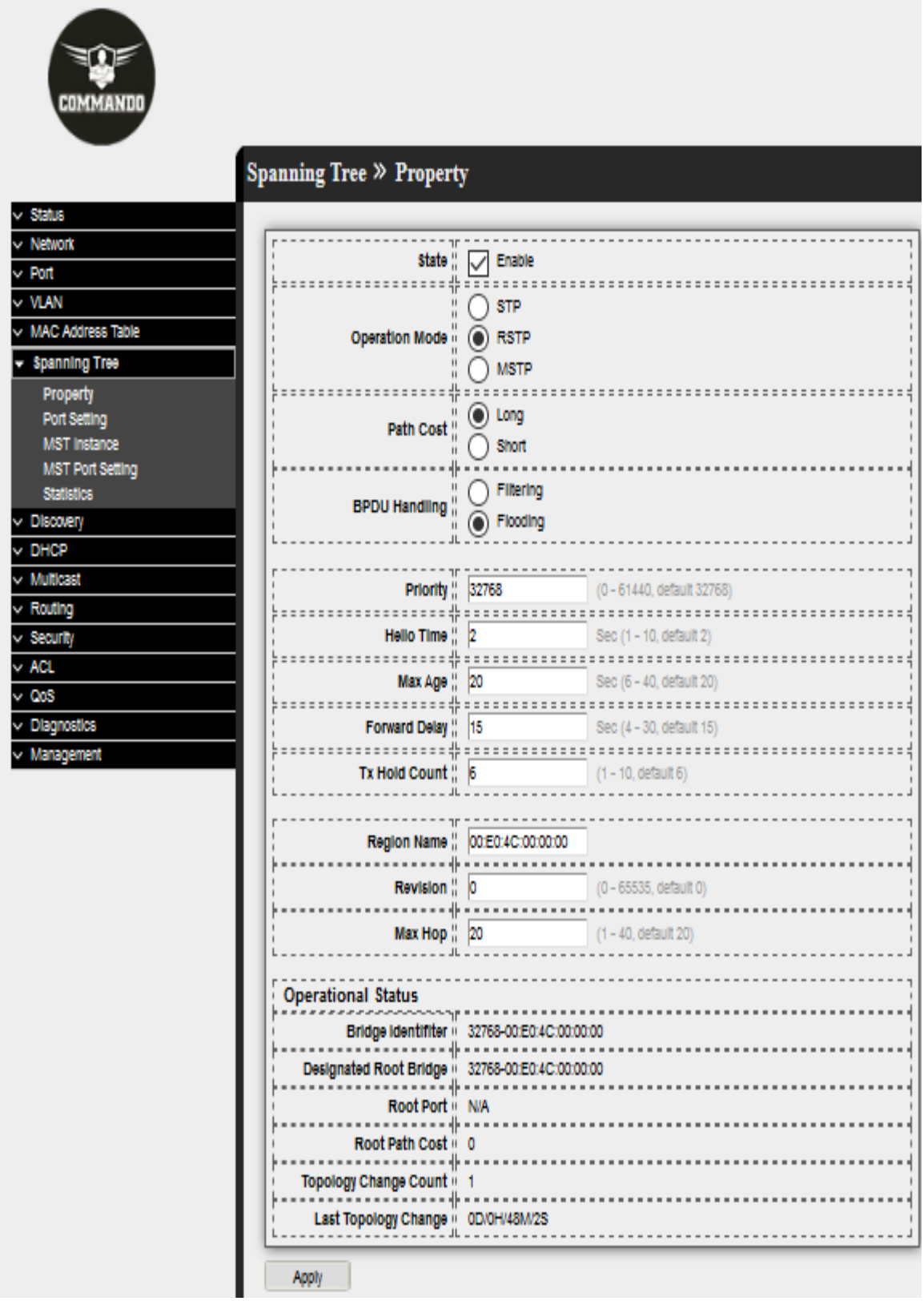


Fig 7.1.2 Default Spanning Tree property page

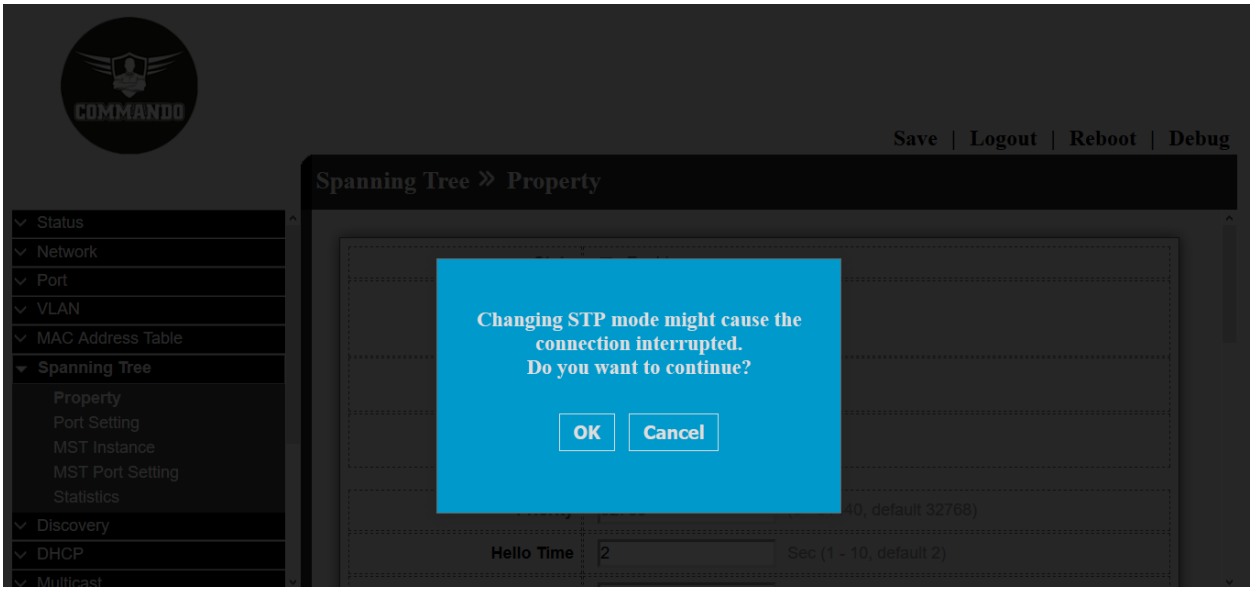


Fig 7.1.2 Change Spanning Tree mode property page

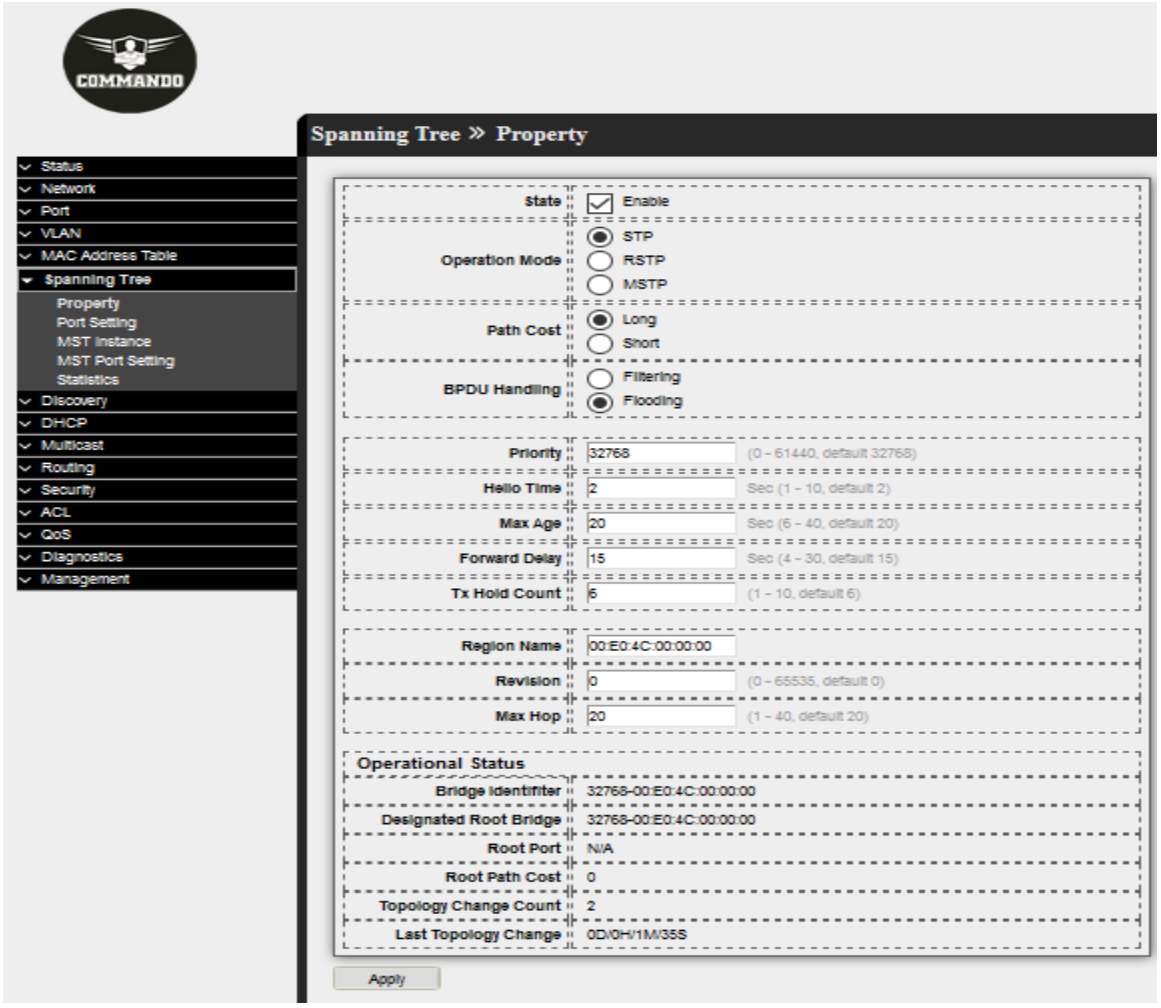
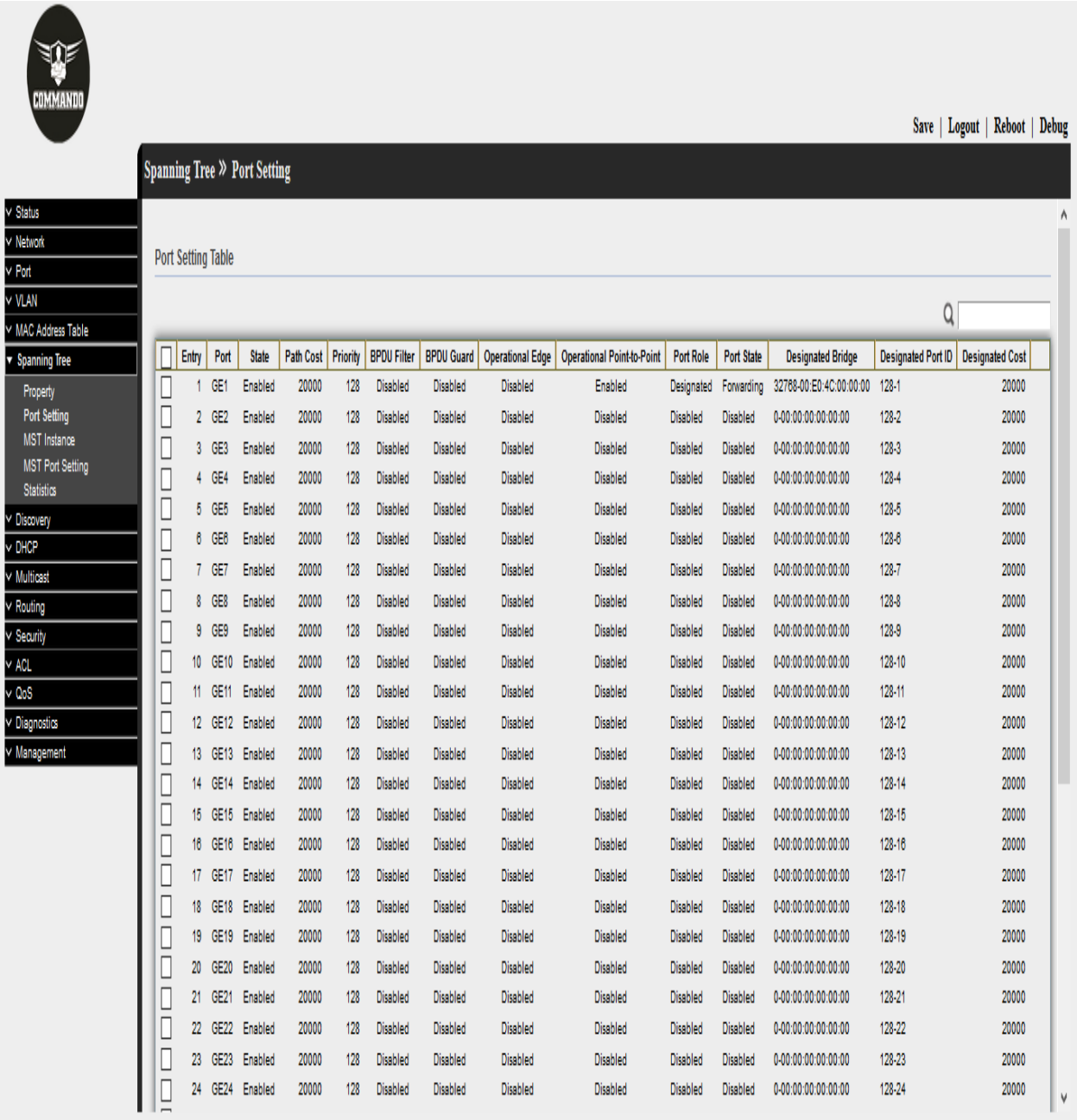


Fig 7.1.3 Change Spanning Tree mode page

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.**



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
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-00:E0:4C:00:00:00	128-1	20000
2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
3	GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
7	GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
9	GE9	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000
10	GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000
11	GE11	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000
12	GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000
13	GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
14	GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
15	GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
16	GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000
17	GE17	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000
18	GE18	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000
19	GE19	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000
20	GE20	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000
21	GE21	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-21	20000
22	GE22	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-22	20000
23	GE23	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-23	20000
24	GE24	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-24	20000

Fig 7.2.1 Spanning tree port setting page

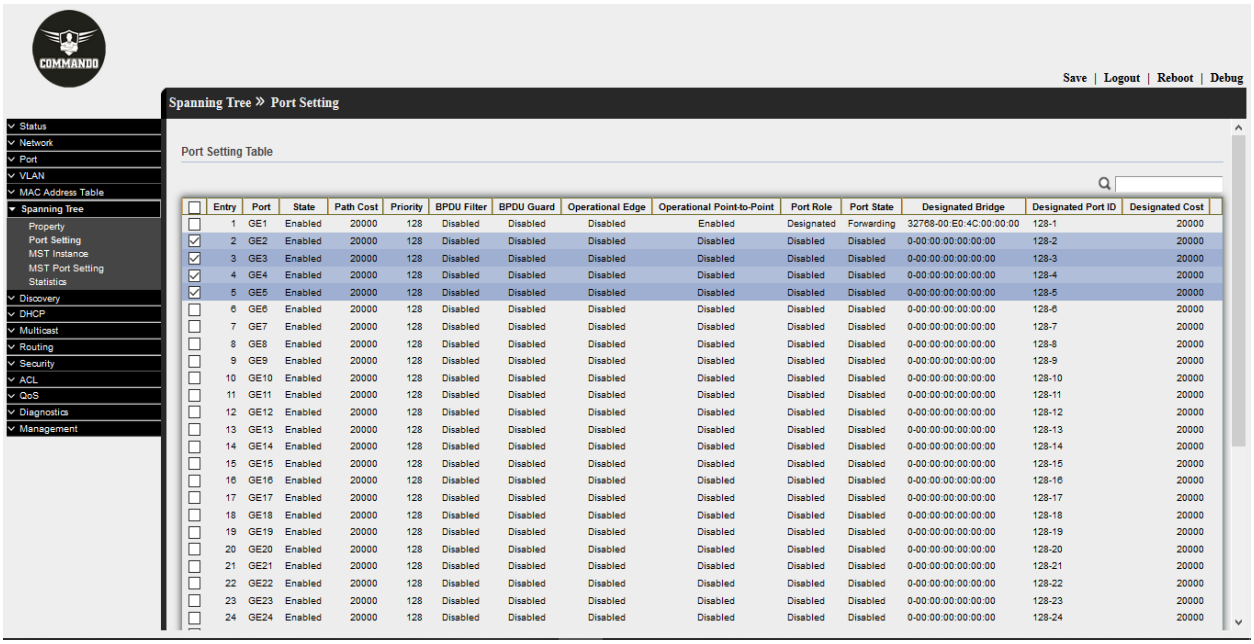


Fig 7.2.2 Selecting port for Setting all Spanning Tree Parameters page

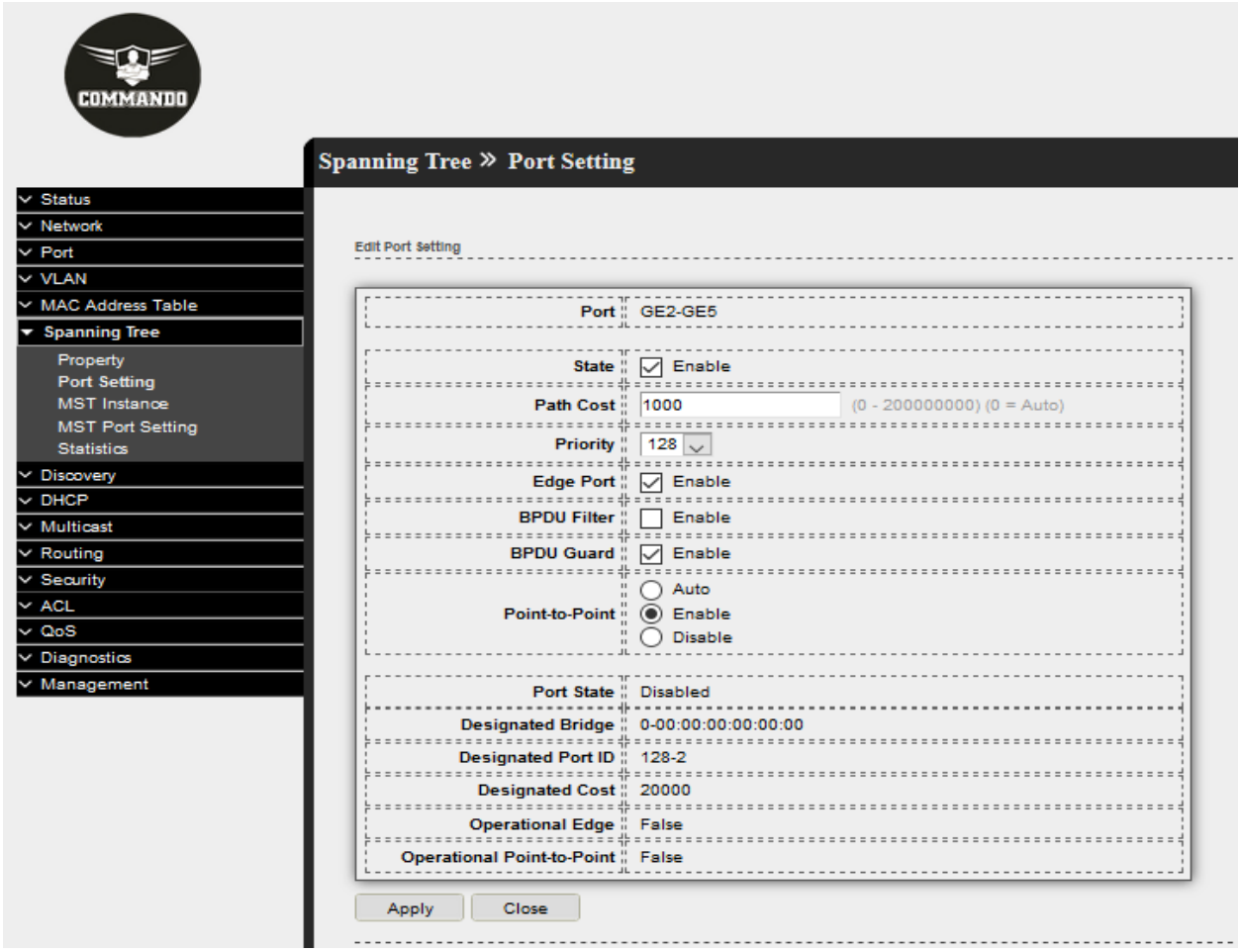
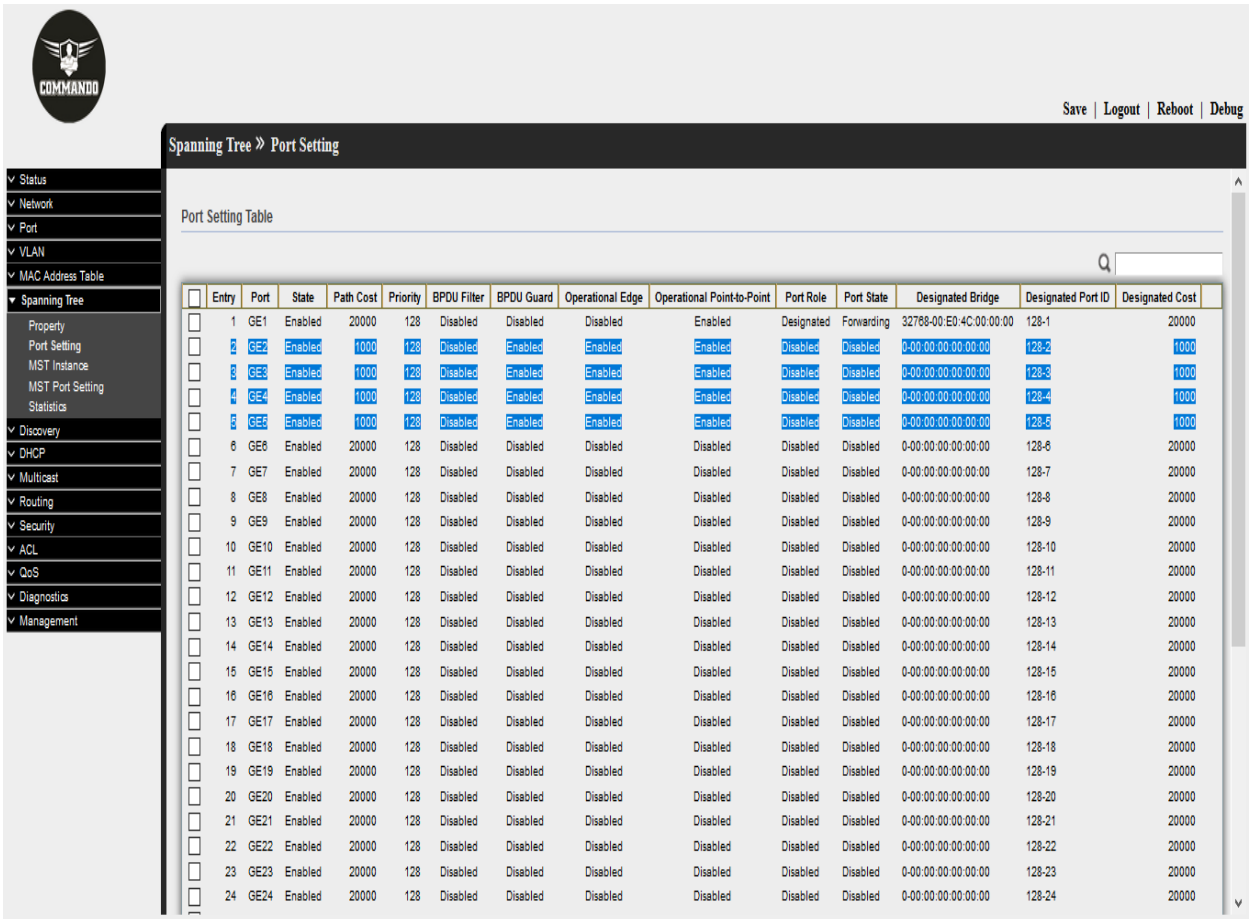


Fig 7.2.3 Setting ports for Spanning Tree Parameters page



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
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-00:E0:4C:00:00:00	128-1	20000
2	GE2	Enabled	1000	128	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	1000
3	GE3	Enabled	1000	128	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	1000
4	GE4	Enabled	1000	128	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	1000
5	GE5	Enabled	1000	128	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	1000
6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
7	GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
9	GE9	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000
10	GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000
11	GE11	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000
12	GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000
13	GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
14	GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
15	GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
16	GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000
17	GE17	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000
18	GE18	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000
19	GE19	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000
20	GE20	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000
21	GE21	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-21	20000
22	GE22	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-22	20000
23	GE23	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-23	20000
24	GE24	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-24	20000

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).

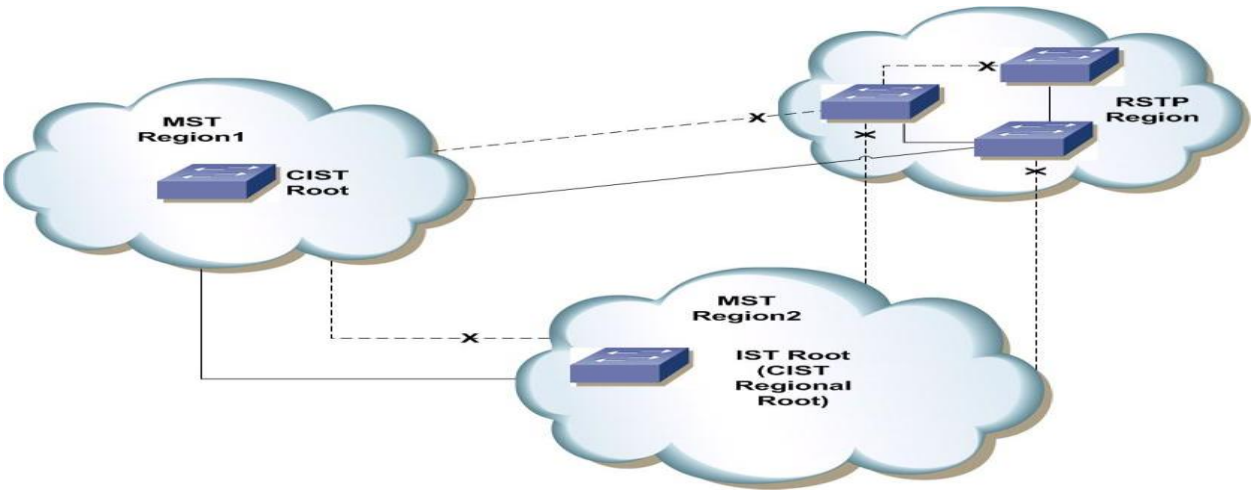


Fig 7.3.1 MST Enabled Network Topology change

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

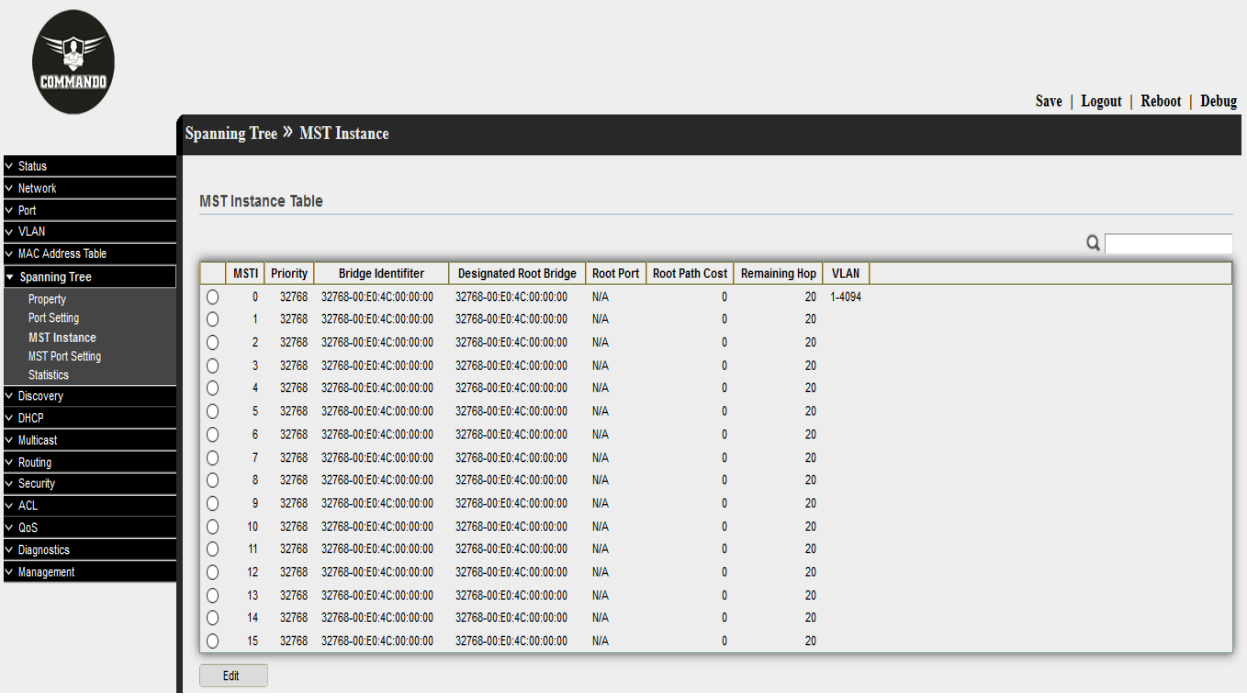


Fig 7.3.1 Fig 7.3.1 Spanning tree MST instance Table page

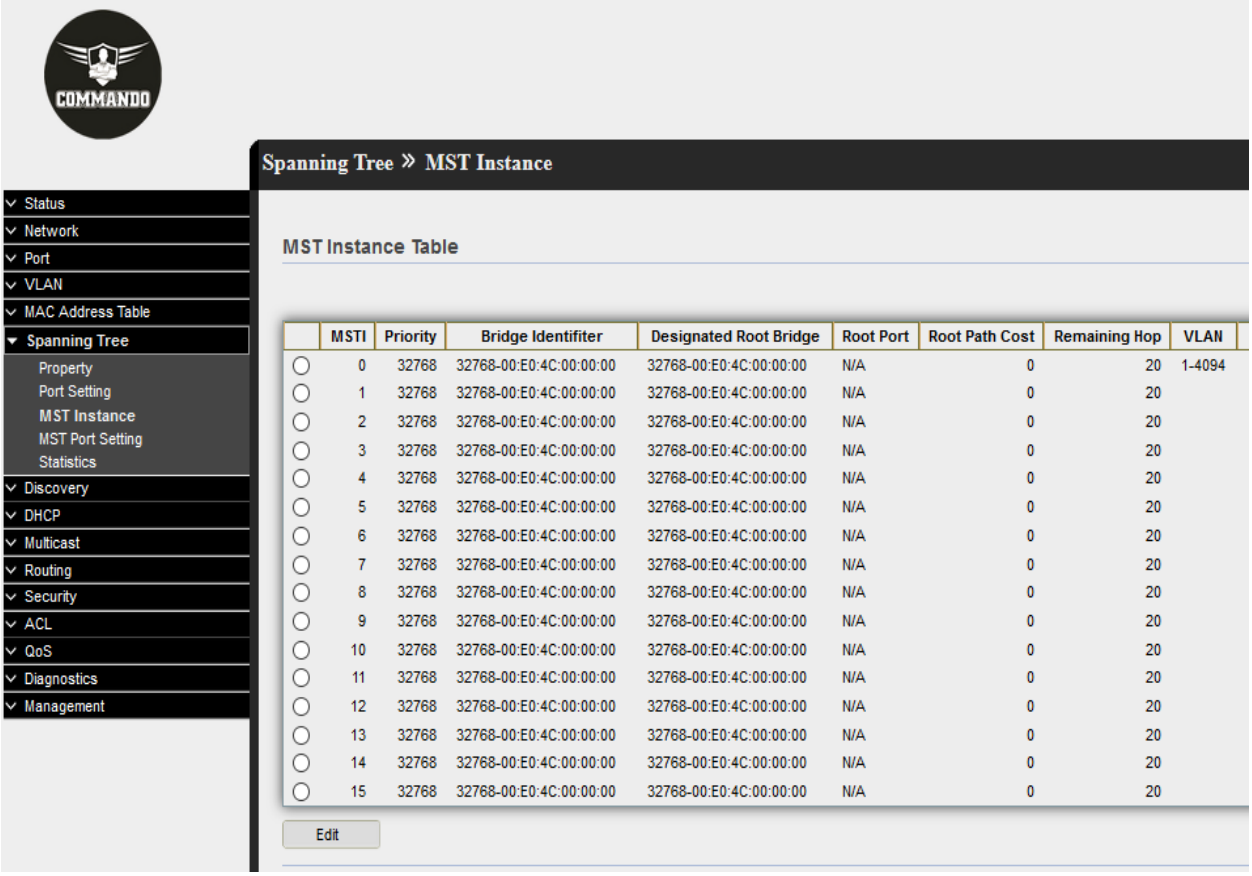


Fig 7.3.2 Spanning tree MST interface setting page

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.**

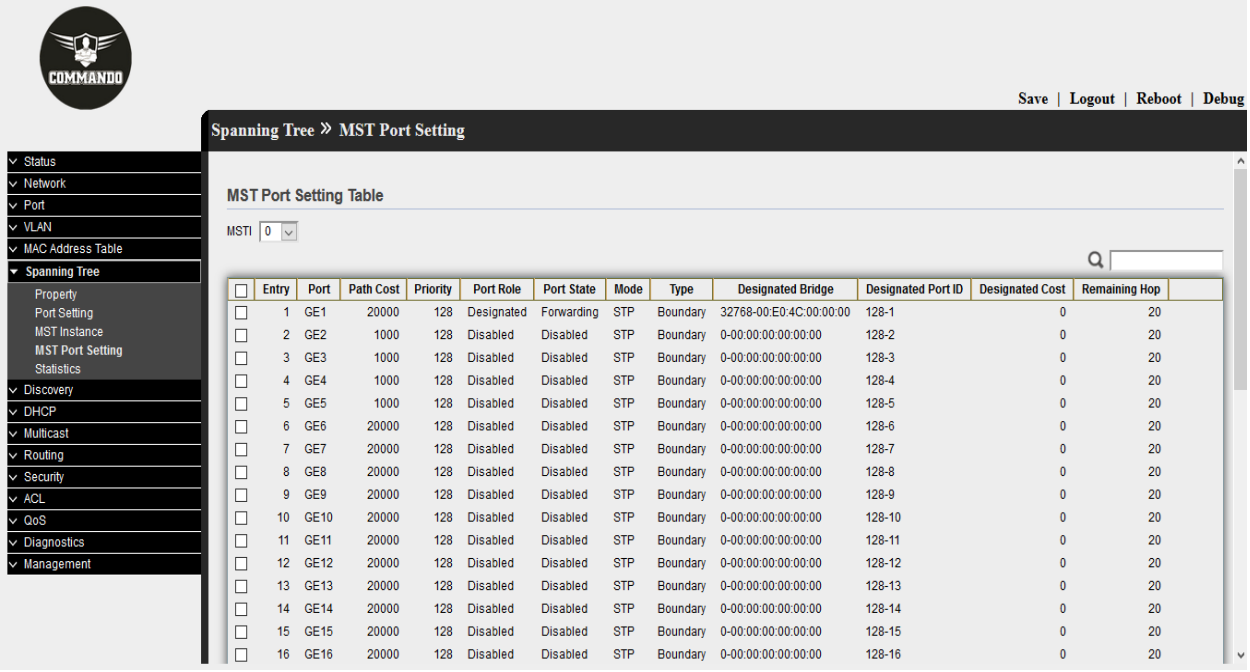


Fig 7.4.1 Spanning tree MST port setting table page

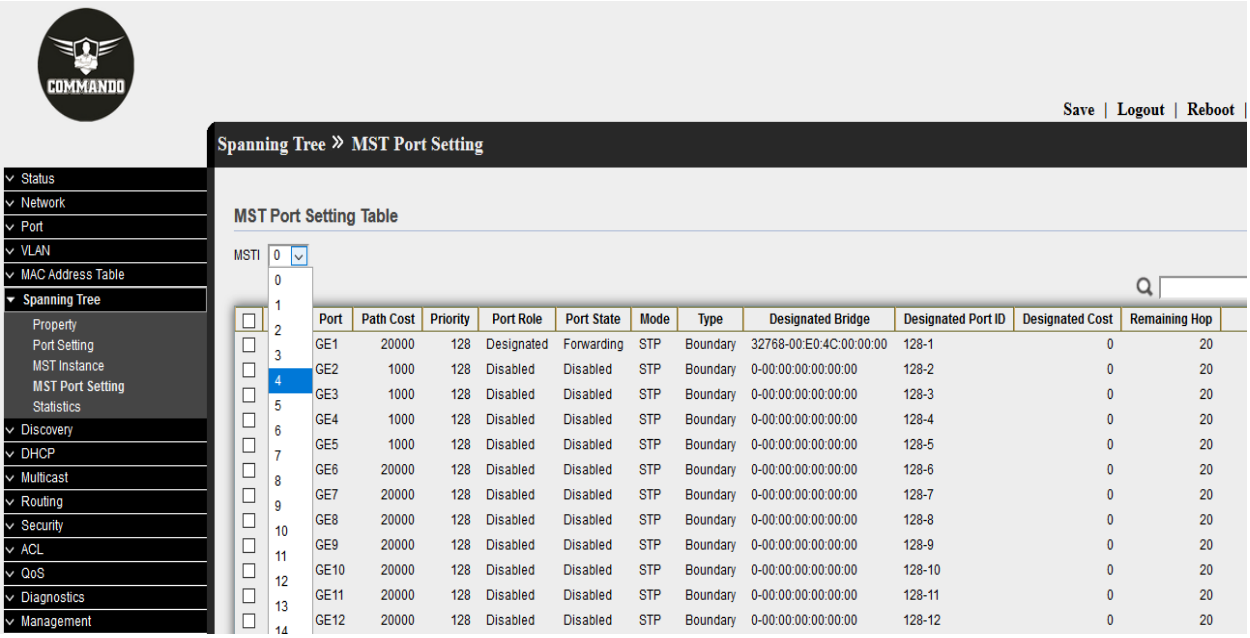


Fig 7.4.2 Spanning tree MST Instant selection page

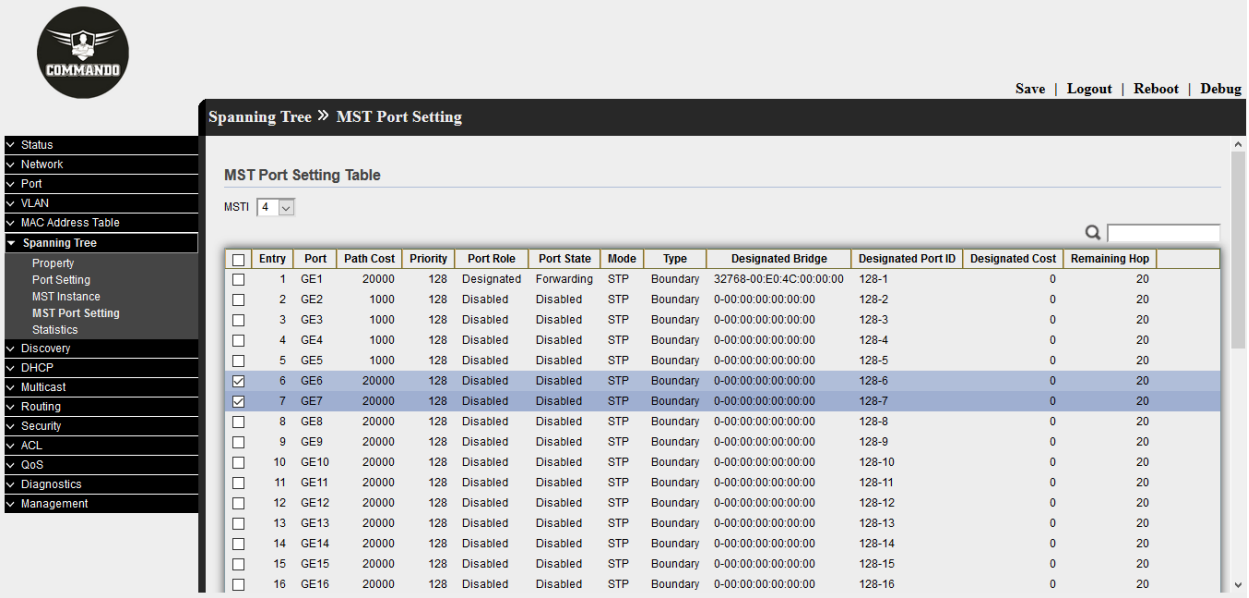


Fig 7.4.3 Spanning tree MST port selection page

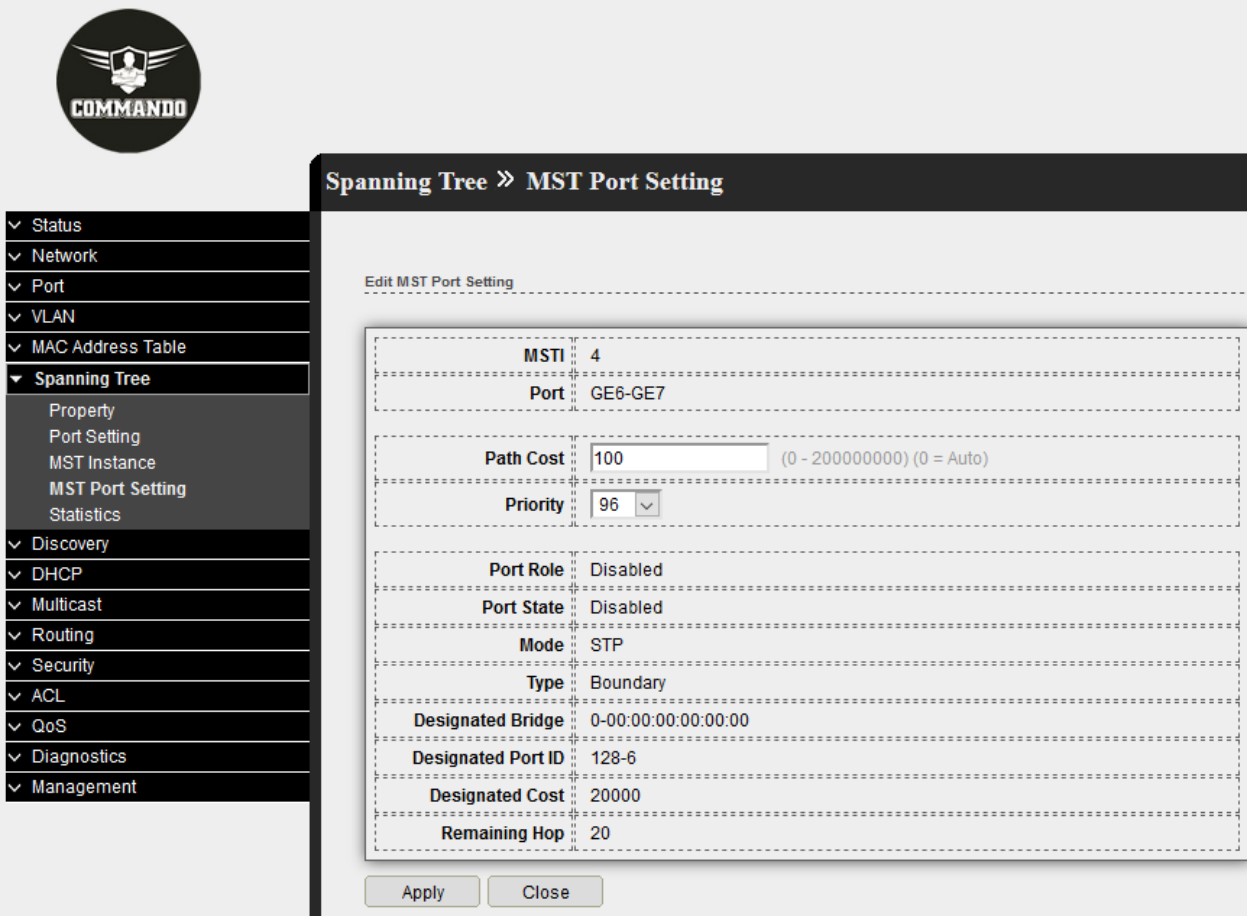


Fig 7.4.4 Edit MST port setting for selected port page

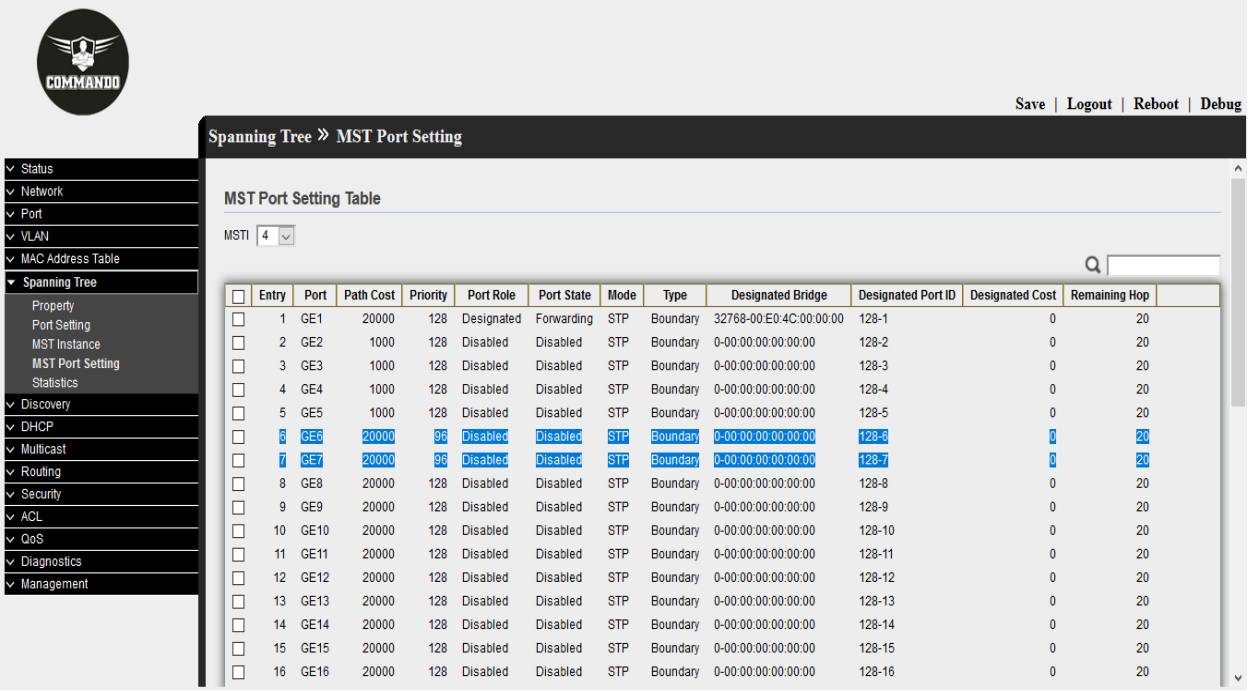


Fig 7.4.5 MST port setting table page

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.**

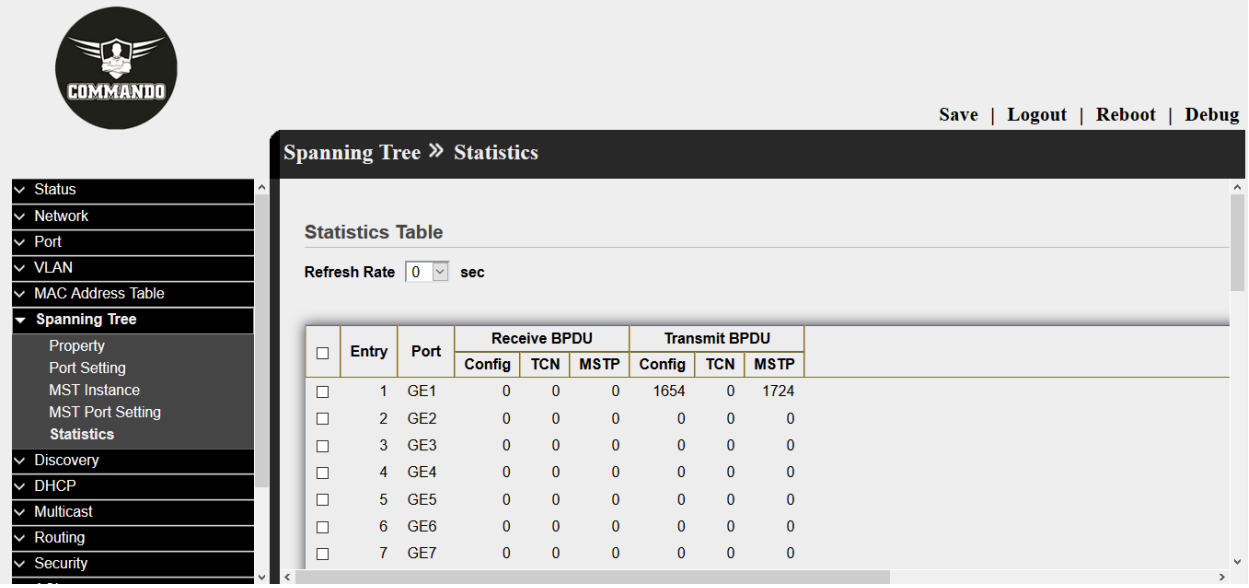


Fig 7.5.1 Spanning tree statistics table page

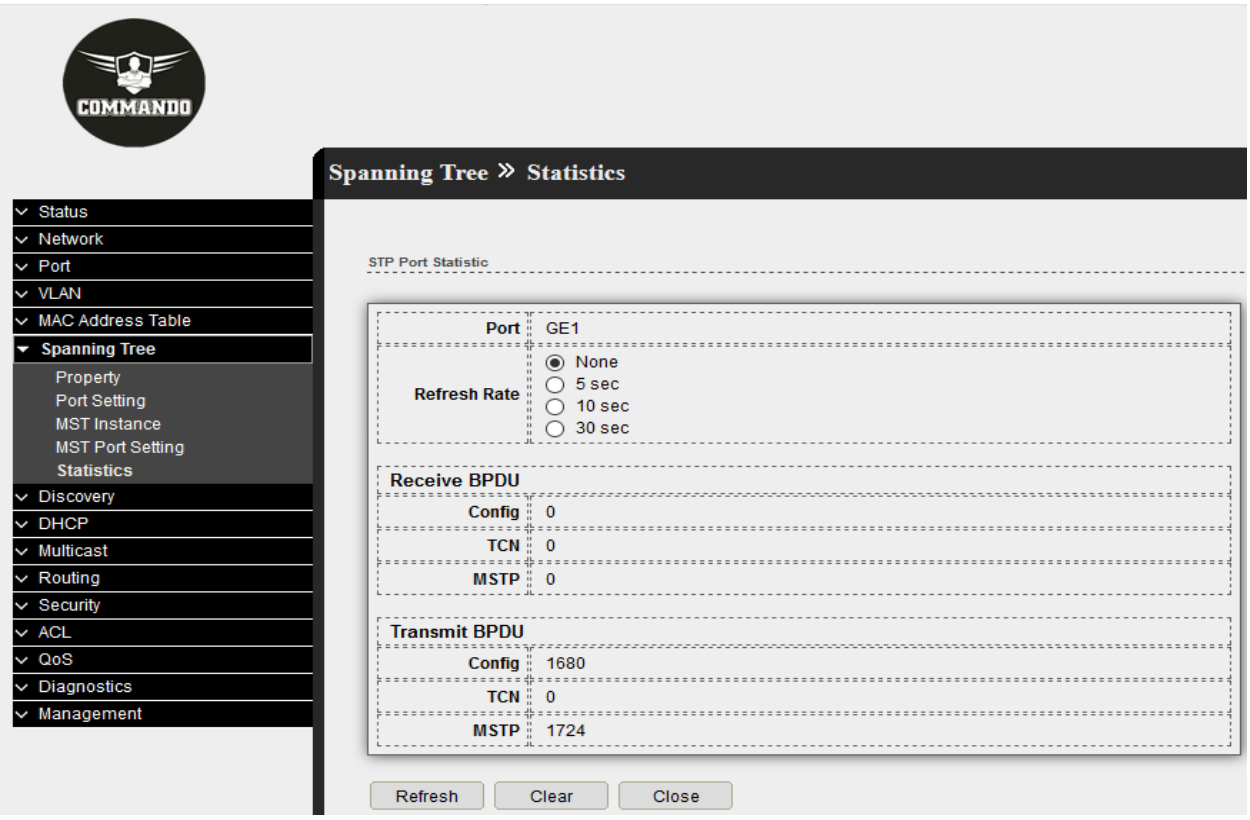


Fig 7.5.2 Spanning tree Port Statistic page

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.**

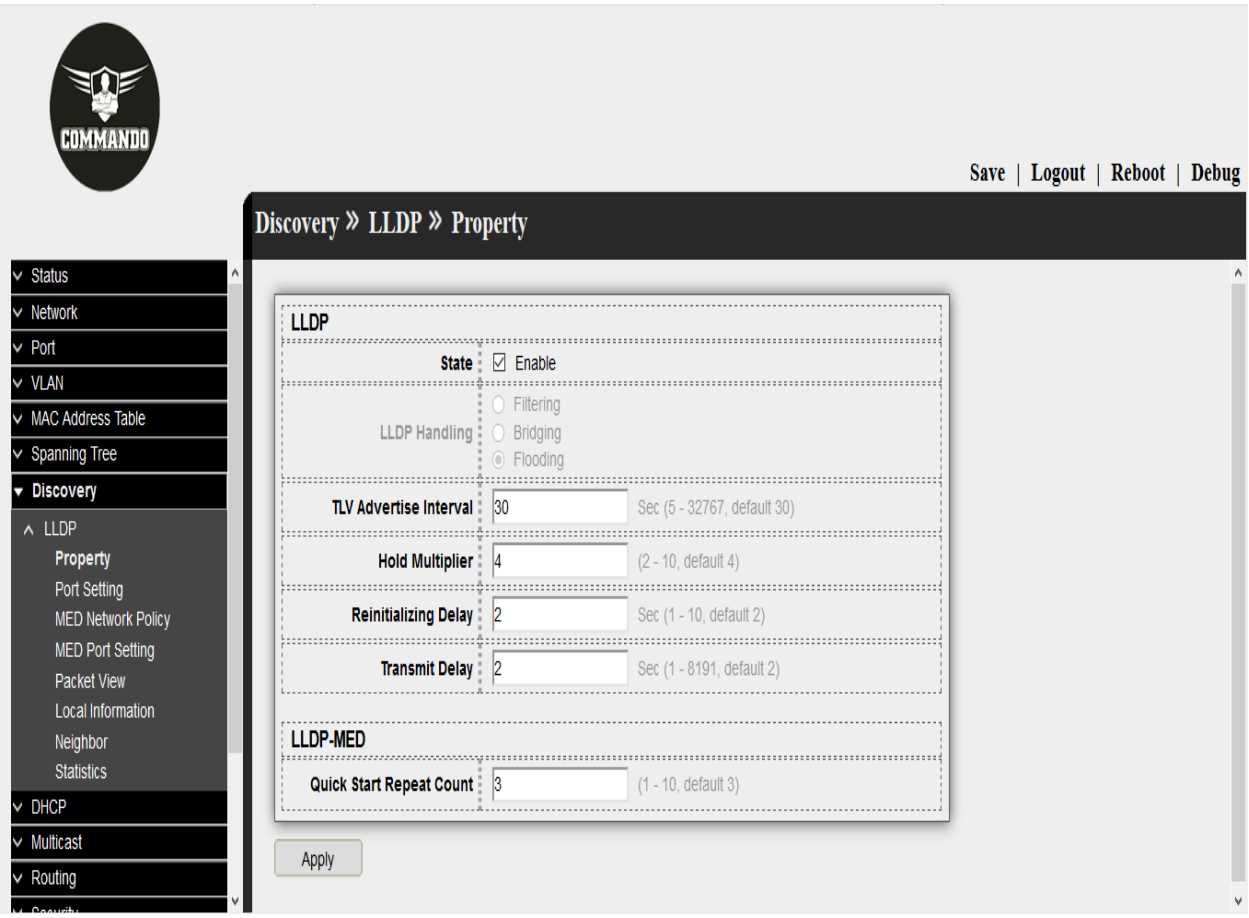


Fig 8.1.1 LLDP property page

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**

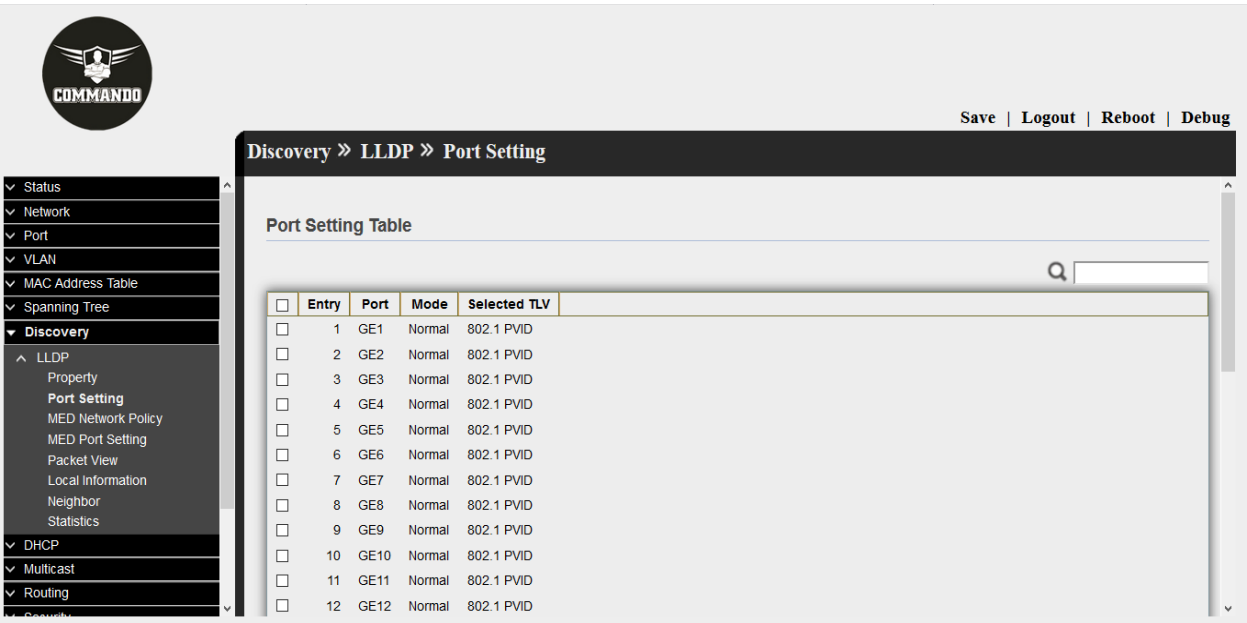


Fig 8.2.1 Default LLDP port setting table page

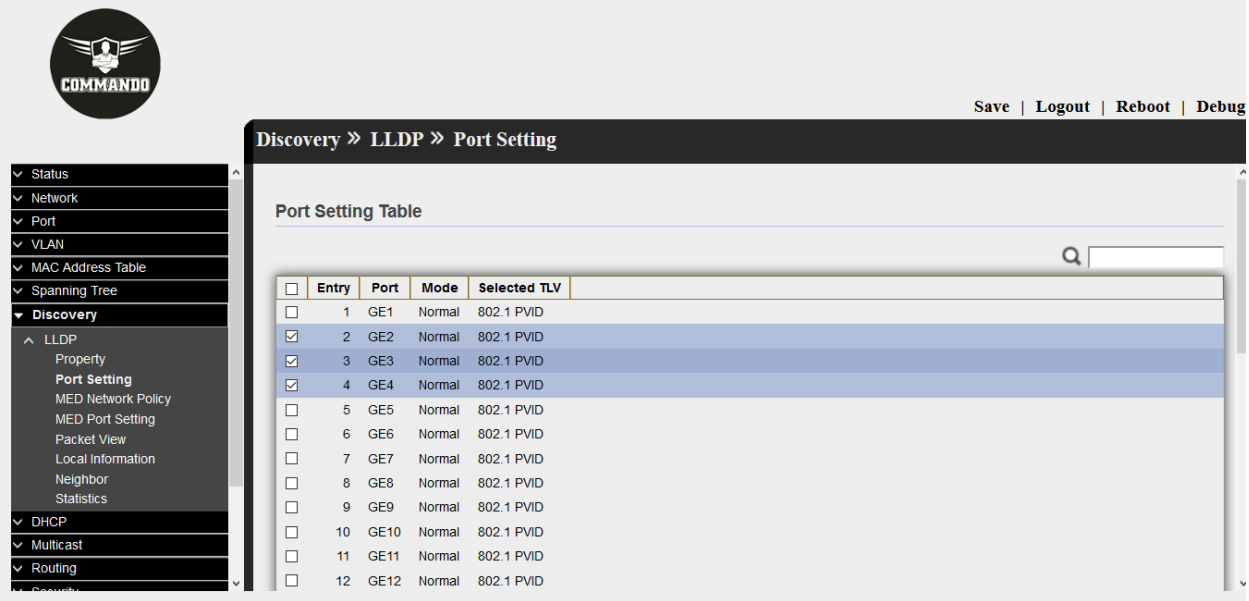


Fig 8.2.2 LLDP port setting selection of GE2, GE3 and GE4 page

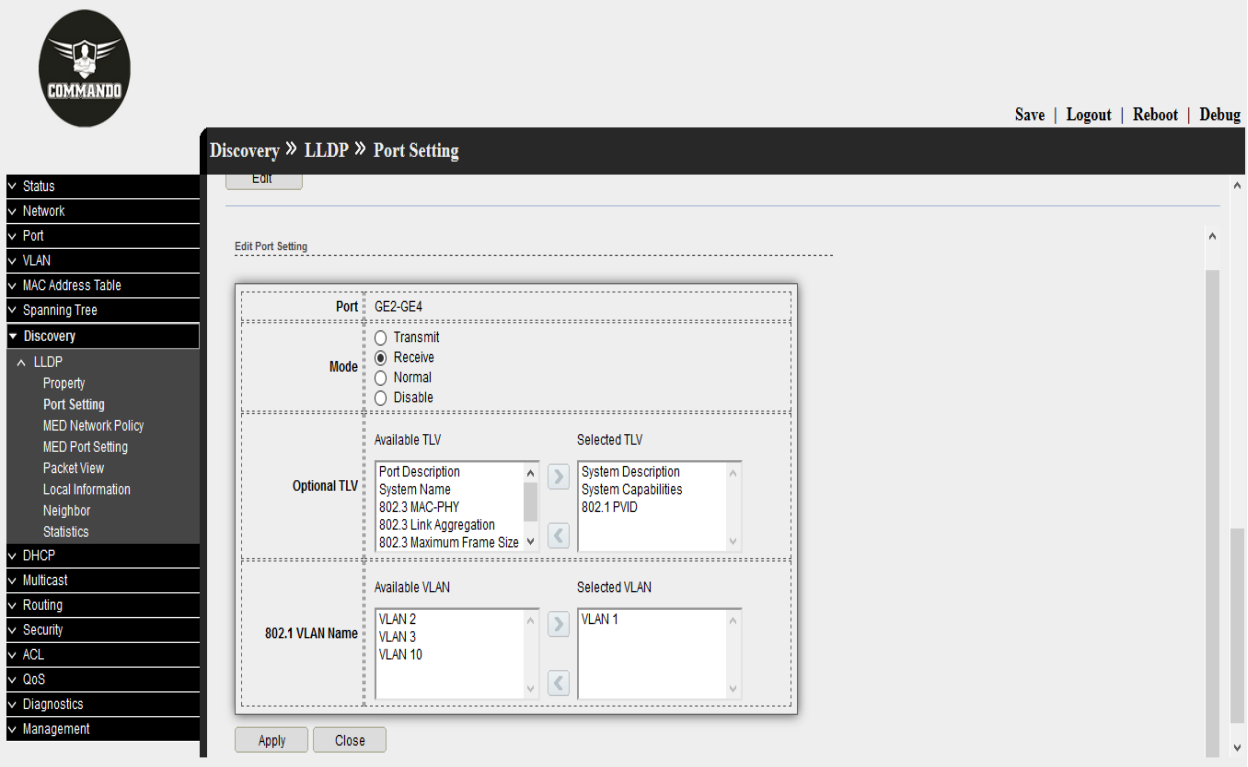


Fig 8.2.3 Edit LLDP port setting of GE2, GE3 and GE4 page

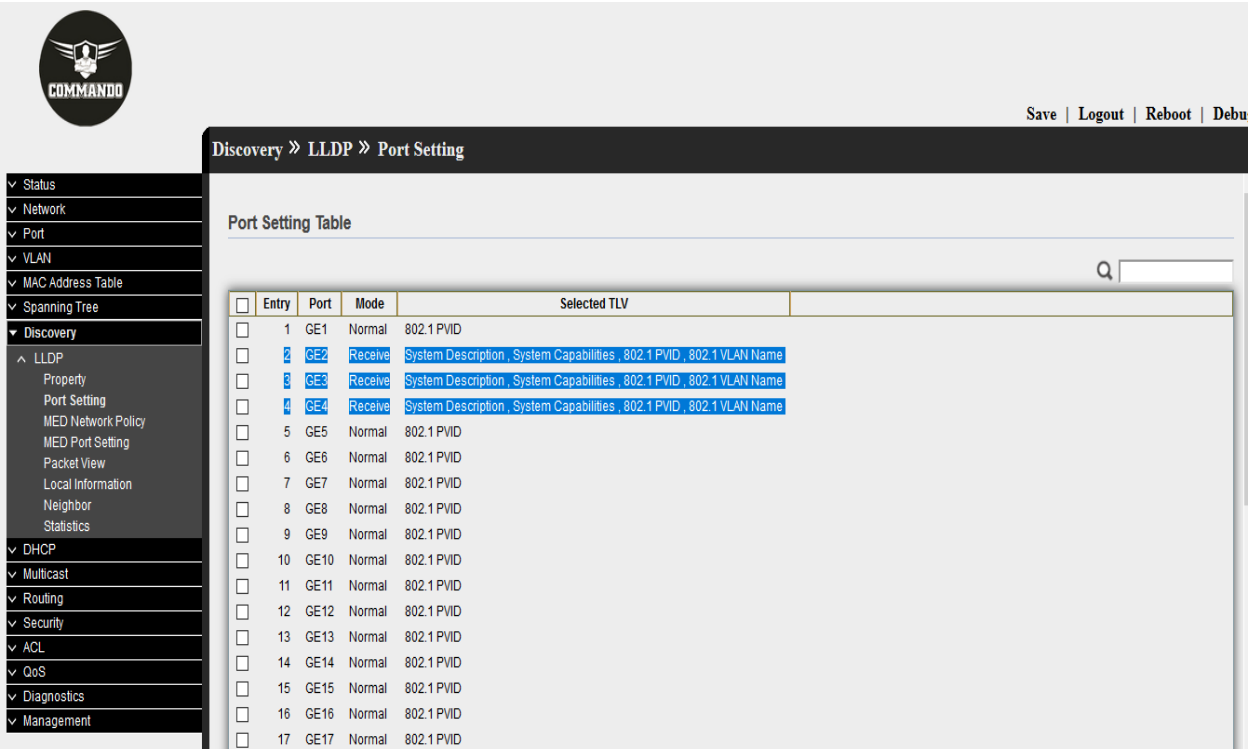


Fig 8.2.4 LLDP port setting table after Editing page

8.3 MED Network Policy

Enables the advertisement and discovery of network polices 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.**

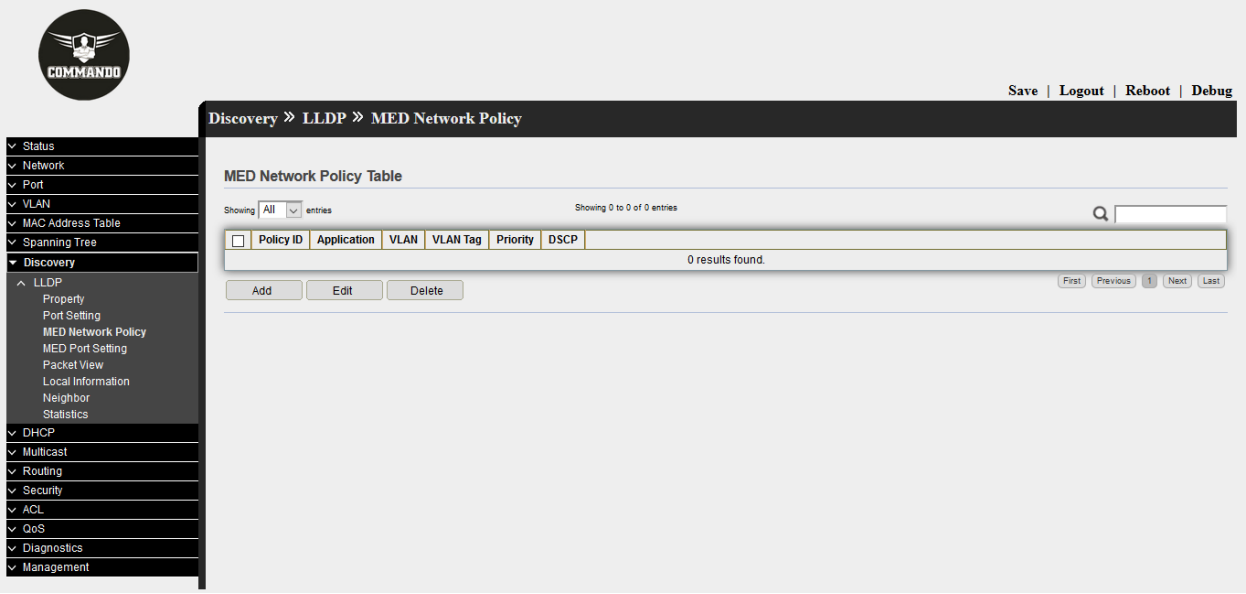


Fig 8.3.1 LLDP MED Network Policy page

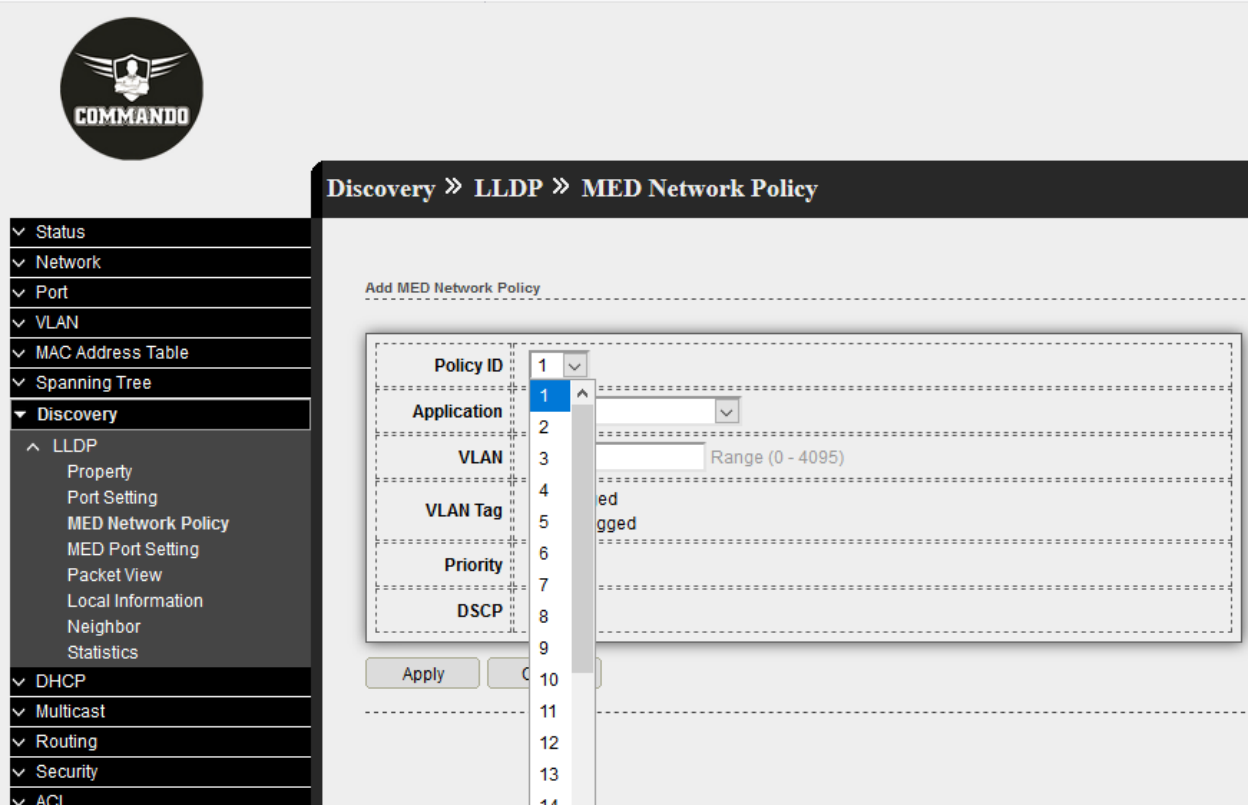


Fig 8.3.2 LLDP MED Network Policy ID page

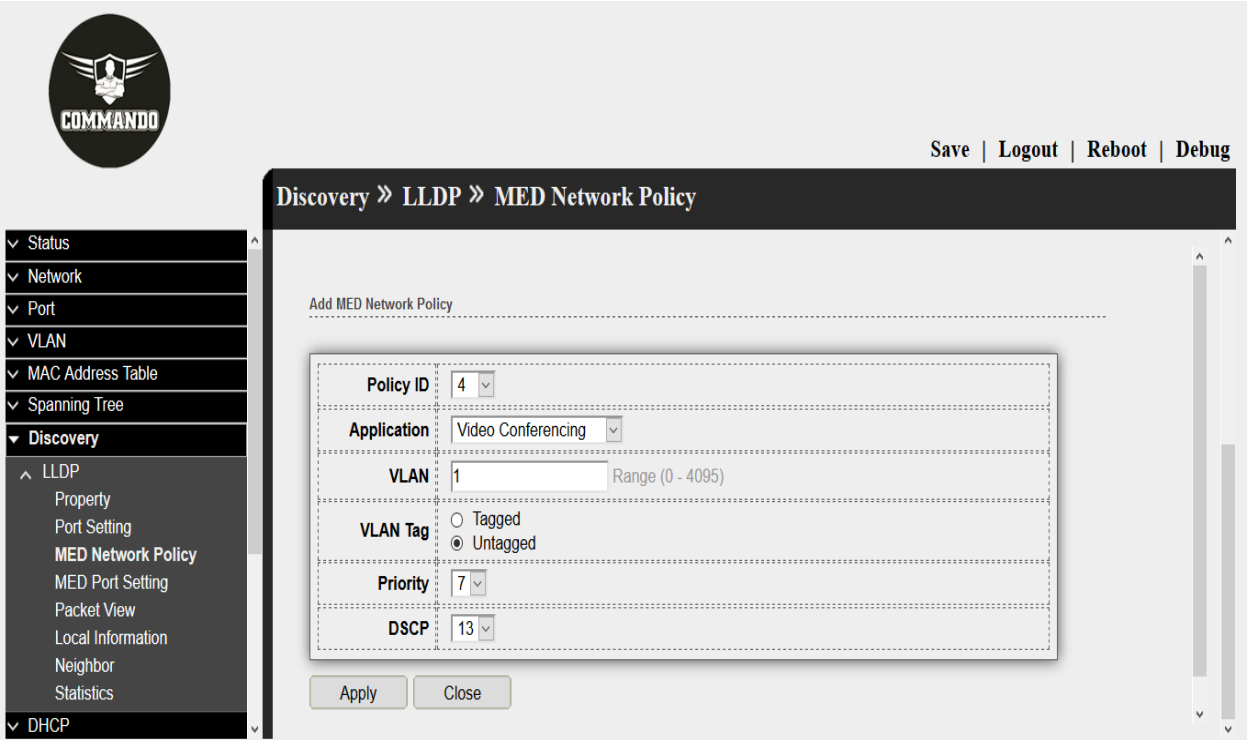


Fig 8.3.3 LLDP Add MED Network Policy page

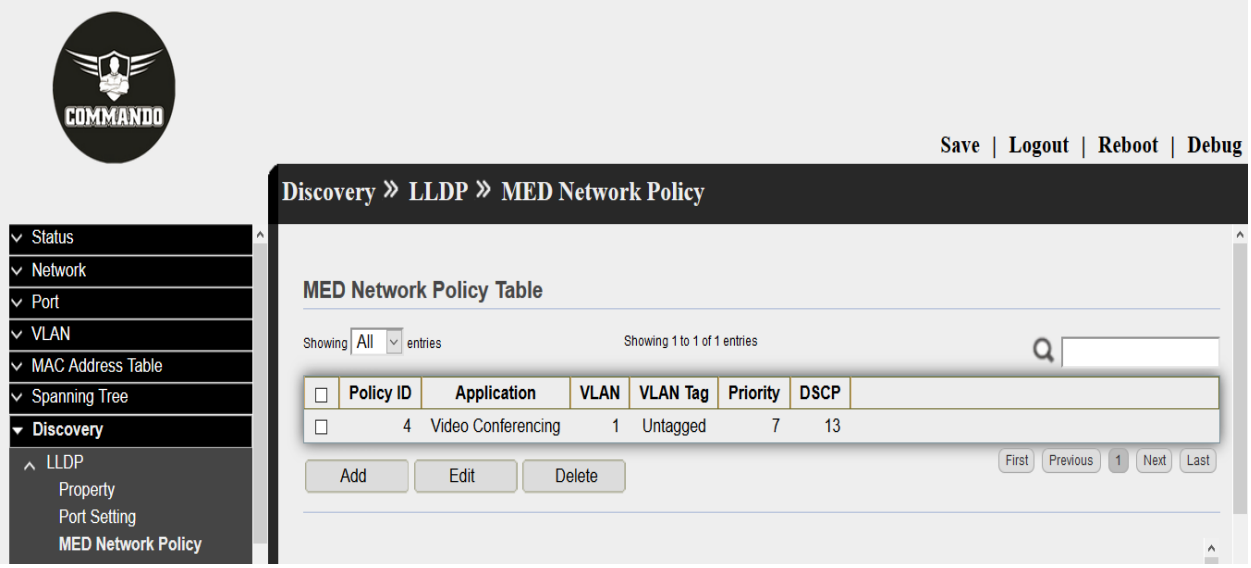


Fig 8.3.4 LLDP MED Network Policy Table after setting for Policy ID 4 page

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.**

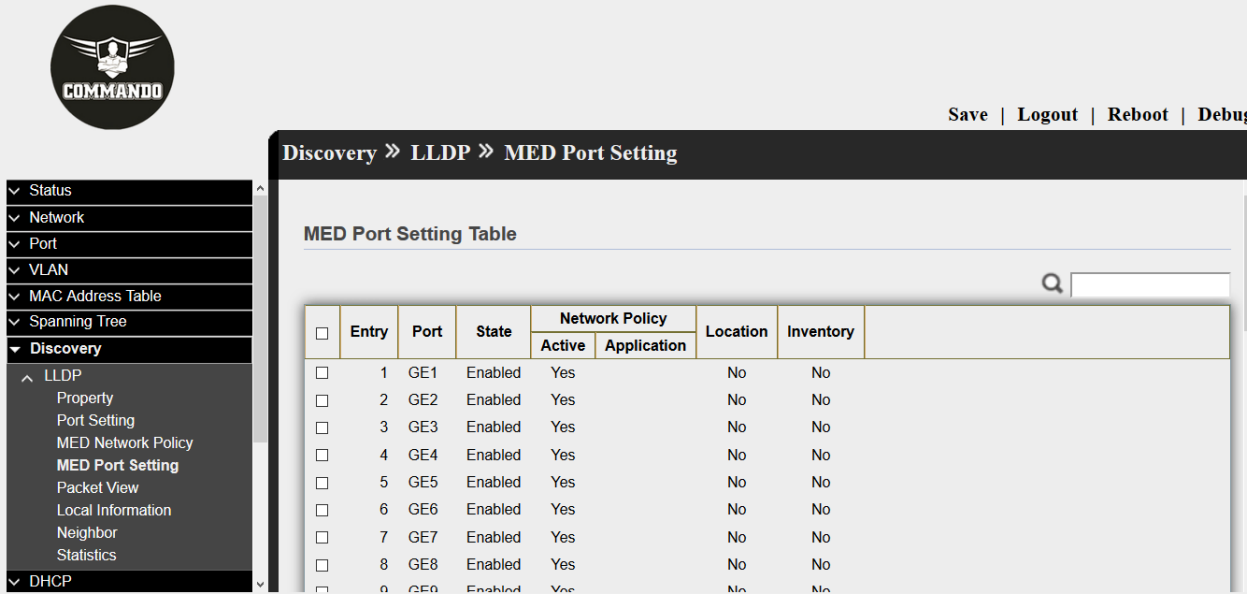


Fig 8.4.1 LLDP MED port setting table page

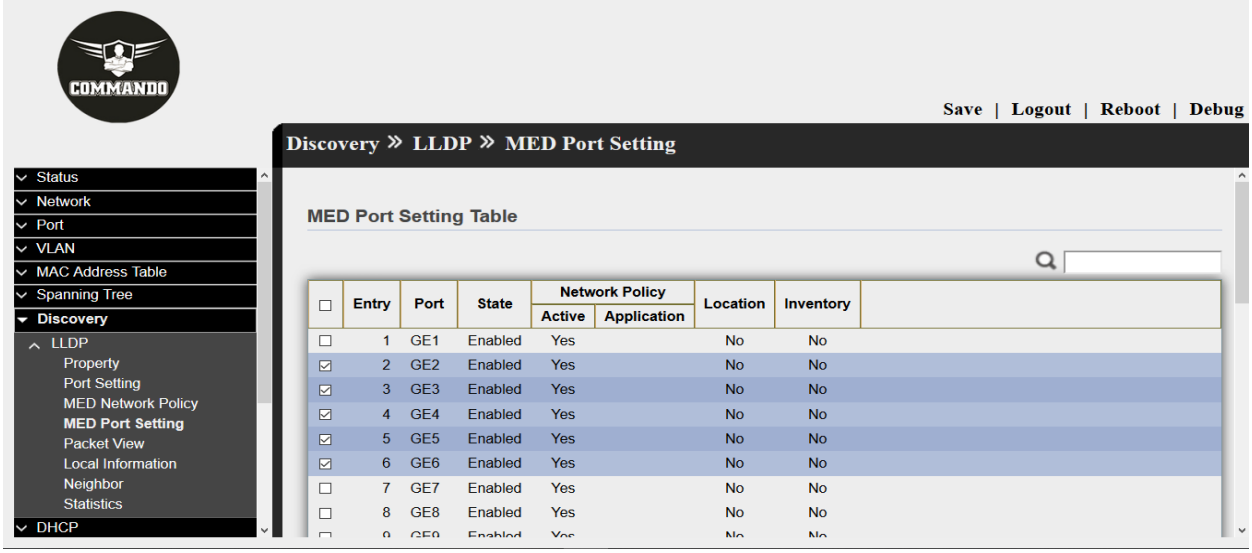


Fig 8.4.2 LLDP MED port setting for ports page

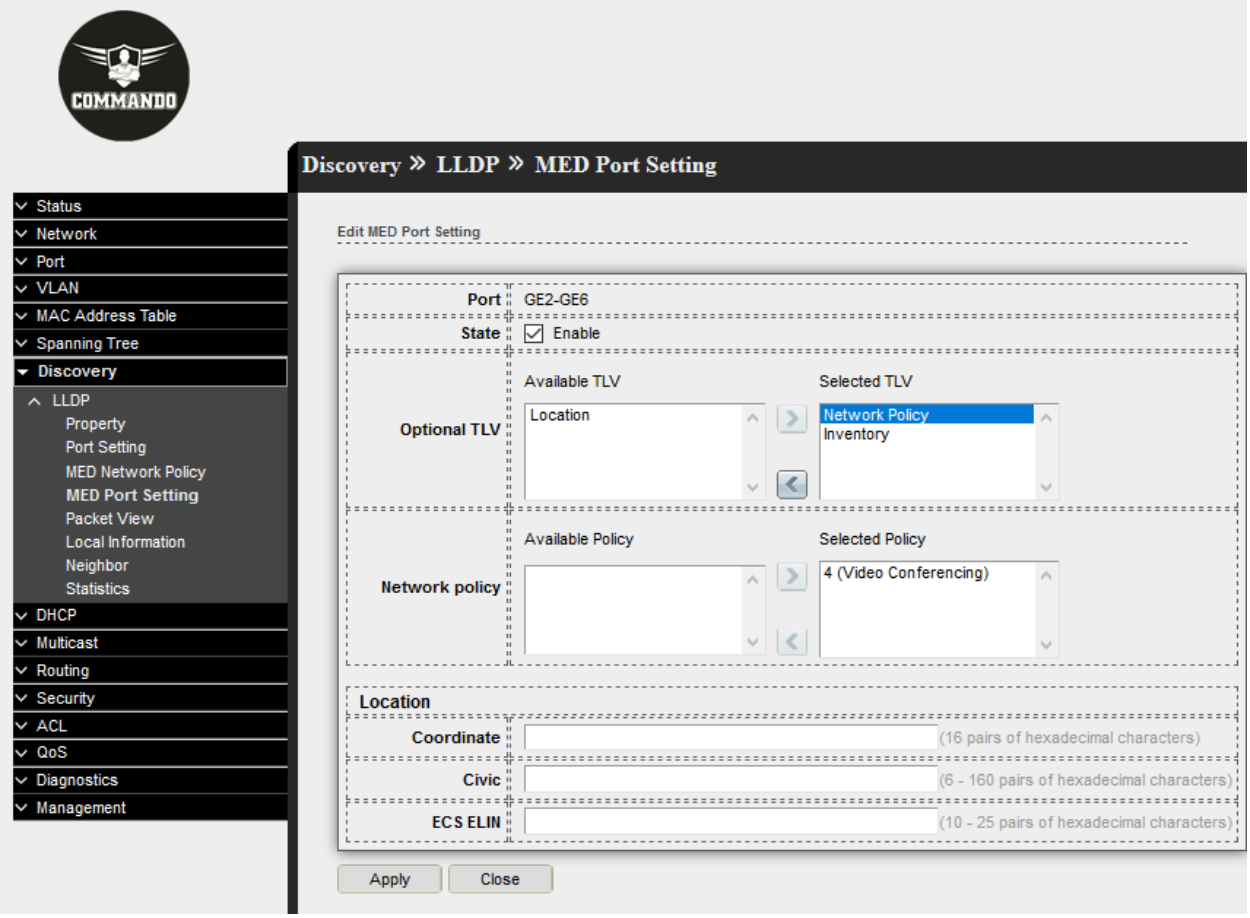


Fig 8.4.3 Edit LLDP MED port setting for selected ports page

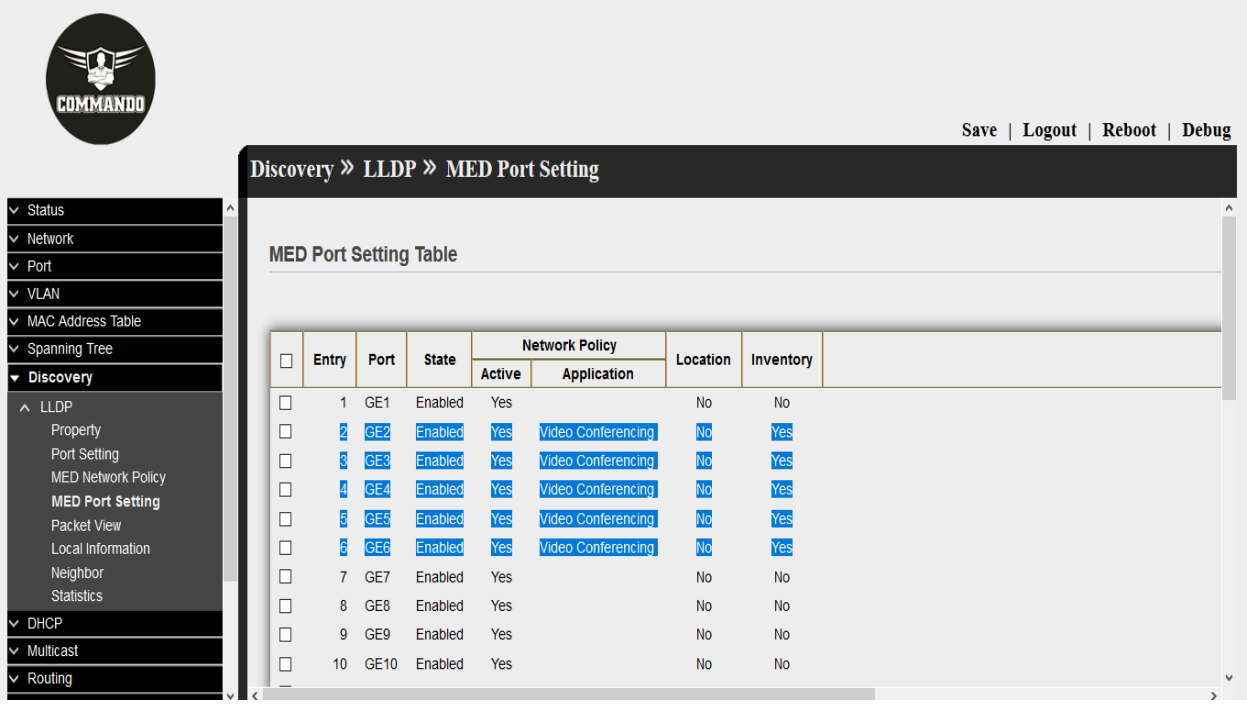


Fig 8.4.4 LLDP MED port setting Table page

8.5 Packet View

LLDP packets are send 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 on trouble shooting.

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

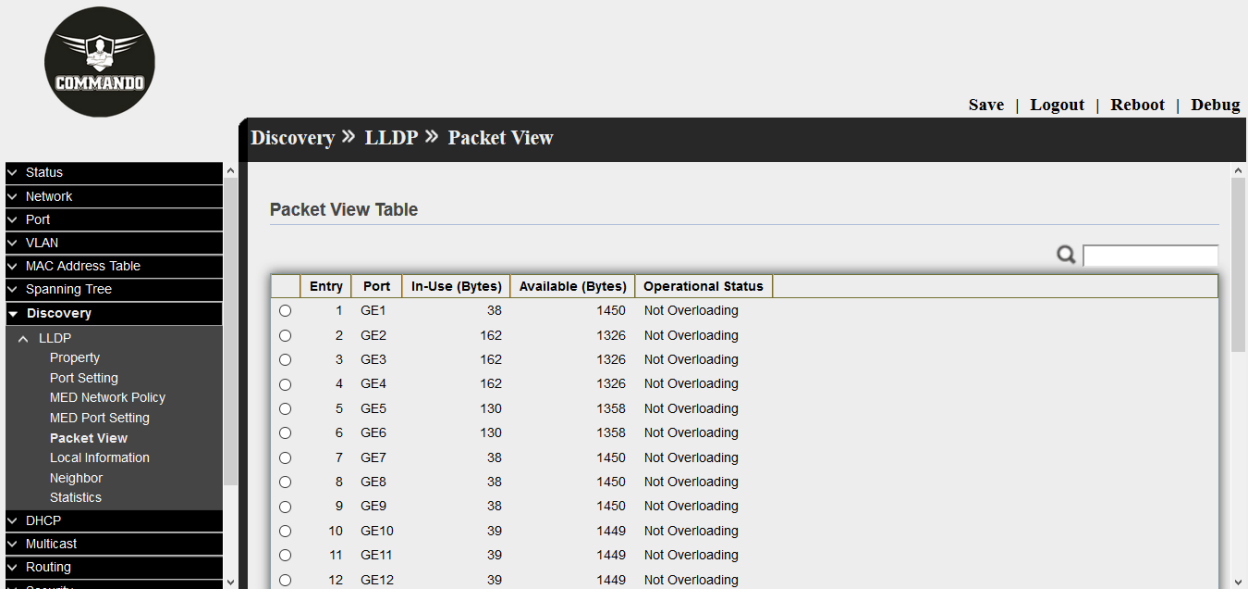


Fig 8.5.1 LLDP Packet view Table page

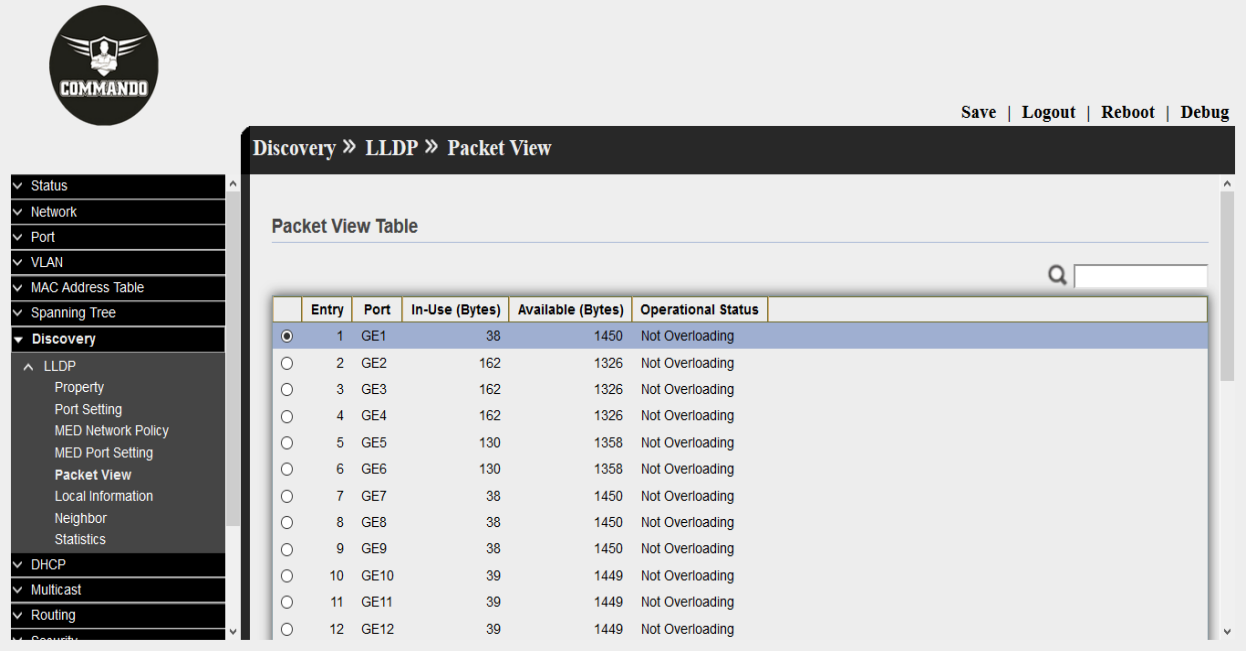


Fig 8.5.2 LLDP Packet view Table selecting GE1 port page

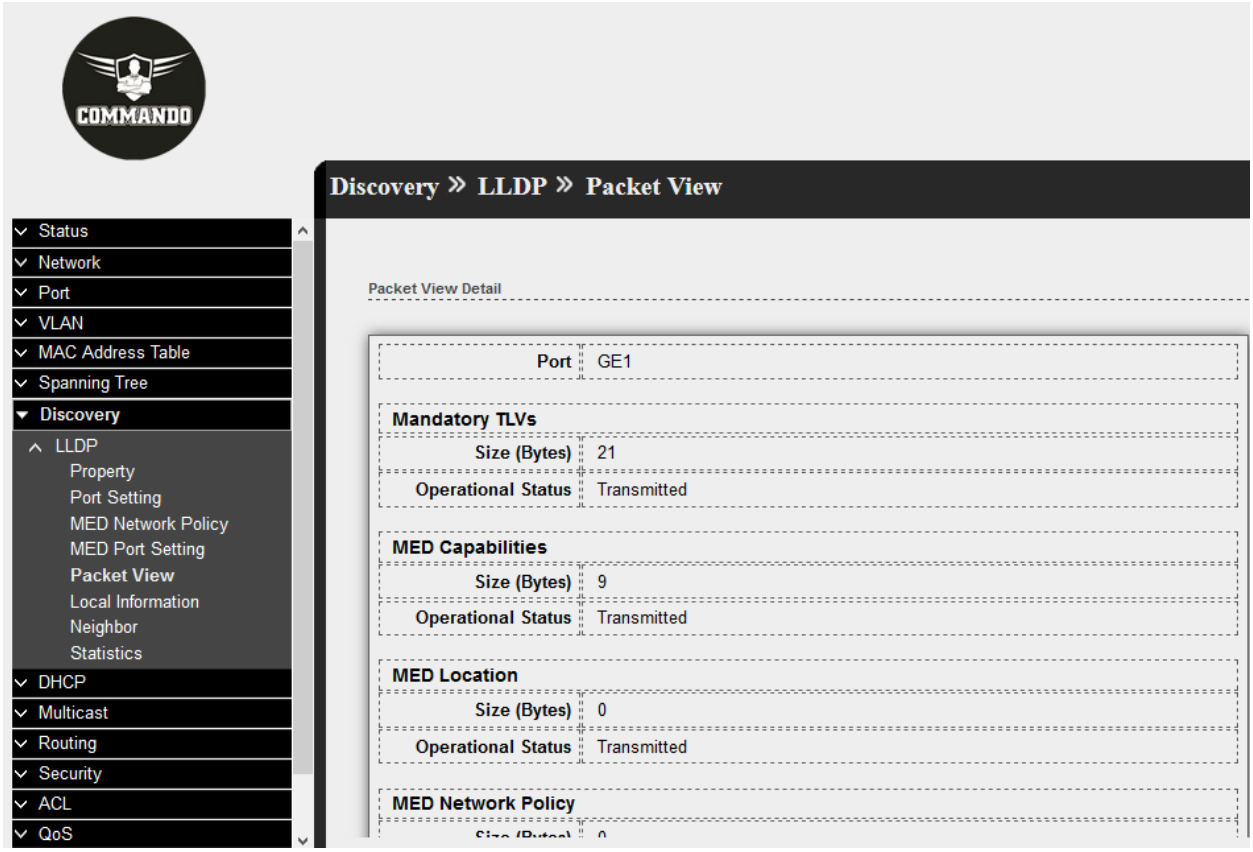


Fig 8.5.3 LLDP Packet view detail for GE1 port page

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.**

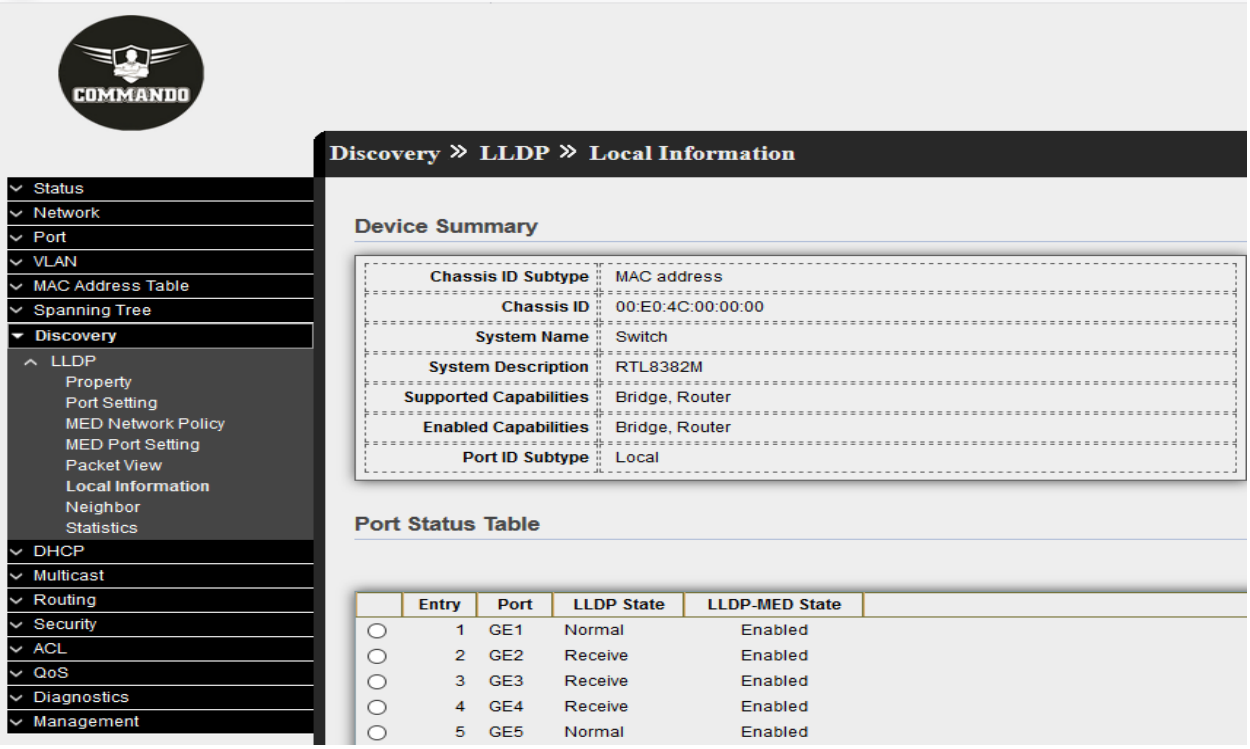


Fig 8.6.1 LLDP Local Information device summary page

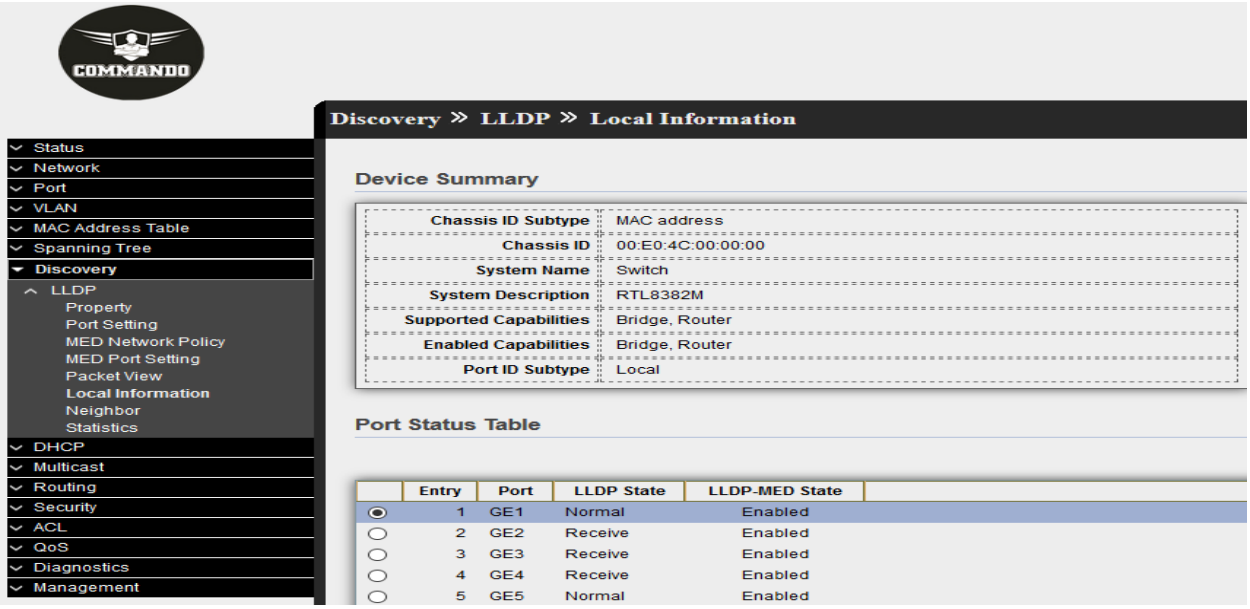


Fig 8.6.2 LLDP Local Information Selecting port GE1 page

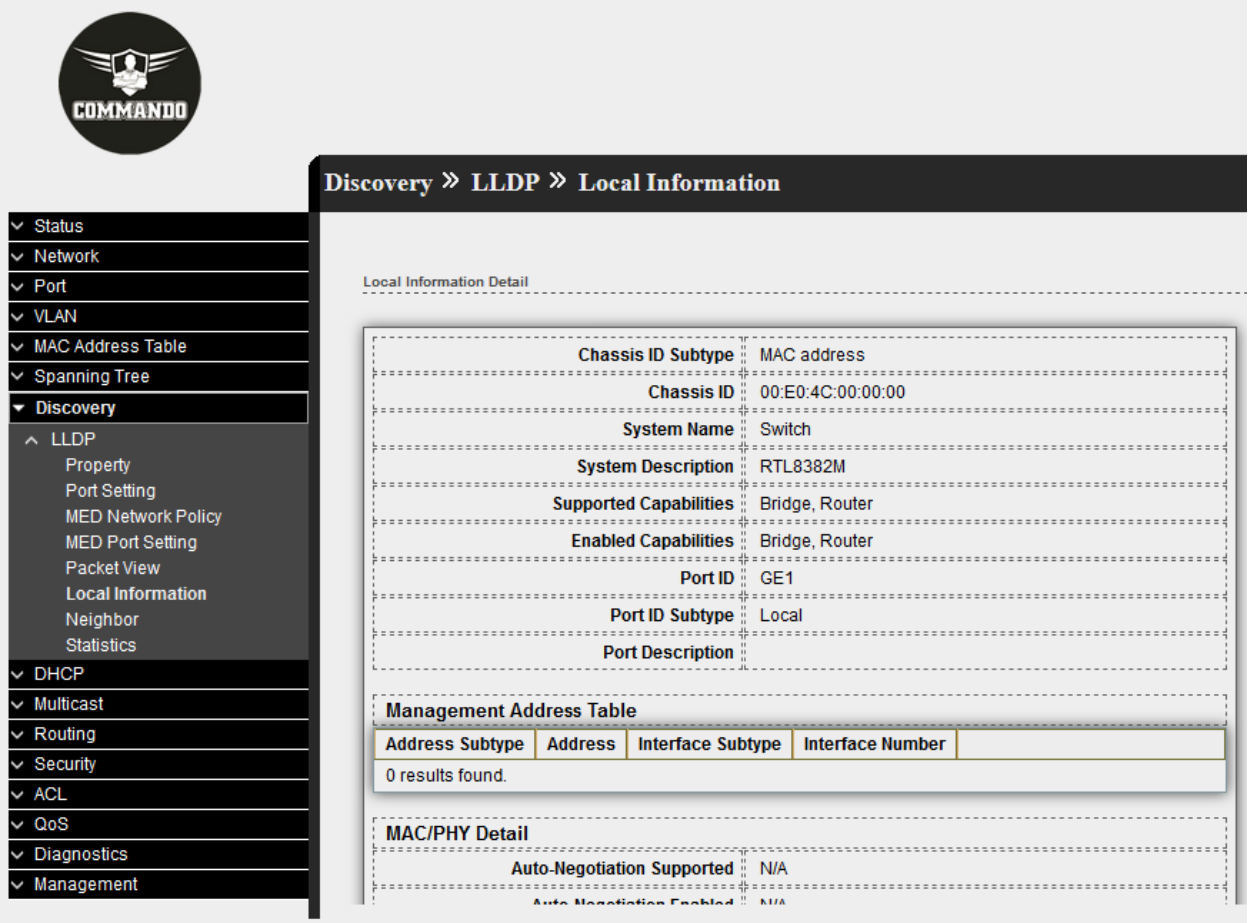


Fig 8.6.3 LLDP Local Information details for port GE1 page

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.**

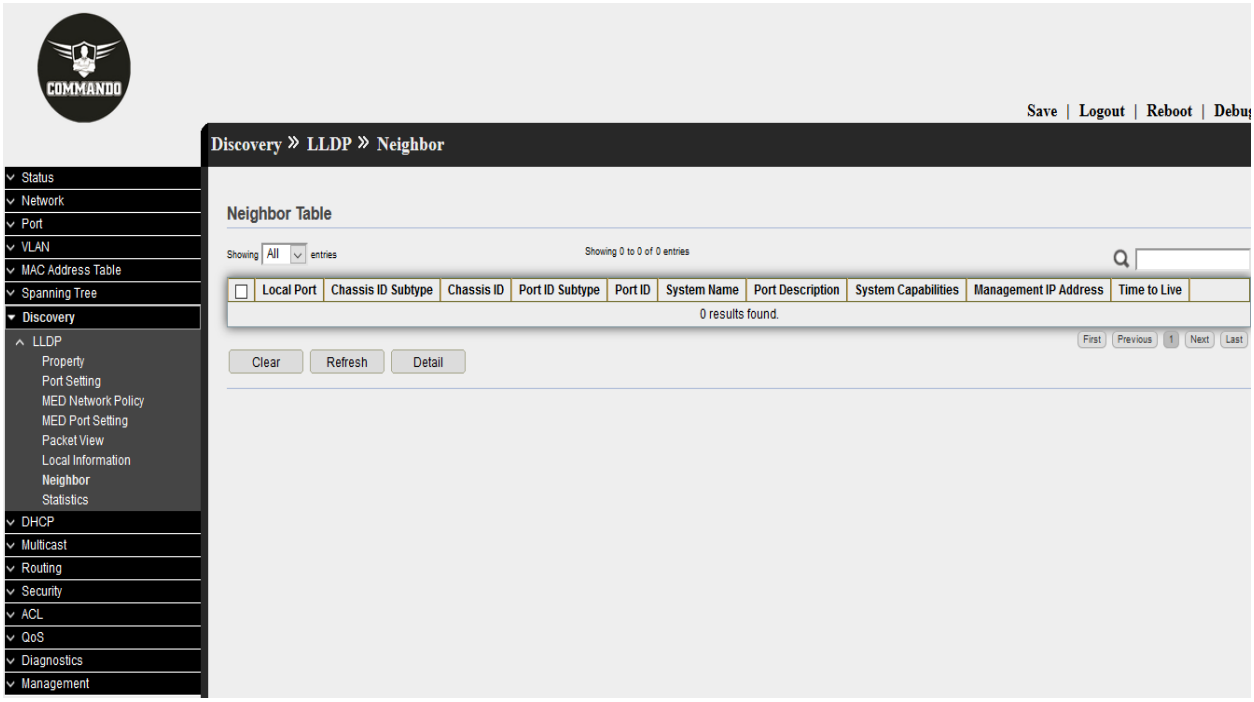


Fig 8.7.1 LLDP Neighbors table default page

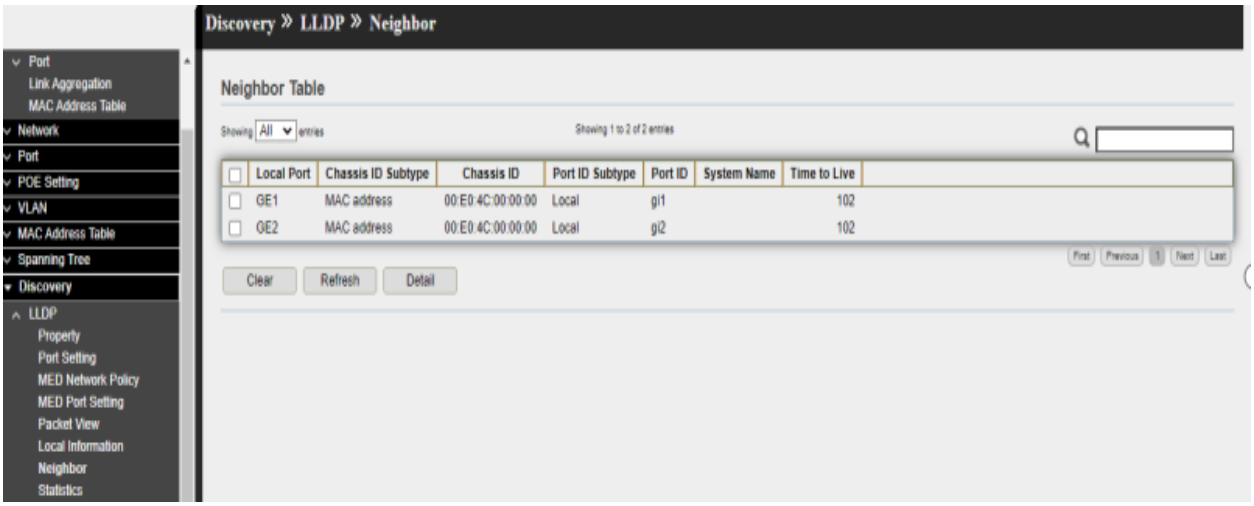


Fig 8.7.2 LLDP Neighbors table after enabling LLDP page

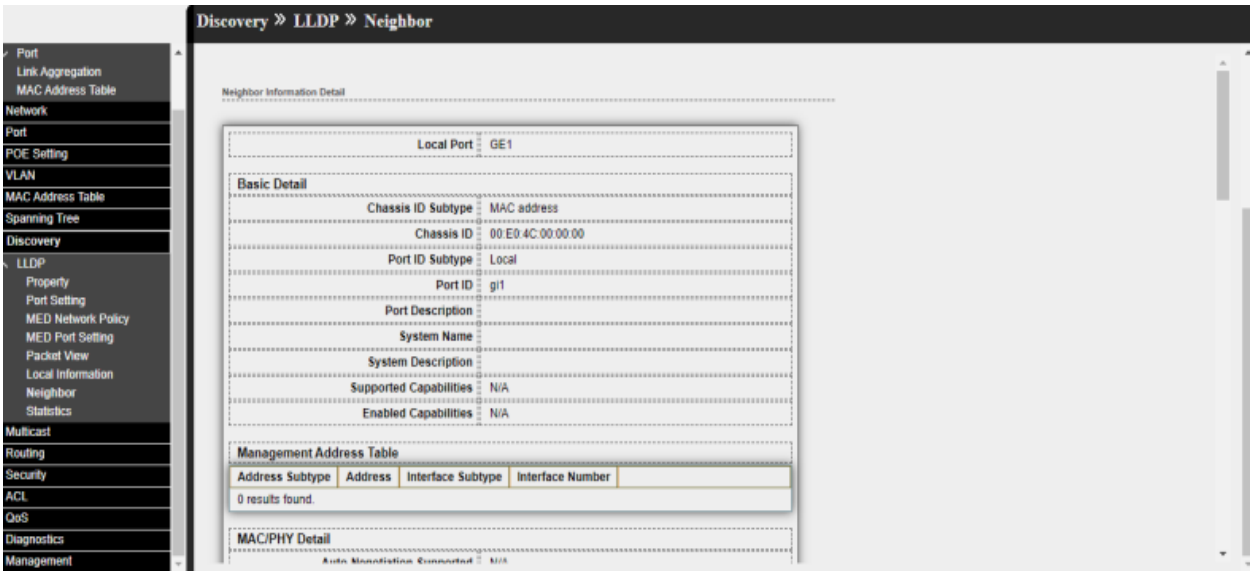


Fig 8.7.3 LLDP Neighbors information detail page

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.**

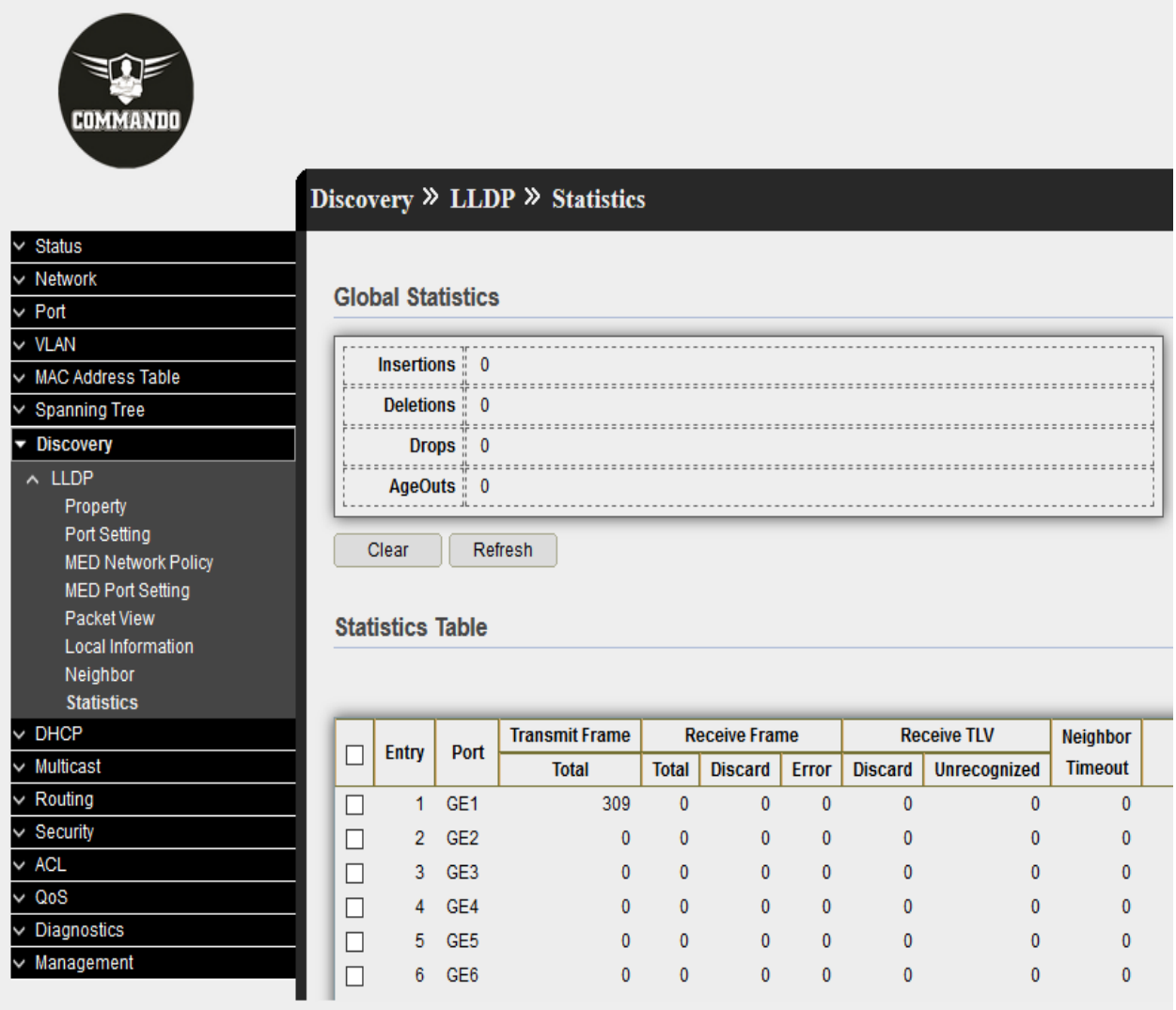


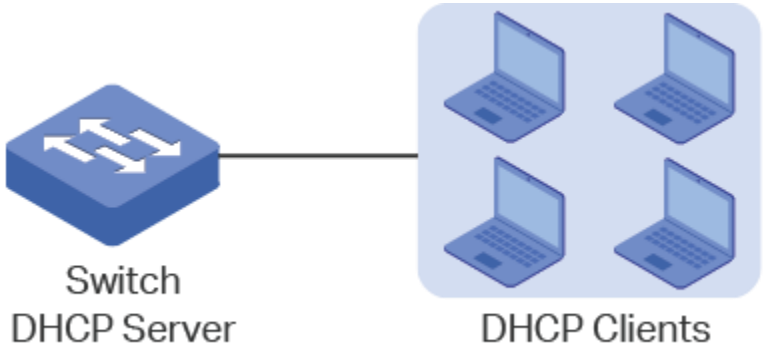
Fig 8.8.1 LLDP Global statistics page

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.



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 realted things automatically to connected hosts.

IP Pool Setting:--> You can customize the DHCP pool subnet and address range to provide simultaneous access to more 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.**

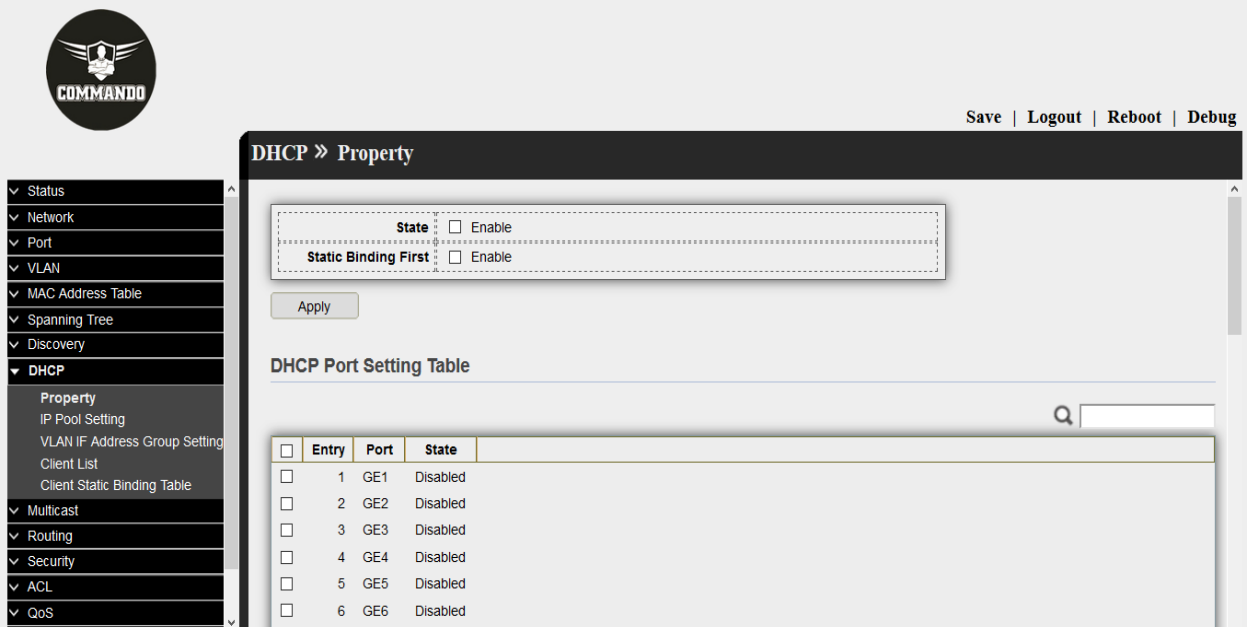


Fig 9.1.1 Default DHCP Property page

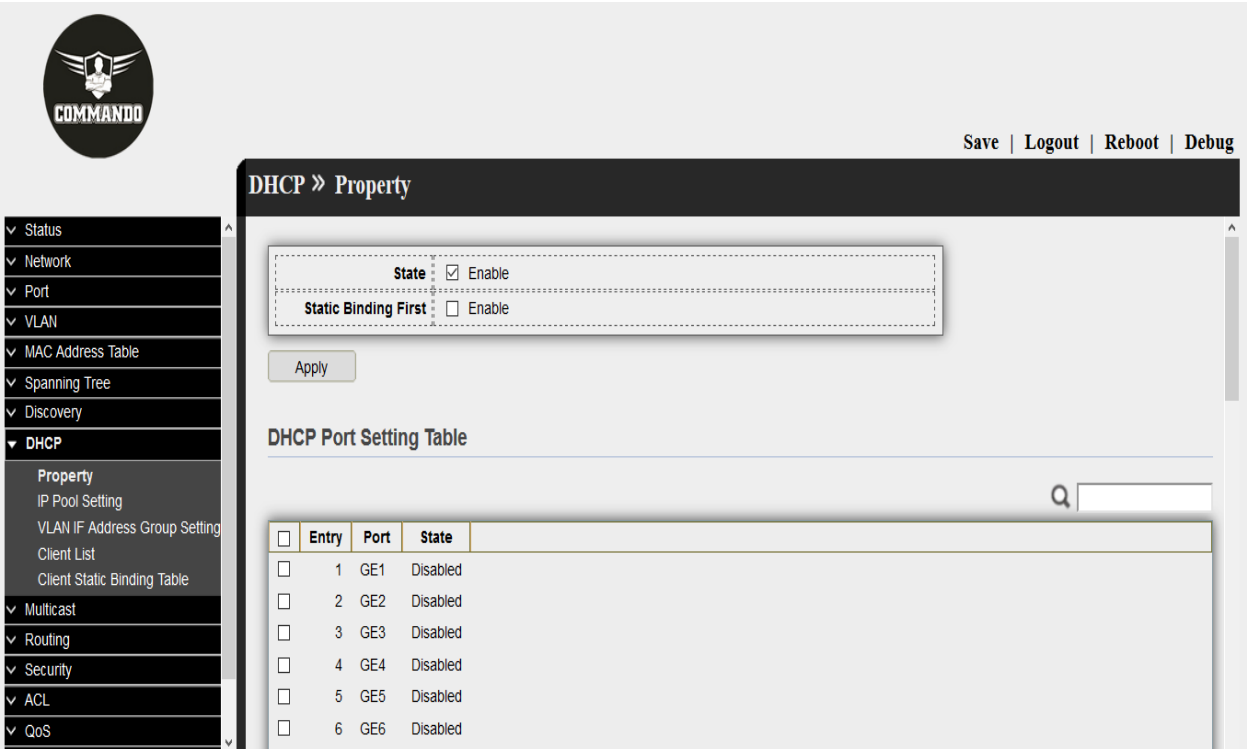


Fig 9.1.2 Enable DHCP Property page

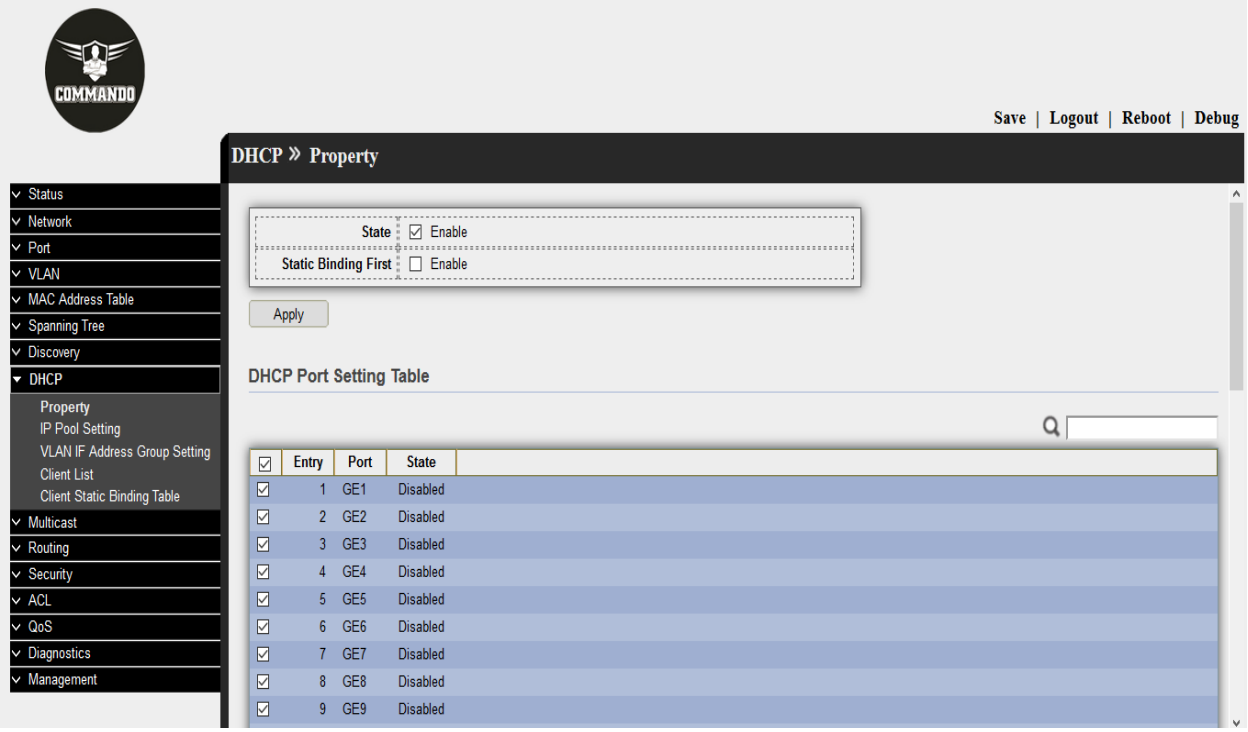


Fig 9.1.3 Selecting ports on DHCP Property page

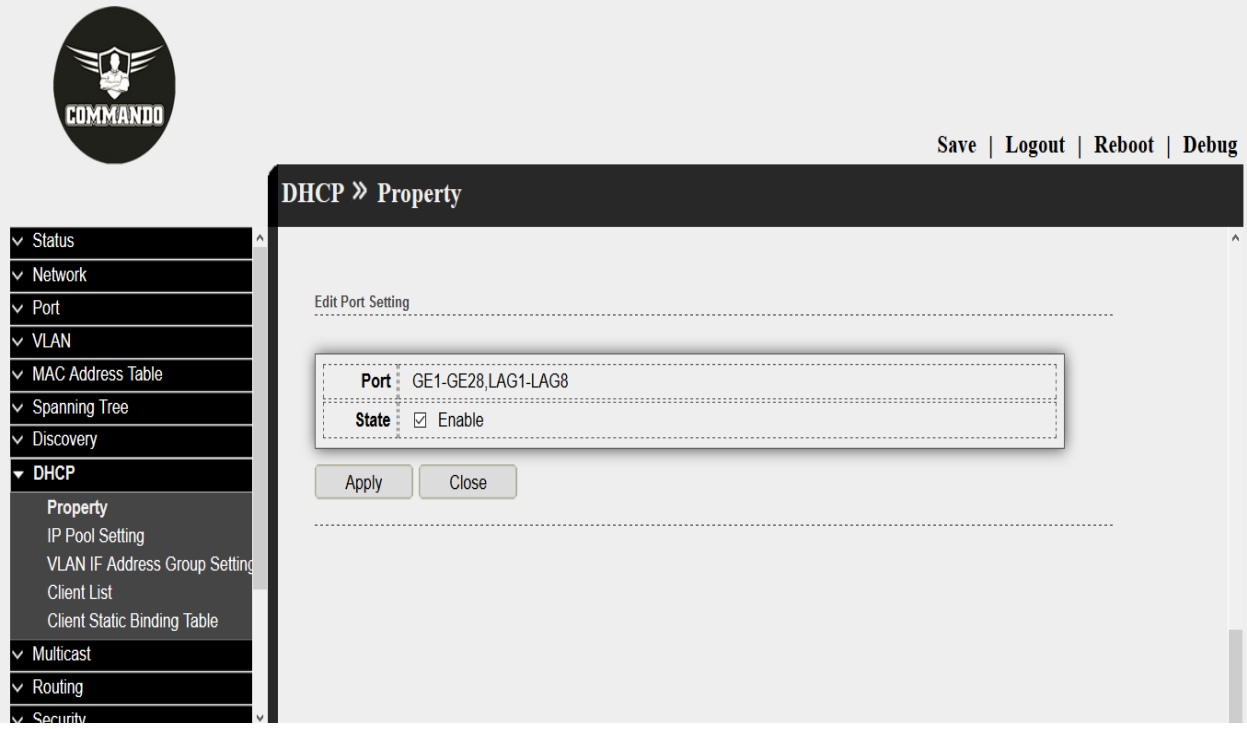


Fig 9.1.4 Edit ports setting DHCP Property page

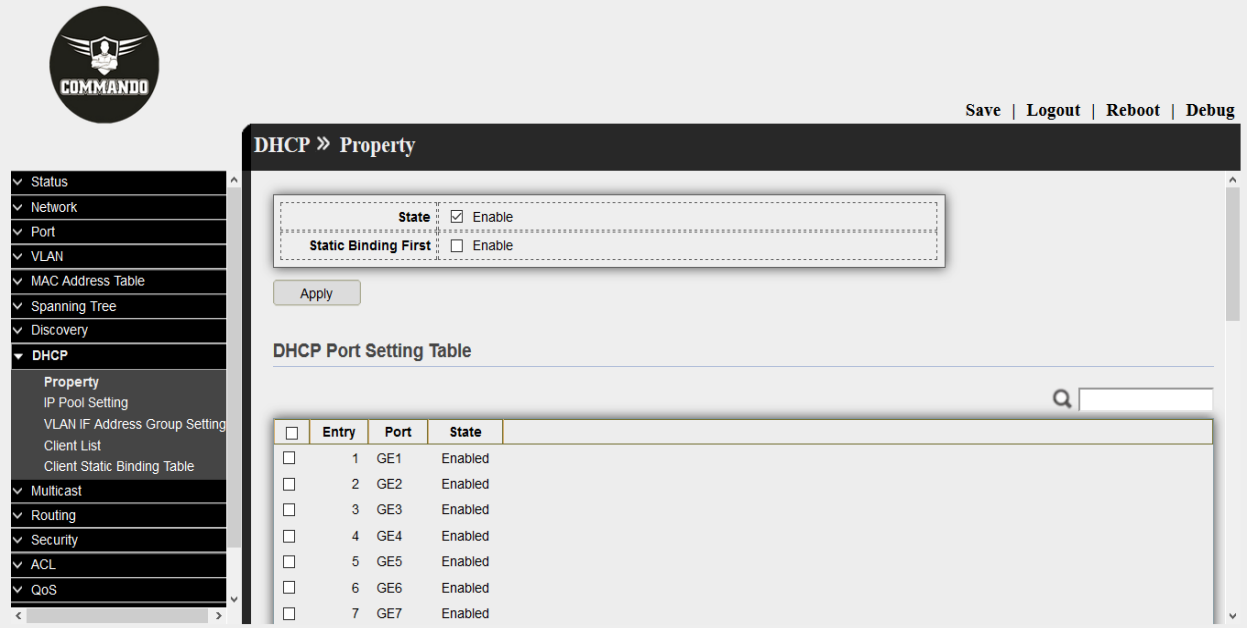


Fig 9.1.5 DHCP port setting table after enabling page

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.**

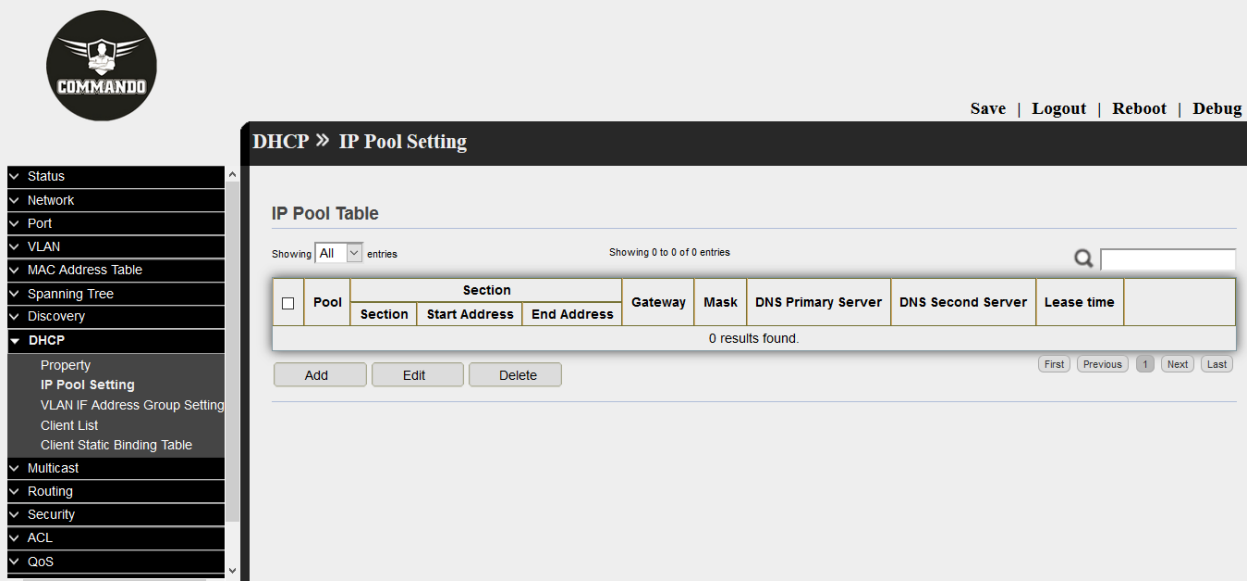


Fig 9.2.1 Default DHCP IP Pool setting page

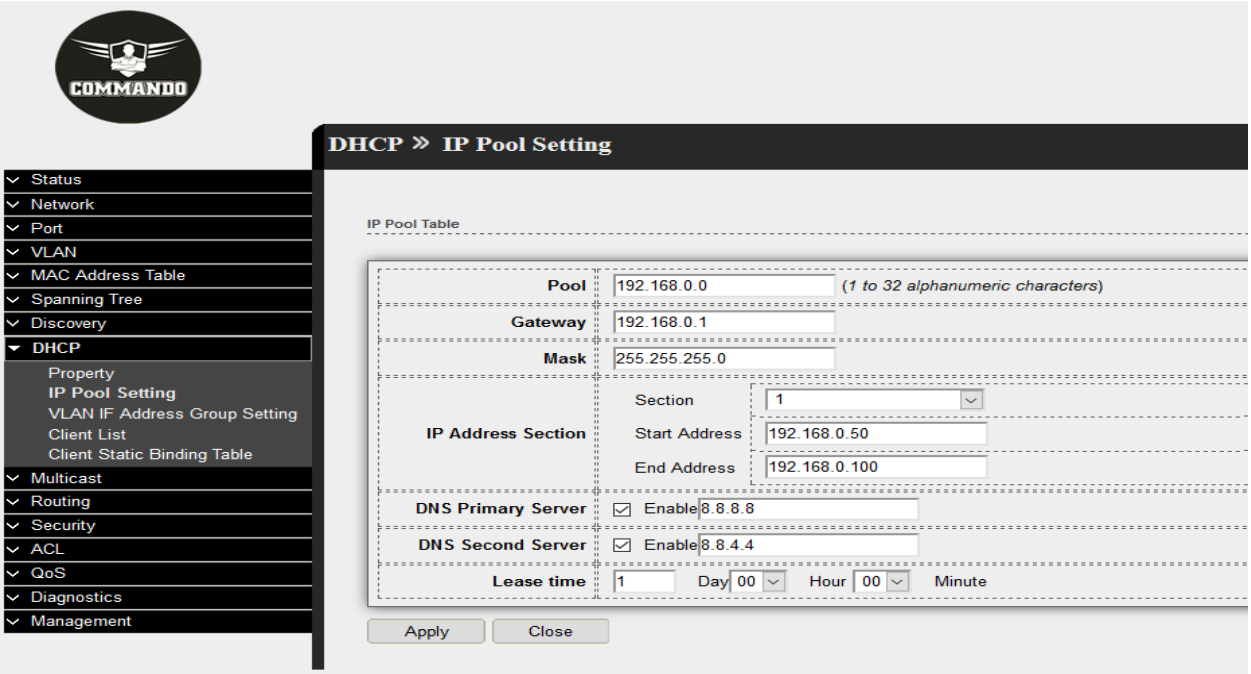


Fig 9.2.2 Edit DHCP IP Pool setting page

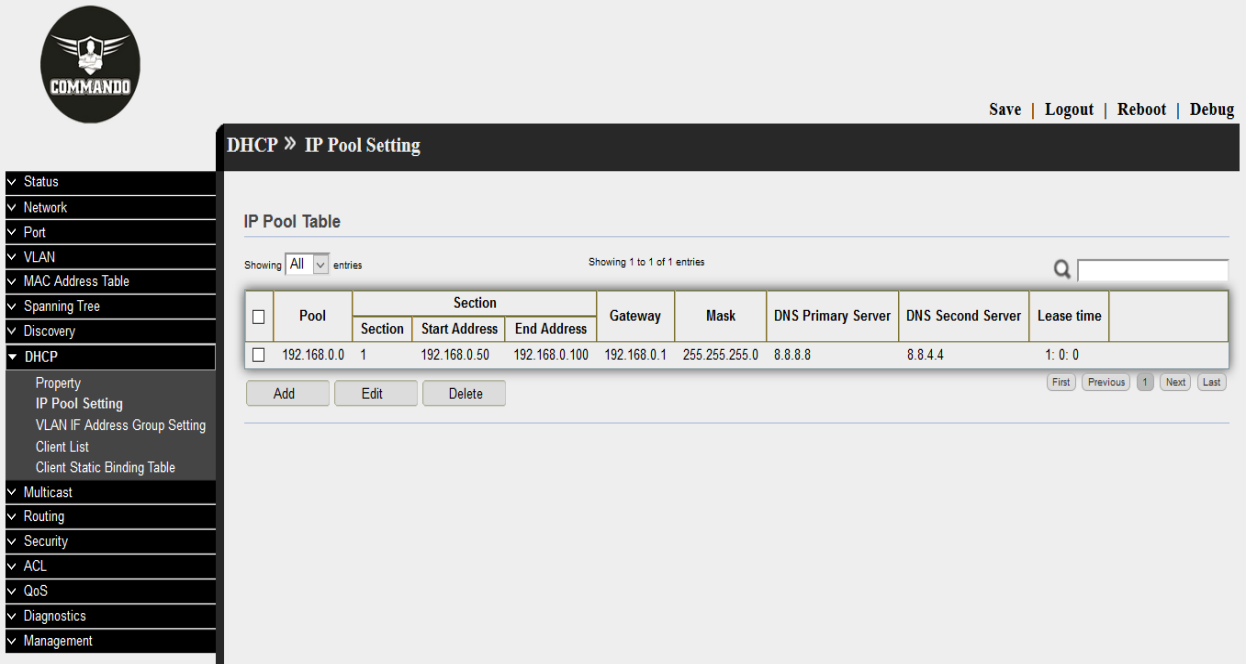


Fig 9.2.3 DHCP IP Pool Table after setting page

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.**

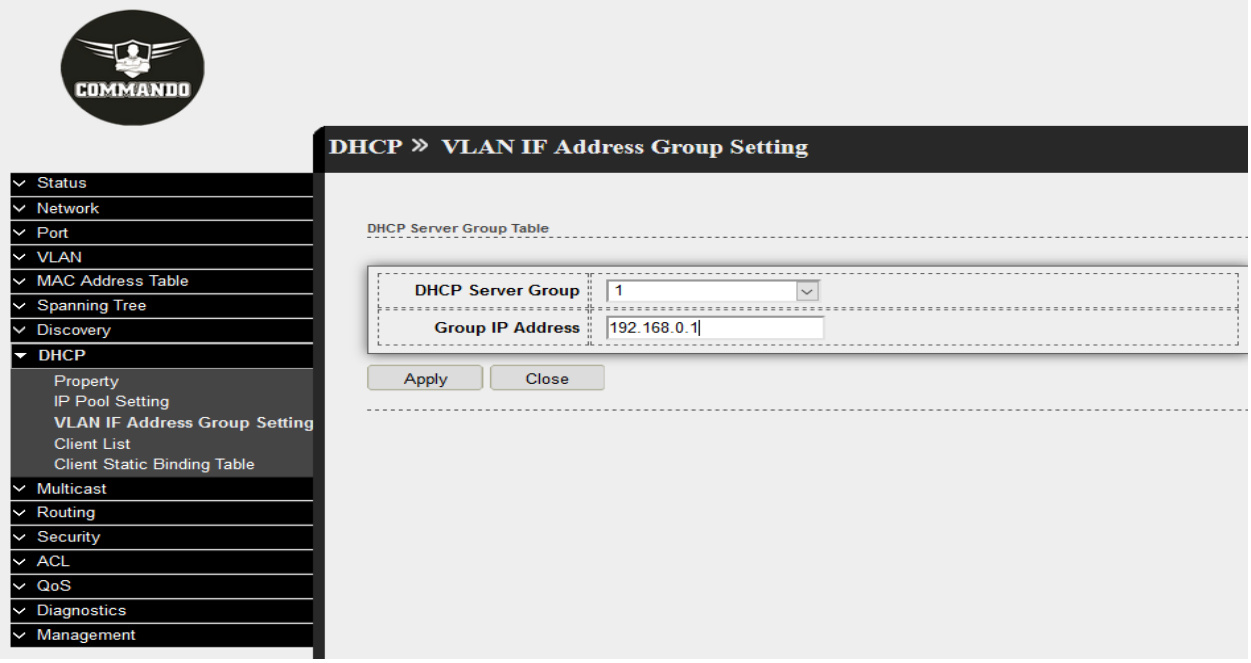


Fig 9.3.1 DHCP Vlan Interface address pool and Server group table page.

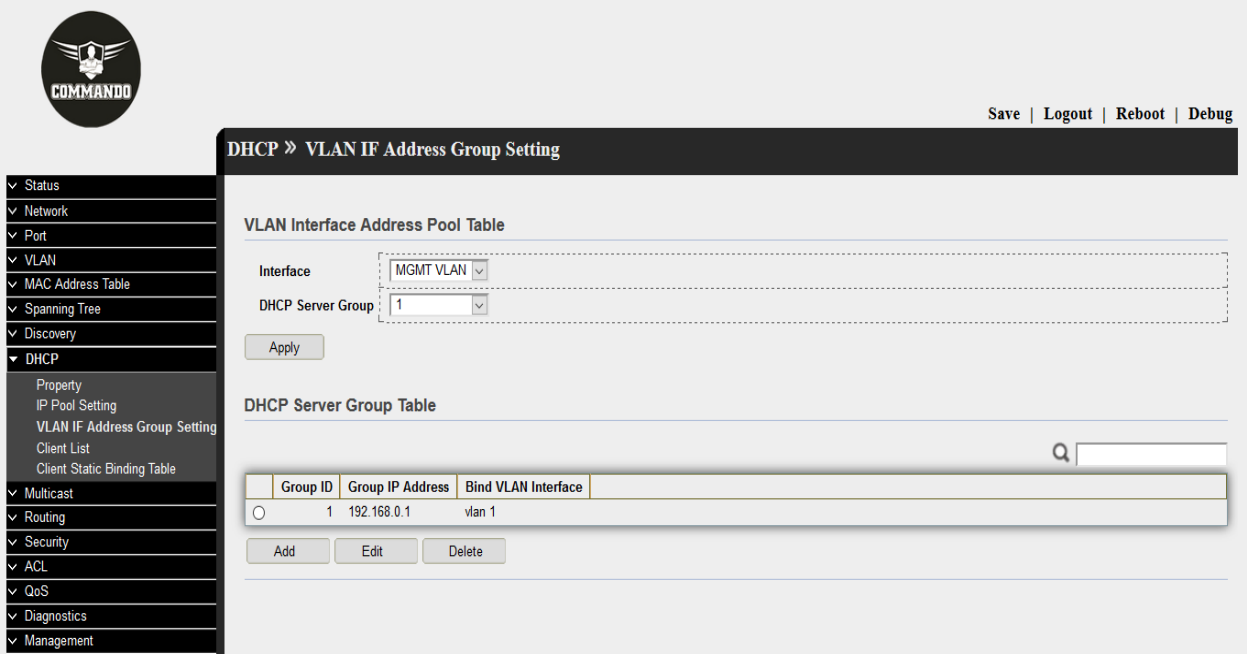


Fig 9.3.2 DHCP Binding Vlan Interface to DHCP server group Ip address page.

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.**

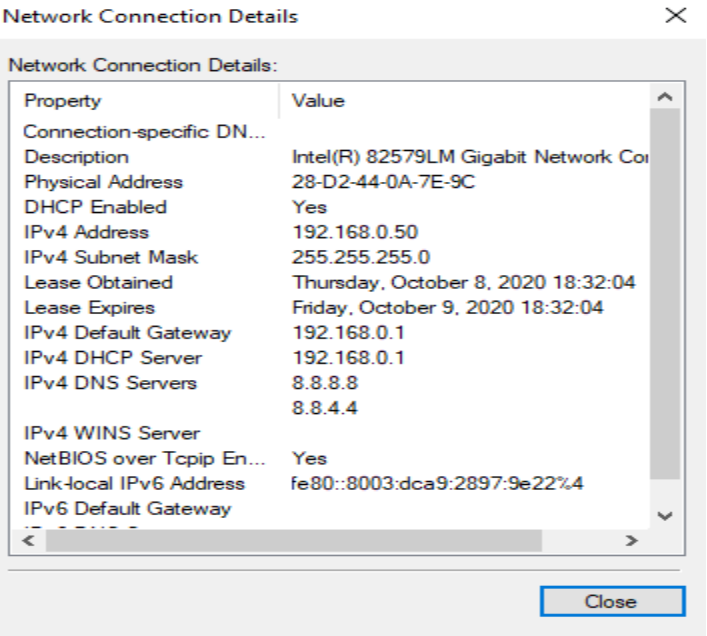


Fig 9.4.1 DHCP Client list page.

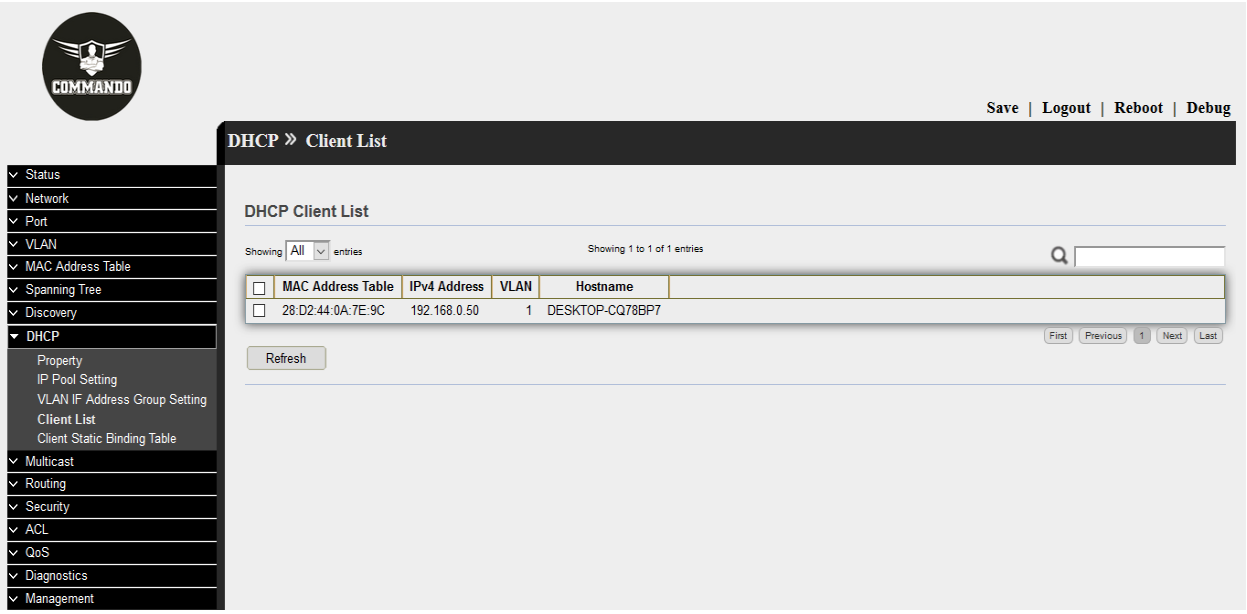


Fig 9.4.2 DHCP Client list page.

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 binded with static IP address and also by perticular name also can be assigned to clients.

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

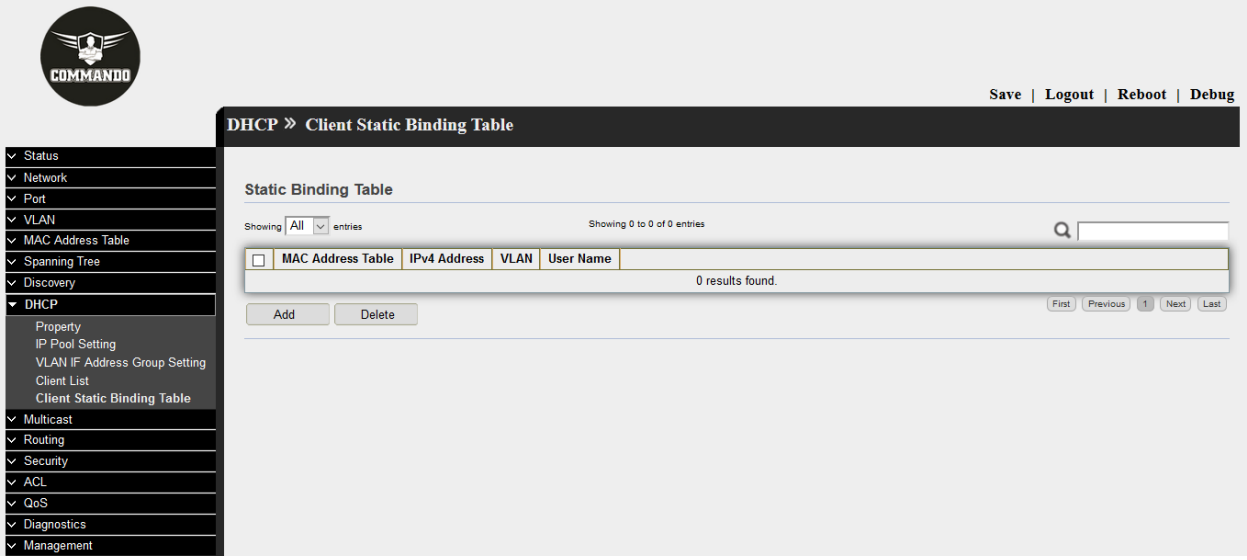


Fig 9.5.1 Default DHCP Client Binding Table page.

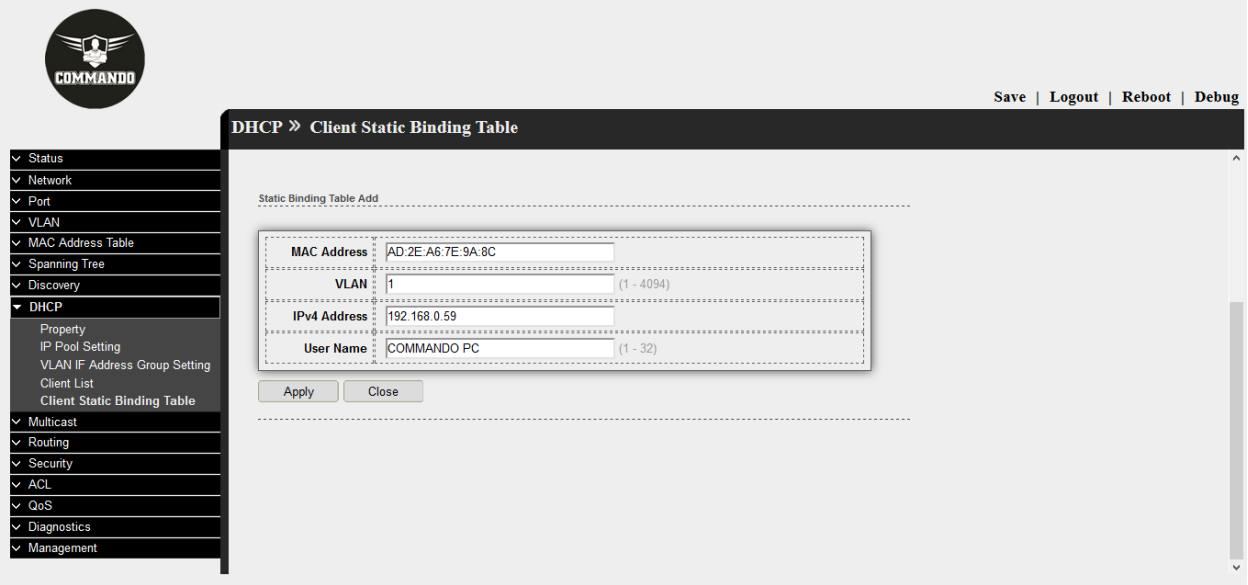


Fig 9.5.2 DHCP Client add static binding page.

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 include 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 display the IGMP throttling configuration 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 multicasts.

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 group 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.

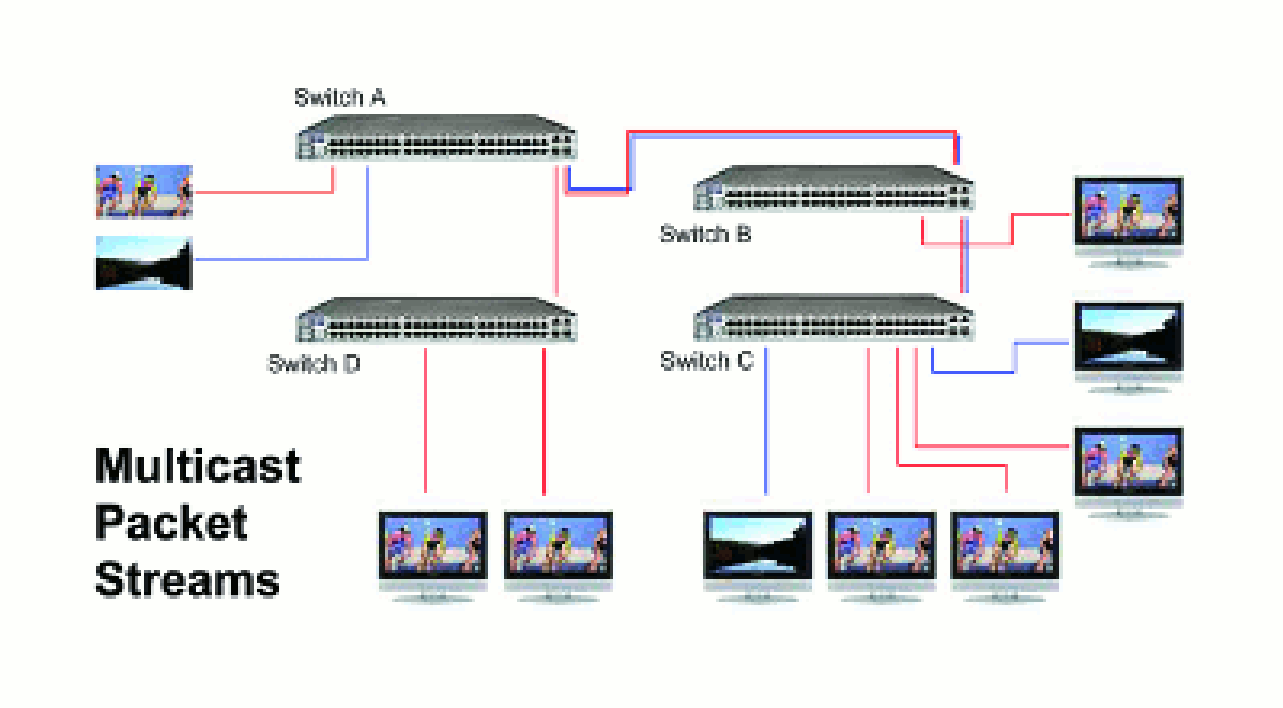


Fig 10.1.1 Multicast Packet Streams page

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.**

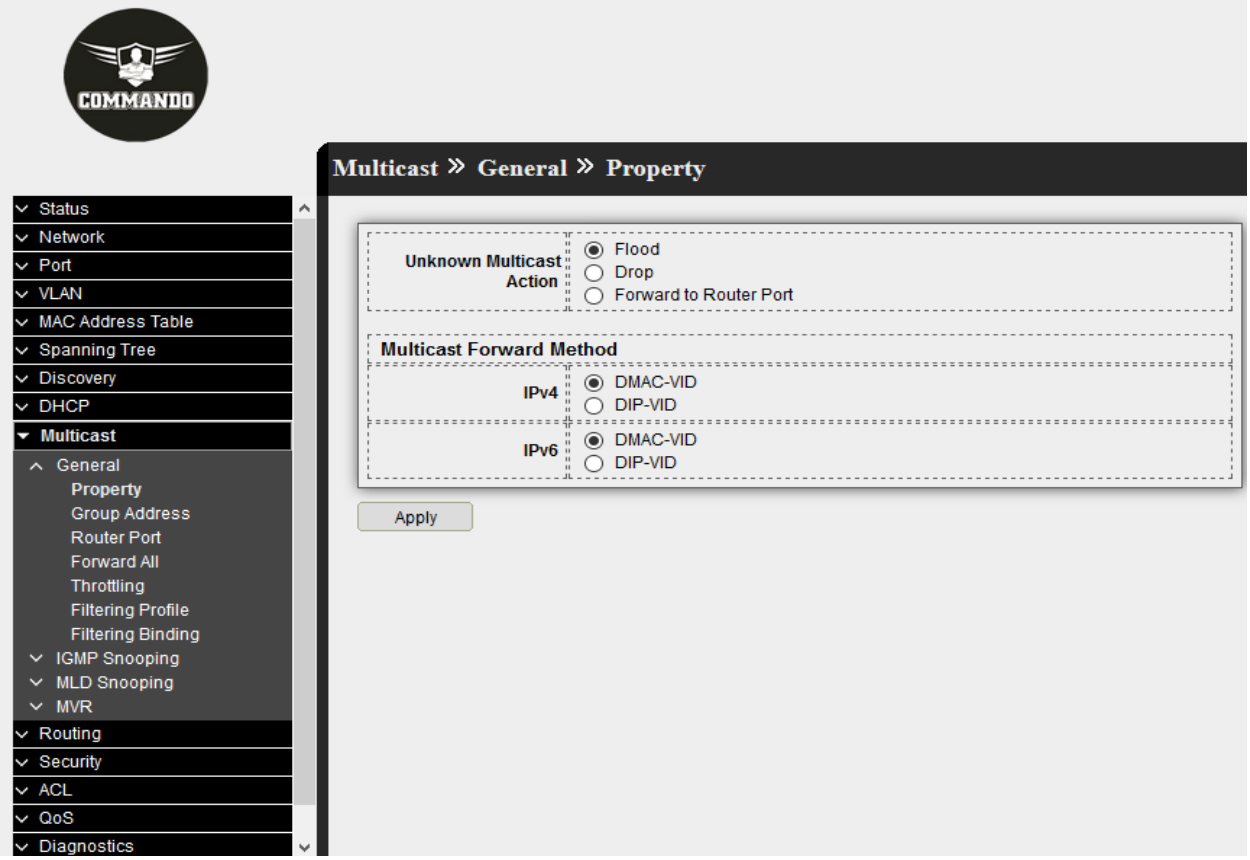


Fig 10.1.1 Multicast general property page

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.**

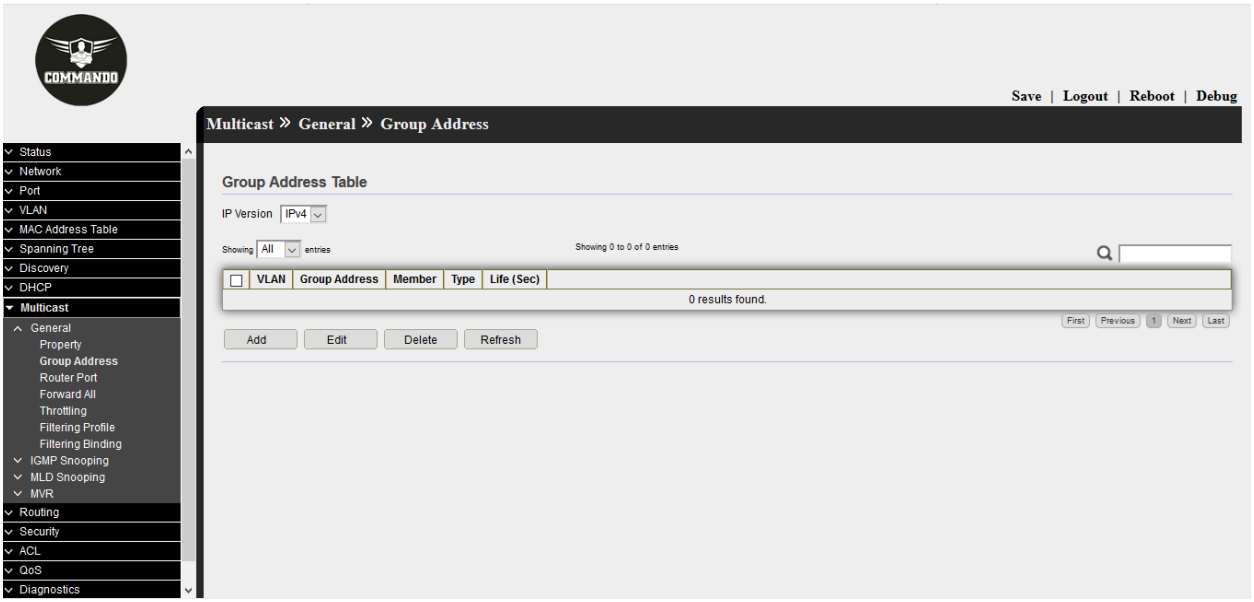


Fig 10.1.2 Multicast default group address table page

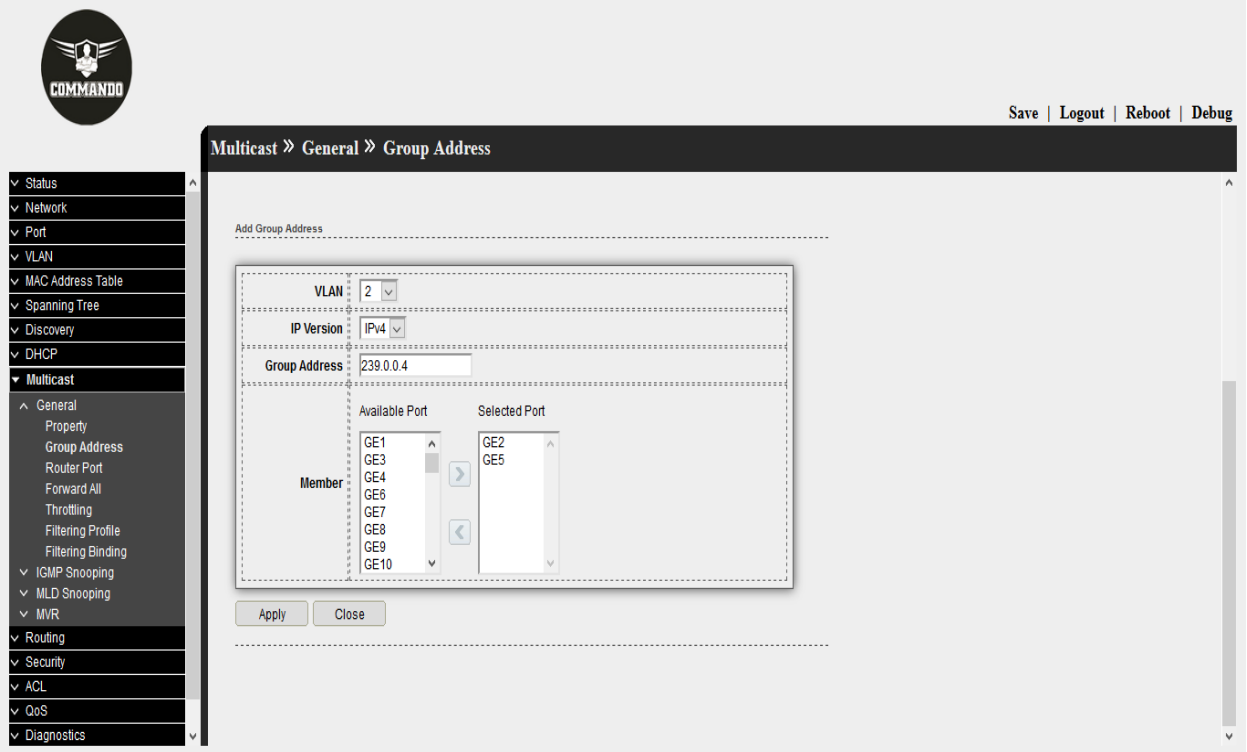


Fig 10.1.3 Multicast add group address page

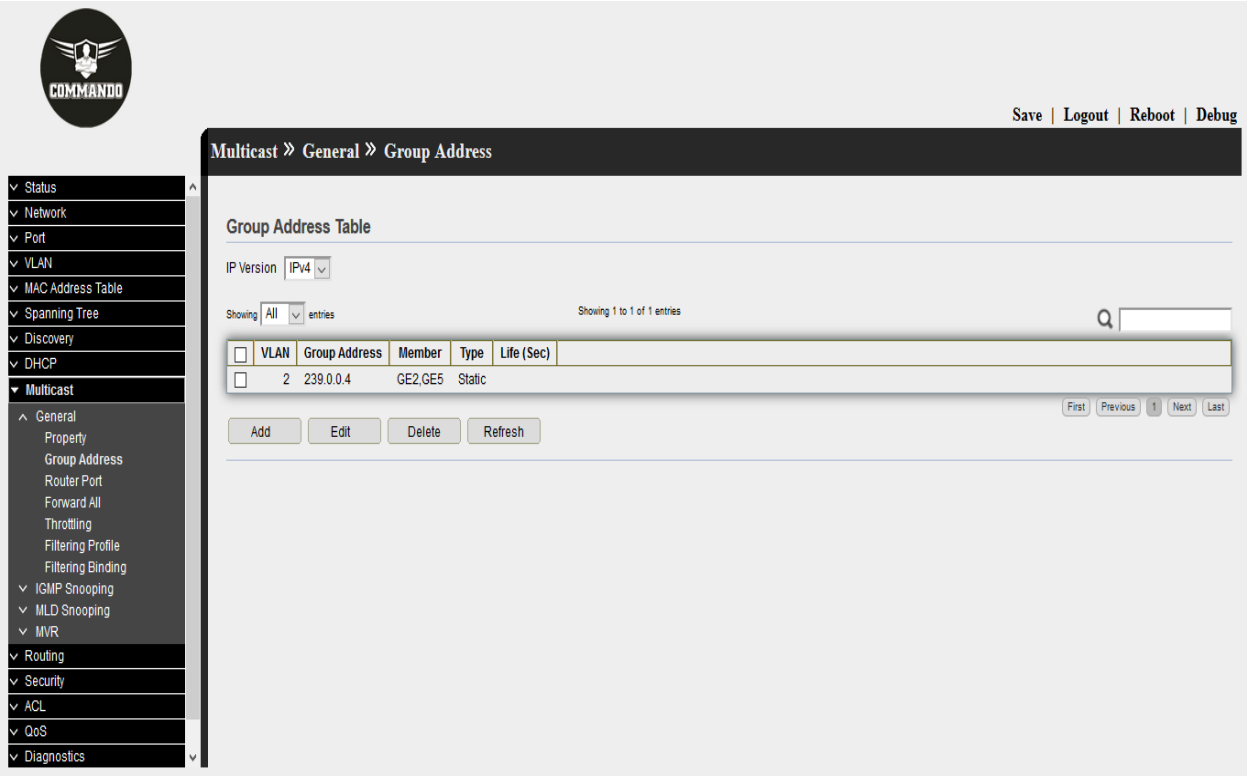


Fig 10.1.4 Multicast group address table page

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.**

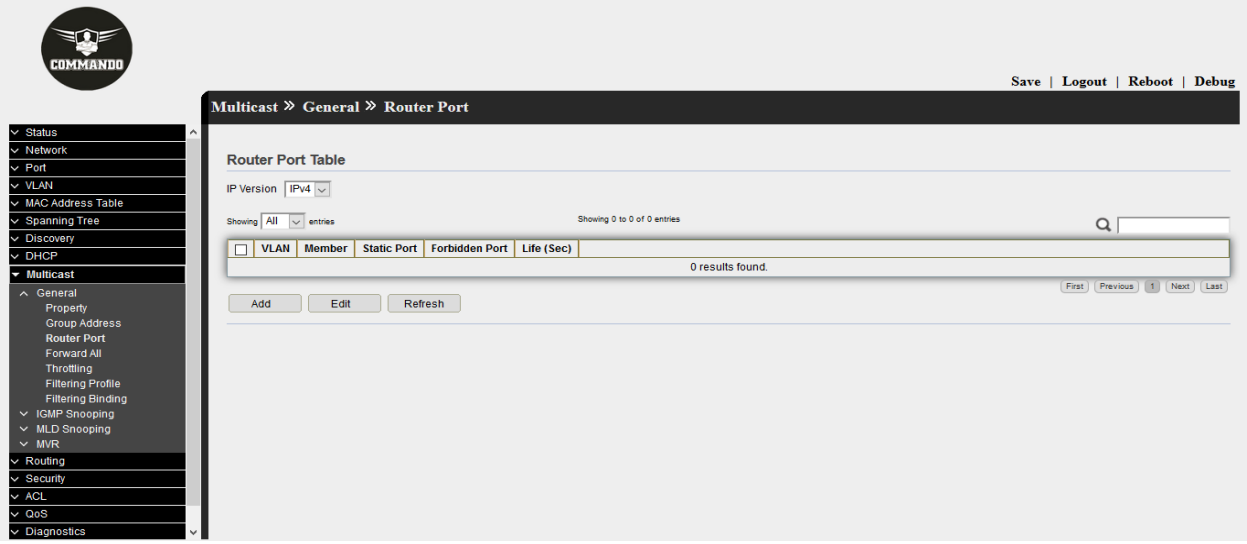


Fig 10.1.5 Multicast default router port table page

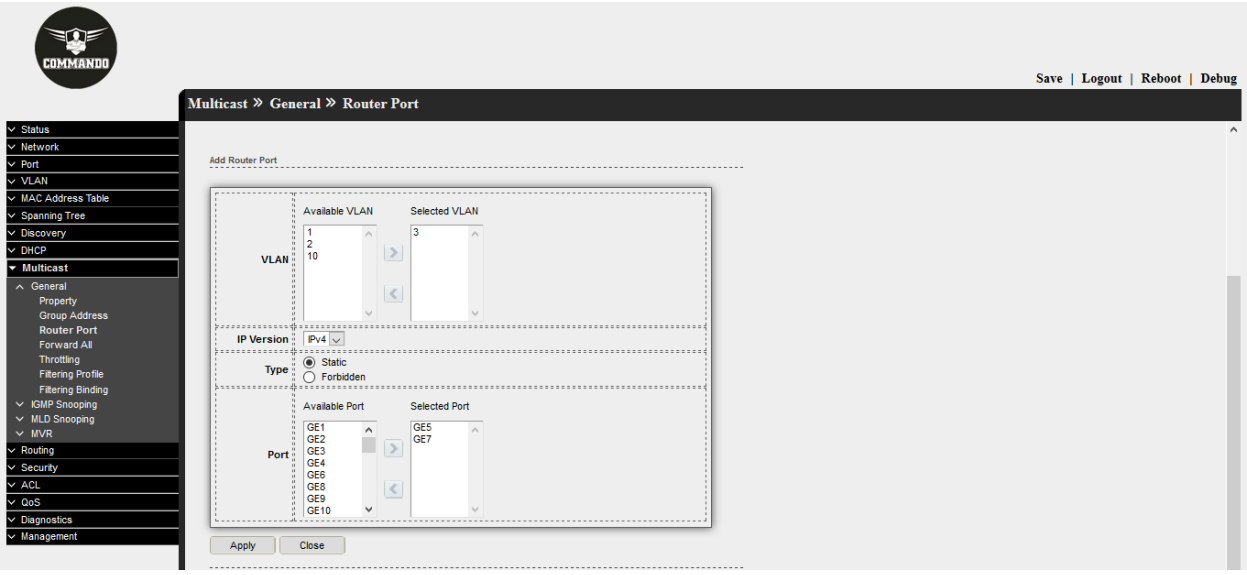


Fig 10.1.6 Multicast router port selection page

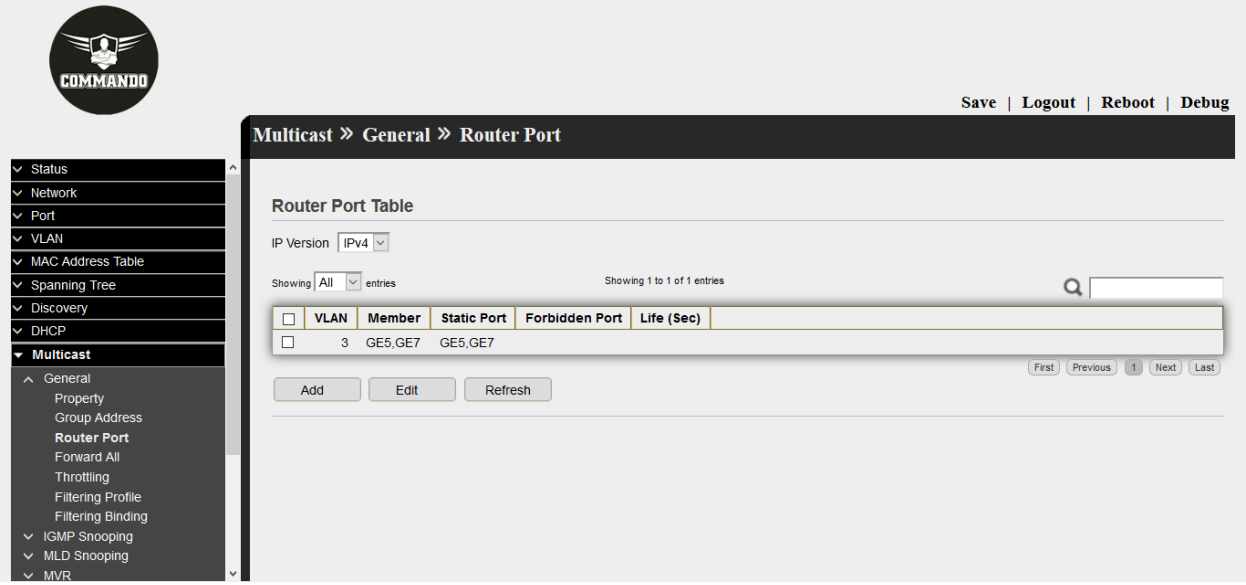


Fig 10.1.7 Multicast router port table by selecting GE5 and GE7 port page

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.**

Fig 10.1.8 Multicast default forward all table page

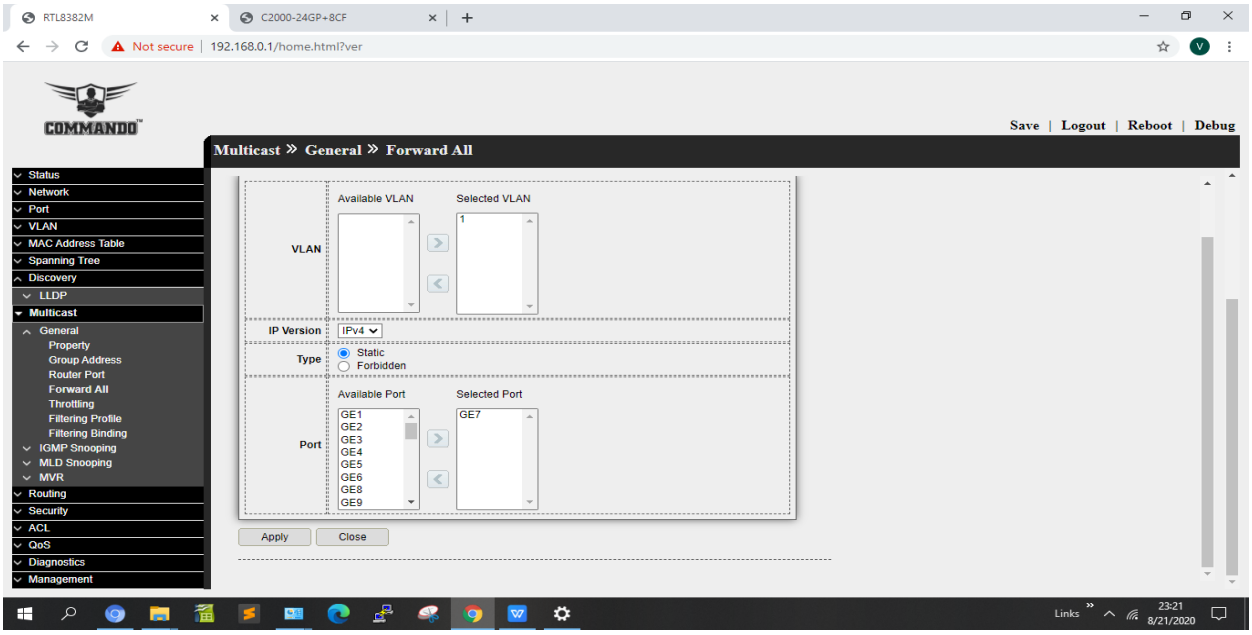


Fig 10.1.9 Multicast default forward all table page

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.**

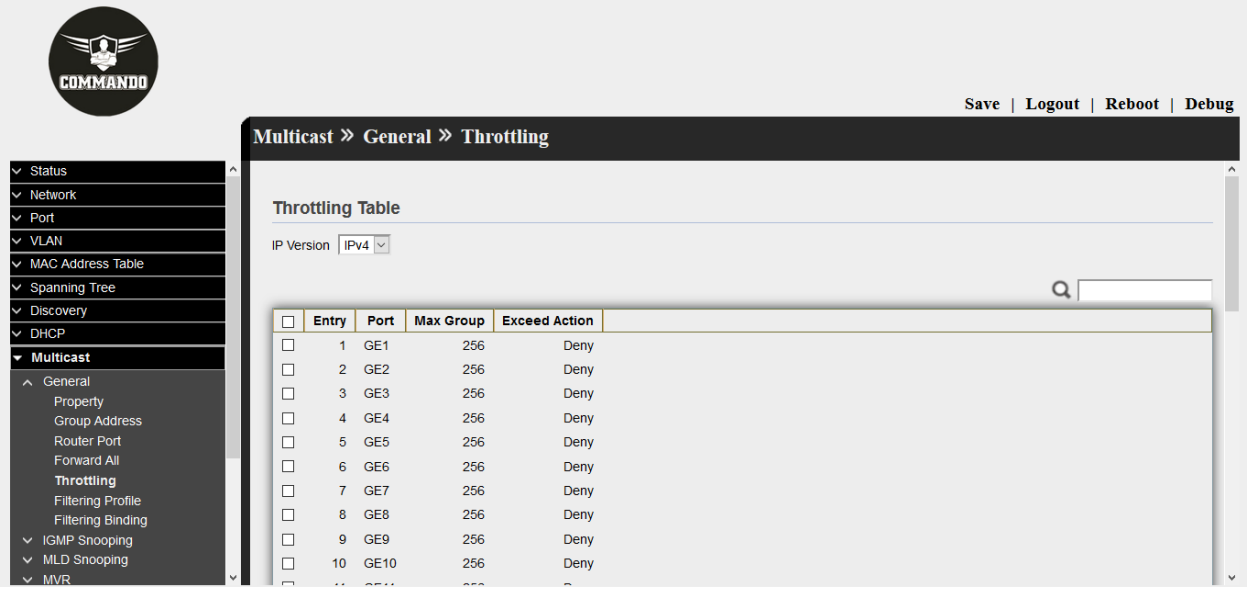


Fig 10.1.10 Multicast Default throttling table page

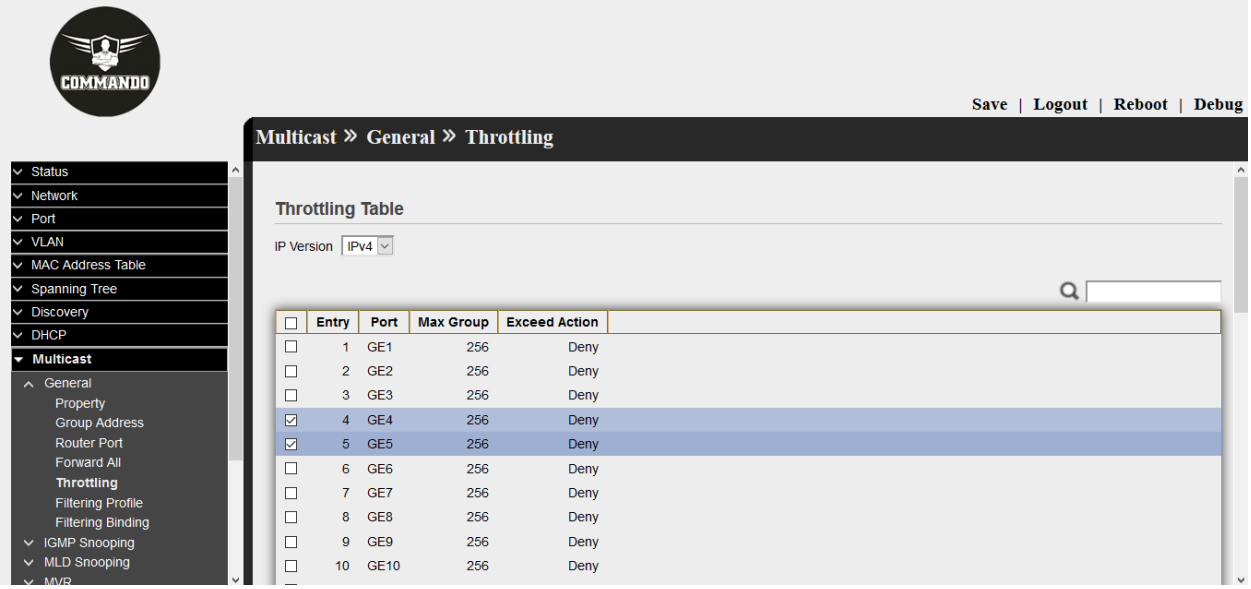


Fig 10.1.11 Multicast Selecting port for throttling page

Fig 10.1.11 Edit Multicast throttling page

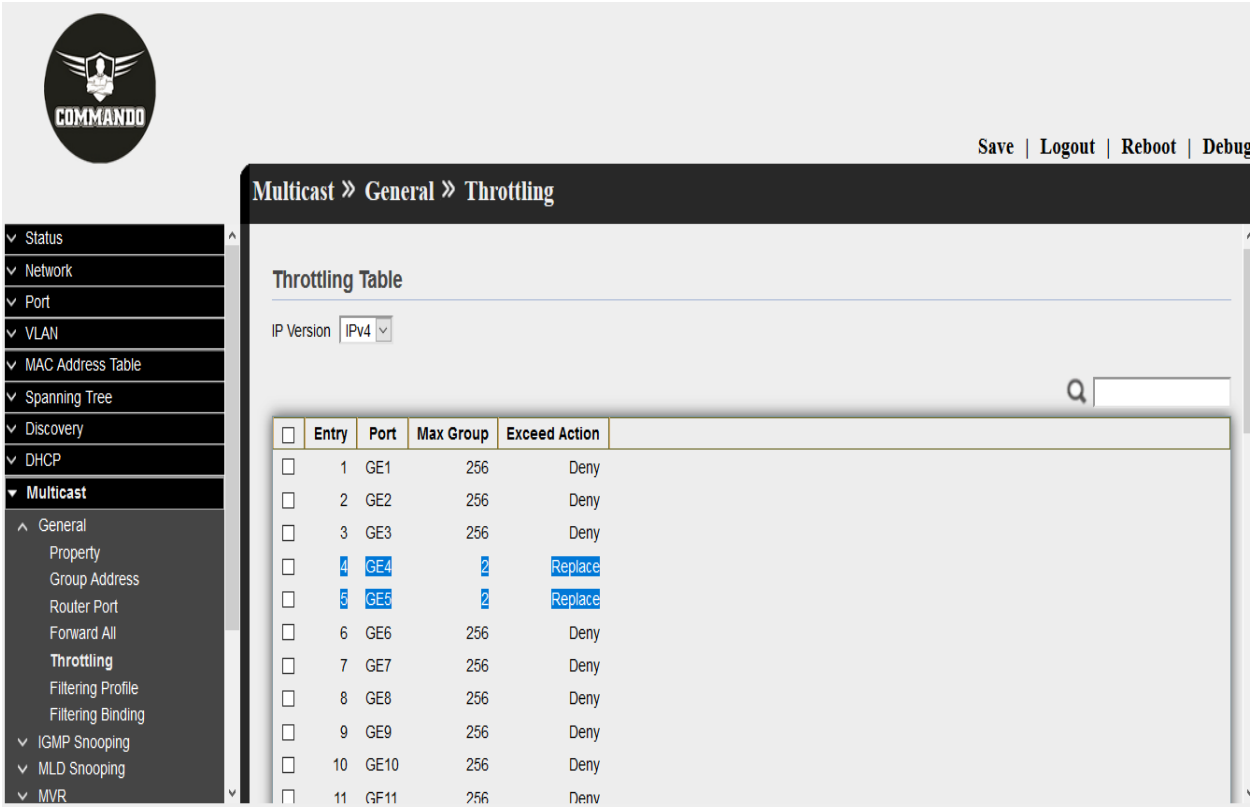


Fig 10.1.12 Multicast throttling Table page

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.**

Fig 10.1.13 Multicast default filtering profile table page

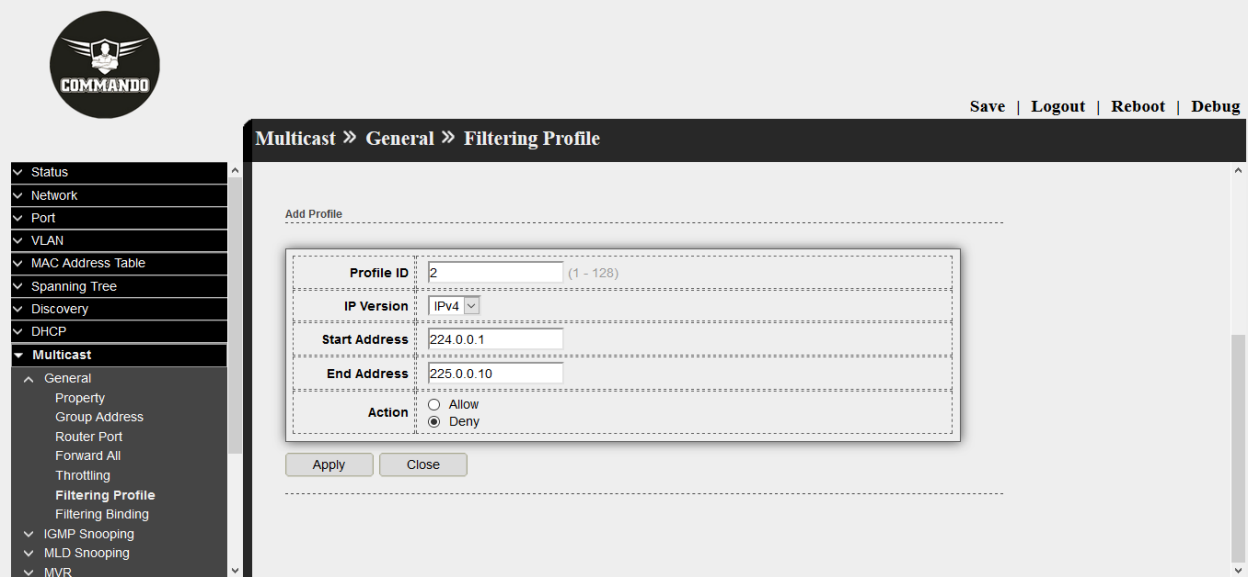


Fig 10.1.14 Multicast Add filtering profile page

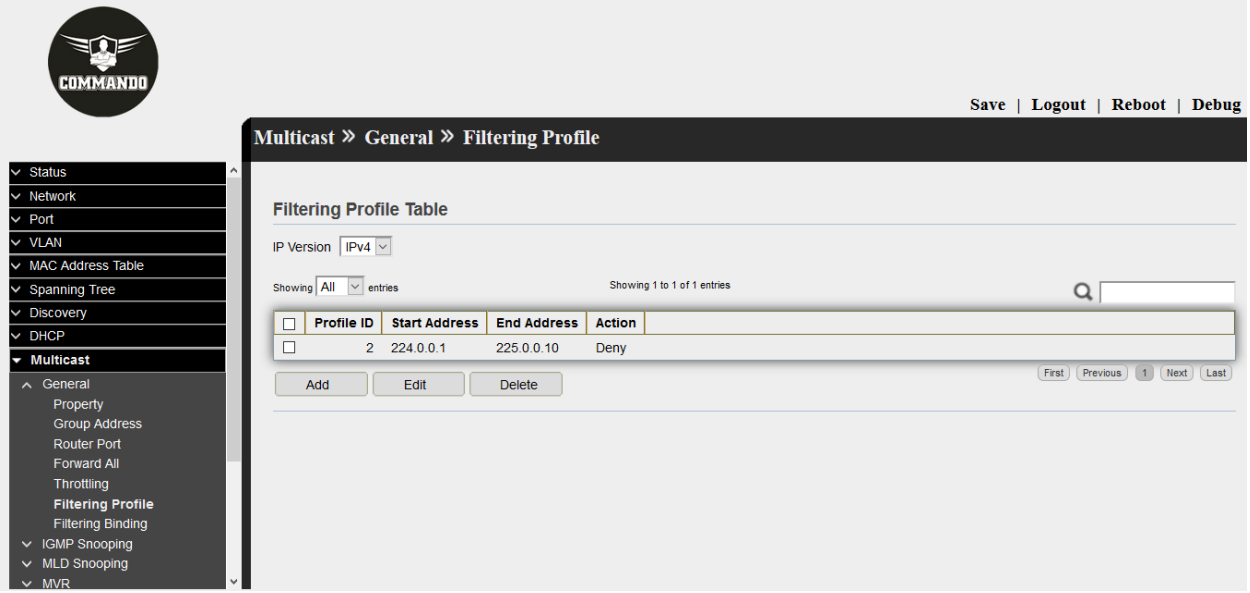


Fig 10.1.15 Multicast filtering profile table page

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.**

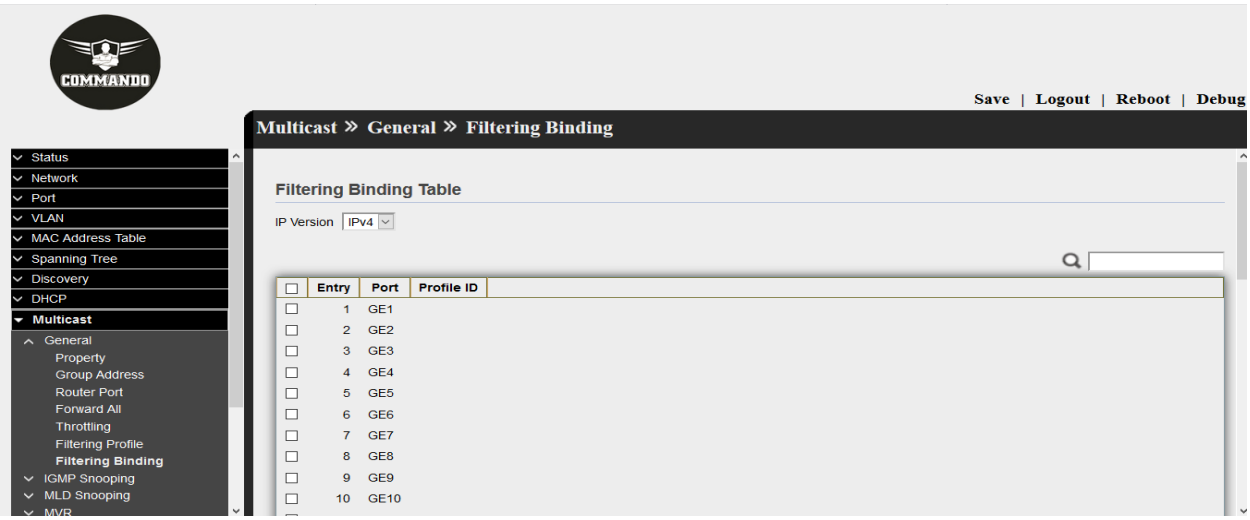


Fig 10.1.16 Multicast default filtering binding table page

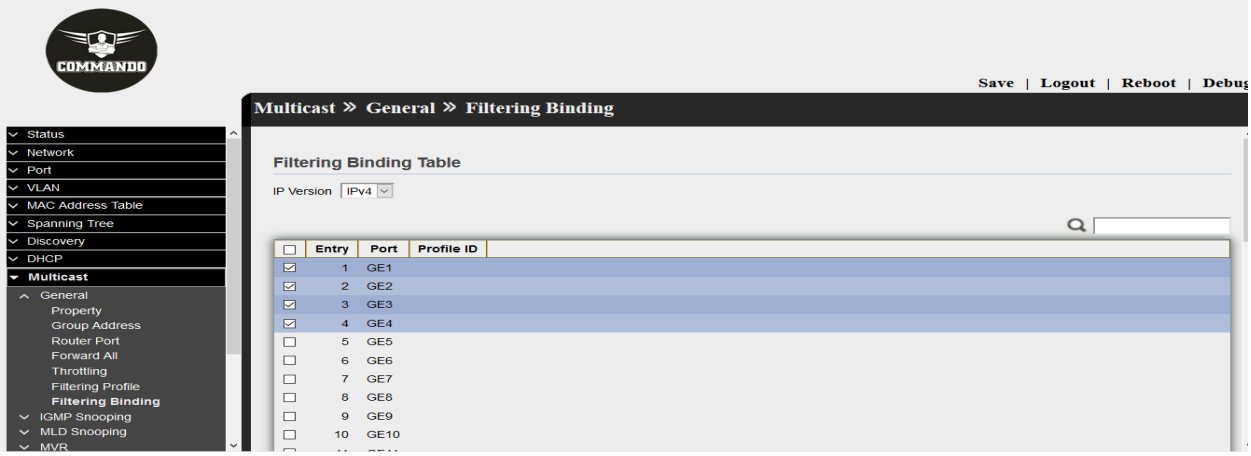


Fig 10.1.17 Multicast filtering Binding Port selection page

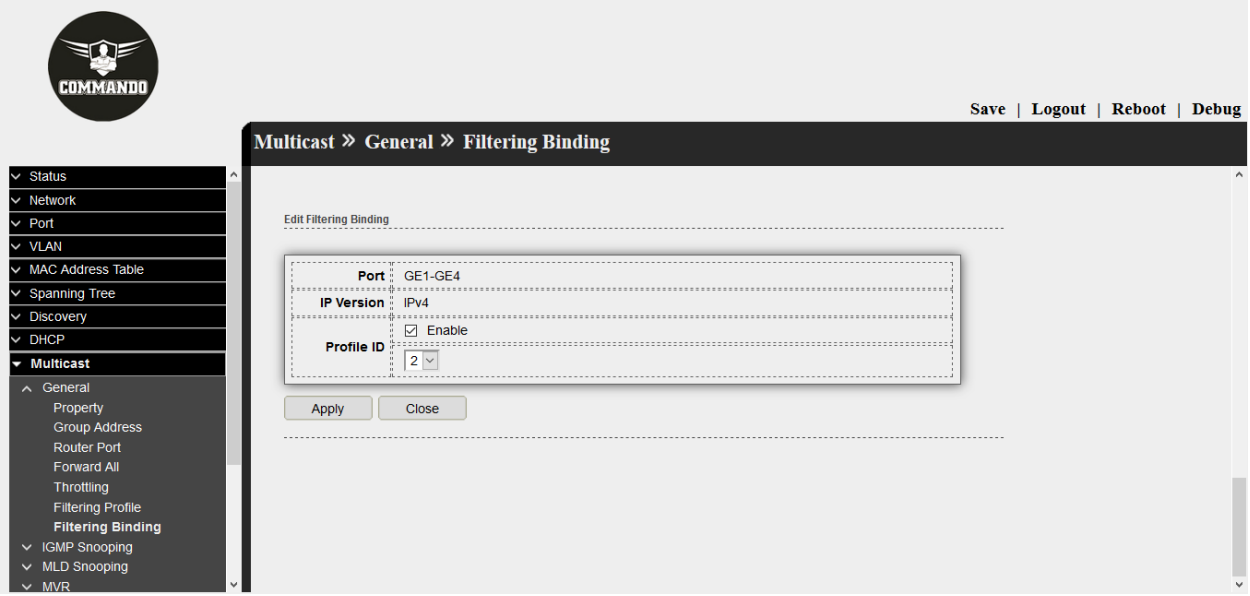


Fig 10.1.18 Multicast Edit filtering Binding page

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.**

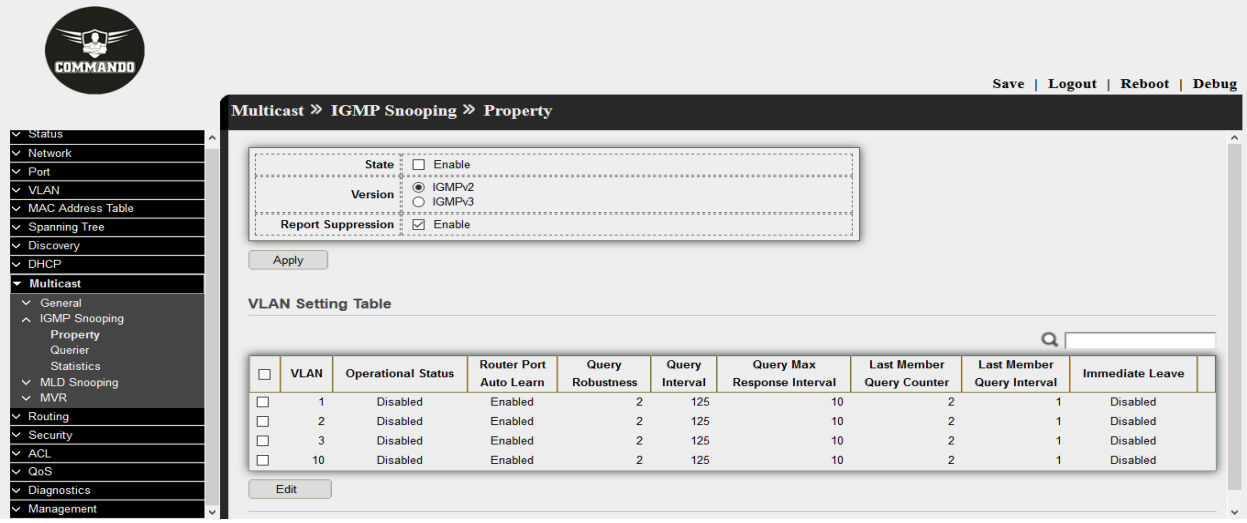


Fig 10.2.1 Default IGMP snooping property page

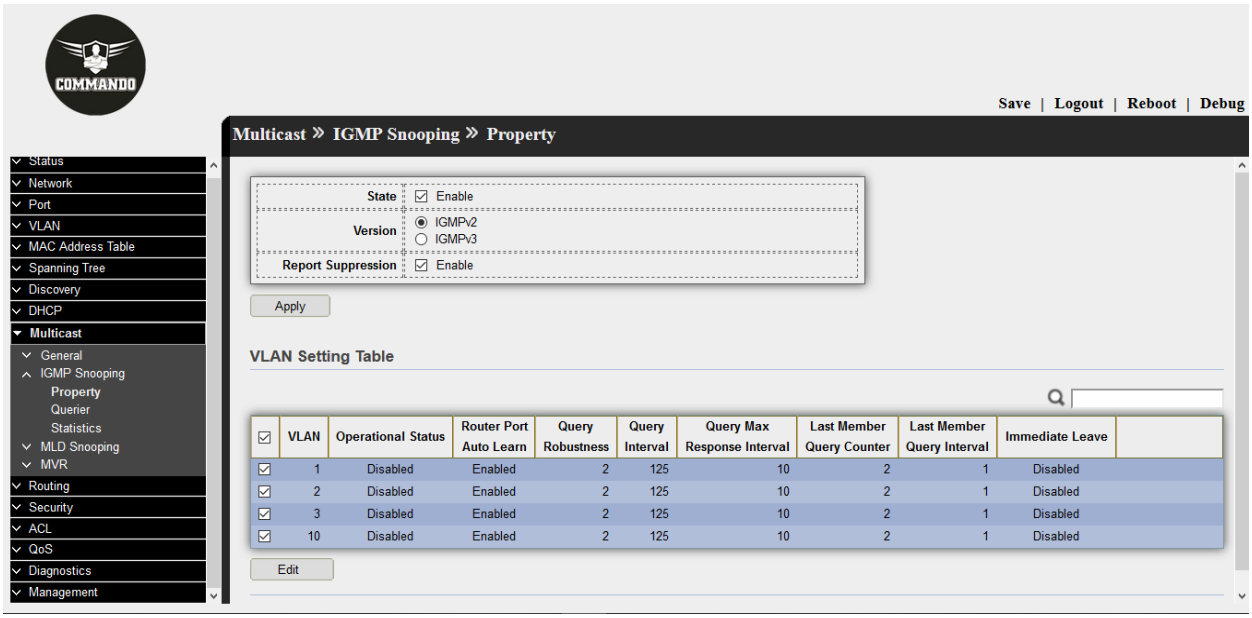


Fig 10.2.2 IGMP snooping property VLAN setting page

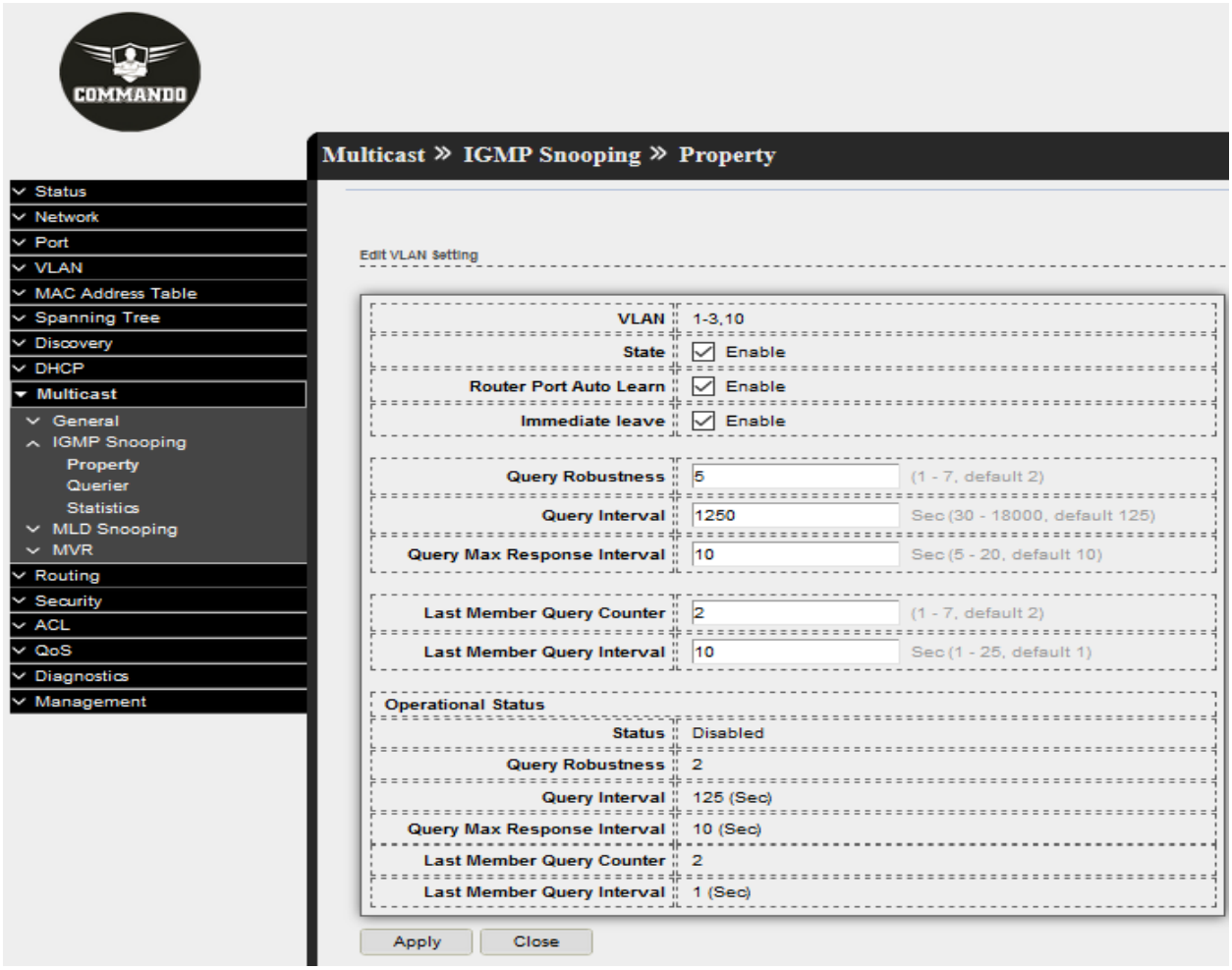


Fig 10.2.3 IGMP snooping Edit VLAN setting page

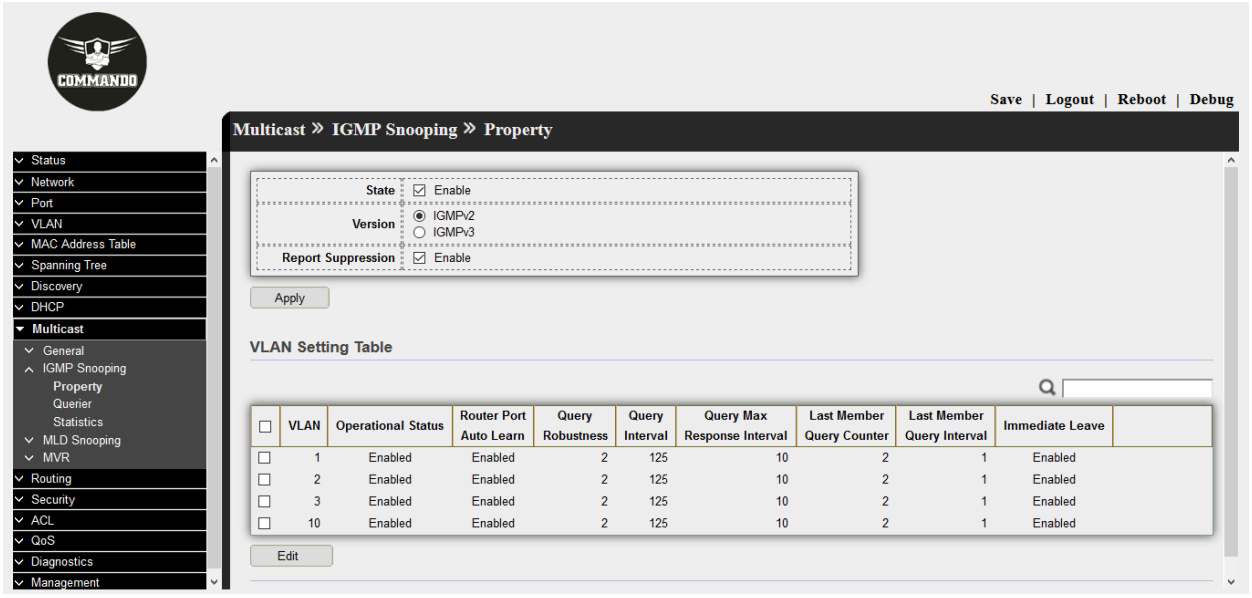


Fig 10.2.4 IGMP snooping property page

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.**

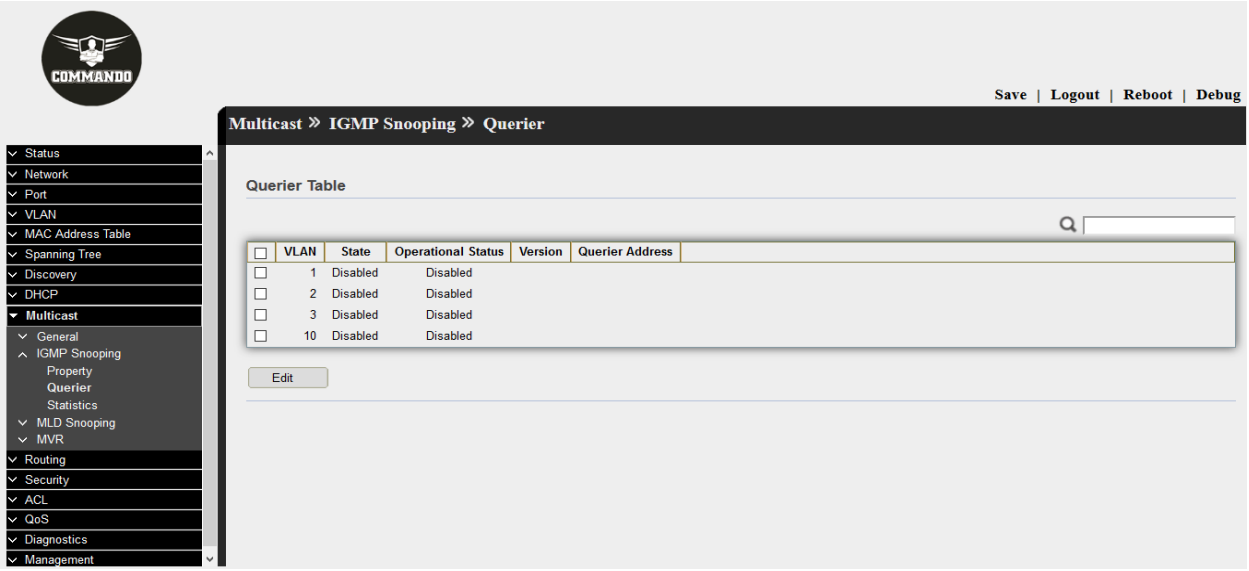


Fig 10.2.5 Default IGMP snooping Querier table page

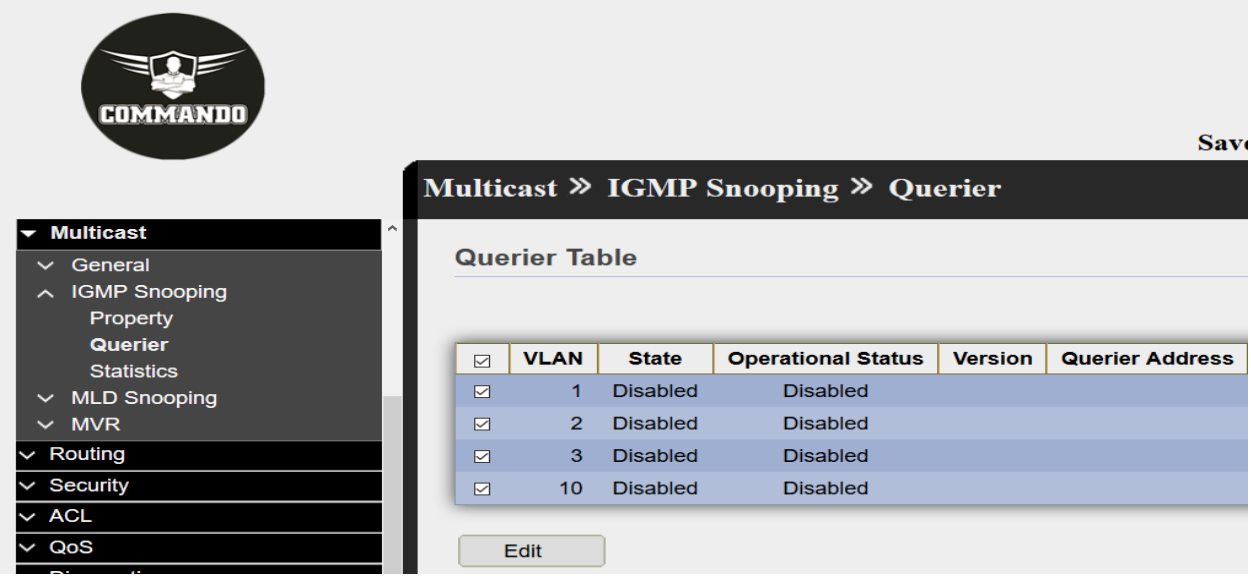


Fig 10.2.6 IGMP snooping Selecting Vlan Querier page

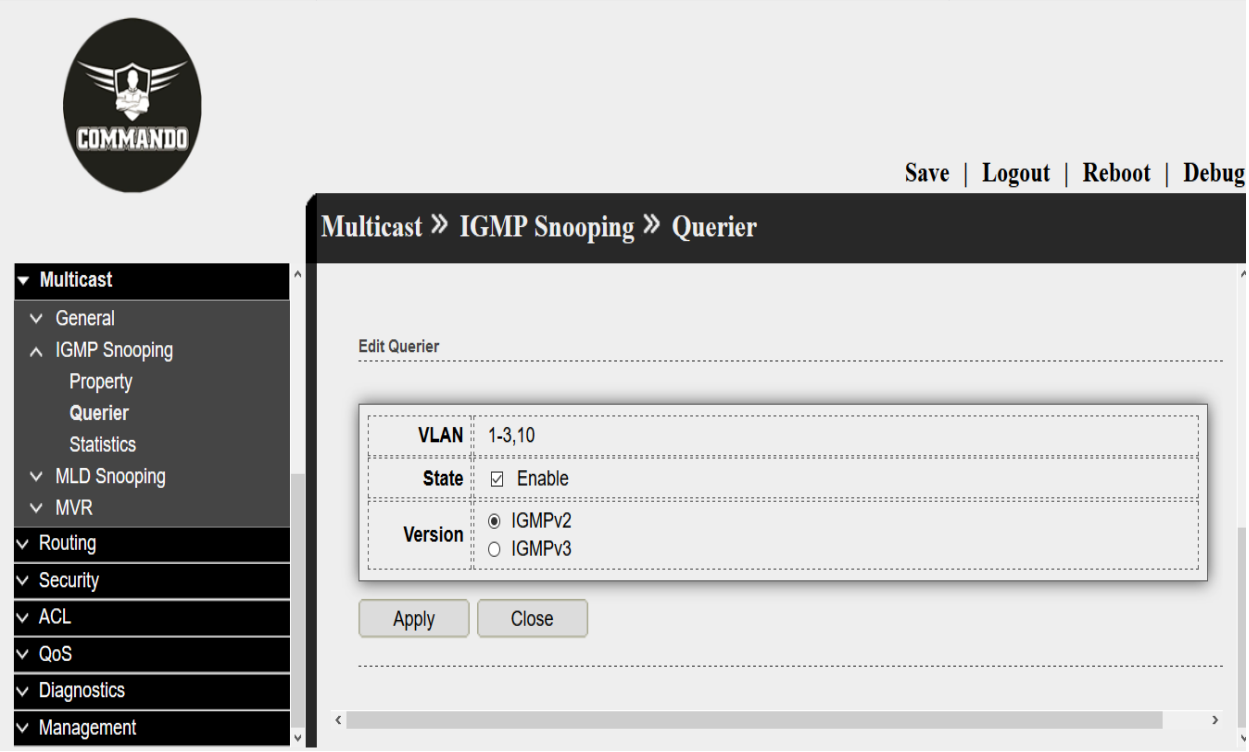


Fig 10.2.7 IGMP snooping Edit Querier page

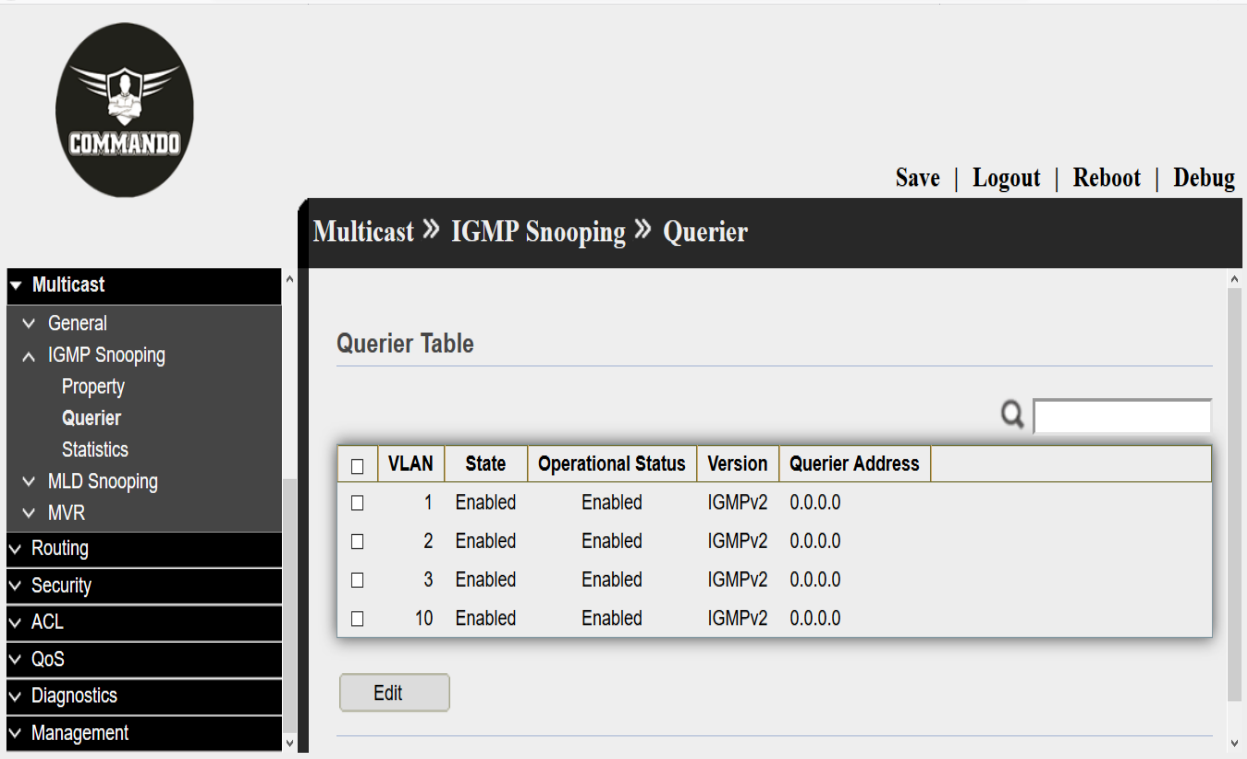


Fig 10.2.8 IGMP snooping Querier table page

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.**

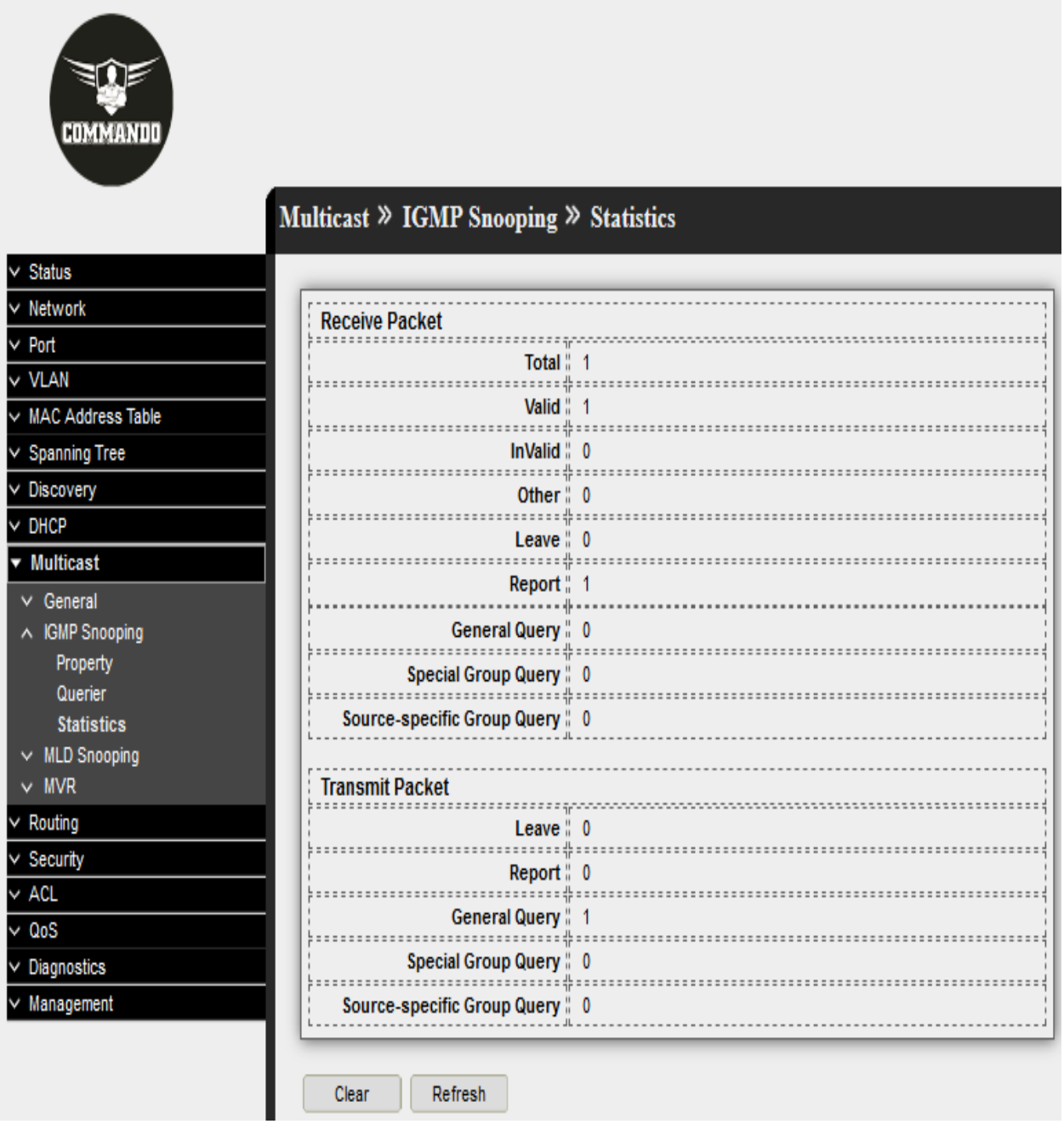


Fig 10.2.9 IGMP snooping statistics page

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 C2000 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.**

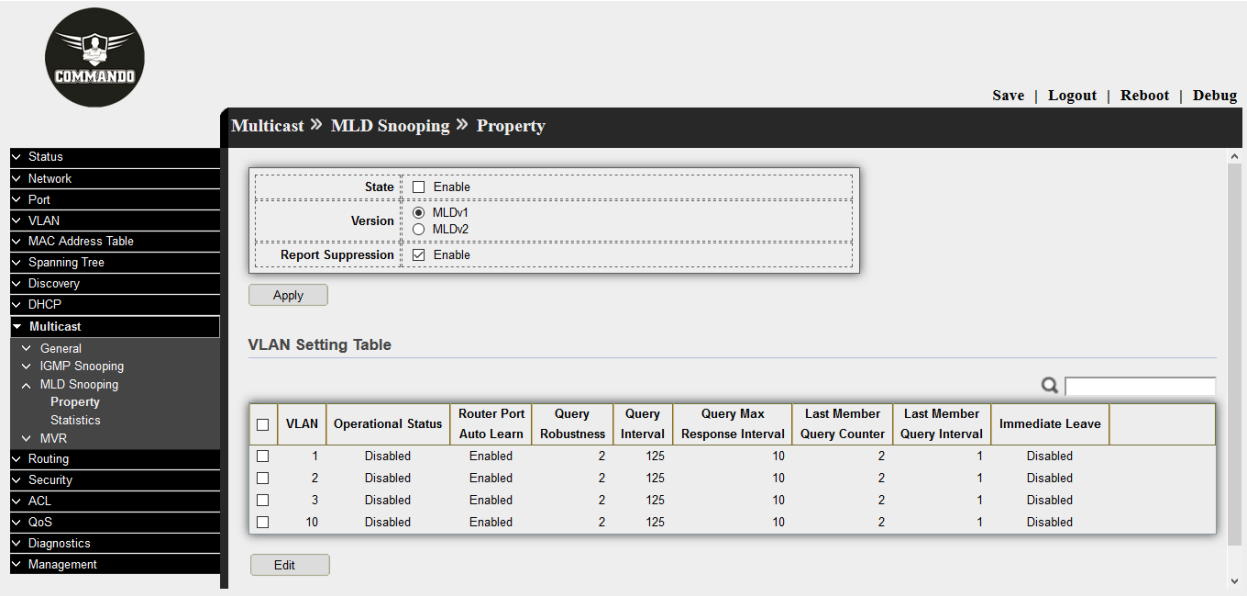


Fig 10.3.1 Multicast MLD Snooping default property page

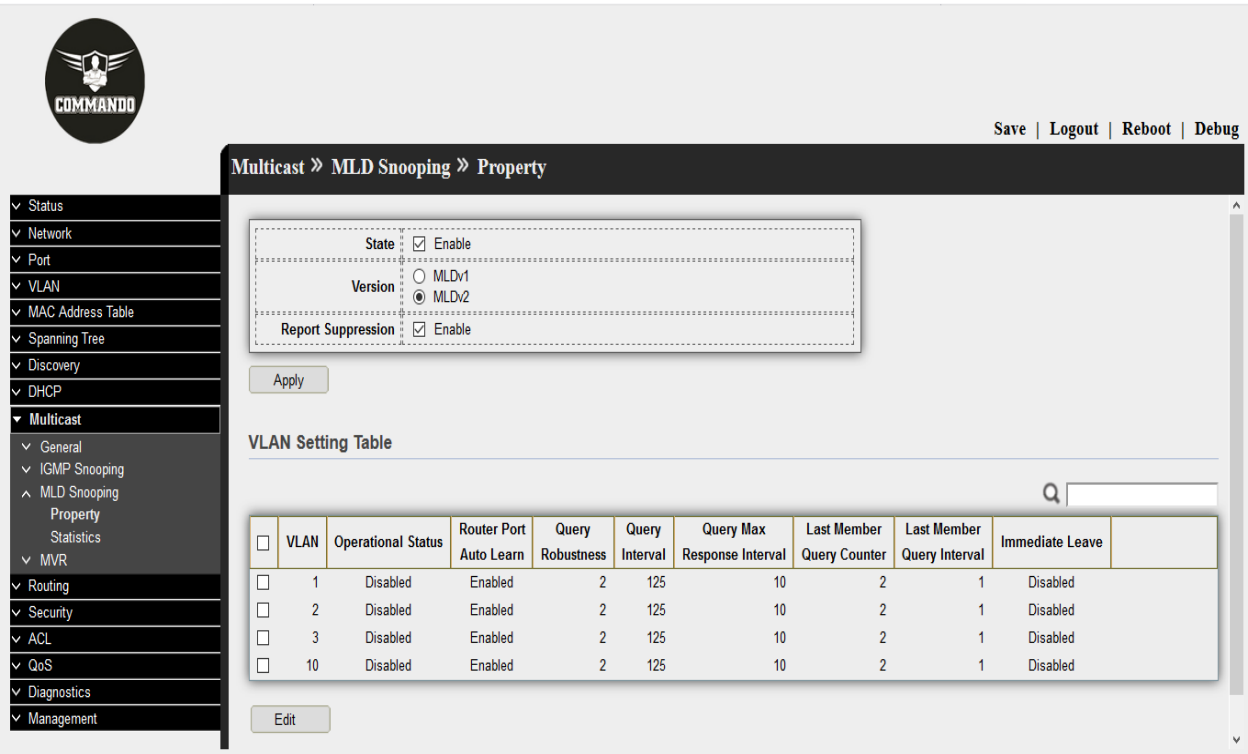


Fig 10.3.2 Enabling MLD Snooping property page

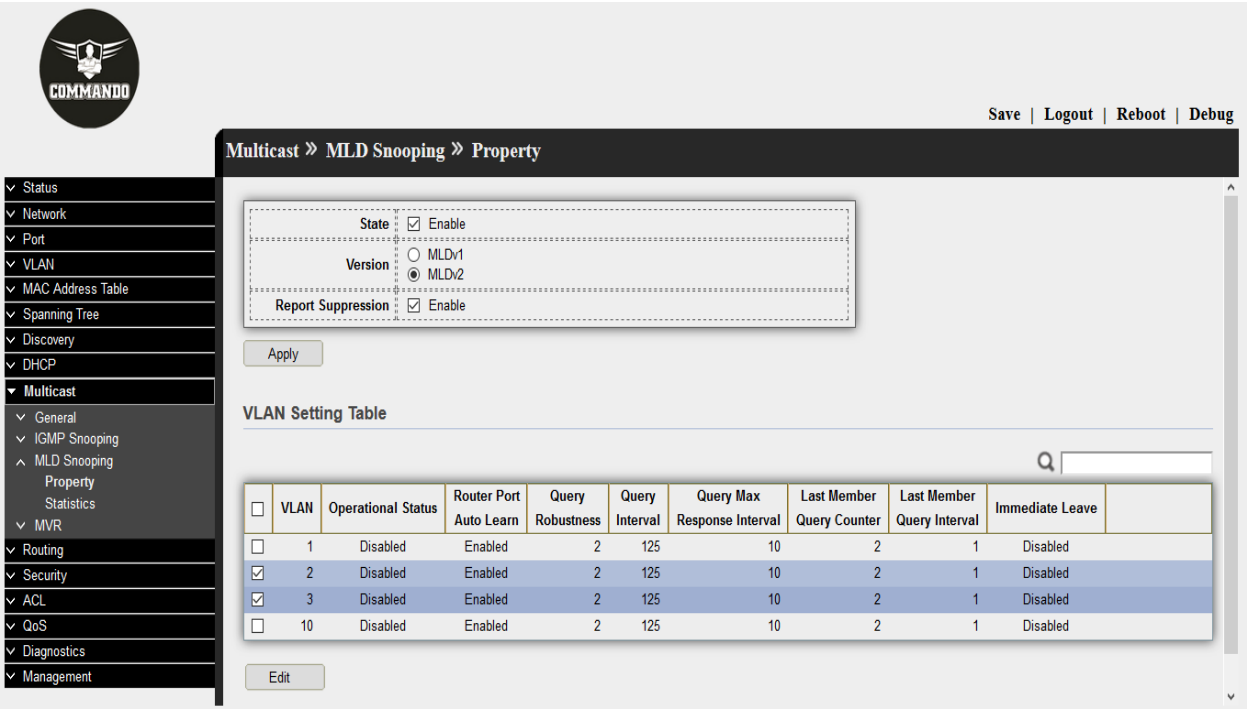


Fig 10.3.3 Selecting Vlan for MLD Snooping property page

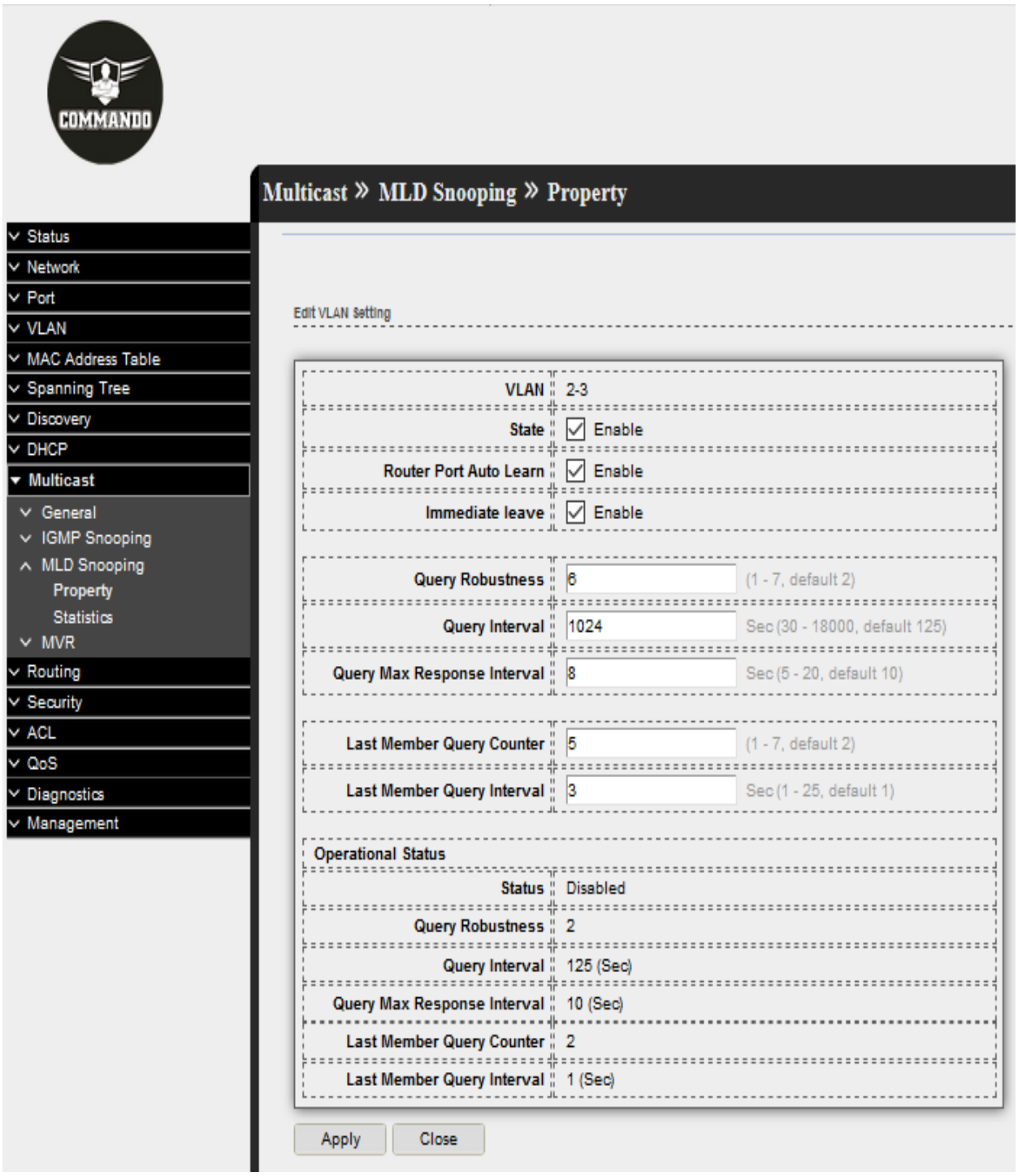


Fig 10.3.4 Edit Vlan Setting for MLD Snooping page

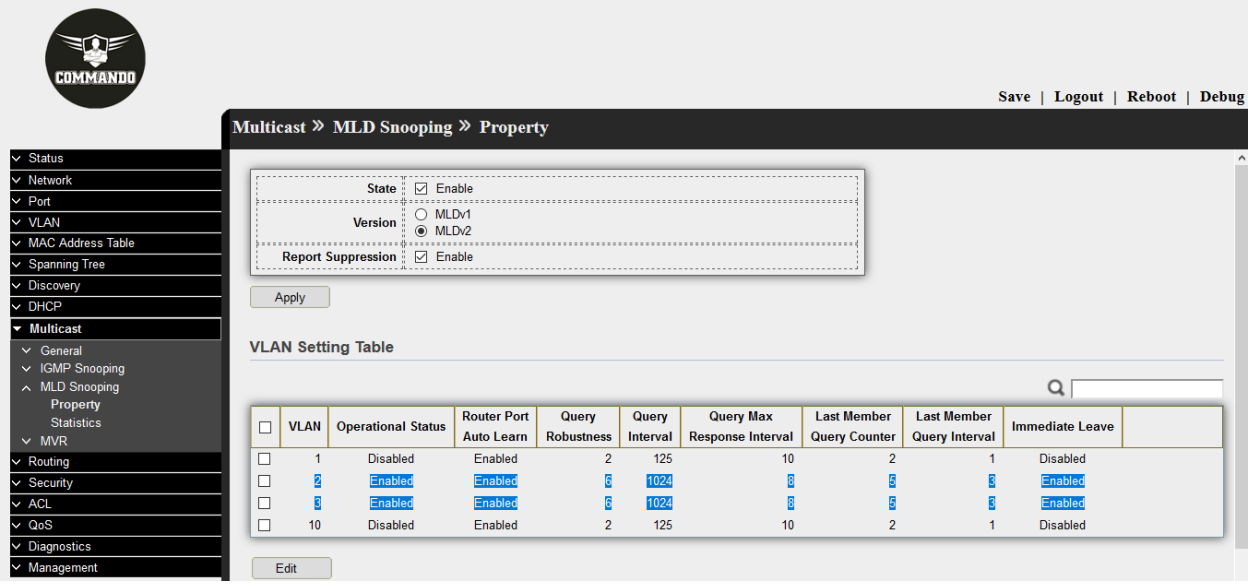


Fig 10.3.5 Multicast MLD Snooping property page

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.**

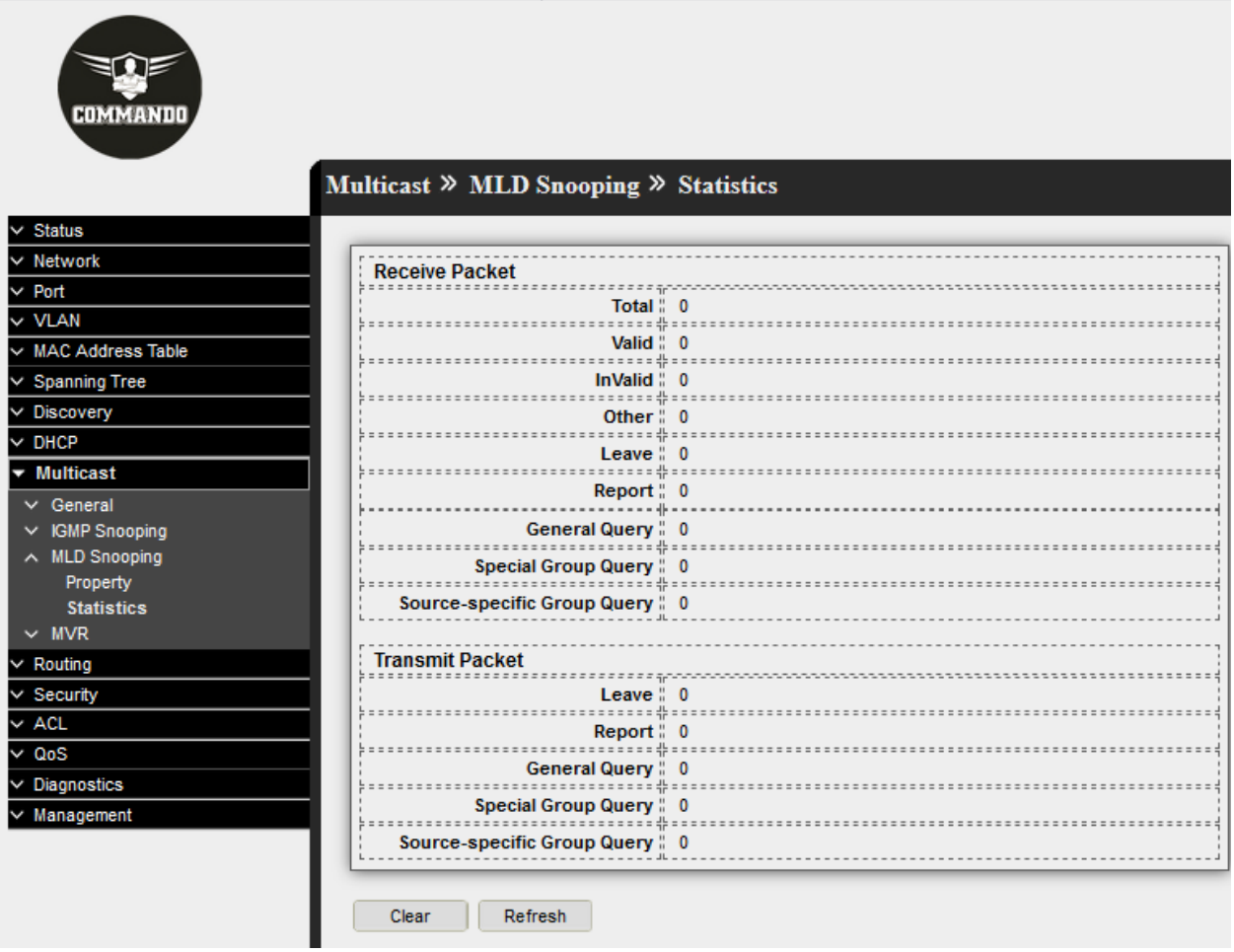


Fig 10.3.6 Multicast MLD Snooping statistics page

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 have to 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.**

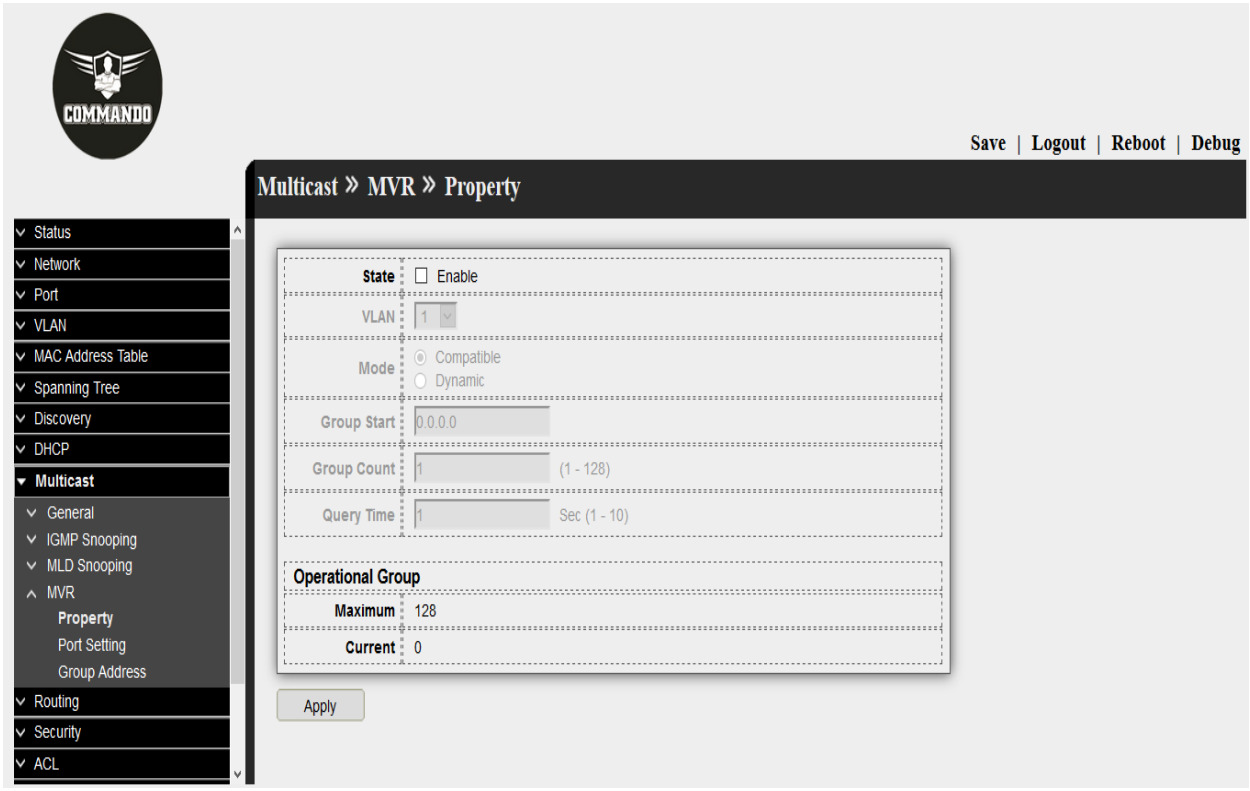


Fig 10.4.1 Default MVR Property page

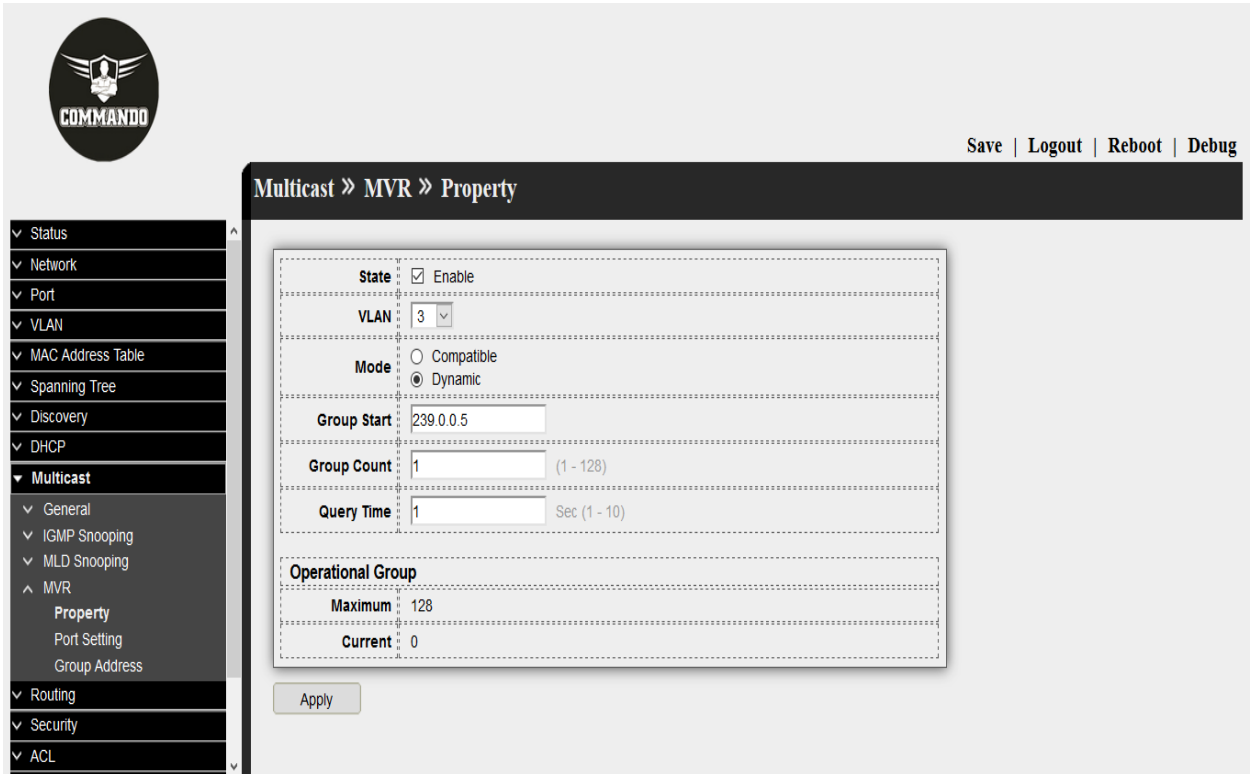


Fig 10.4.2 Setting MVR Property page

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.**

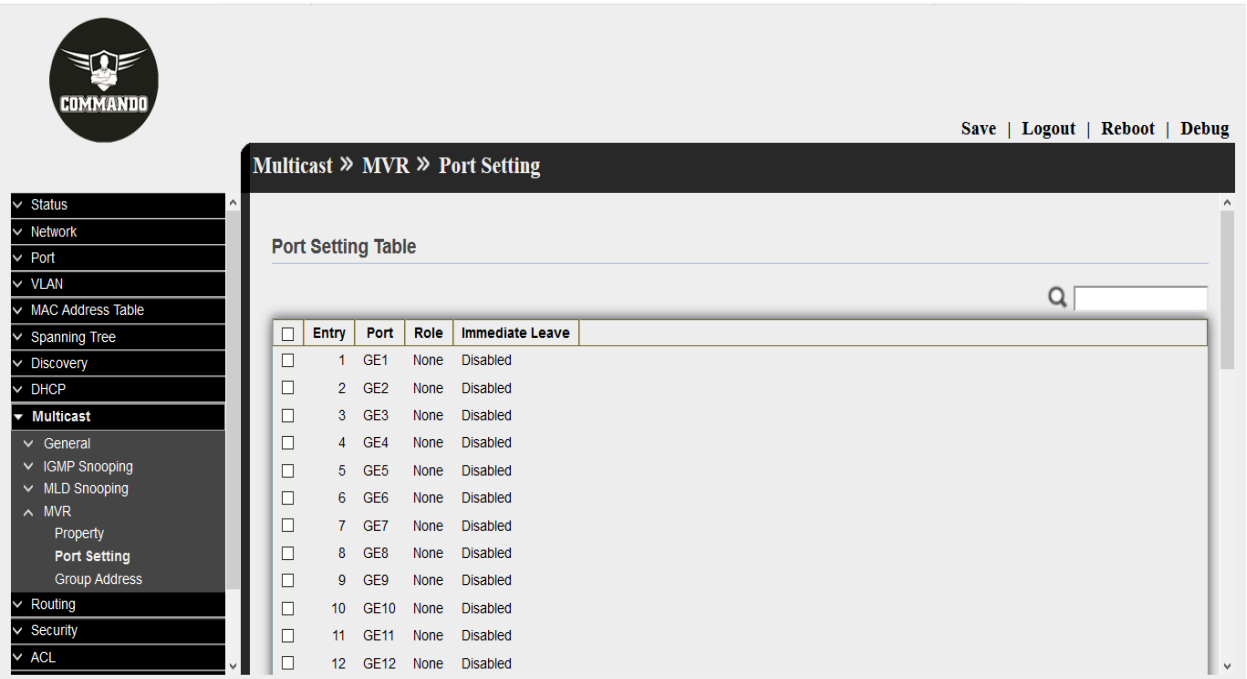


Fig 10.4.3 Multicast MVR Port Setting page

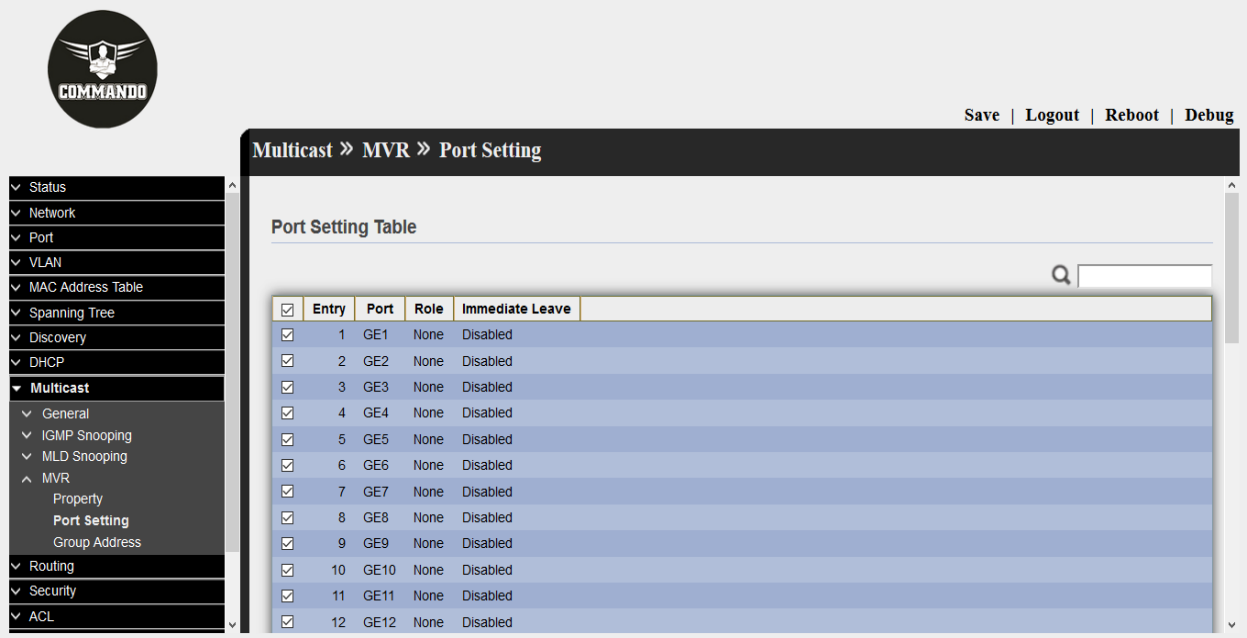


Fig 10.4.4 Multicast MVR Port Selection page

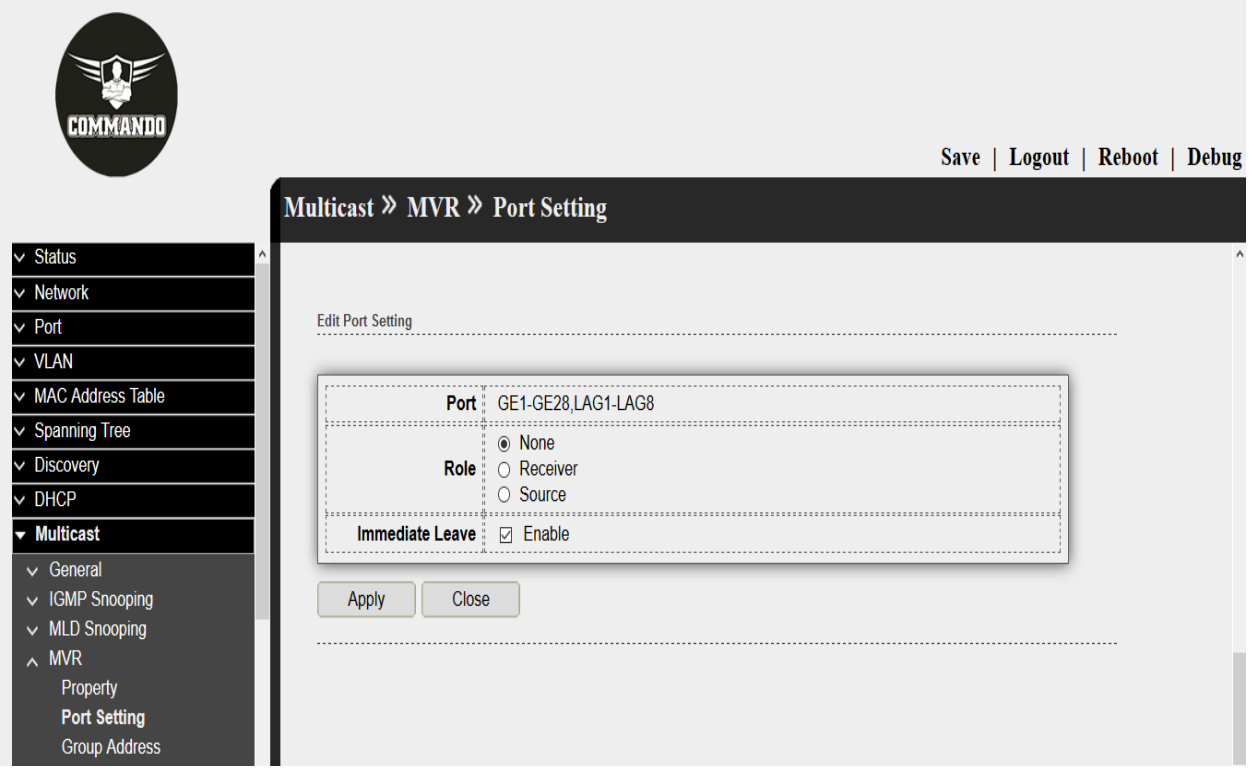


Fig 10.4.5 Multicast MVR Edit port setting page

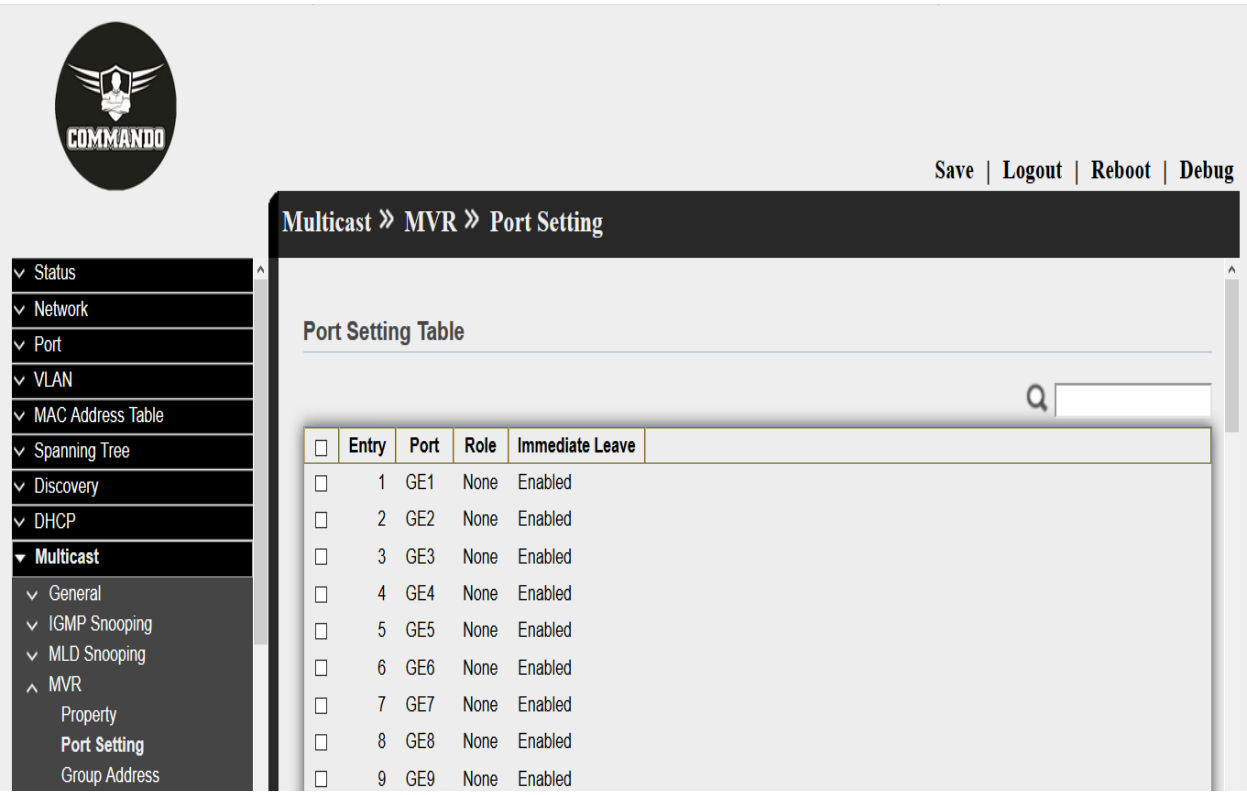


Fig 10.4.6 Multicast MVR Port setting Table page

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.**

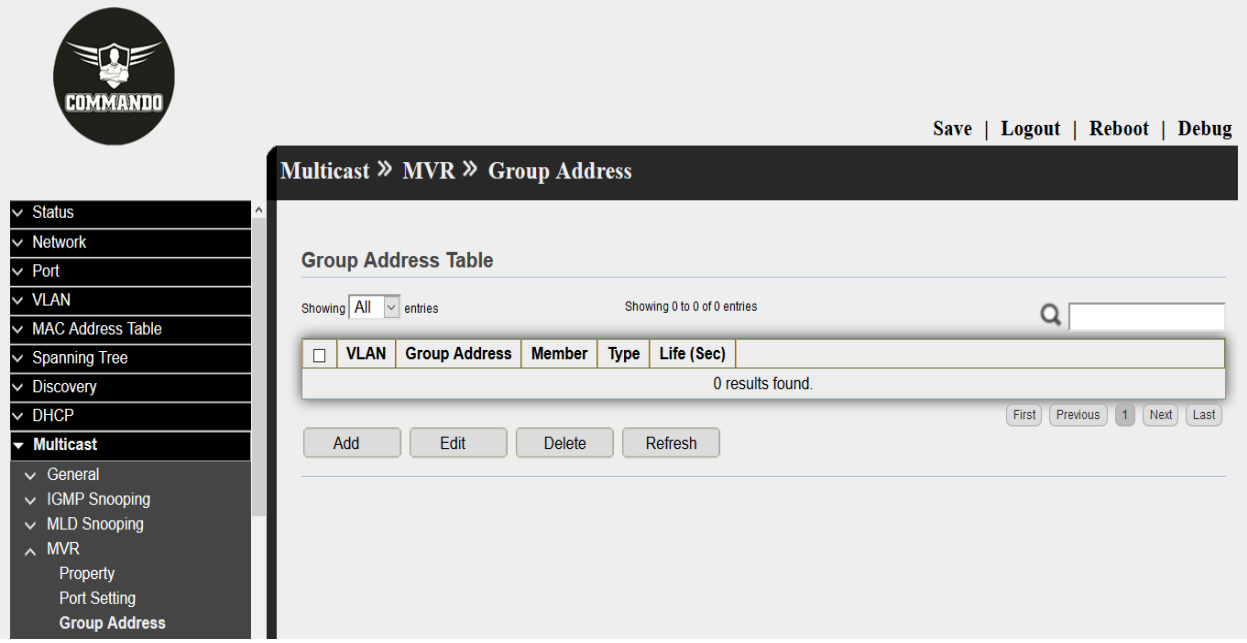


Fig 10.4.7 Multicast MVR default group address Table page

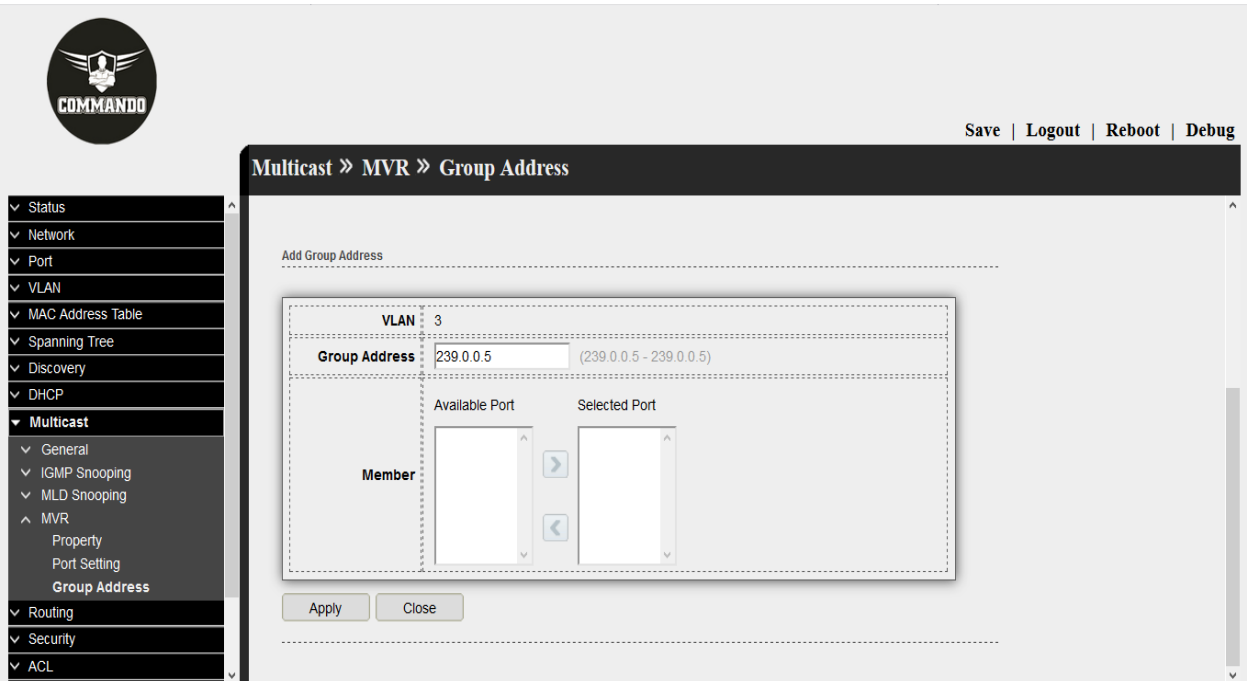


Fig 10.4.8 Multicast MVR Add group address page

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 hextet). 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.

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

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.**

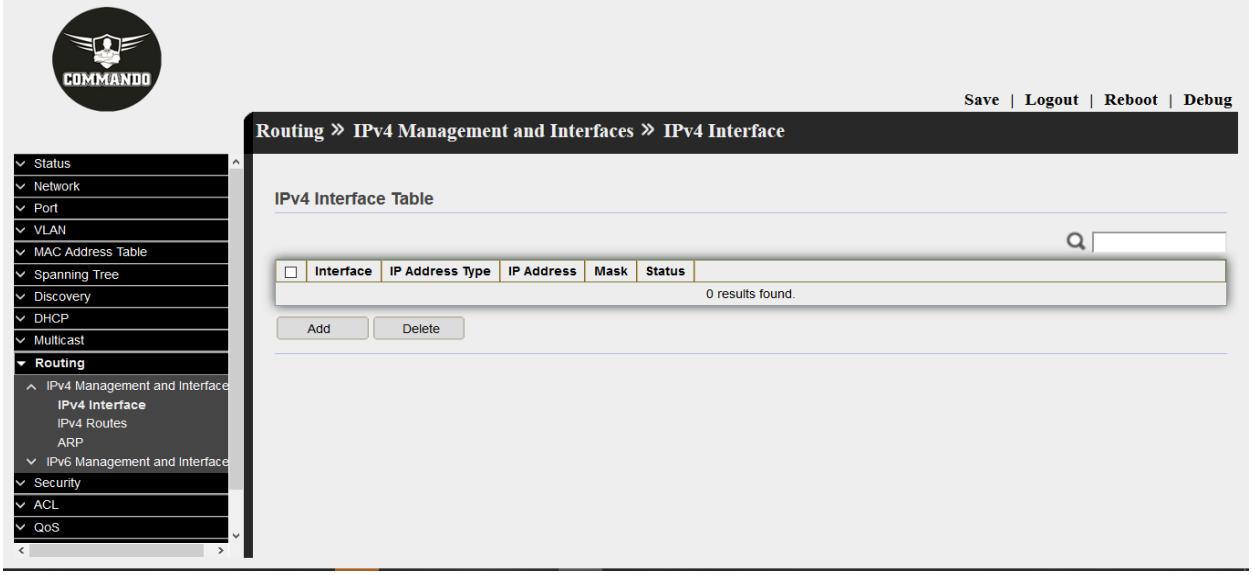


Fig 11.1.1 Default IPv4 interface table page

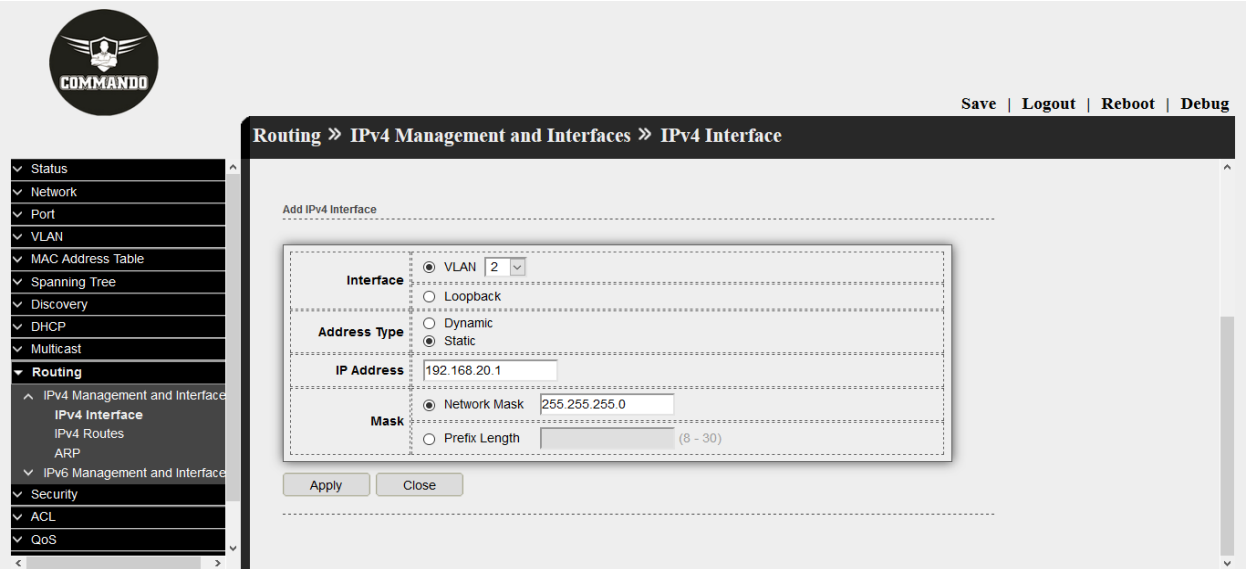


Fig 11.1.2 IPv4 interface configuration page

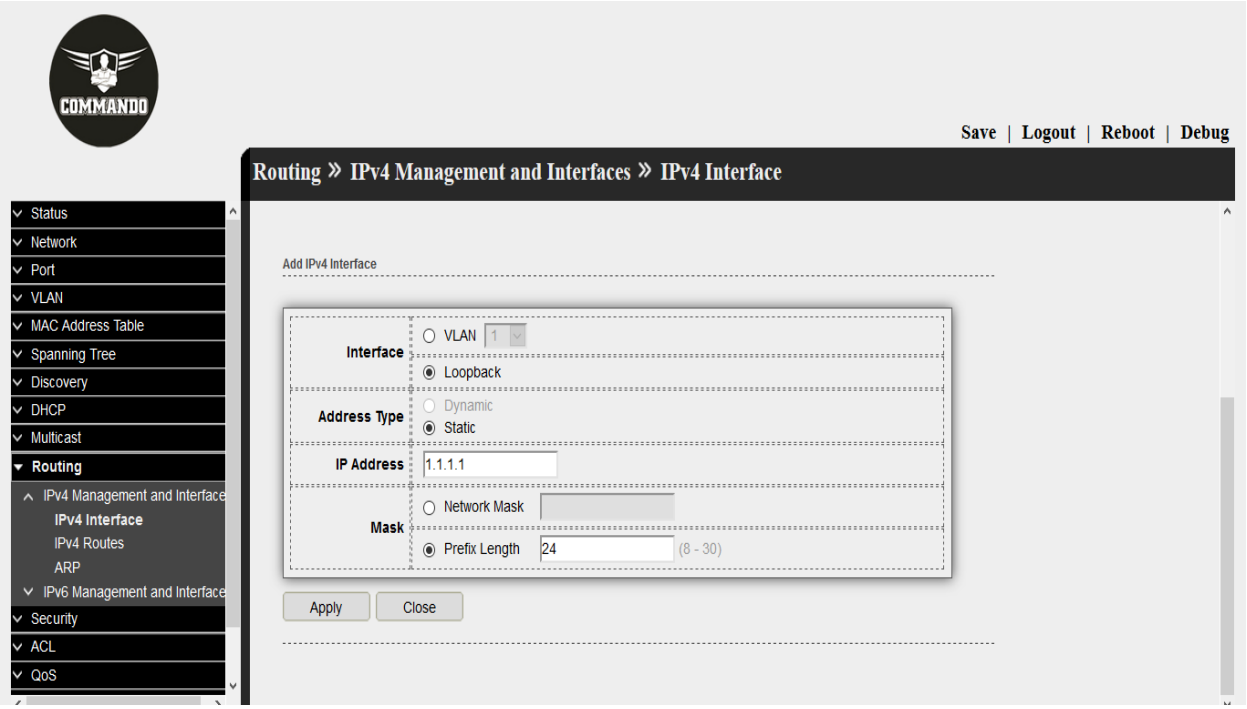


Fig 11.1.3 Creating IPv4 loopback interface configuration page

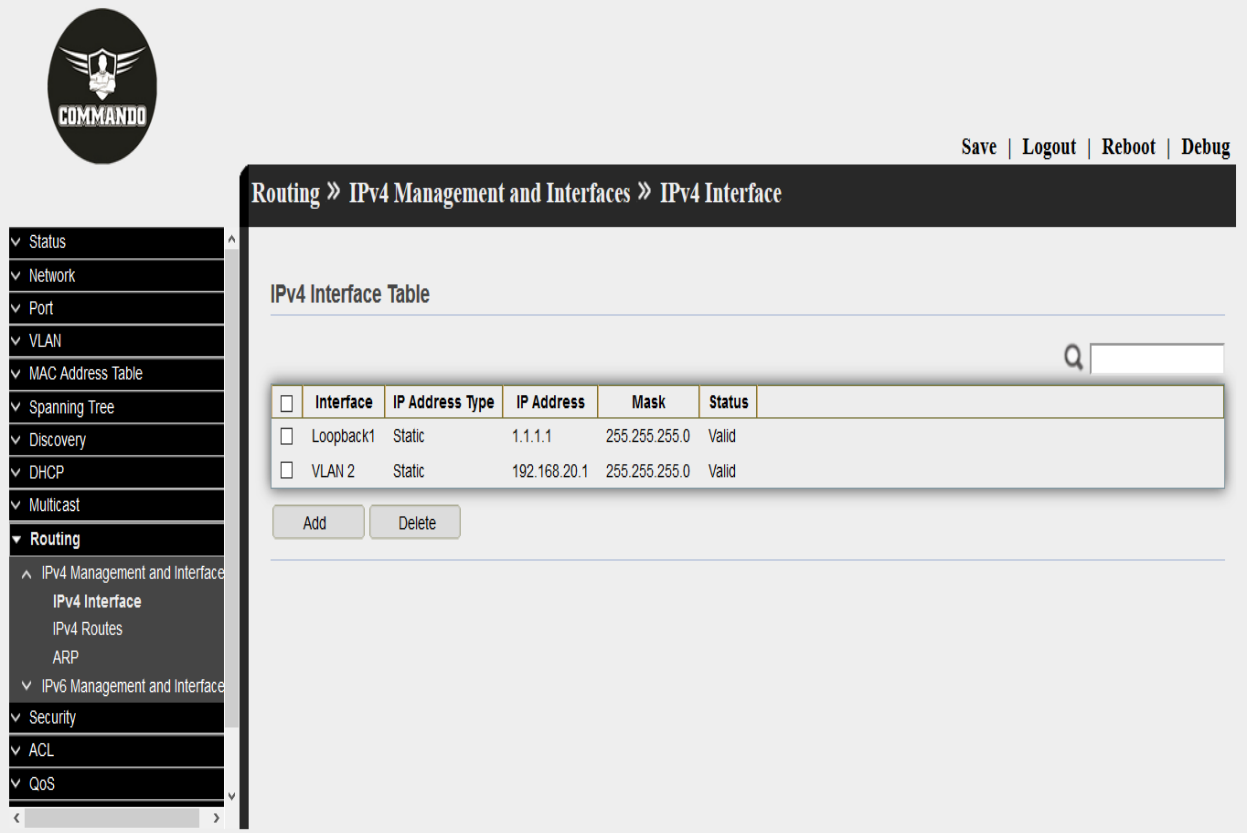


Fig 11.1.4 IPv4 interface table page

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. Which is having

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 manly 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. The switch use dynamic routing protocols to automatically calculate the best route to forward packets.

Static routing entries: Static routing entries are manually added none-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.

The C2000 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.

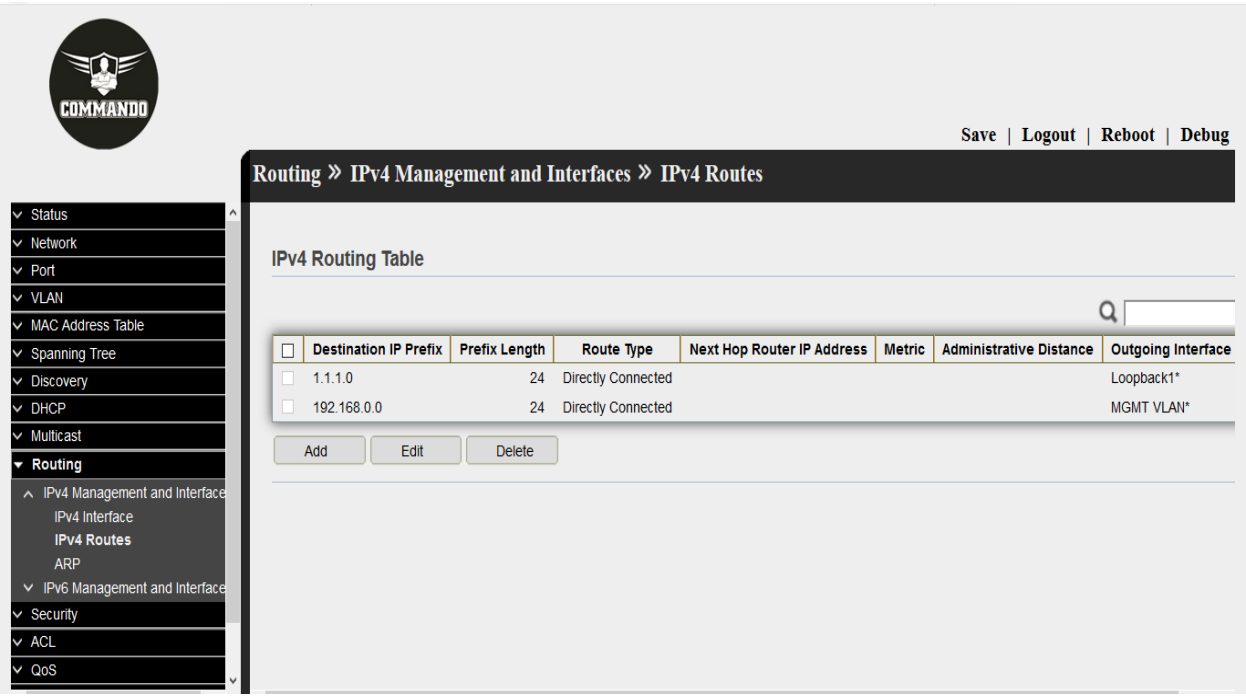


Fig 11.2.1 Default IPv4 Routing Table as per created Layer 3 interface page

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 perticular network.

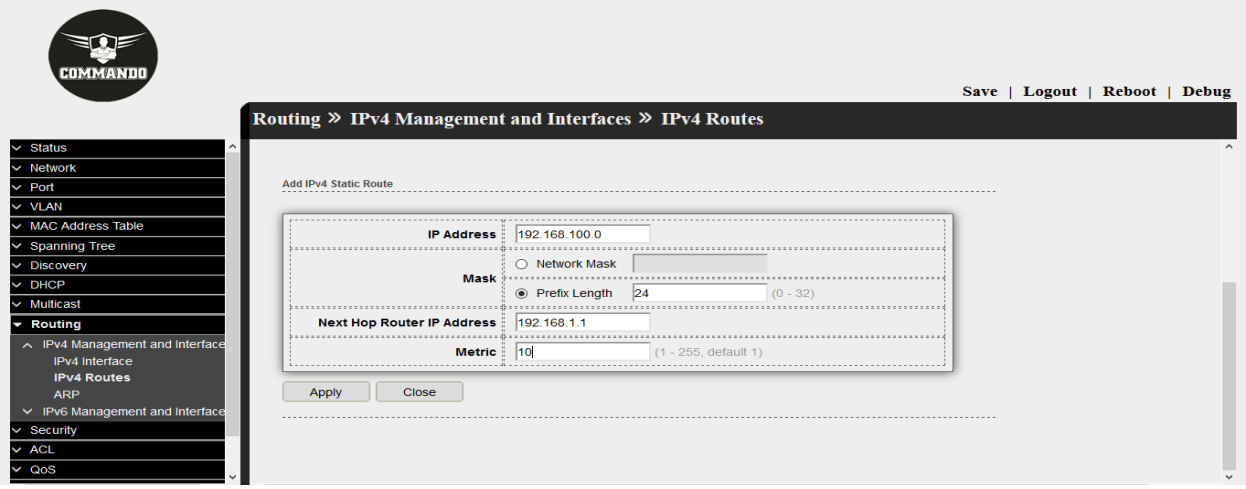


Fig 11.2.2 Add IPv4 Static route page

Default IPv4 Routes Configuration:

Keep Network and mask all zero with Next hop Ip as prefered and can set metric also.

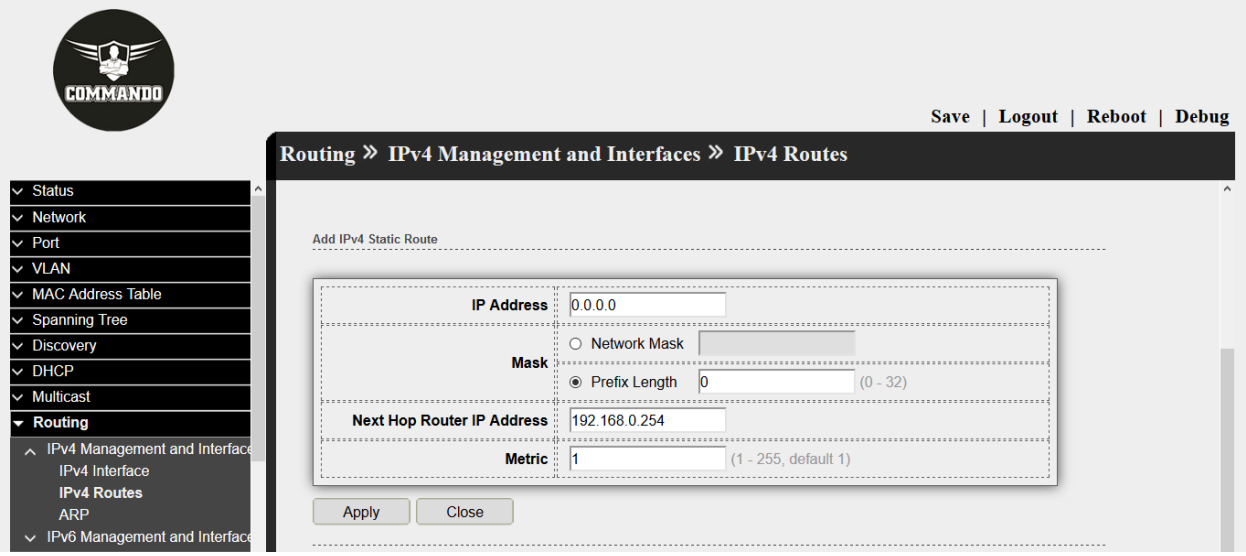


Fig 11.2.3 Add IPv4 Default route page

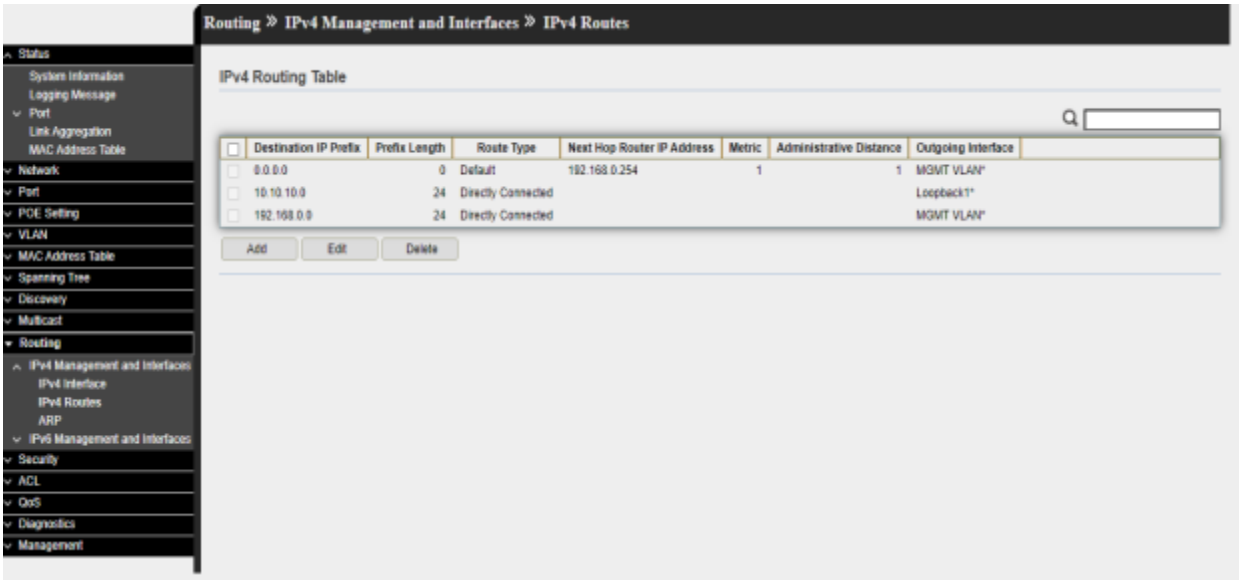


Fig 11.2.4 IPv4 routing table page

11.1.3 ARP

The C2000 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.

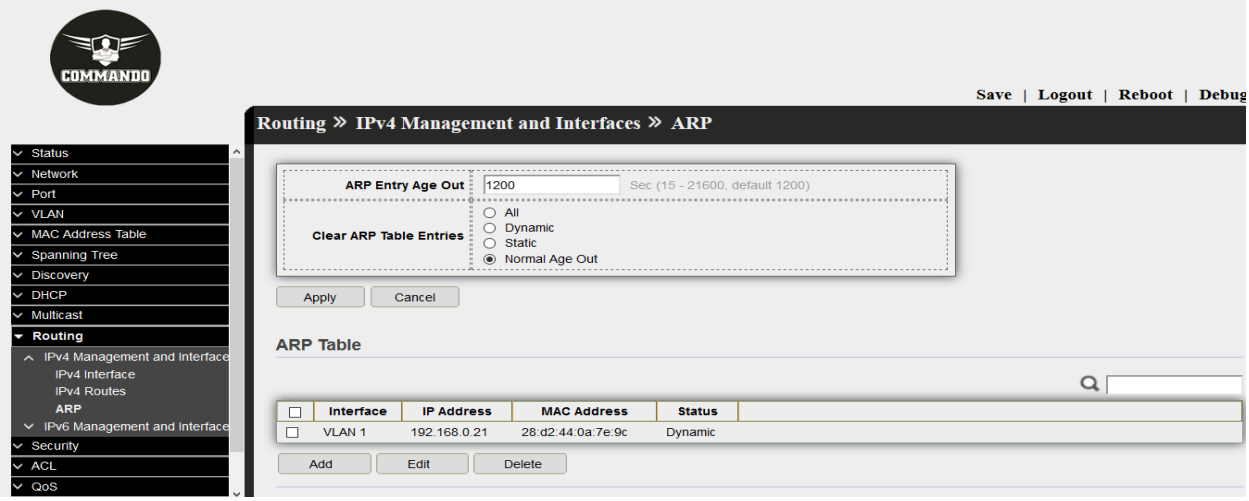


Fig 11.1.4 Default ARP table page

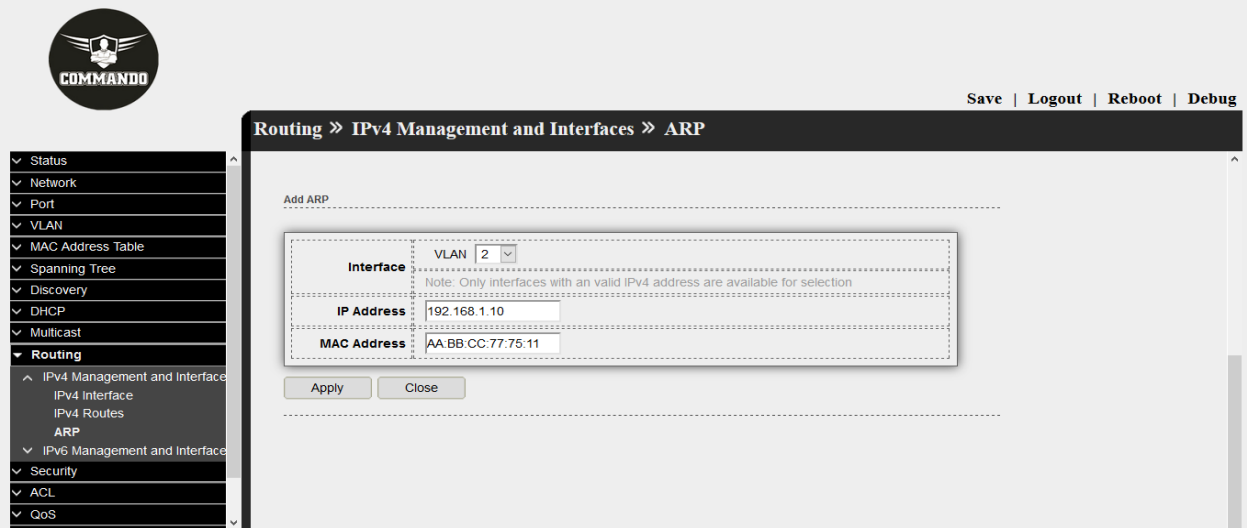


Fig 11.1.5 Add ARP page

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.**

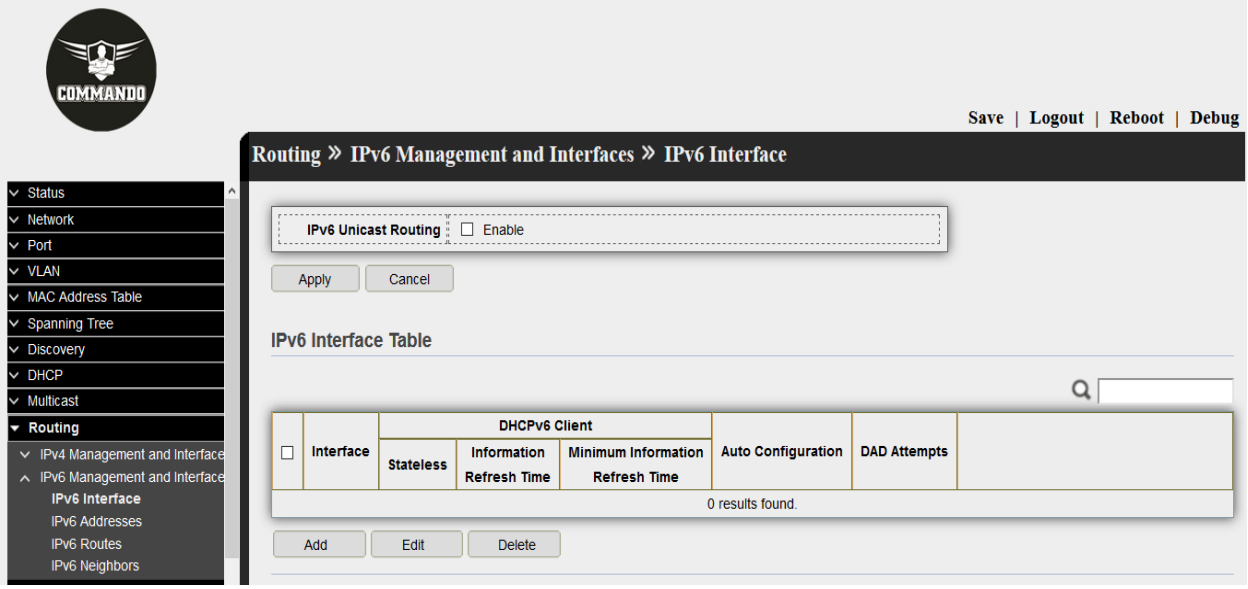


Fig 11.2.1 Default IPv6 interface Table page

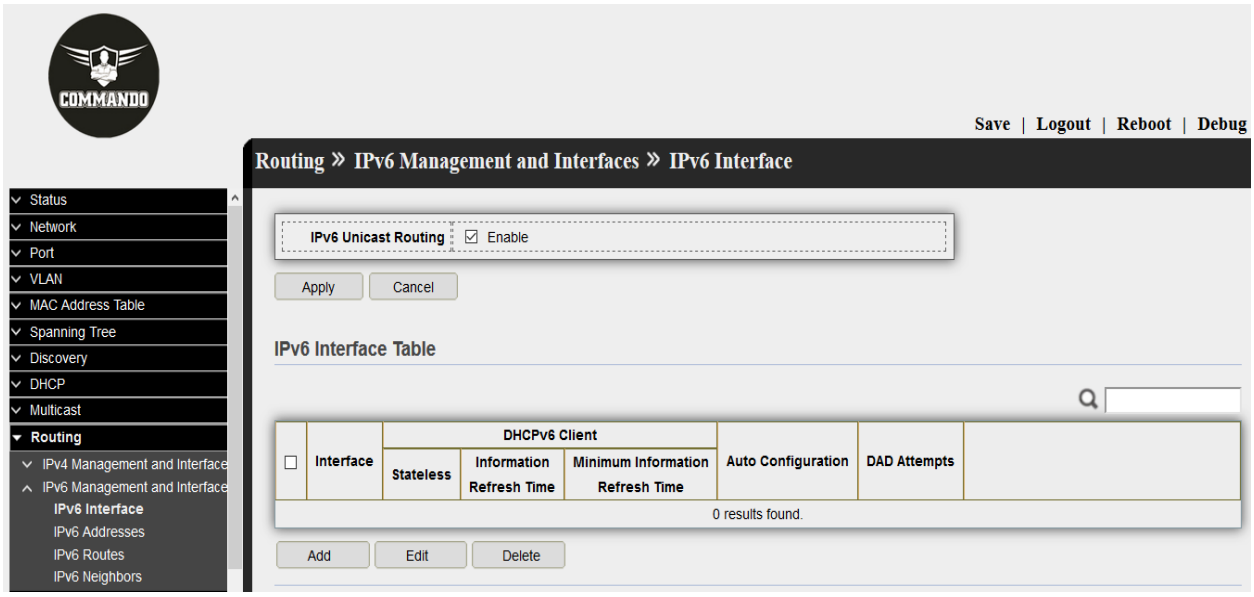


Fig 11.2.2 Enableing IPv6 Unicast Routing page

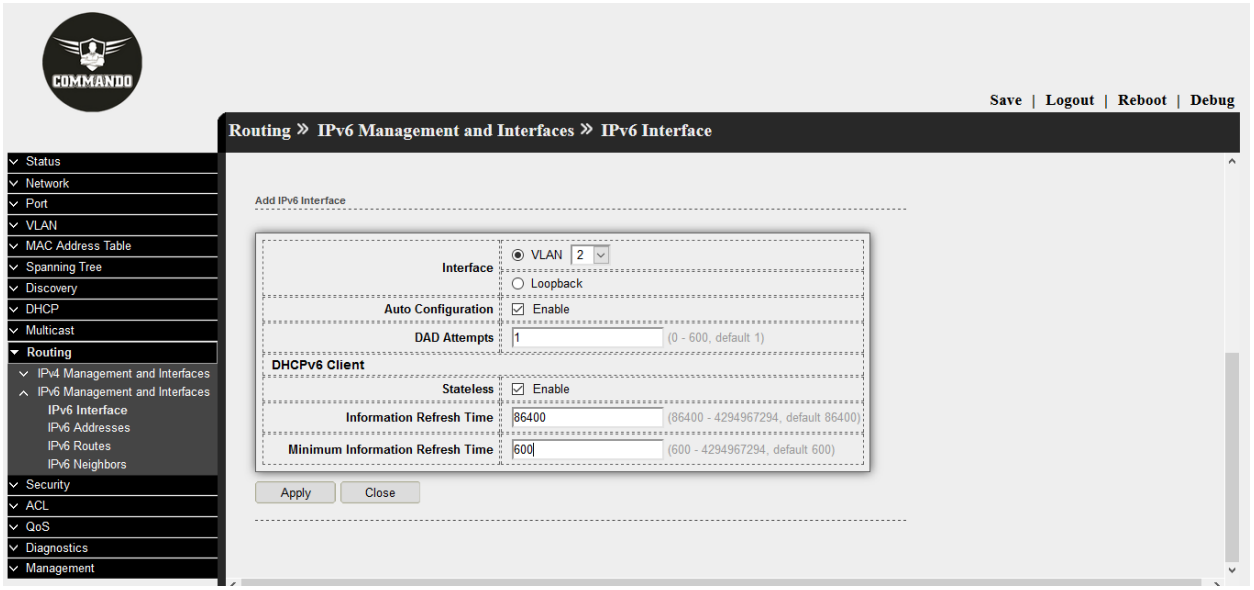


Fig 11.2.3 Add IPv6 interface page

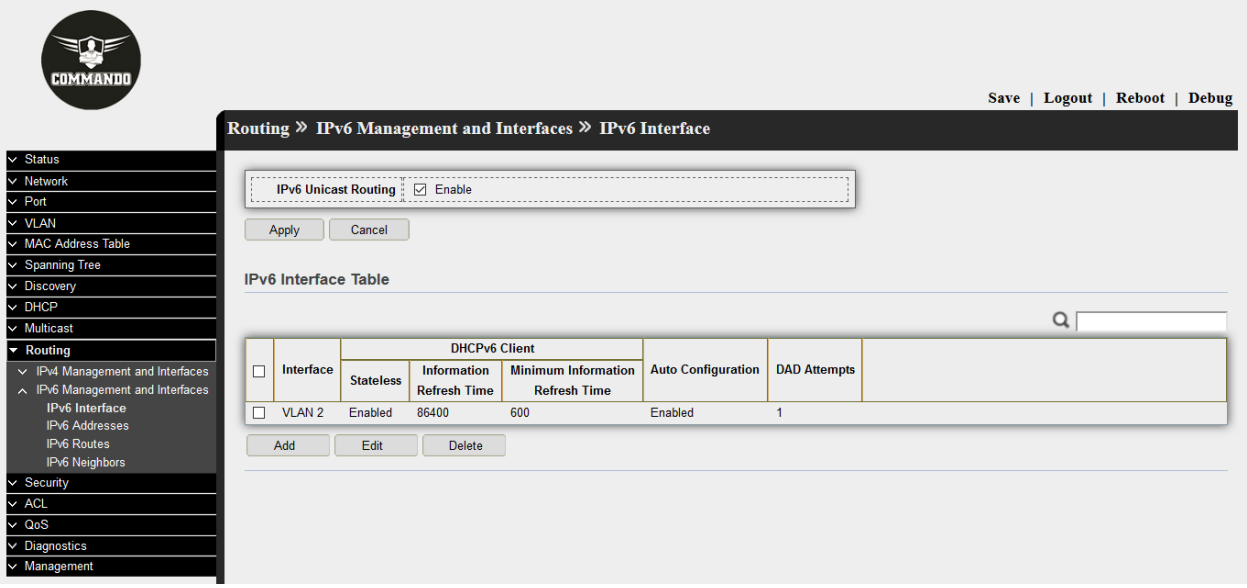


Fig 11.2.4 IPv6 interface Table page

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.**

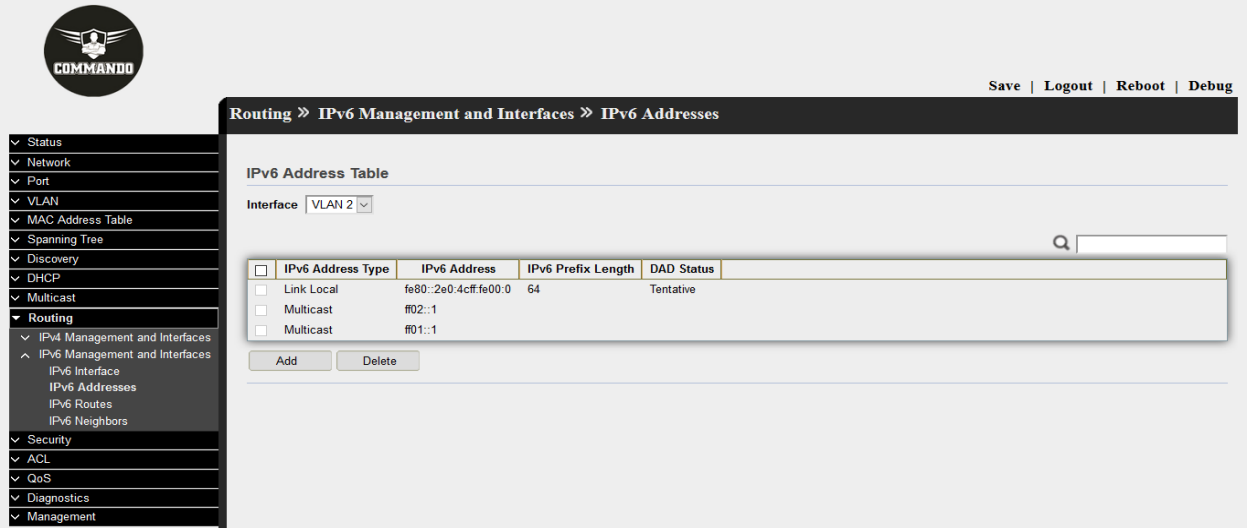


Fig 11.2.5 IPv6 address table page

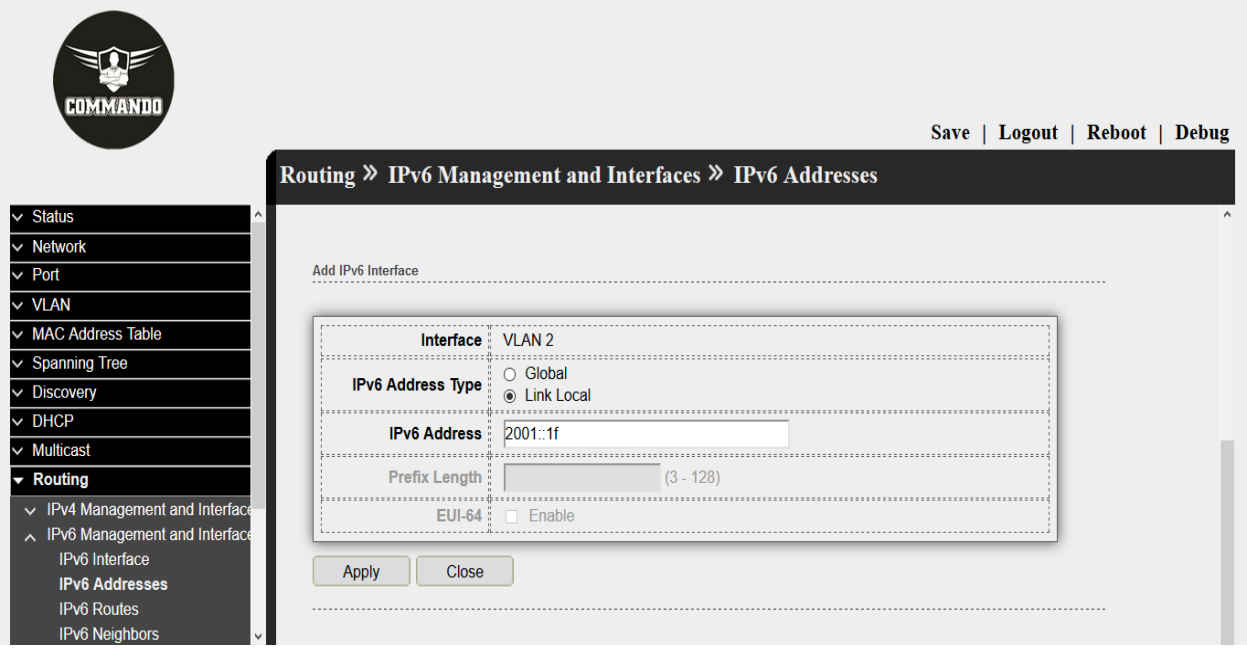


Fig 11.2.6 Add IPv6 interface page

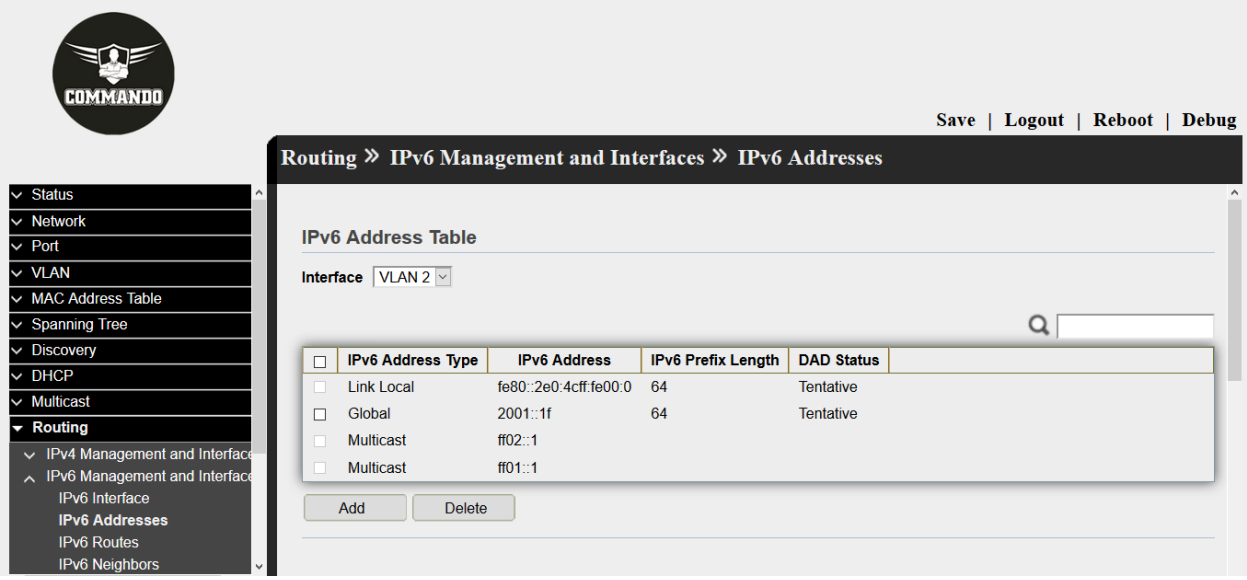


Fig 11.2.7 IPv6 address table after adding IPv6 address page

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.**

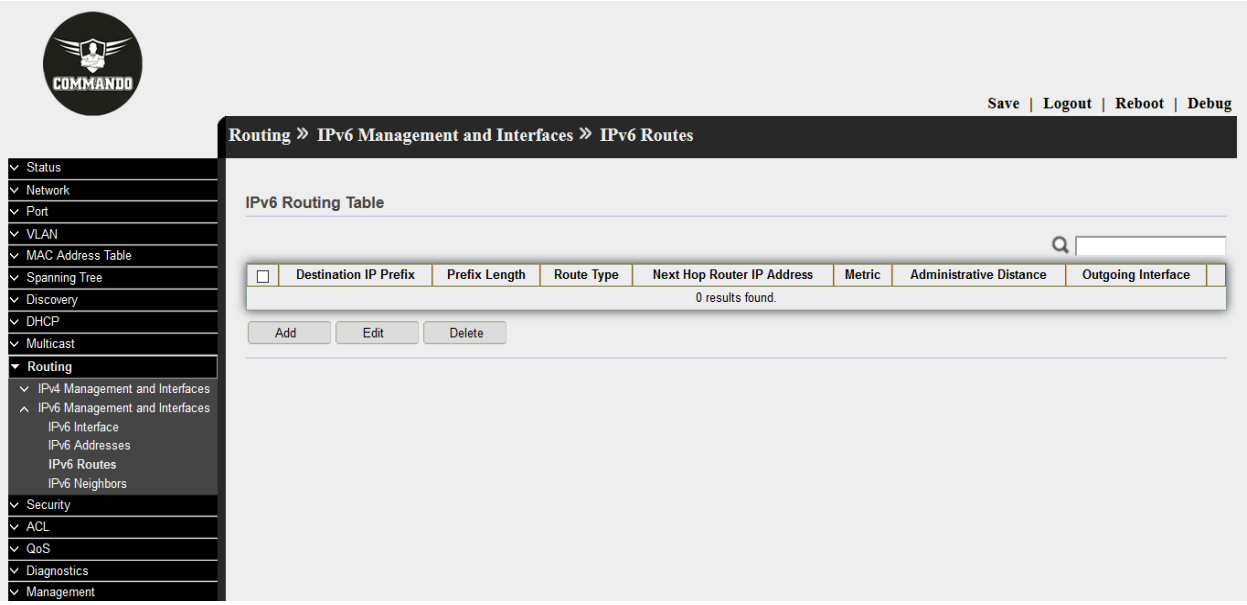


Fig 11.2.8 Default IPv6 routing table page

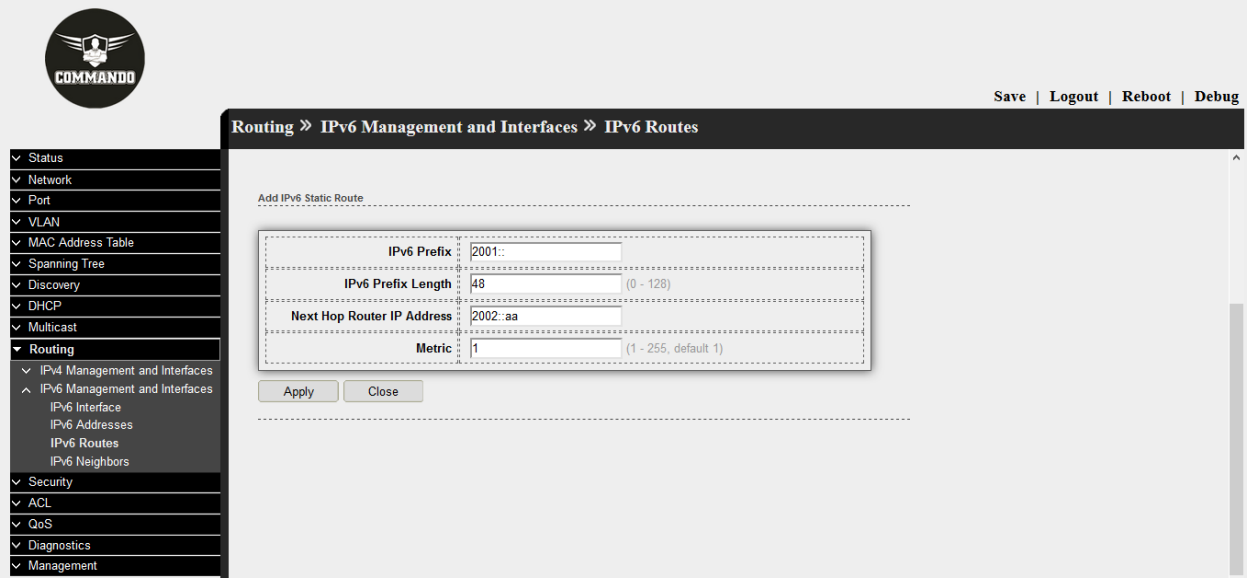


Fig 11.2.9 Add IPv6 static route page

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.

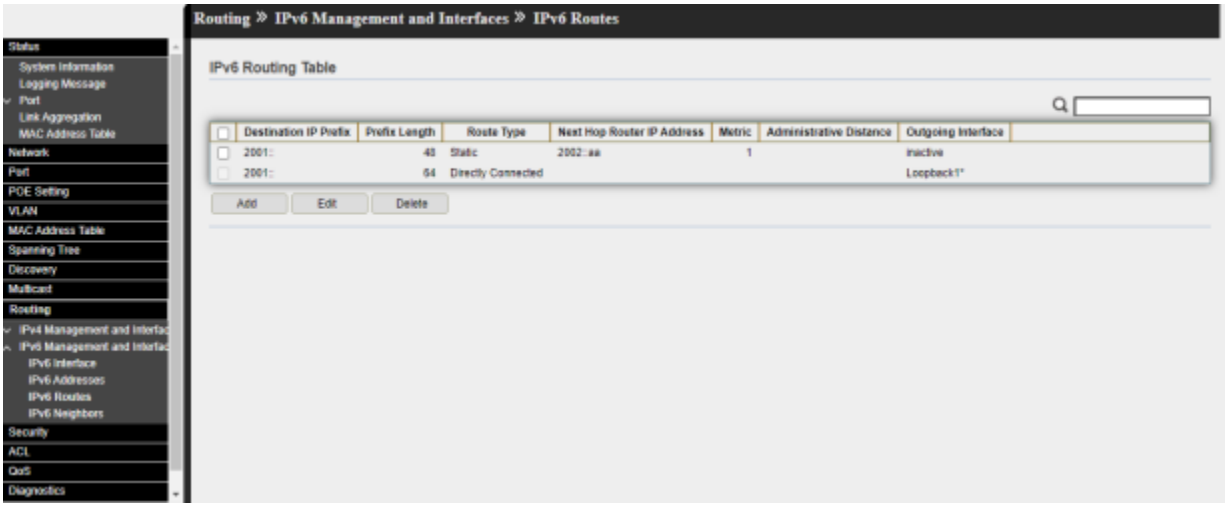


Fig 11.2.10 IPv6 static route page

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.**

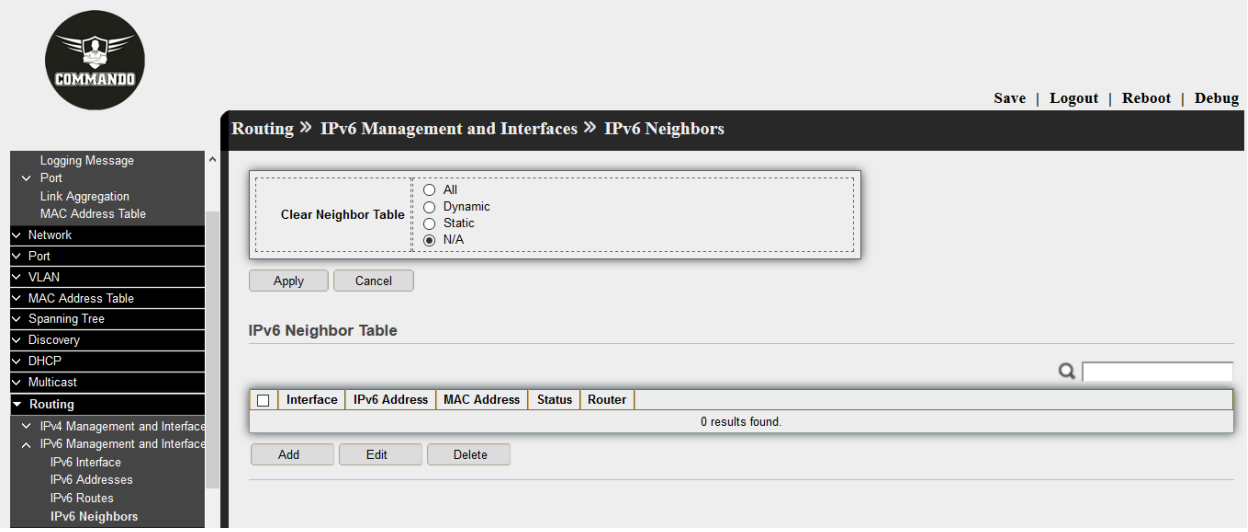


Fig 11.2.11 Default IPv6 neighbor page

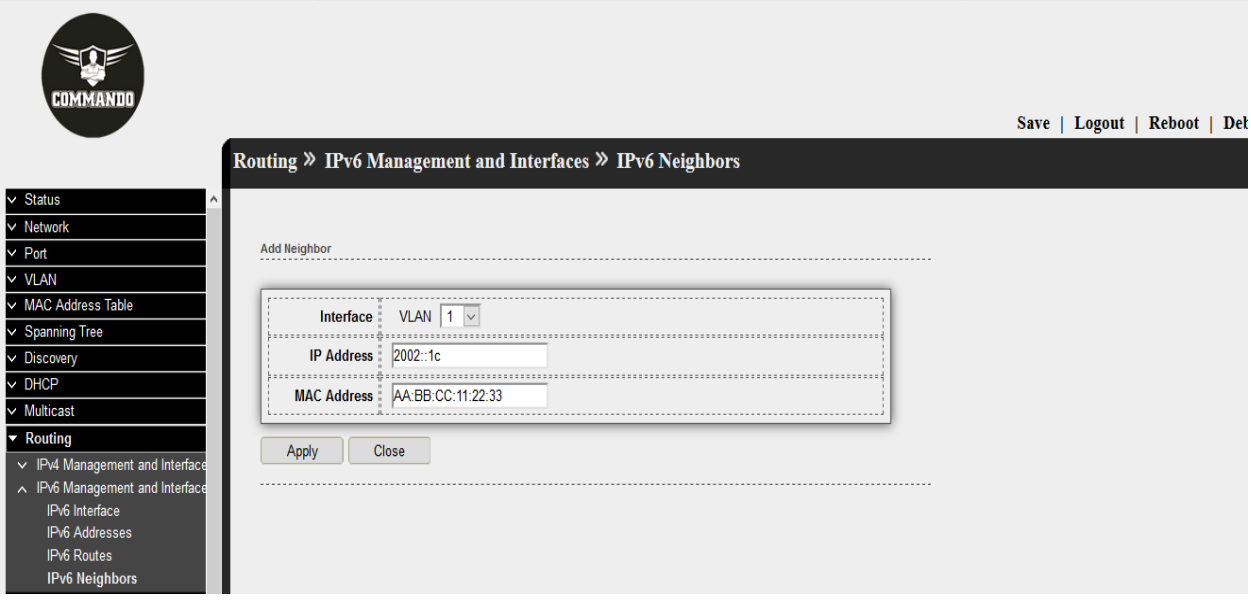


Fig 11.2.12 Add IPv6 neighbor page

Chapter 12 Security

Group Header:- Security

After clicking **Security** [redacted] down arrow keys following four our 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 in order to disrupt it's 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 exhustions 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

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 of 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

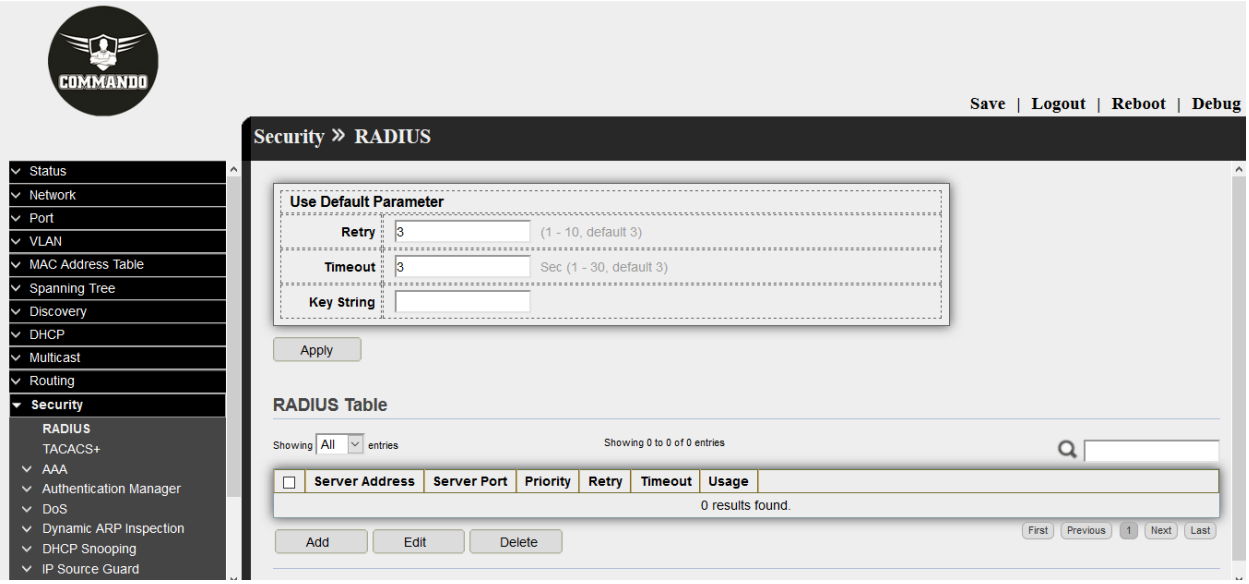


Fig 11.1.1 Default RADIUS Table page

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.

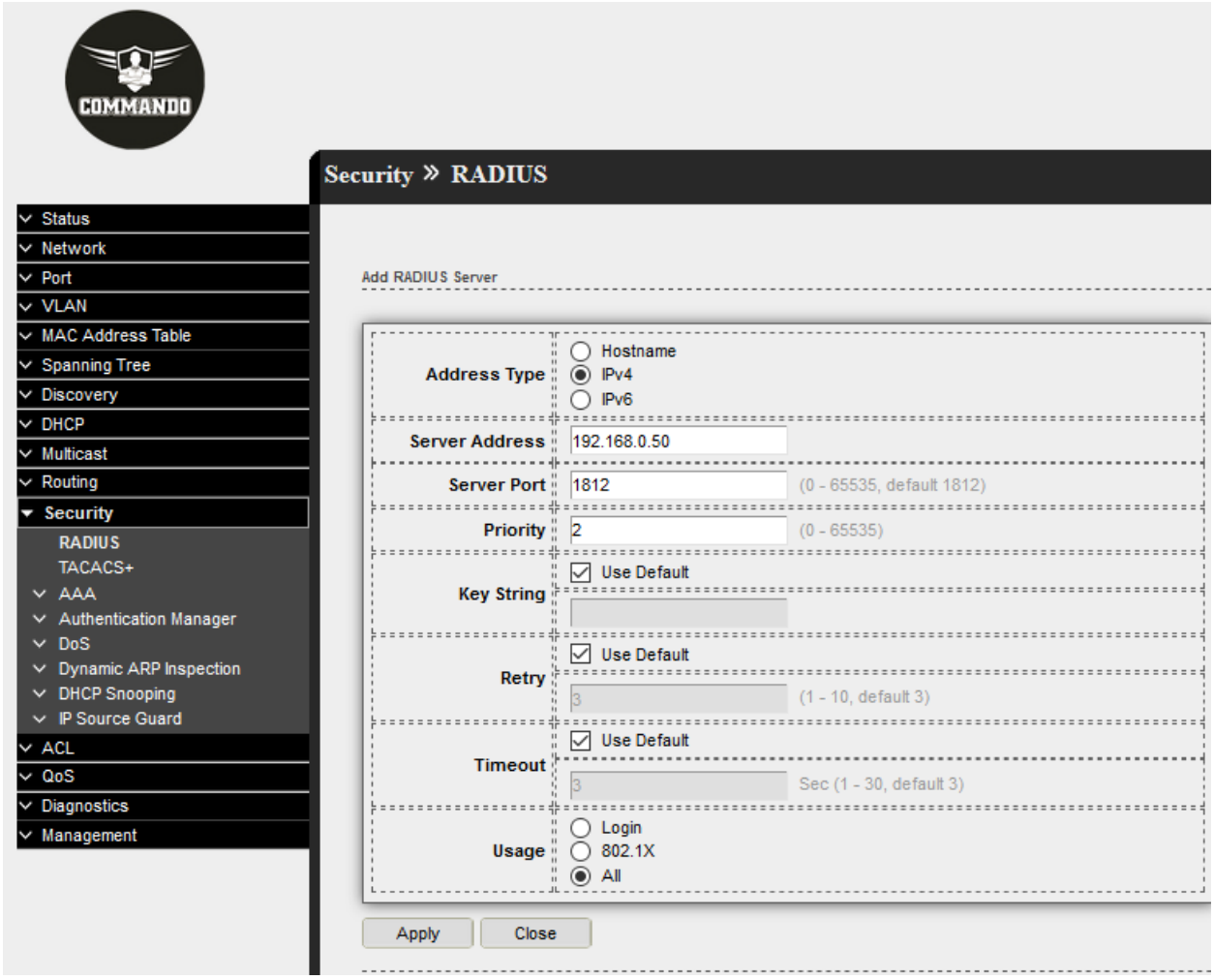


Fig 11.1.2 Add RADIUS server page

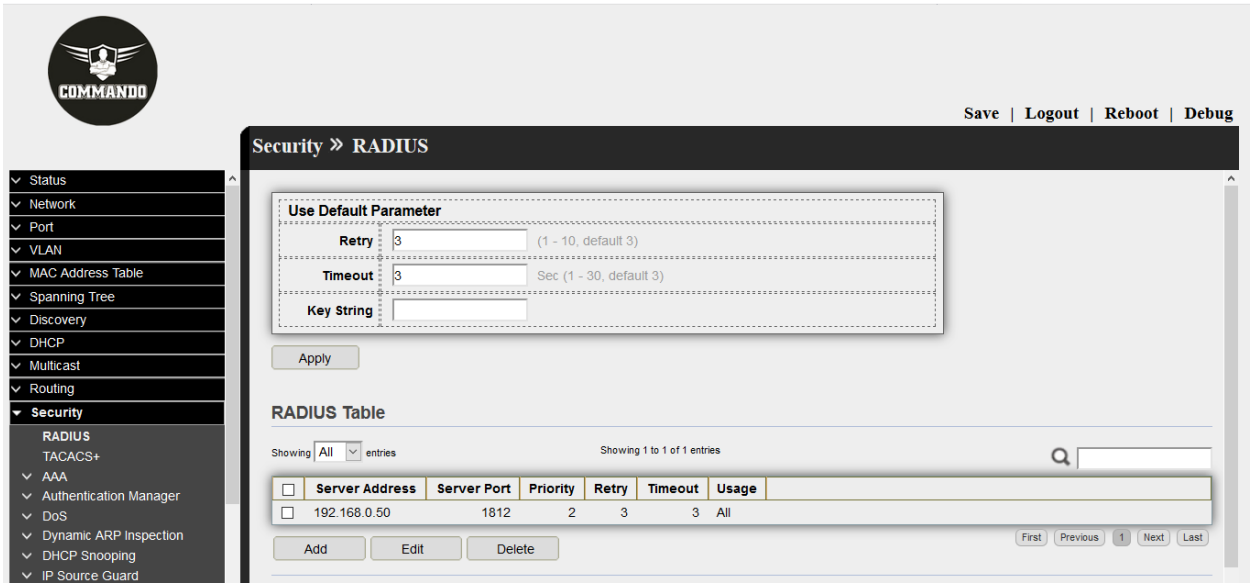


Fig 11.1.3 RADIUS Table page

12.2 TACACS+

TACACS+, stands for Terminal Access Controller Access Control Server, is a security protocol used in AAA framework to provide centralised 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+**

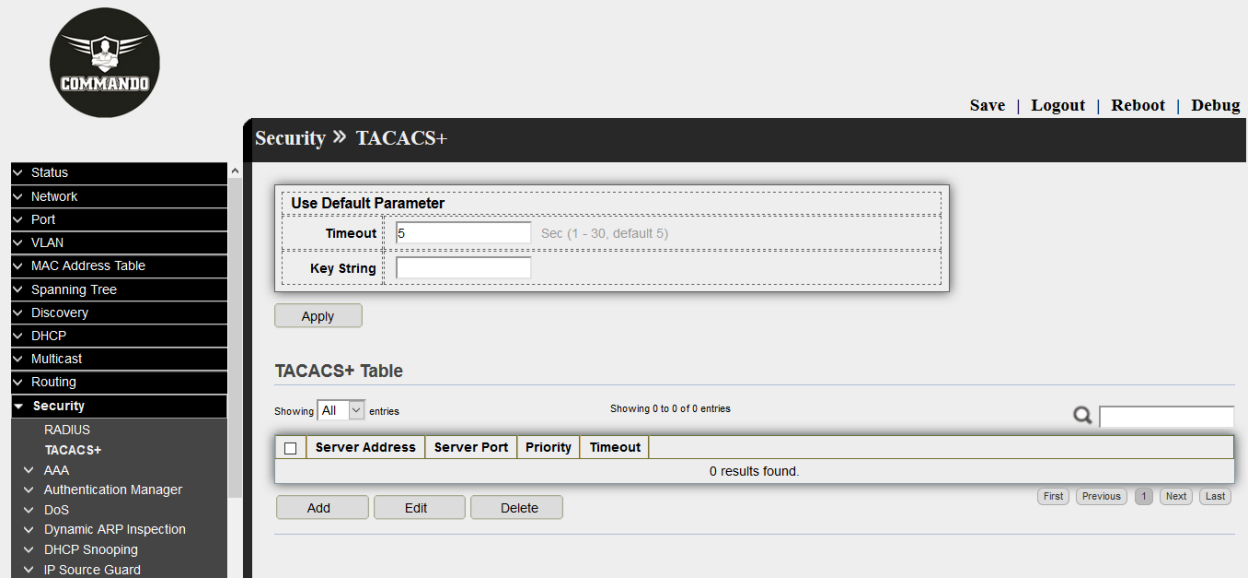


Fig 12.2.1 Default TACACS+ Table page

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.

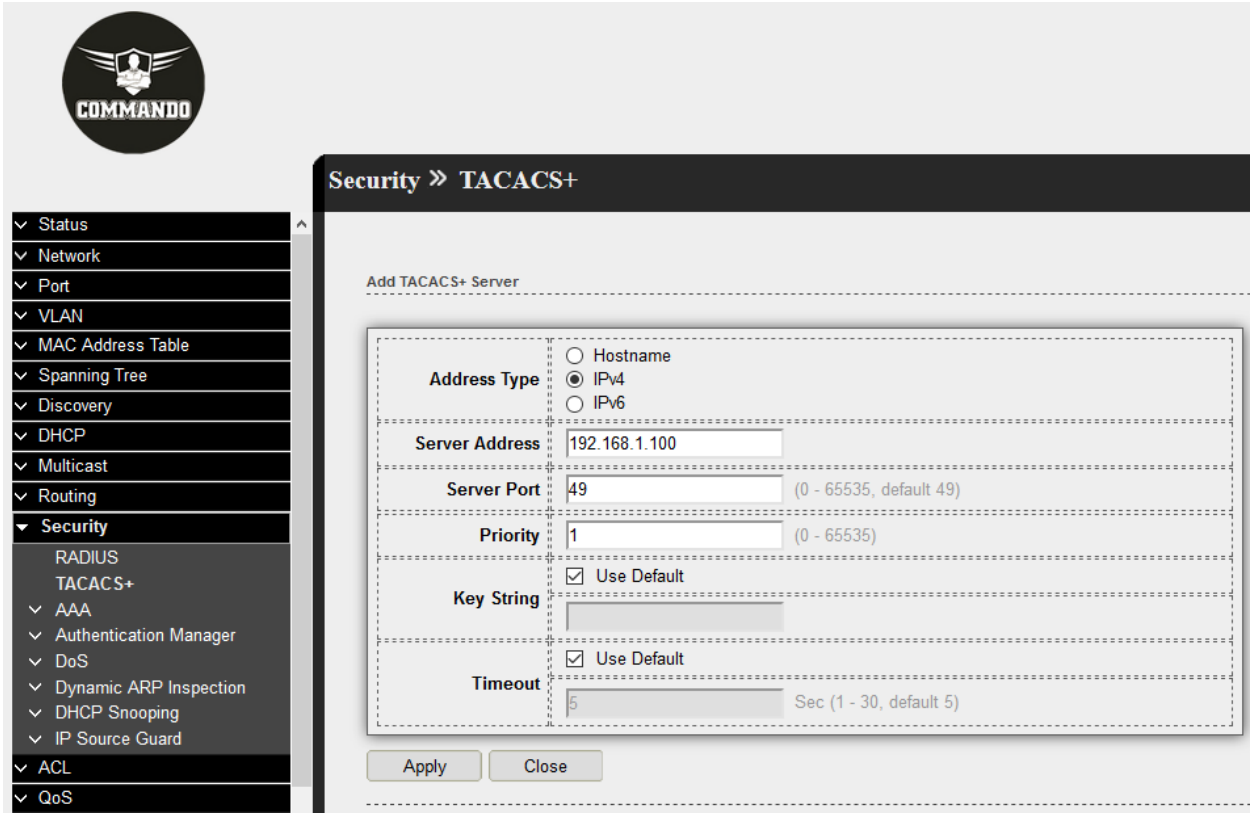


Fig 12.2.2 Add TACACS+ server page

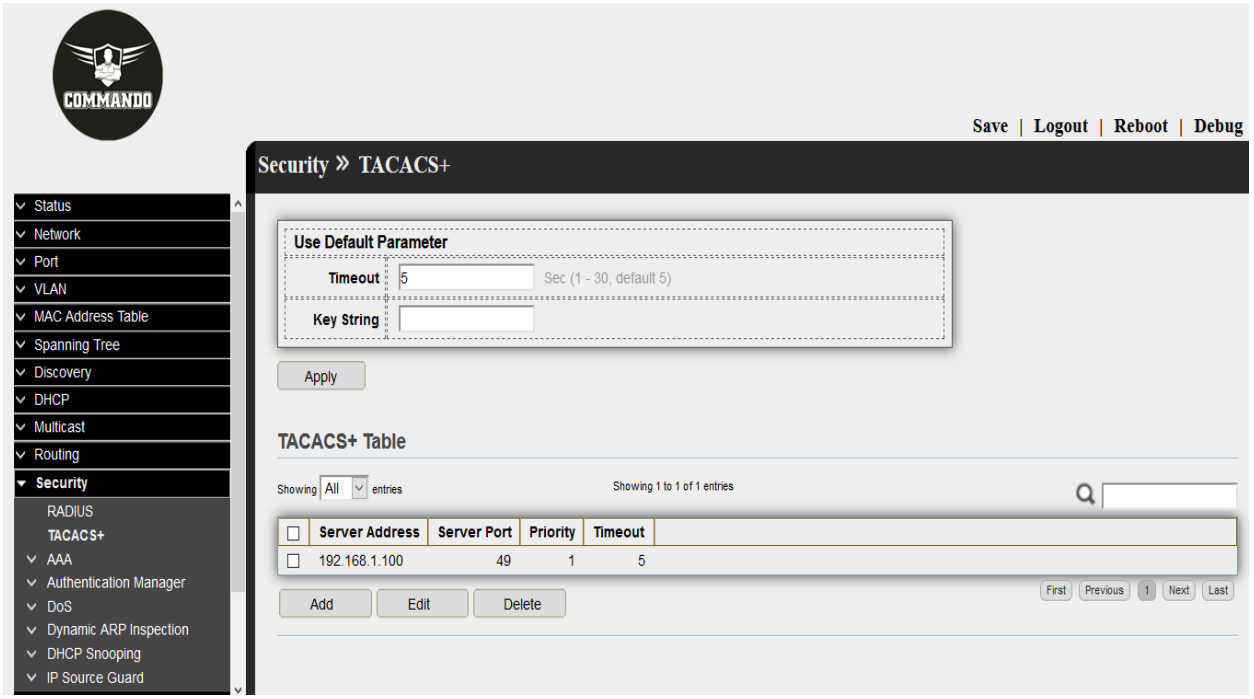


Fig 12.2.3 TACACS+ table page

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 is 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.

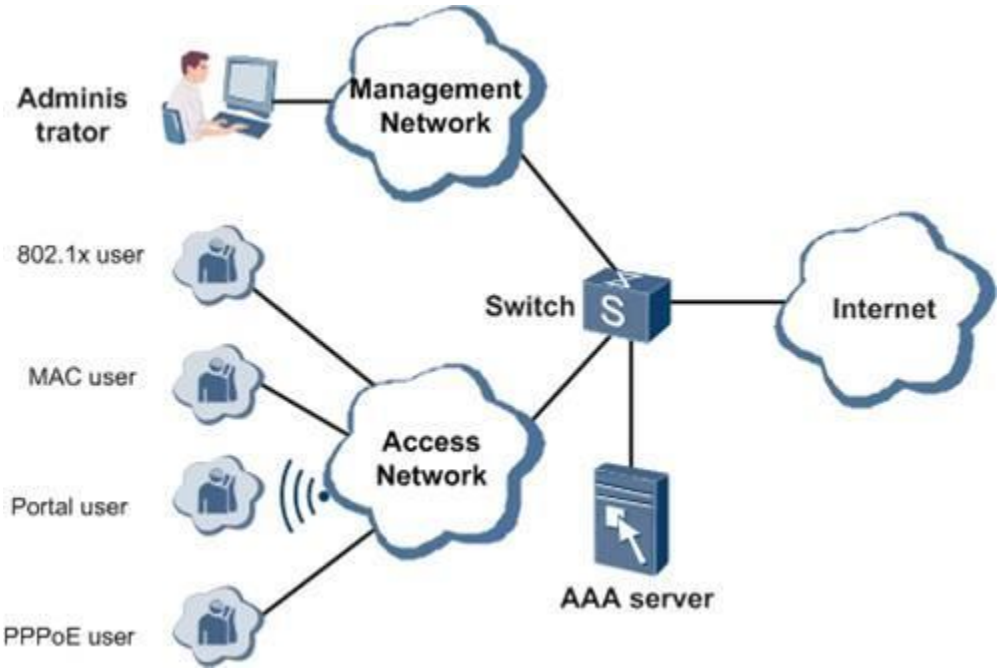


Fig 12.3.1 AAA Server Concept

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.**

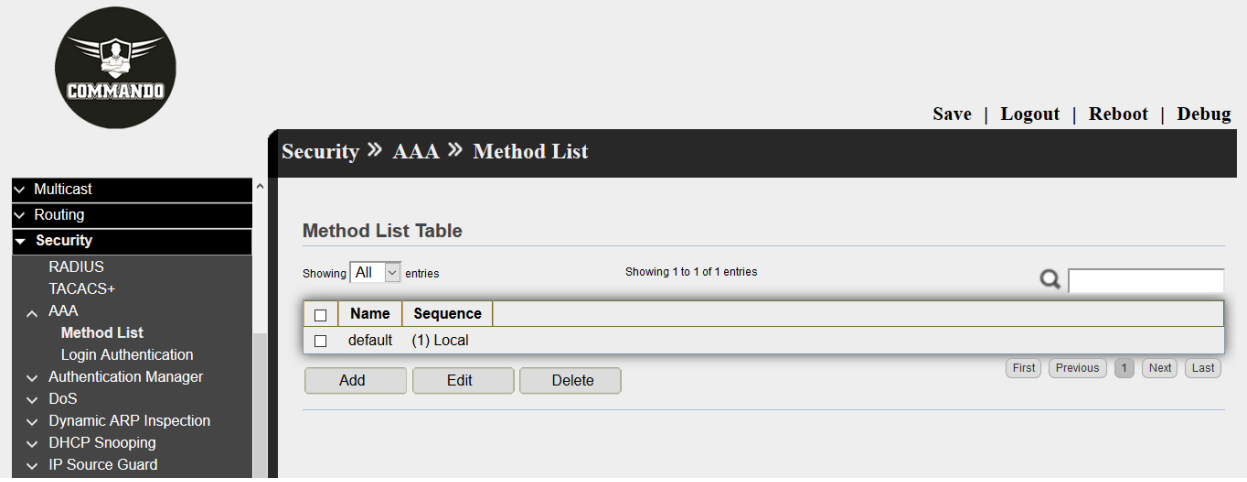


Fig 12.3.2 Default AAA Method List table page

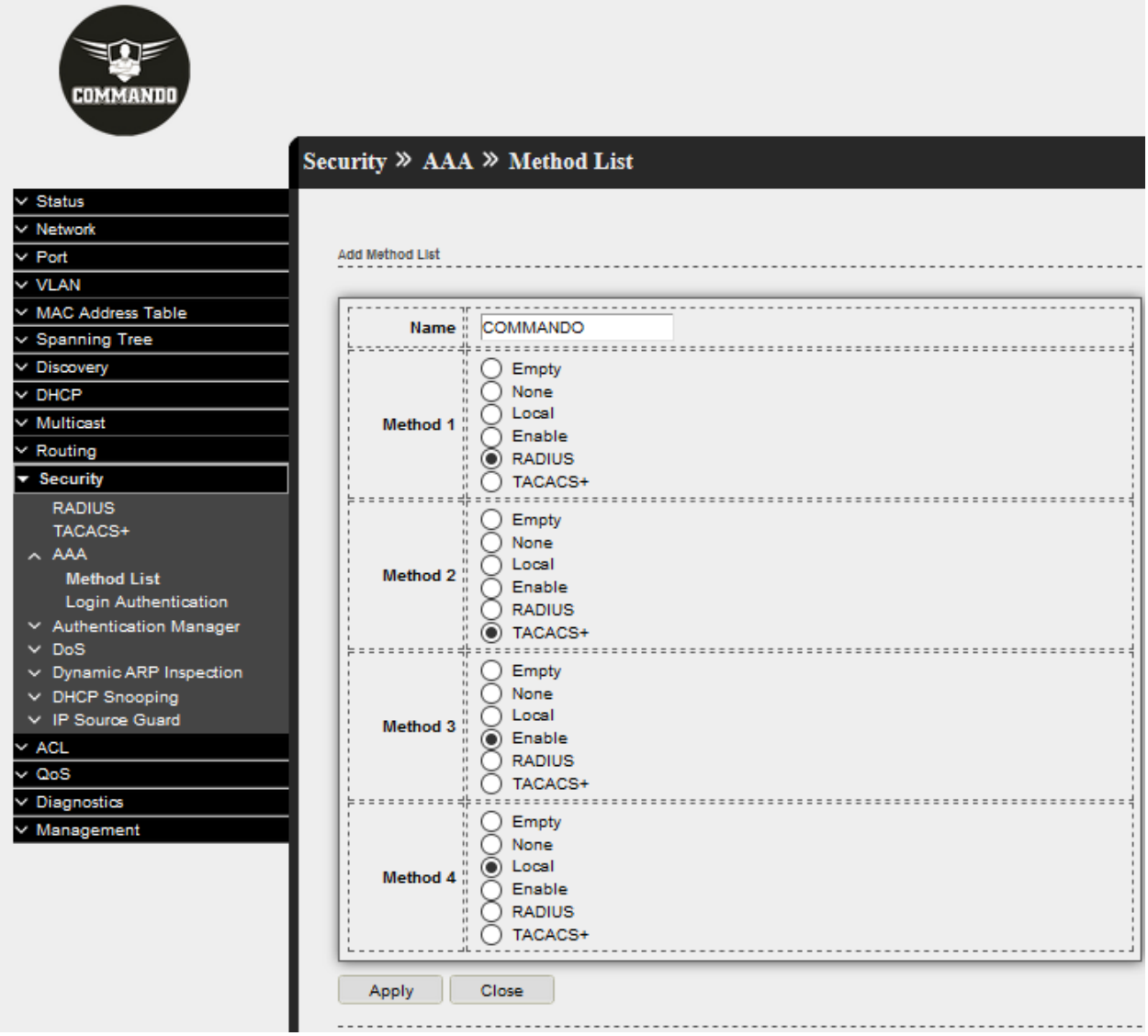


Fig 12.3.3 Edit AAA Method List page

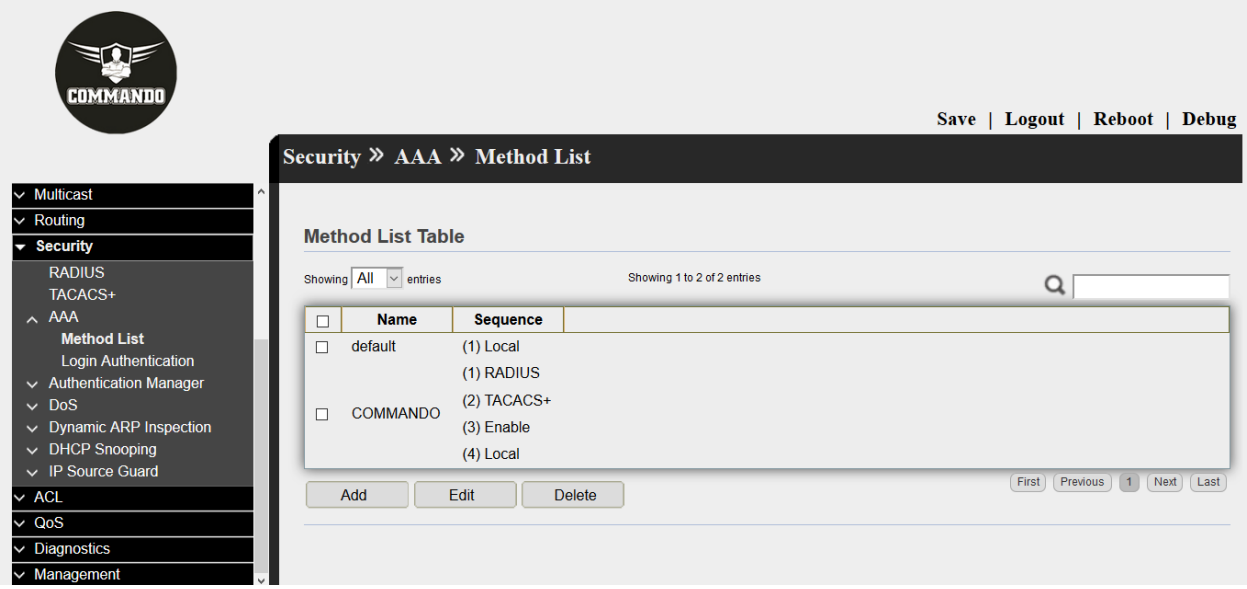


Fig 12.3.4 AAA Method List Table page

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.**

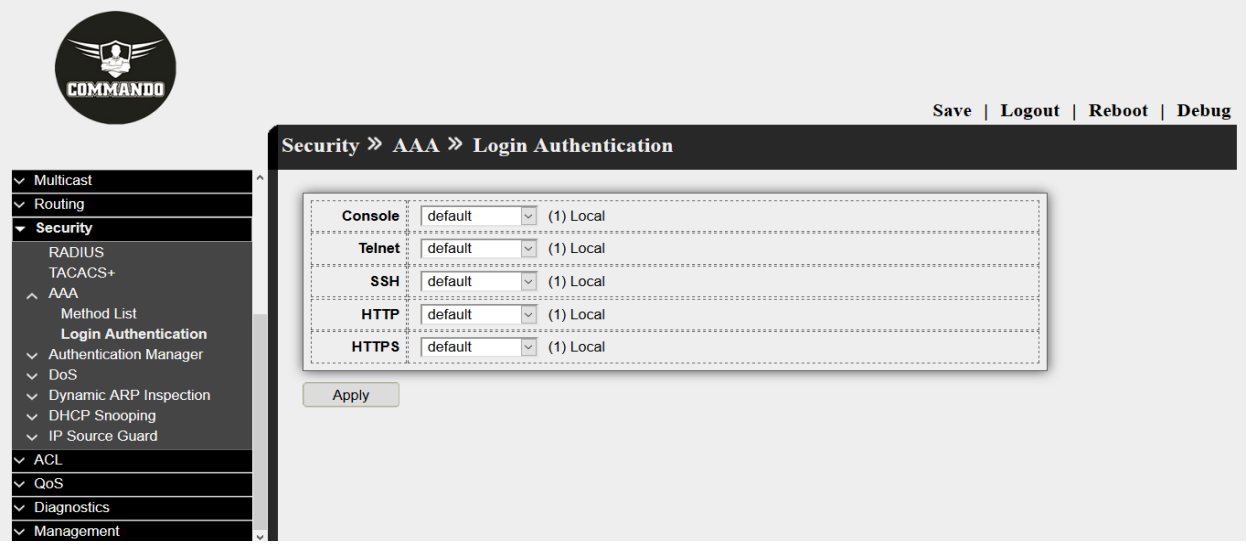


Fig 12.3.5 AAA Login Authentication page

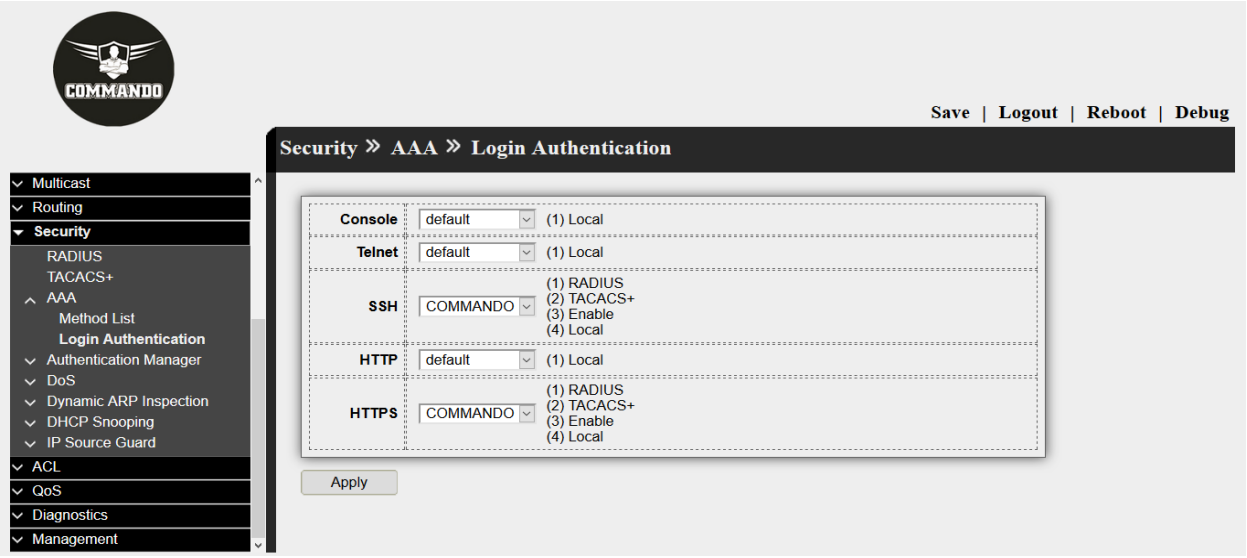


Fig 12.3.6 Setting AAA Login Authentication page

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.**

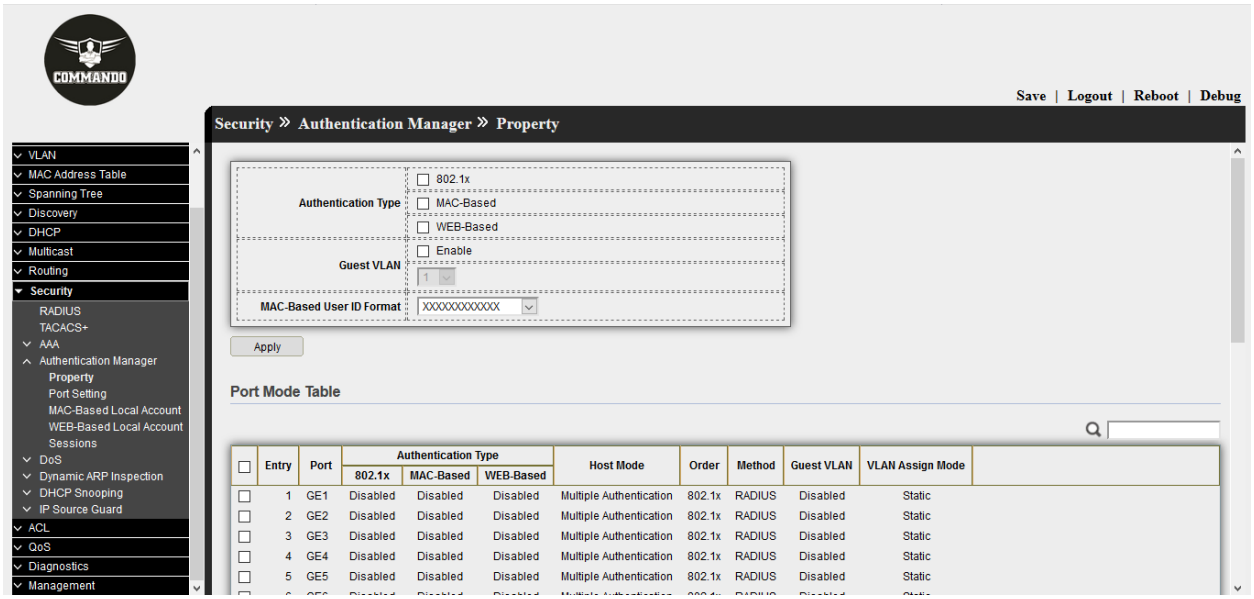


Fig 12.4.1 Default Authentication Manager Port Mode Table page

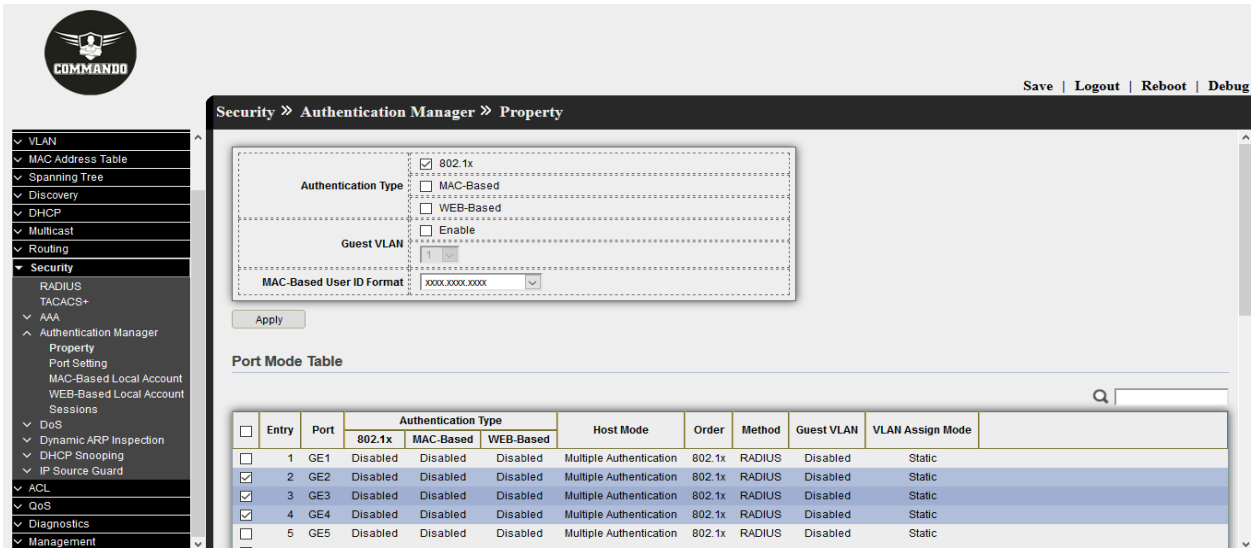


Fig 12.4.2 Authentication Manager Selecting Ports page

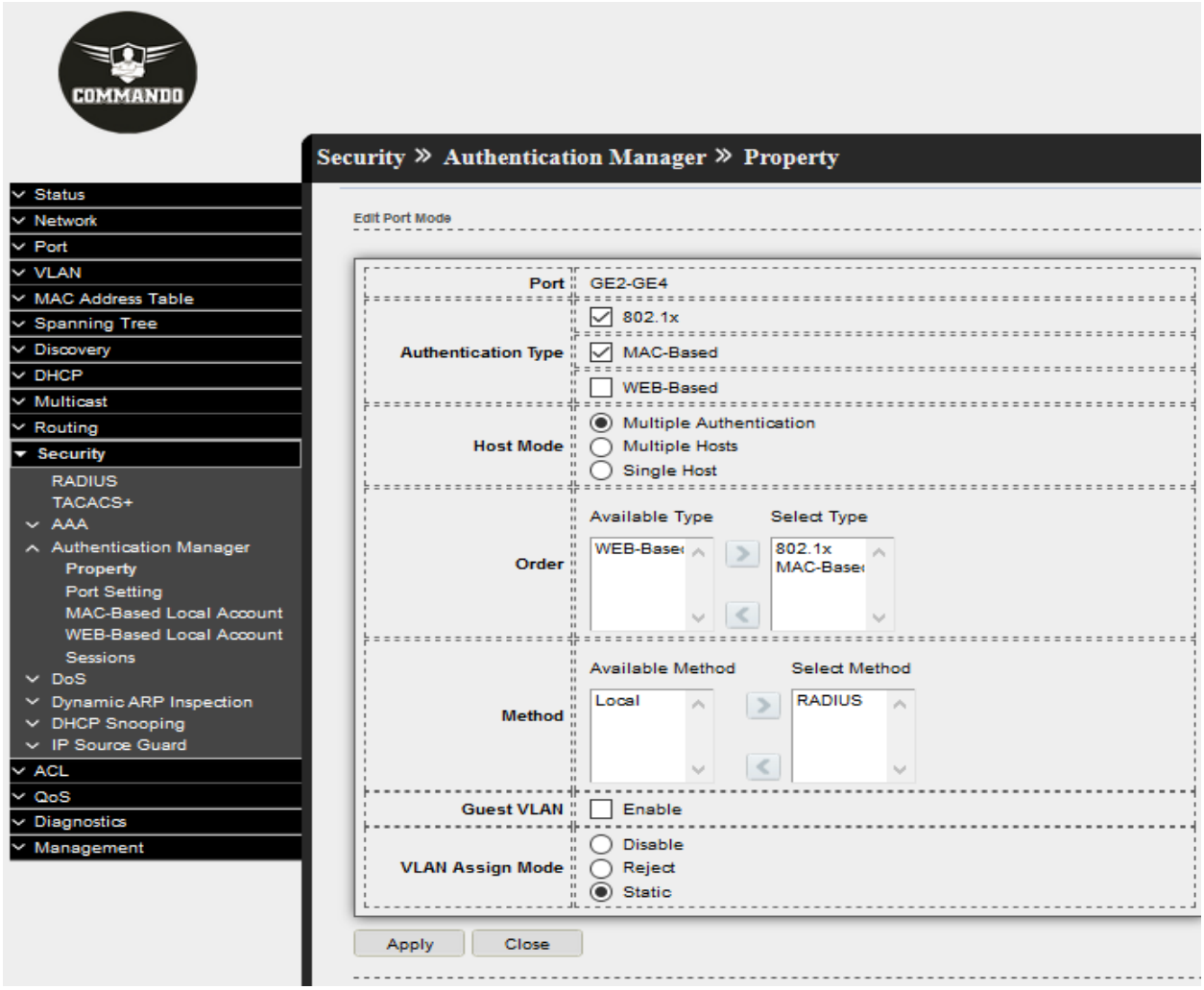


Fig 12.4.3 Authentication Manager Property edit page

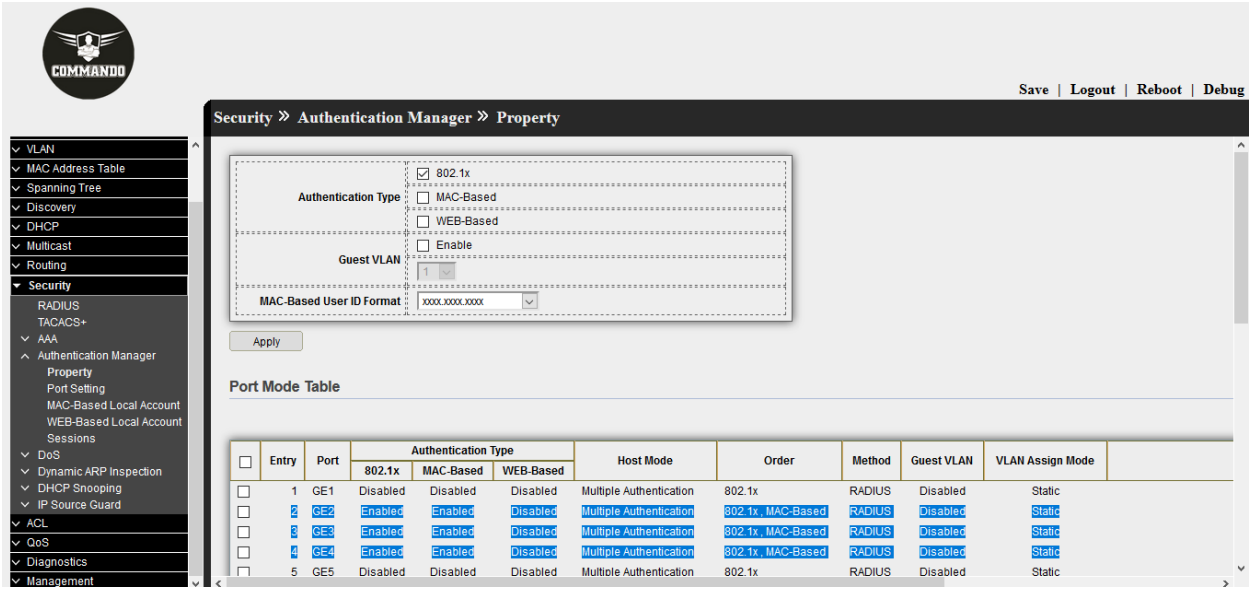


Fig 12.4.4 Authentication Manager Property Port Mode Table page

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 authentications is in process, only 802.1X traffic and control traffic can transit the network.

To view and configure the Authentication Manager Port Setting, click **Security >> Authentication Manager >> Port Setting.**

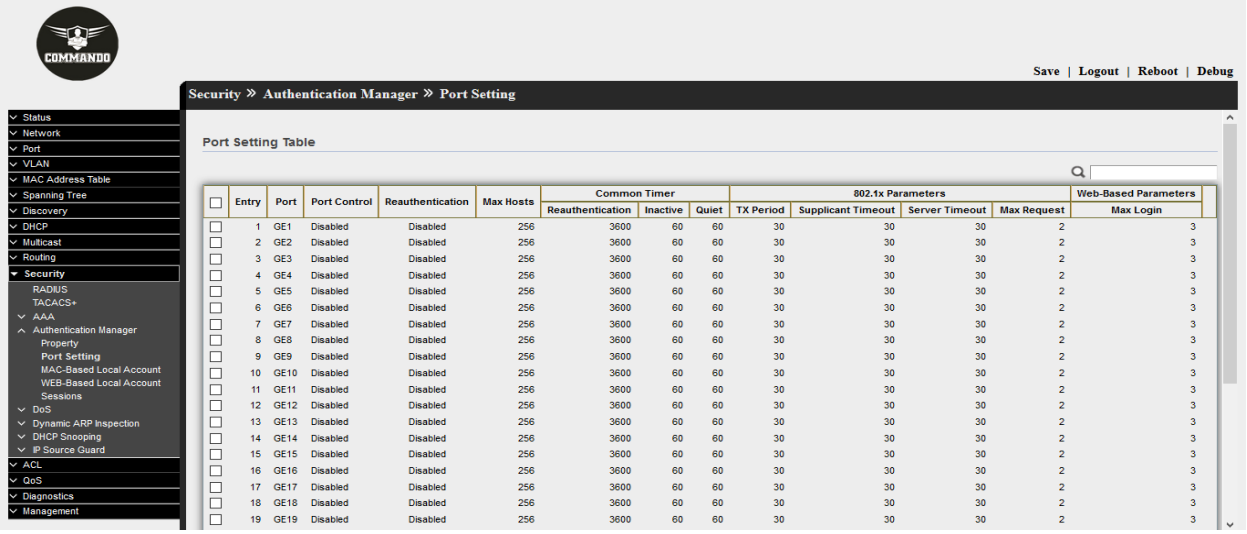


Fig 12.4.5 Authentication Manager Property Port Mode Table page

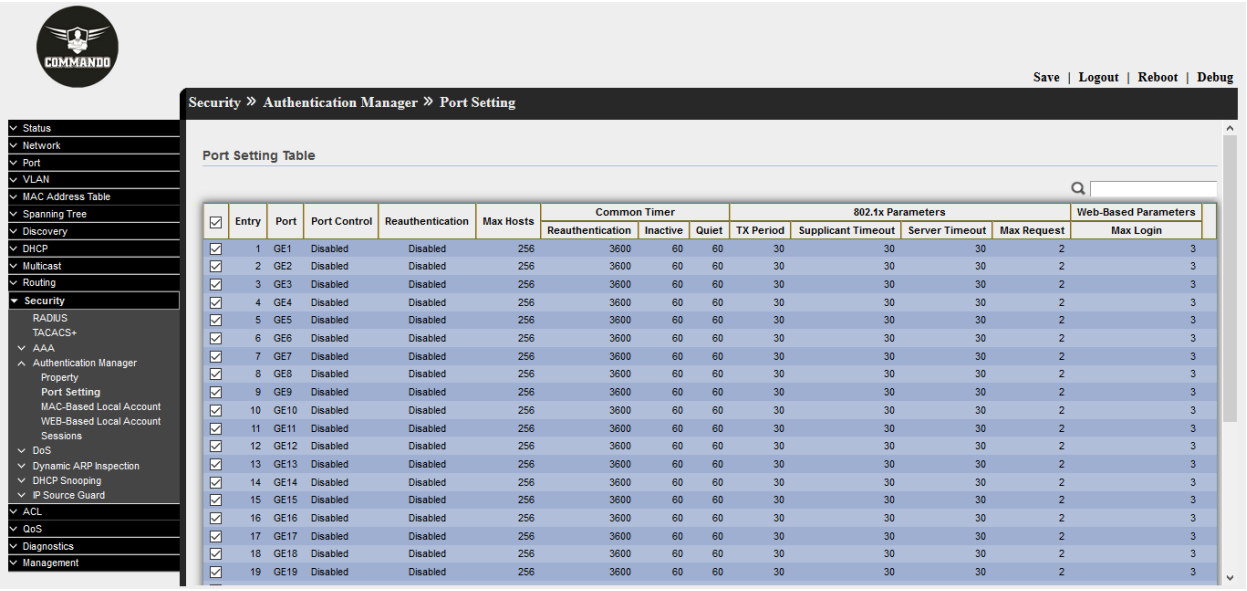


Fig 12.4.6 Authentication Manager Property Selecting Port page

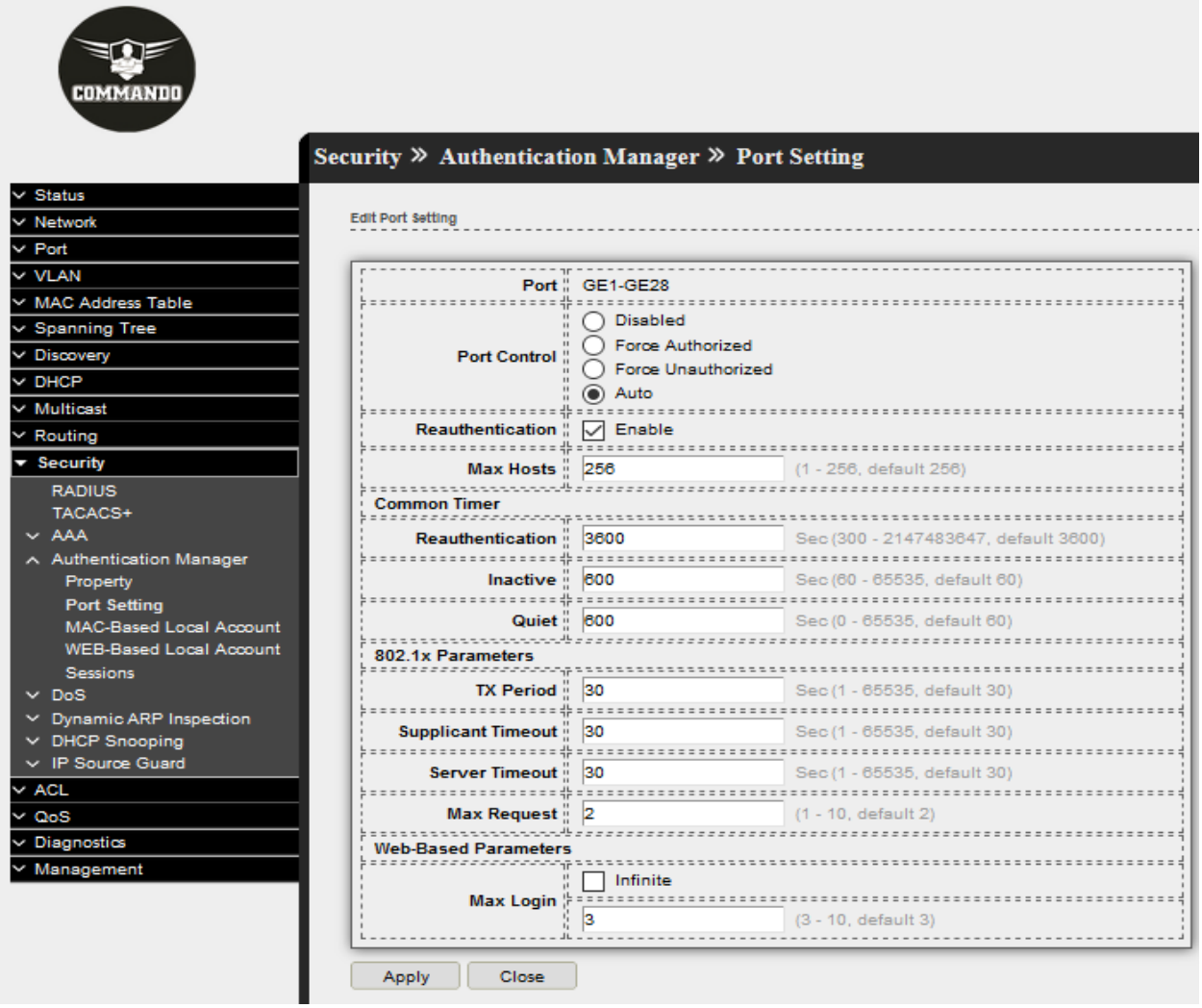


Fig 12.4.7 Authentication Manager Property edit port setting page

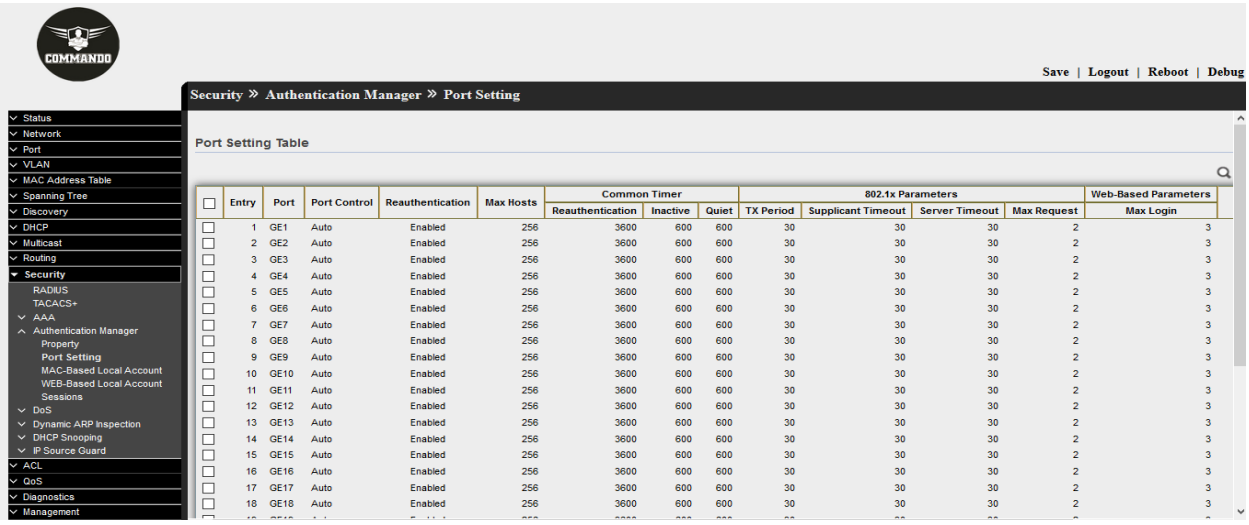


Fig 12.4.8 Authentication Manager Port setting table page

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”.

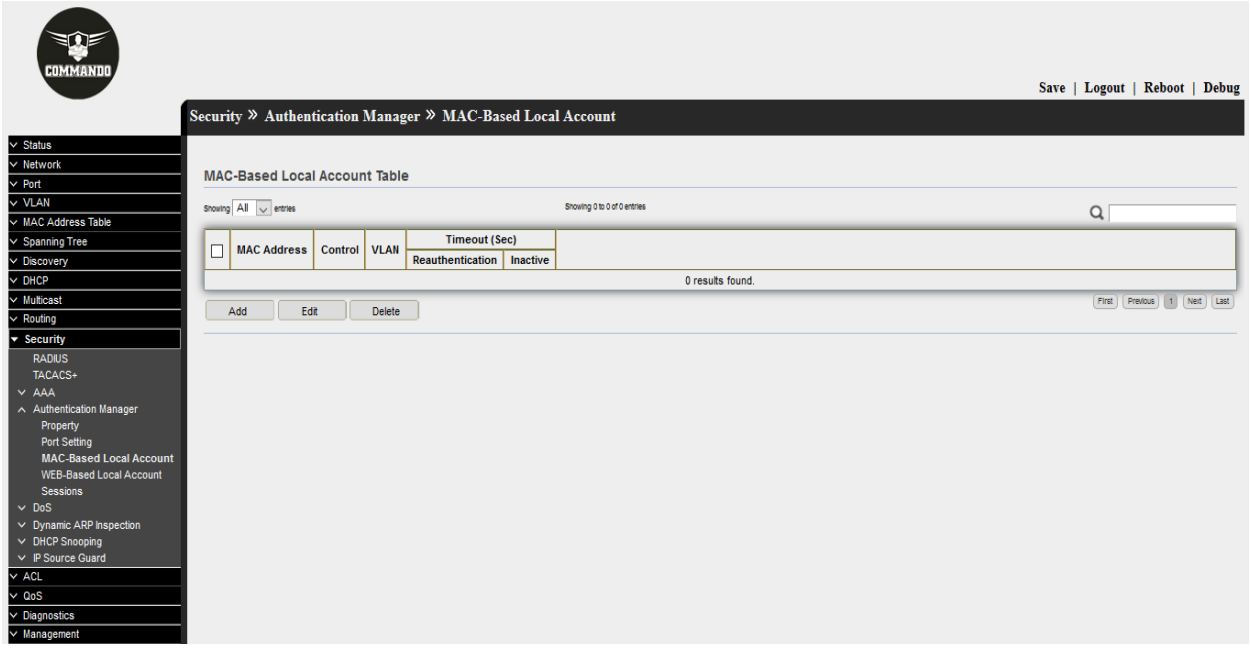


Fig 12.4.9 Authentication Manager Default MAC -Based Local Account page

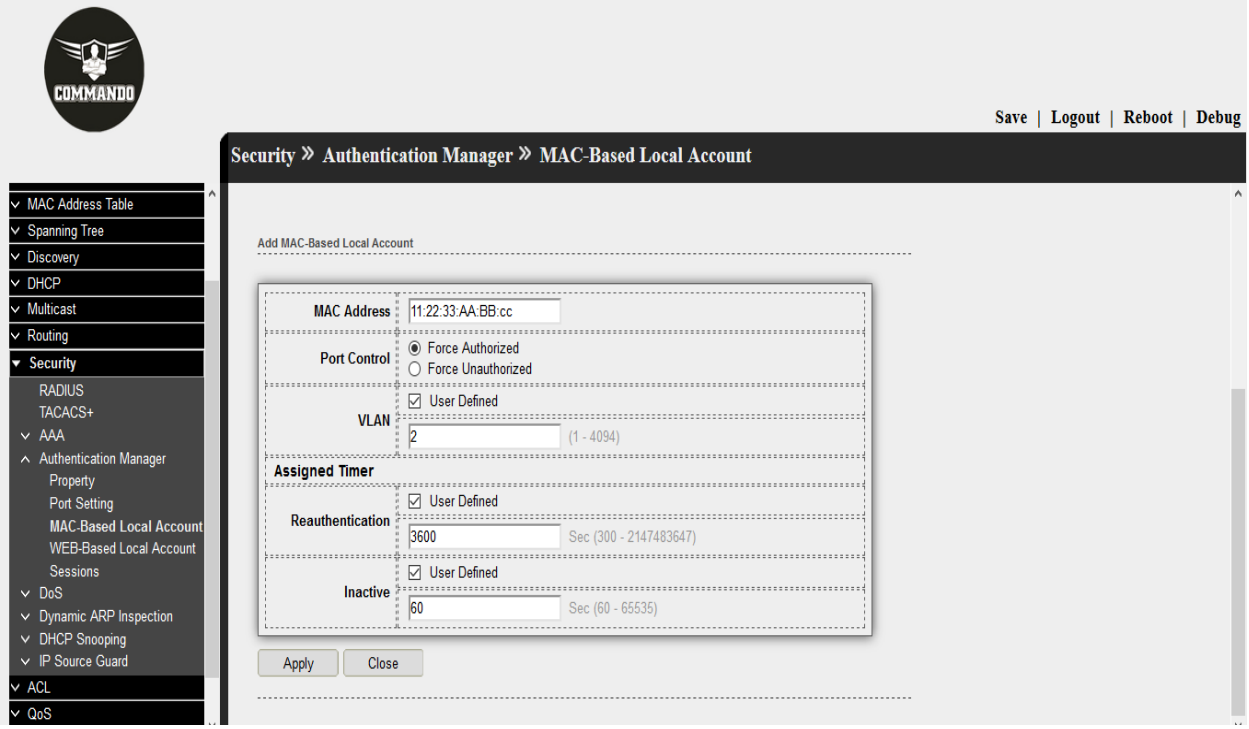


Fig 12.4.10 Authentication Manager MAC -Based user defined Local Account page

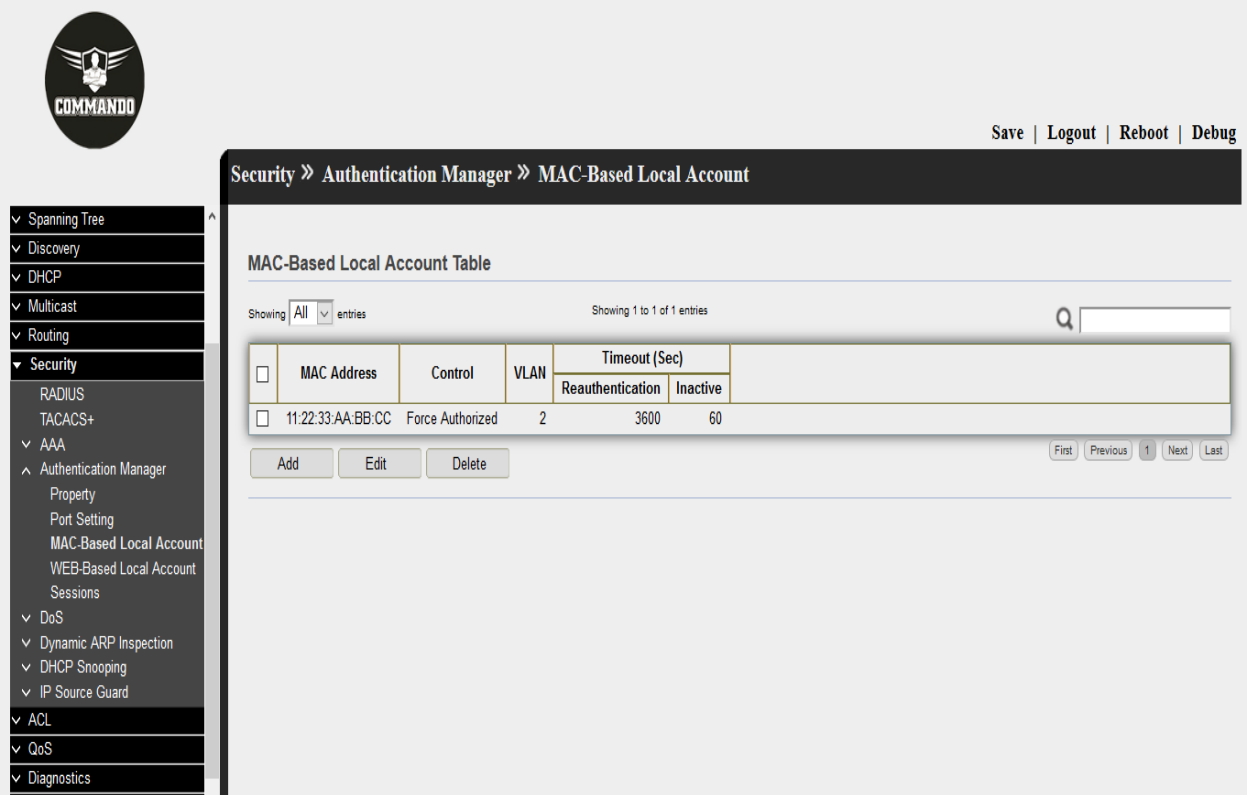


Fig 12.4.11 MAC -Based user defined Local Account Table page

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.**

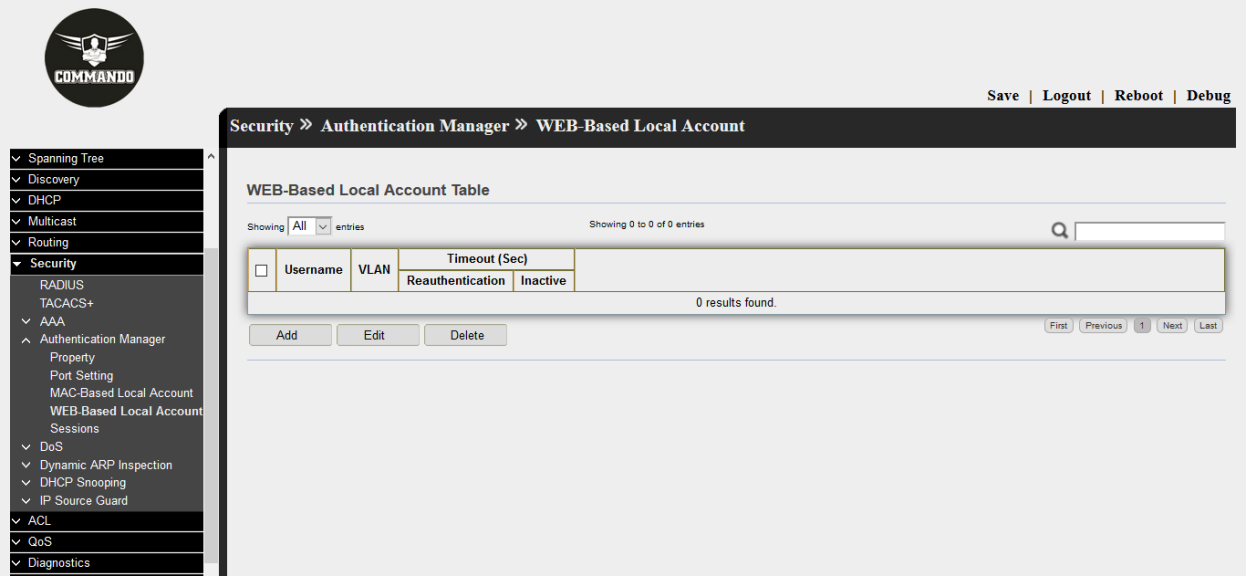


Fig 12.4.12 Default WEB-Based Local Account Table page

WEB-Based Configuration:

Click on “Security”, then “Authentication Manager” >> ” WEB-Based Local Account” from menu. Click on “Add” & enter “Username”, “Password”& “VLAN” ID.

Next enter Assigned Timer parameters like “Reauthentication”, “Inactive”” value. &Click on “Apply”.

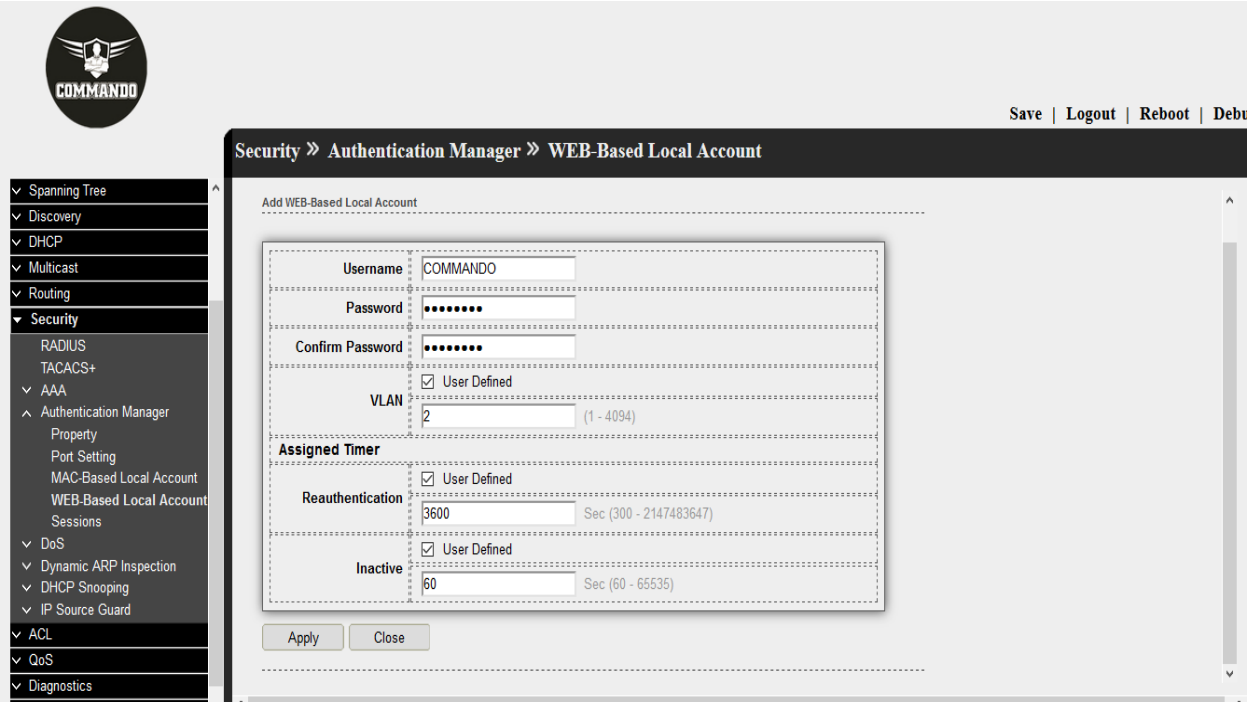


Fig 12.4.13 Add WEB-Based Local Account page

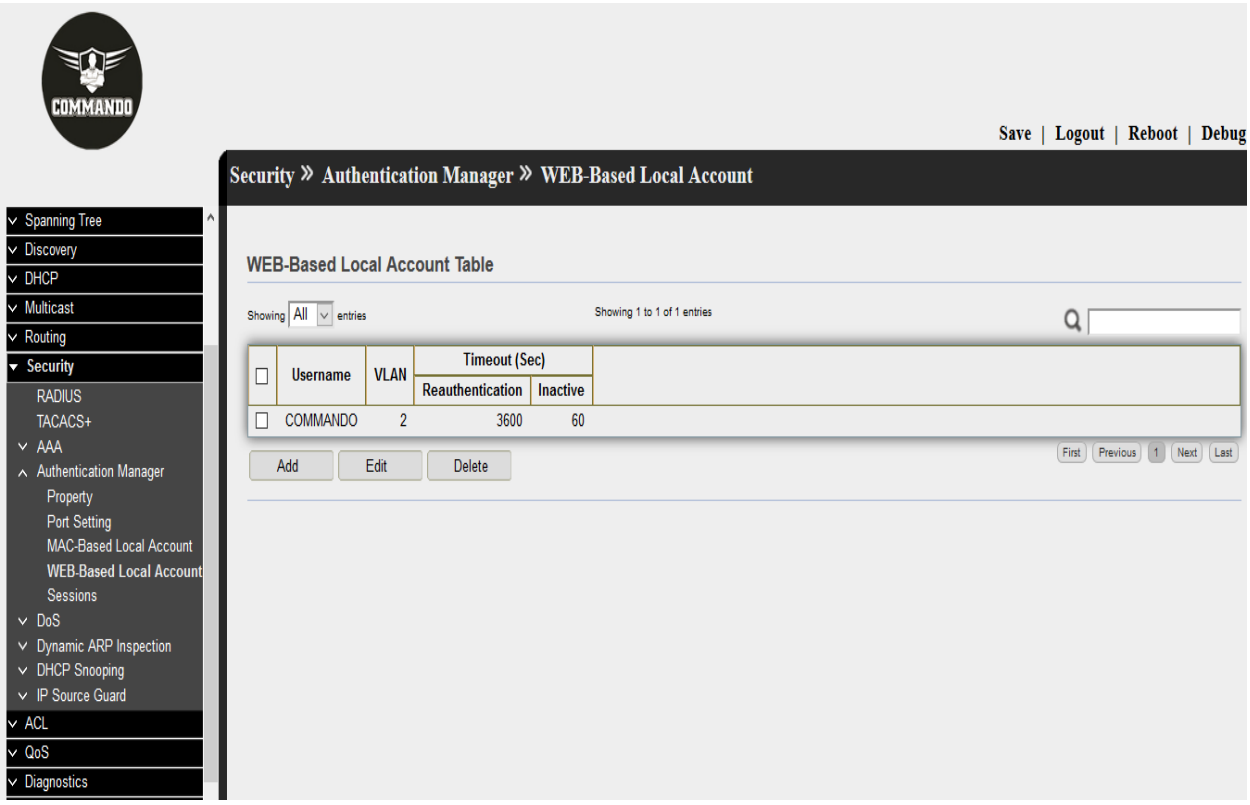


Fig 12.4.14 WEB-Based Local Account table page

12.4.5 Sessions

This page show 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.**

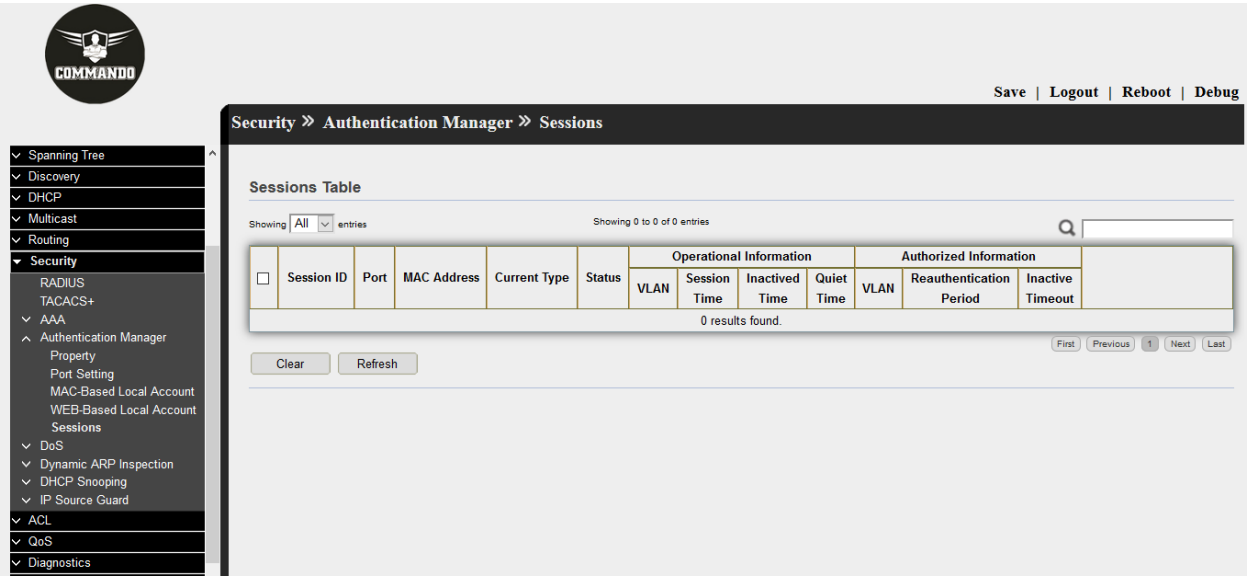


Fig 12.4.15 Authentication Manager Sessions Table page

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.**

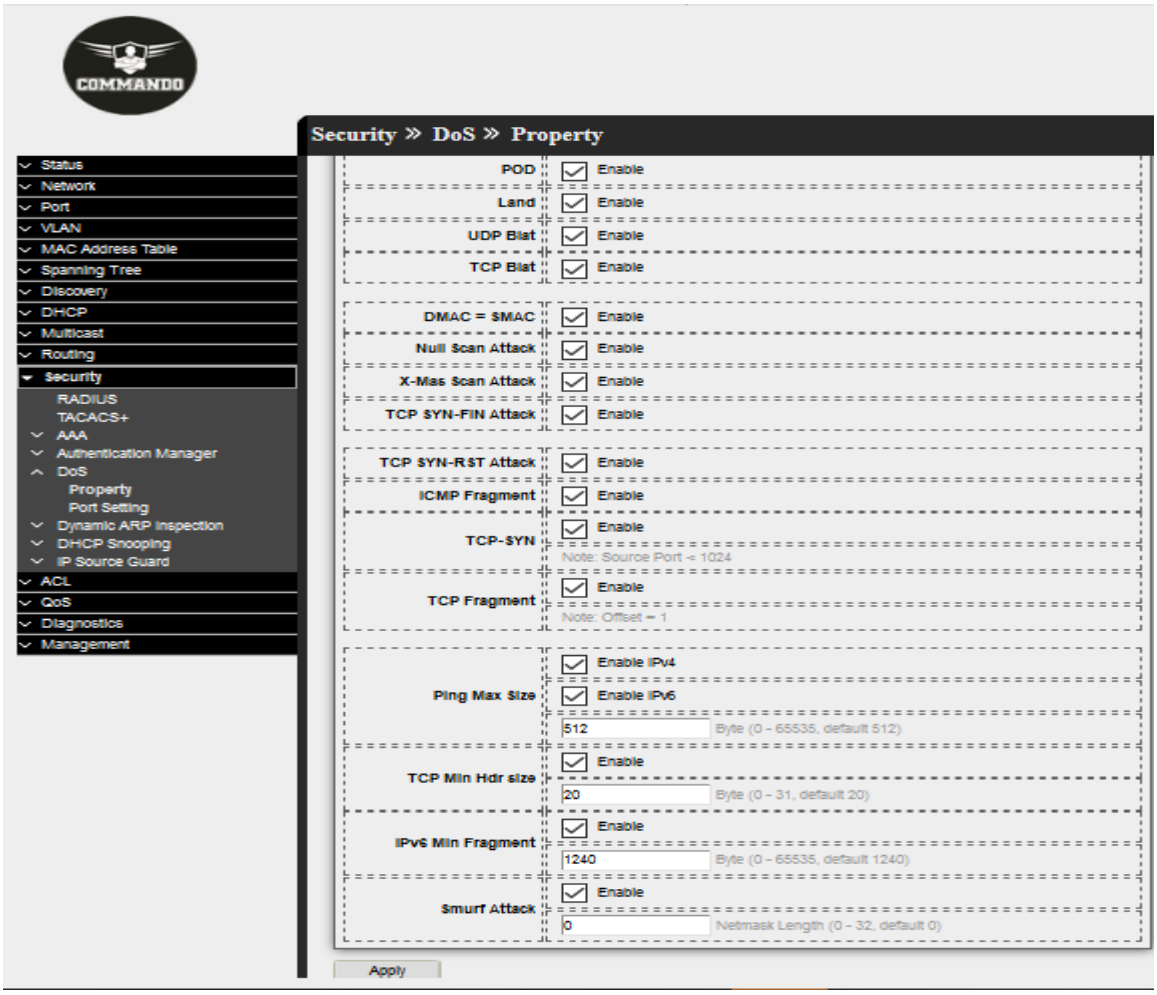


Fig 12.5.1 DoS property page

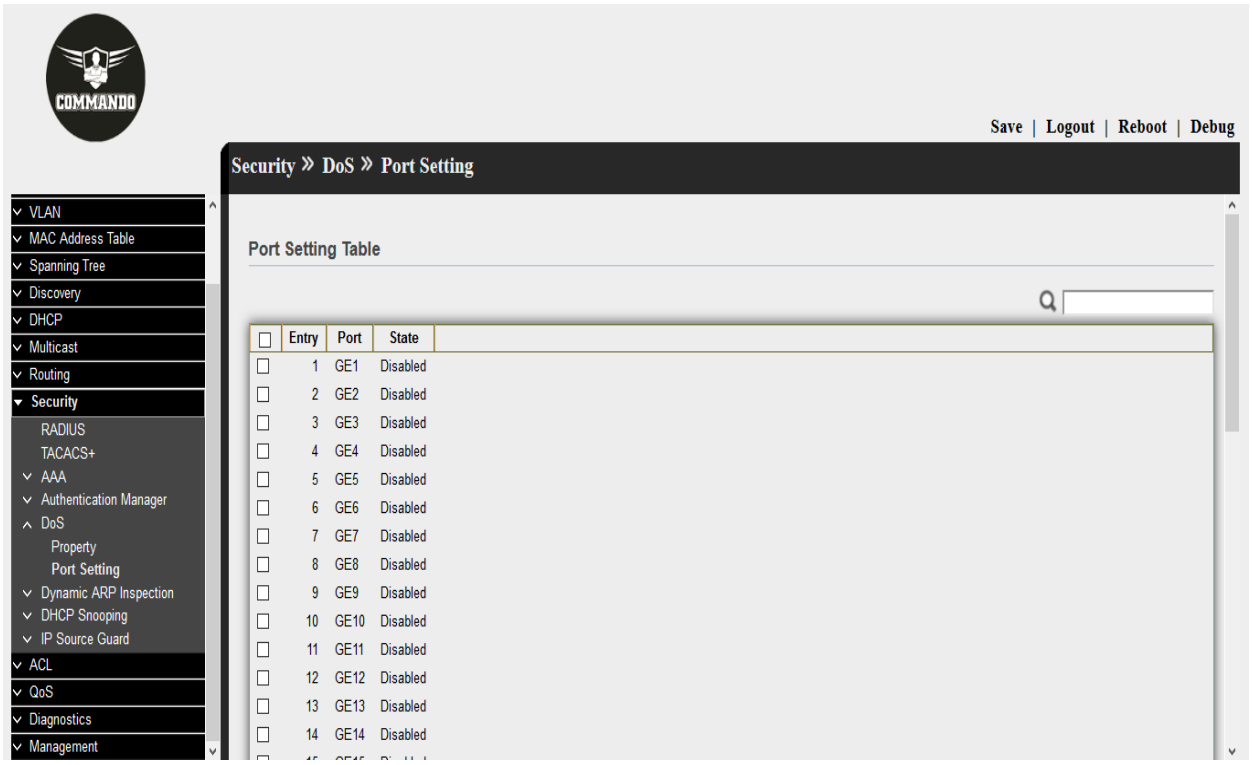


Fig 12.5.2 Default DoS Port Setting page

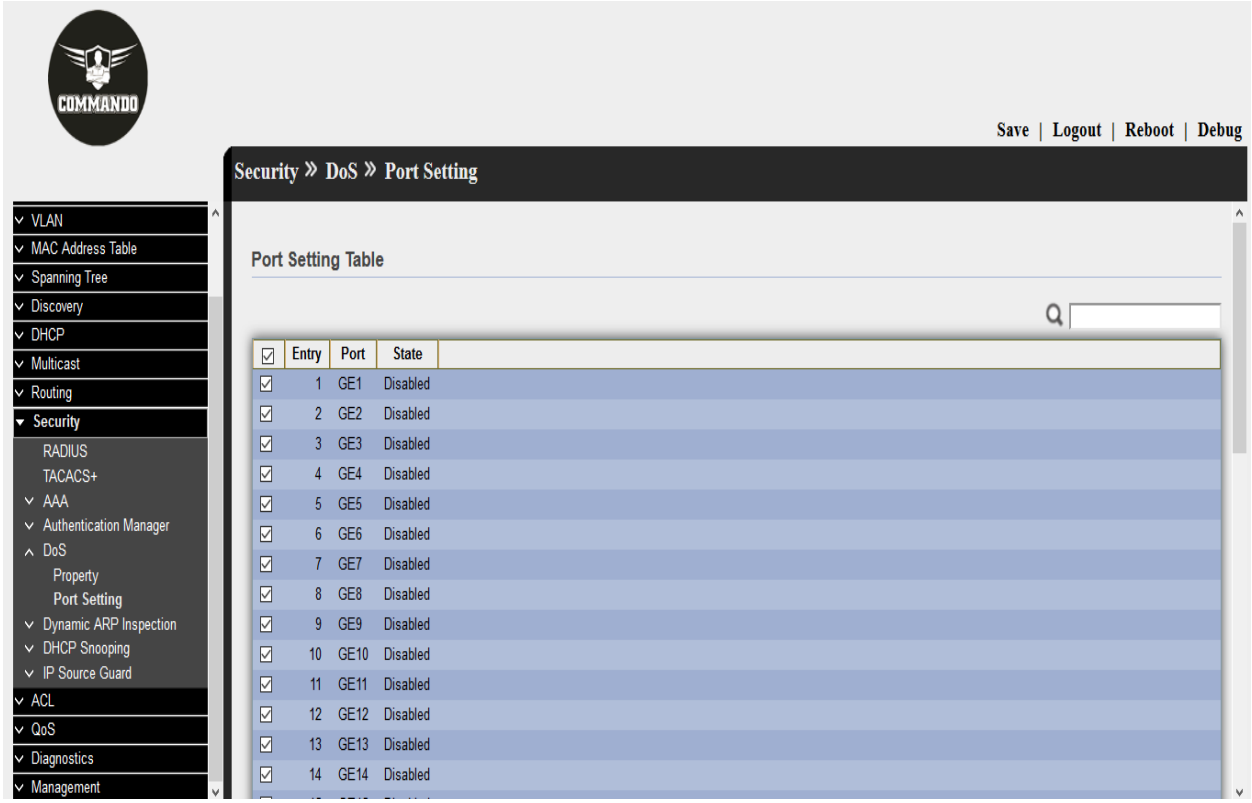


Fig 12.5.3 Selecting Port DoS Setting page

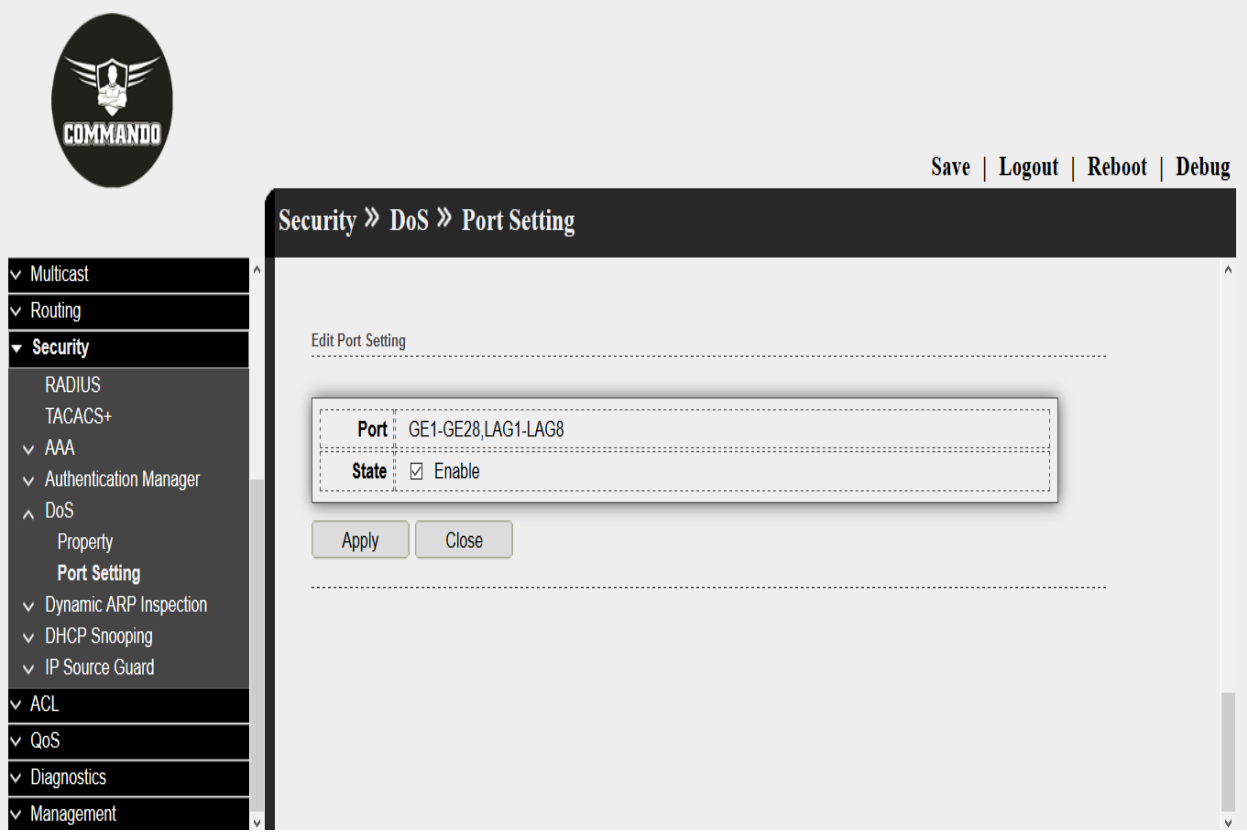


Fig 12.5.4 DoS Port Setting Table after enableing all ports page

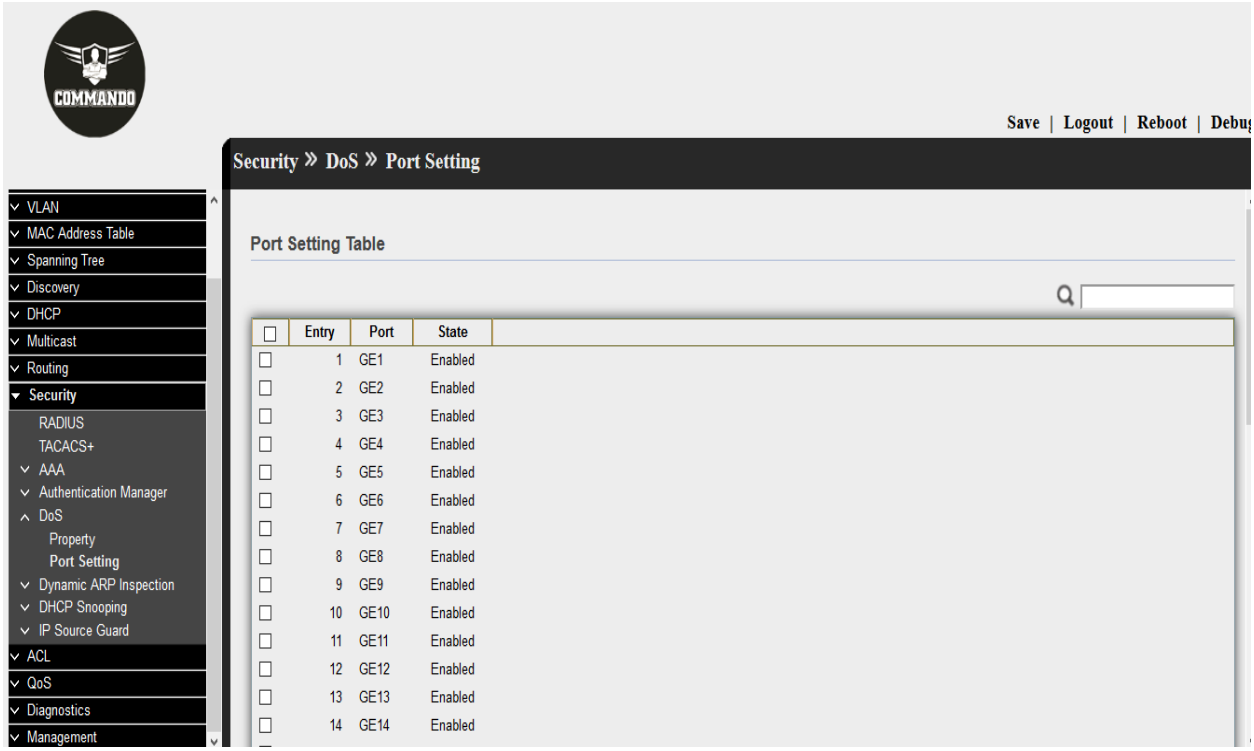


Fig 12.5.5 DoS Port Setting Table after enableing all ports page

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.

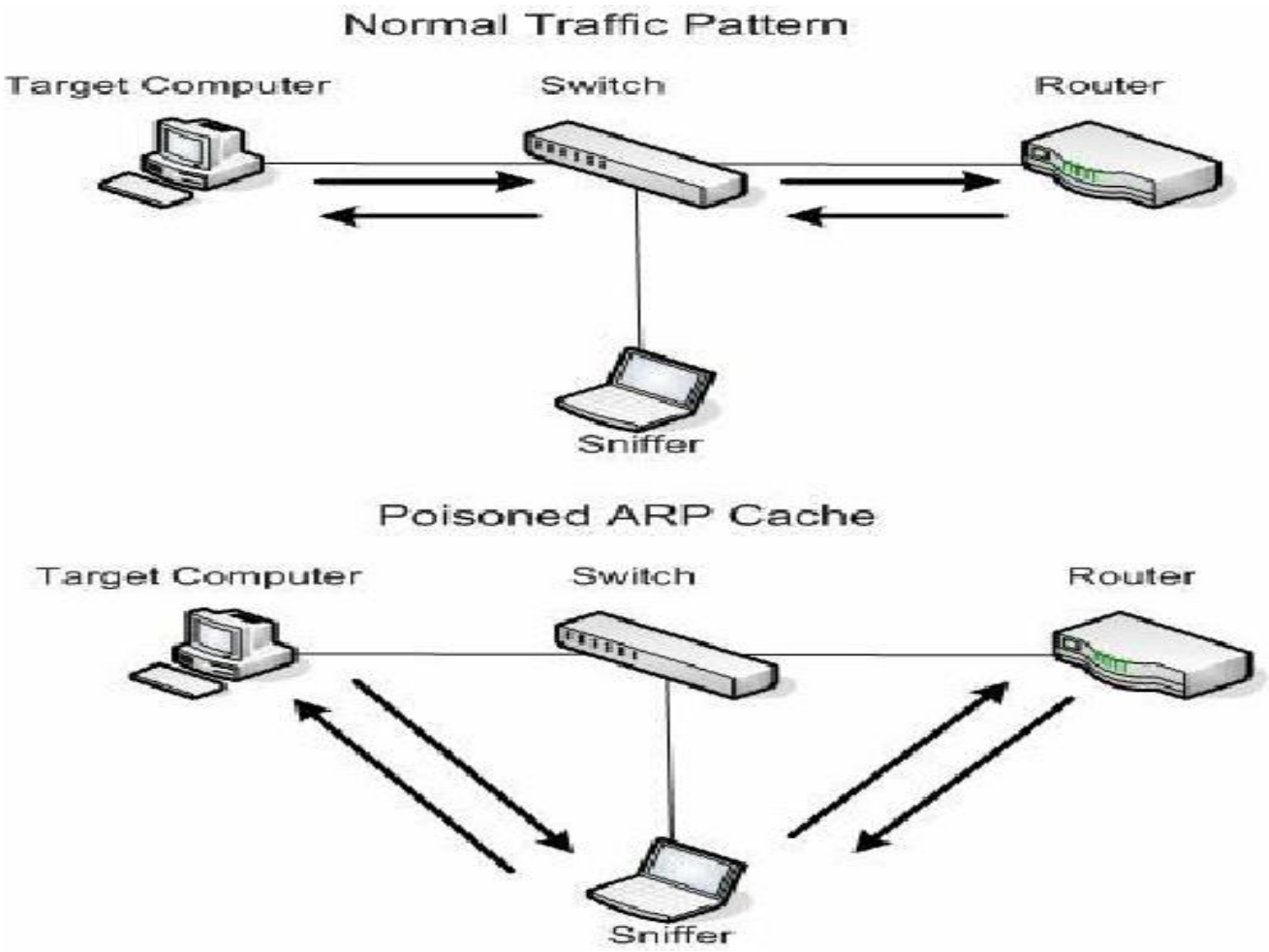


Fig 12.6.1 Dynamic ARP Inspection (DAI) Poisoned ARP Cache Concept

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.**

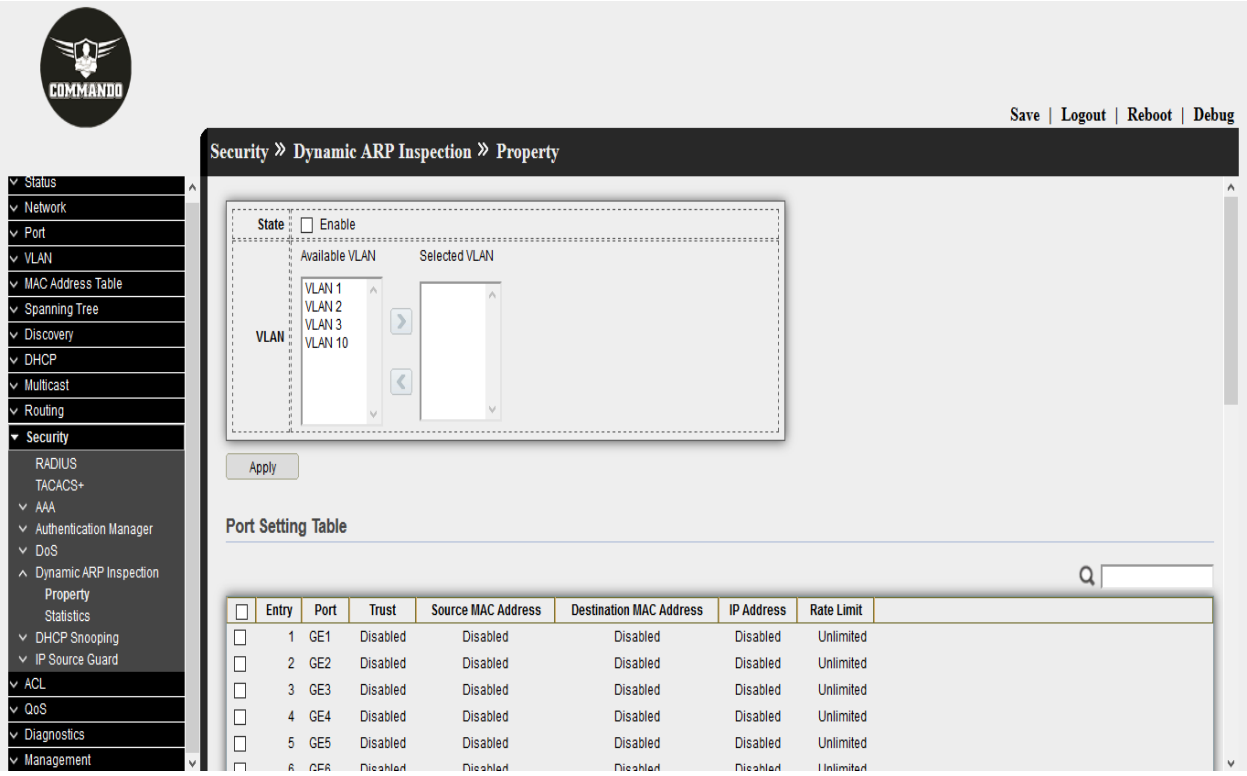


Fig 12.6.2 Dynamic ARP Inspection (DAI) port setting table page

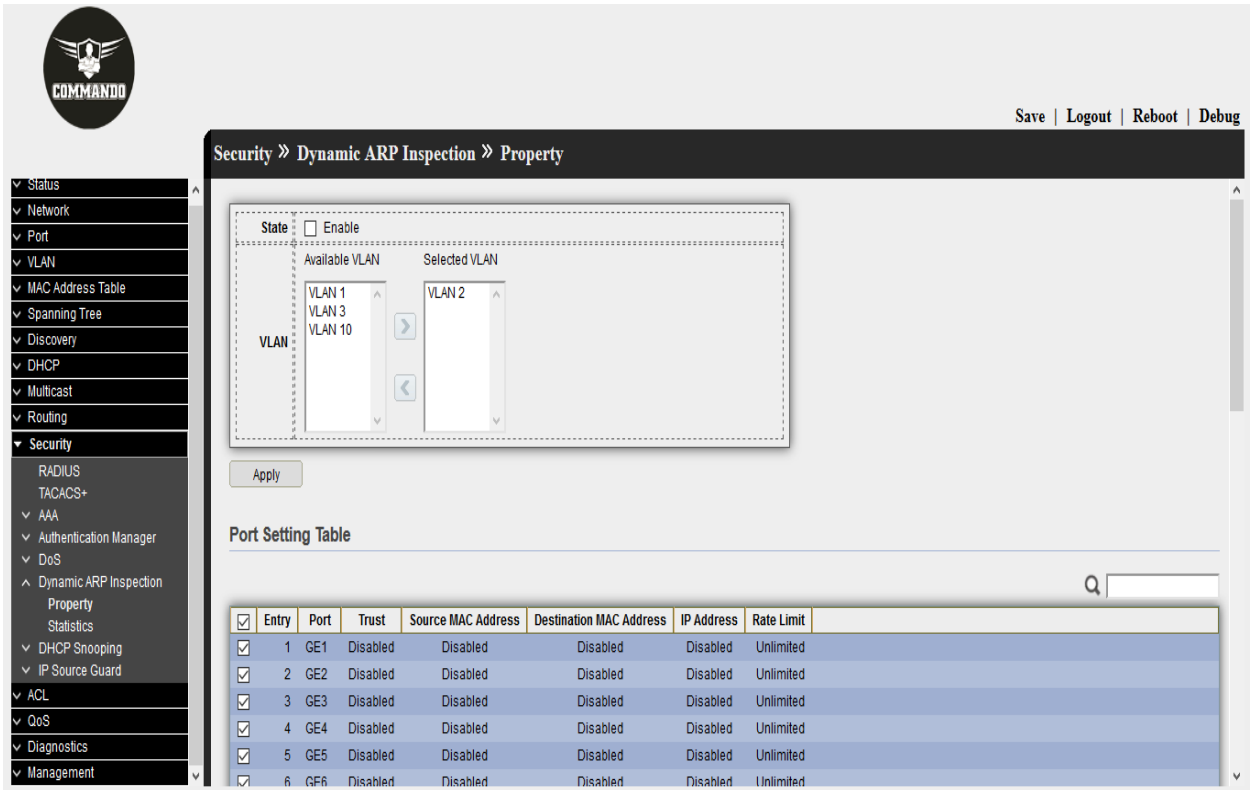


Fig 12.6.3 Dynamic ARP Inspection (DAI) port selection page

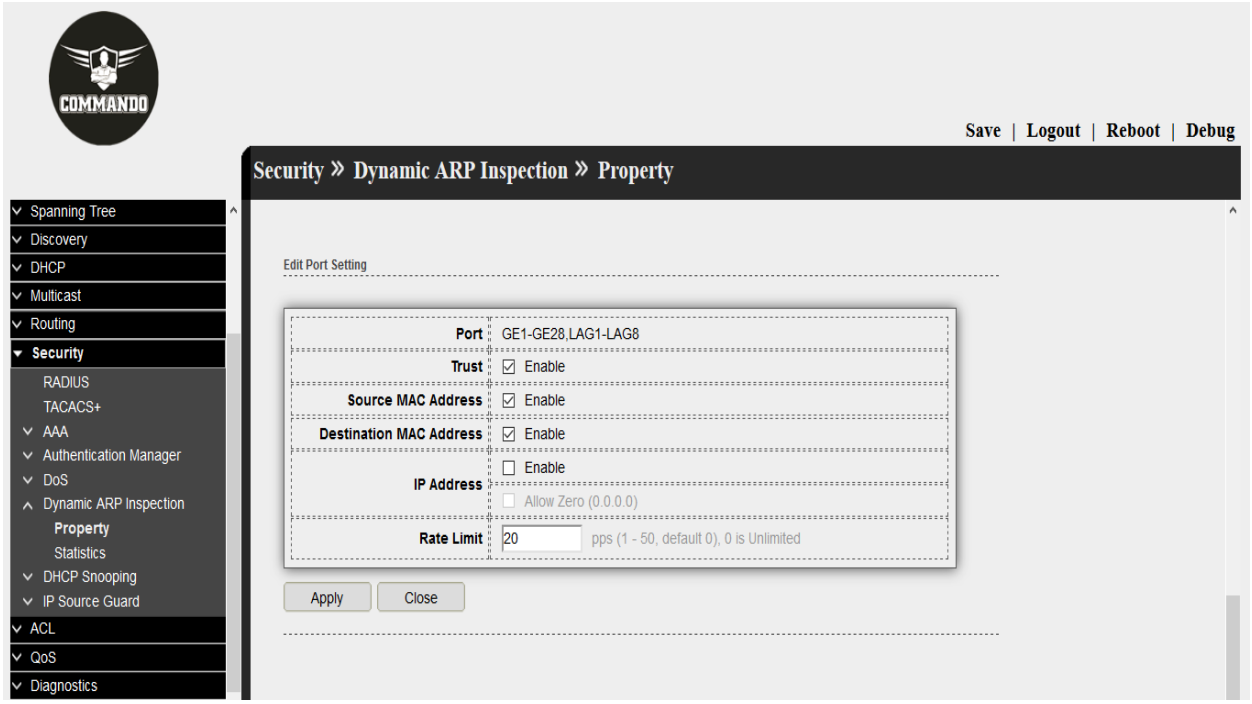


Fig 12.6.4 Dynamic ARP Inspection (DAI) Edit Port Setting page

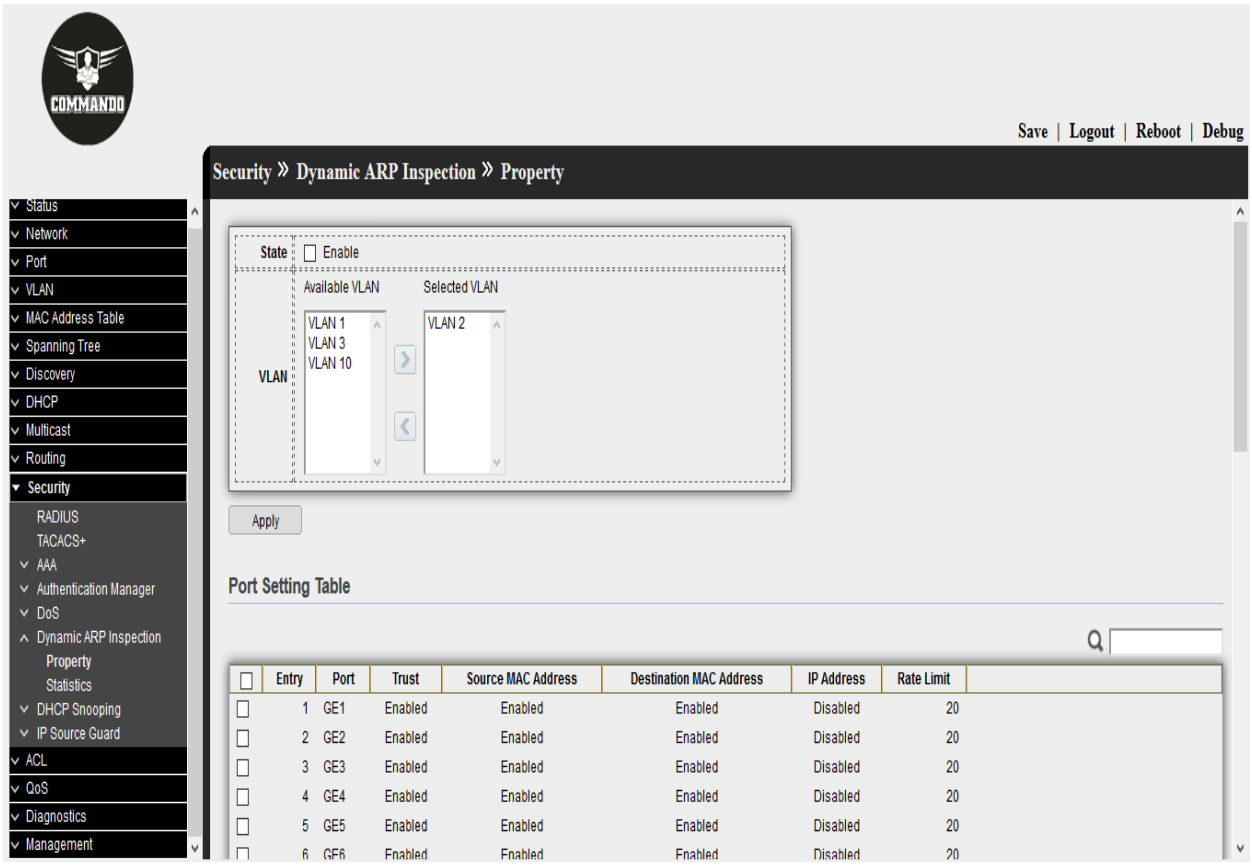


Fig 12.6.5 DAI Port Setting Table page after enabling ports page

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.**

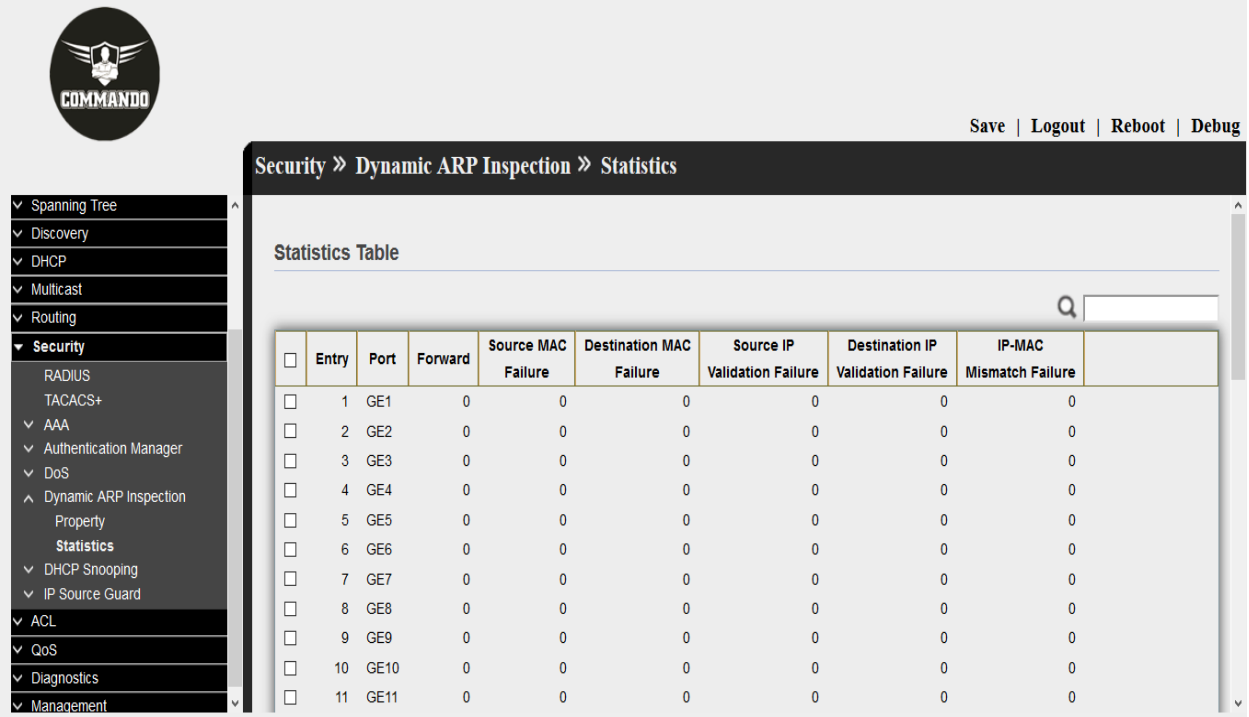


Fig 12.6.7 Dynamic ARP Inspection (DAI) Statistics Table page

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.

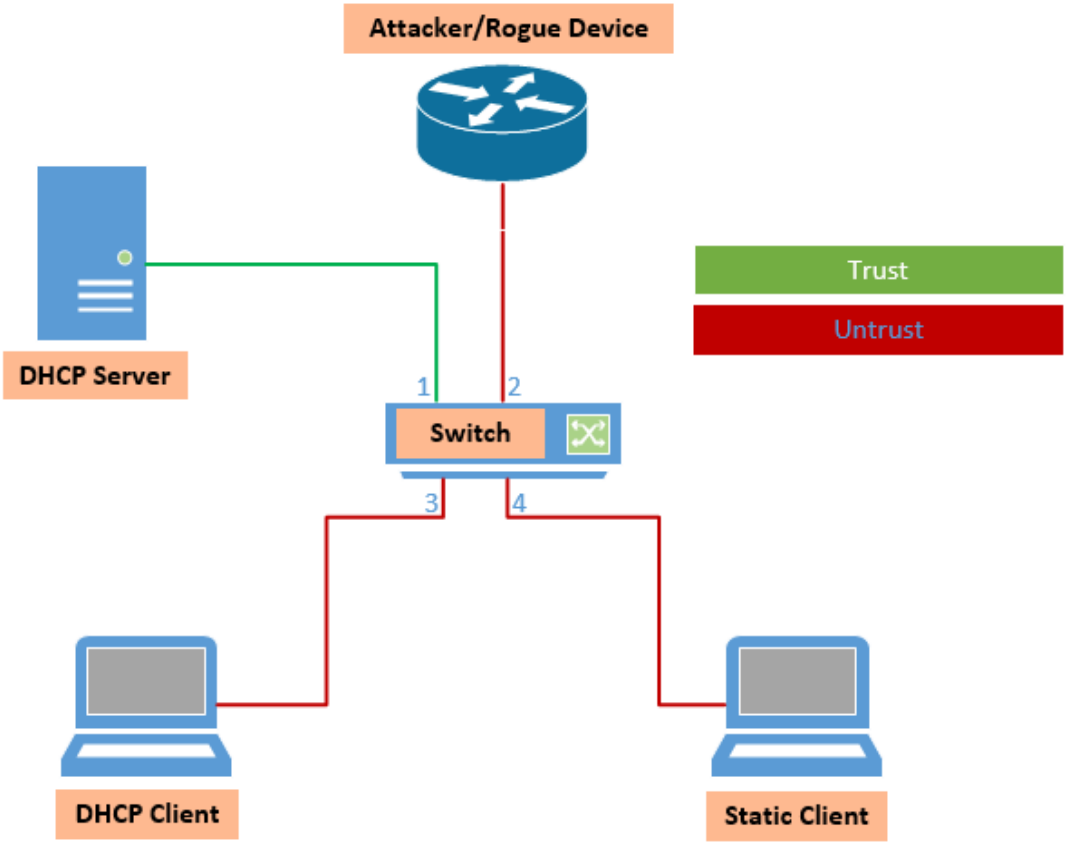


Fig 12.7.1 DHCP Snooping Concept

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.**

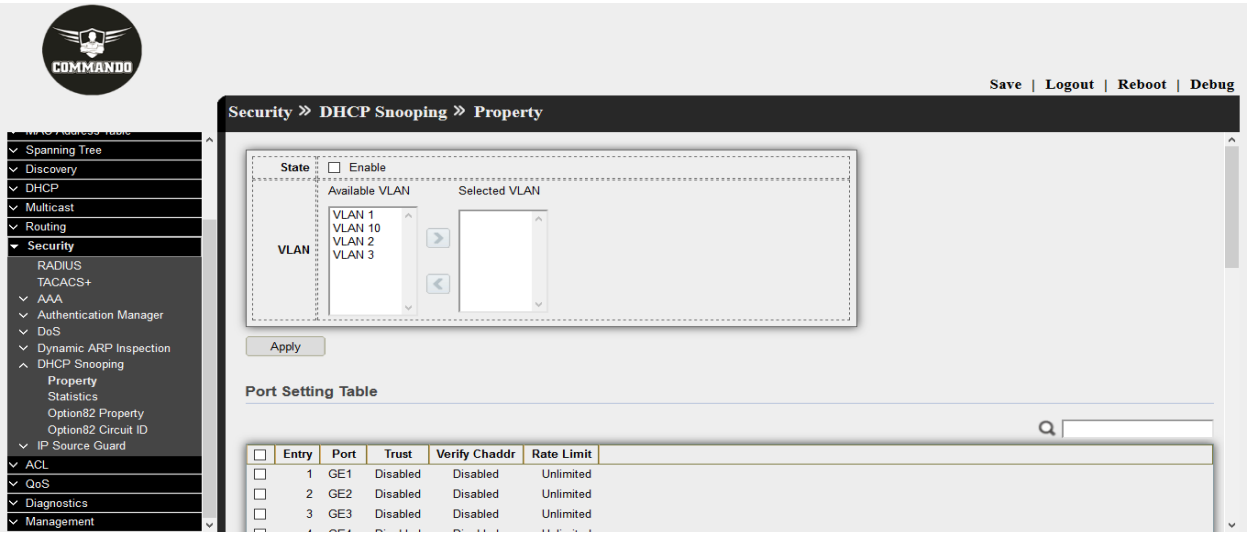


Fig 12.8.1 Default DHCP Snooping Port setting Table page

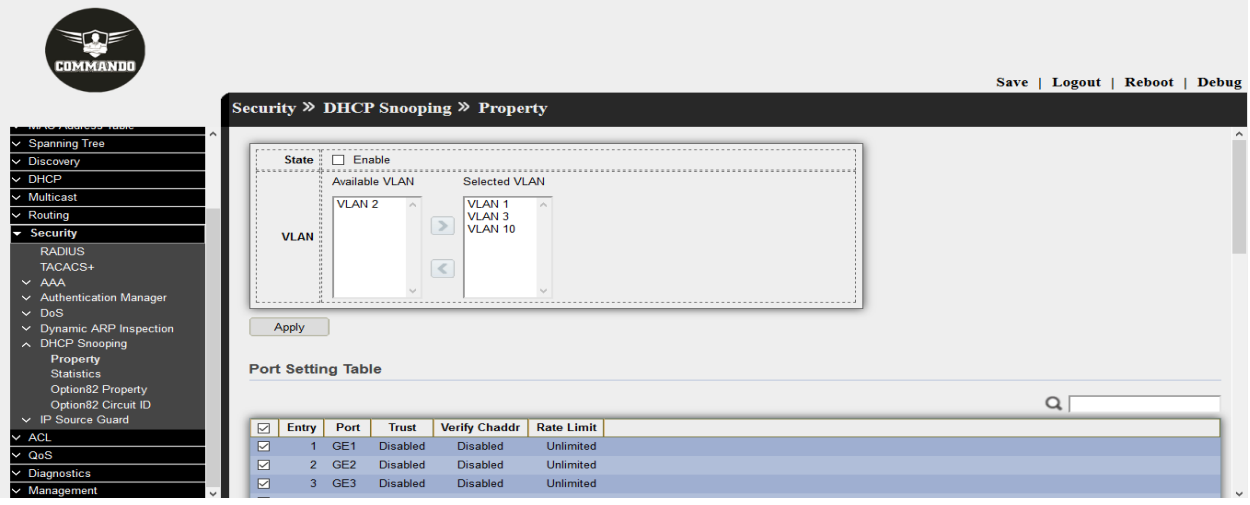


Fig 12.8.2 DHCP Snooping for selected Port setting page

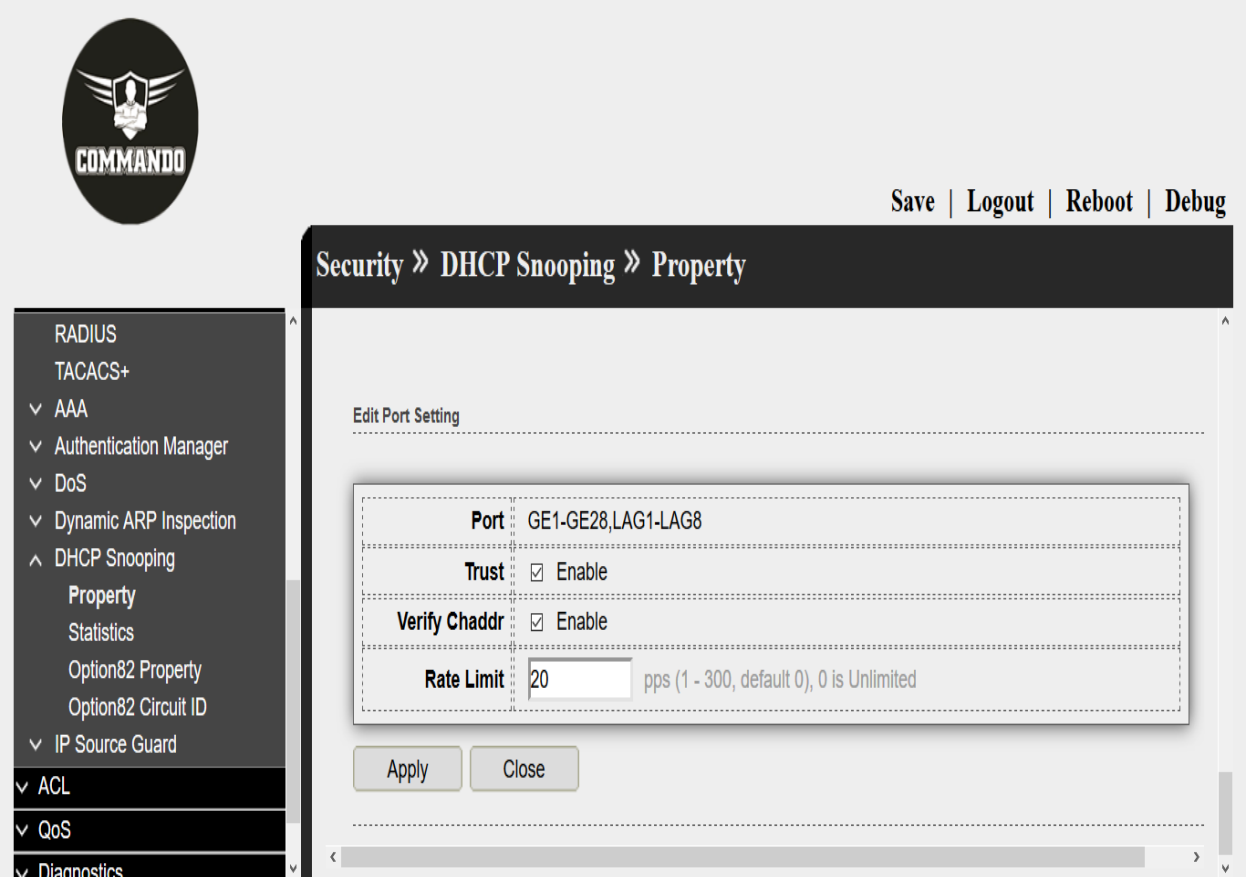


Fig 12.8.3 Created VLAN DHCP Snooping State page

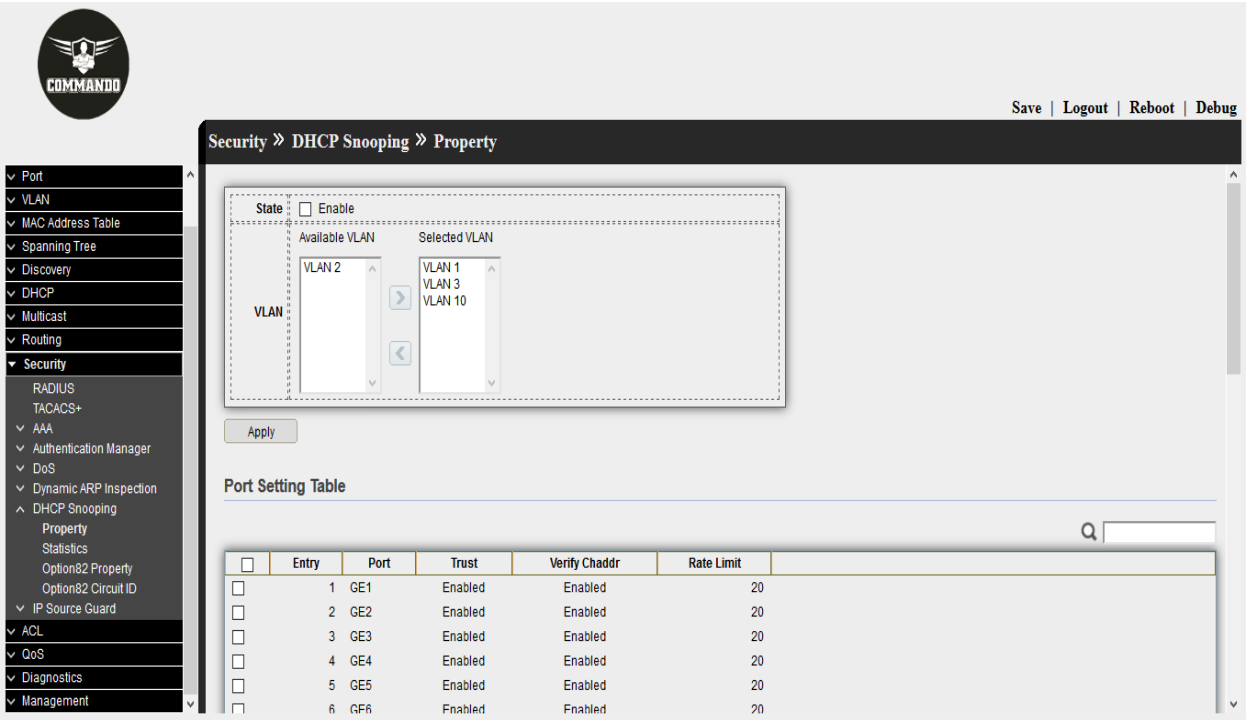


Fig 12.8.4 DHCP Snooping Port setting Table After Enabling Ports page

12.8.2 Statistics

This page allow user to browse all statistics that recorded by DHCP snooping function. Display information about trusted ports and also display dhcp snooping trust.
To view the DHCP Snooping Statistics ,click **Security >> DHCP Snooping >> Statistics.**

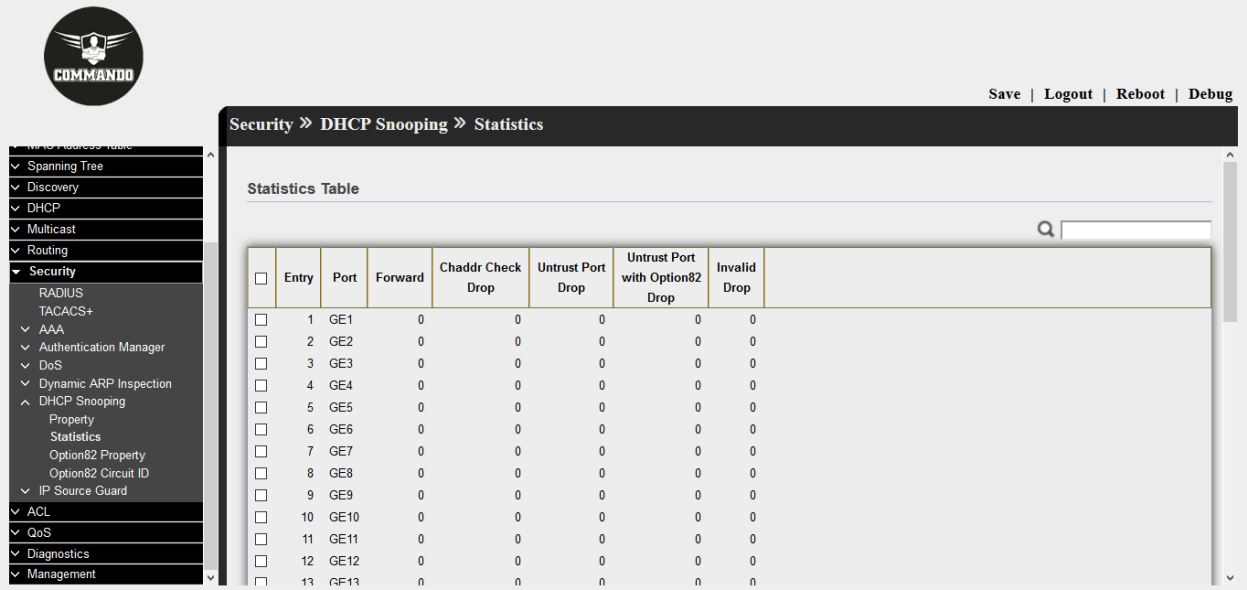


Fig 12.8.5 DHCP Snooping statistics Table page

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.**

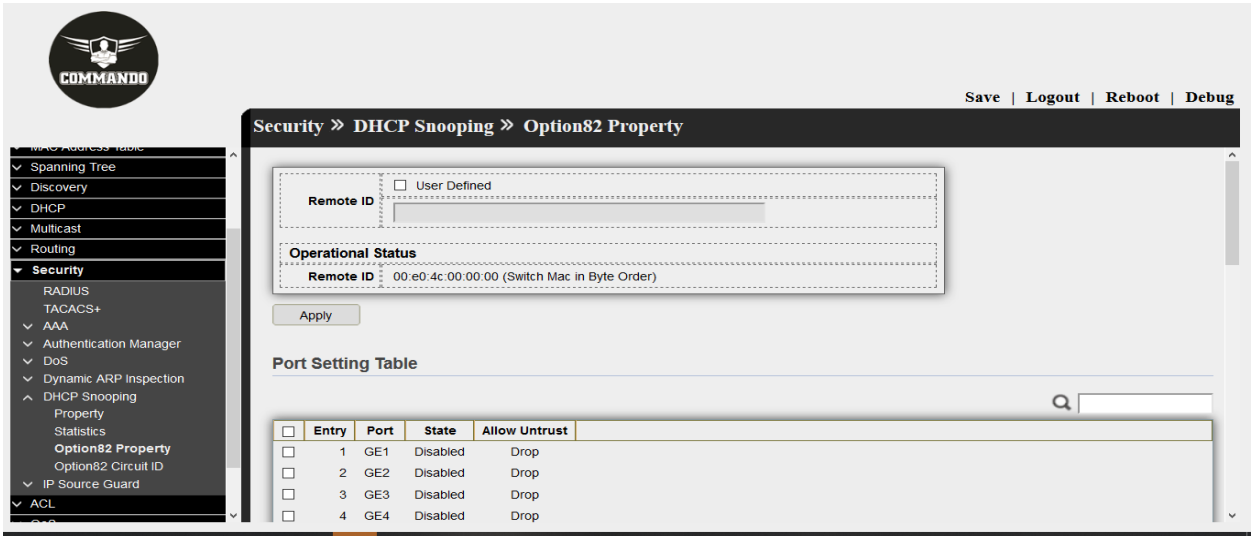


Fig 12.8.6 Default DHCP Snooping Option82 Port setting table page

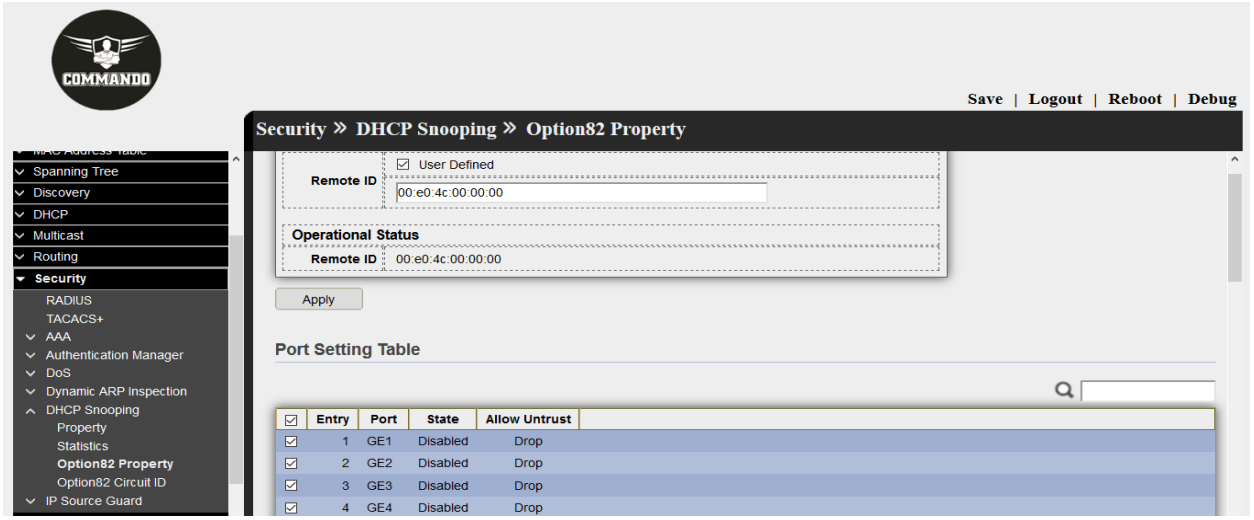


Fig 12.8.7 DHCP Snooping Option82 Port Selecting Ports page

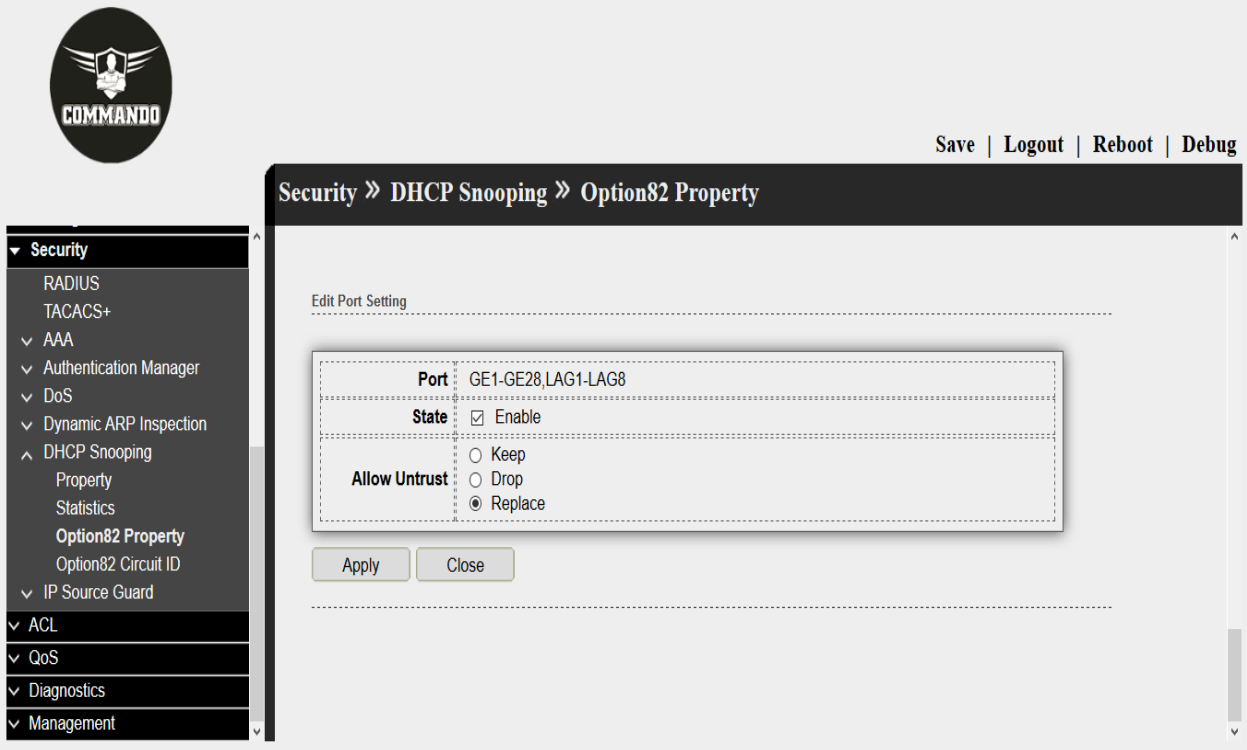


Fig 12.8.8 DHCP Snooping Option82 Edit Port Setting page

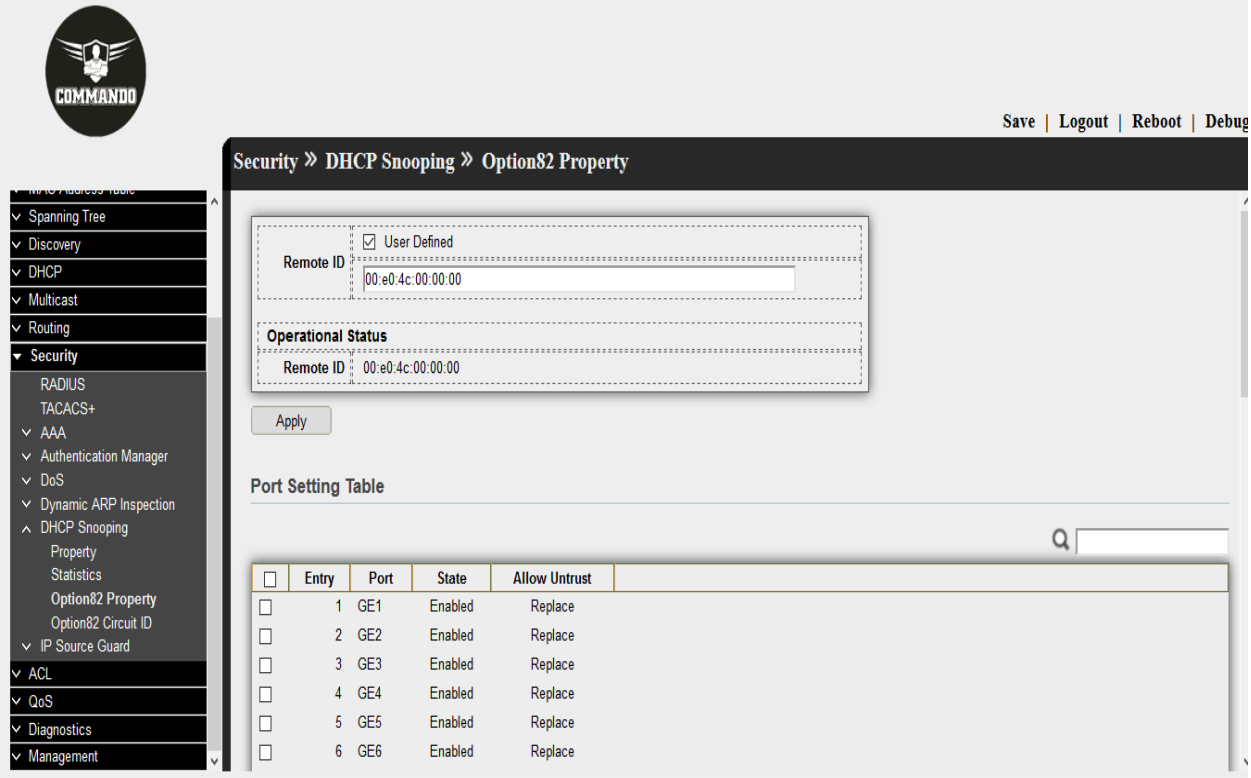


Fig 12.8.9 DHCP Snooping Option82 Edit Port Setting Table page after Enabling Ports page

12.8.4 Option82 Circuit ID

This page allow user to set string of DHCP option82 circuit ID filed. The string will attach in option82 if option inserted.

To view and configure DHCP Snooping Option82 Circuit ID , click **Security >> DHCP Snooping >> Option82 Circuit ID.**

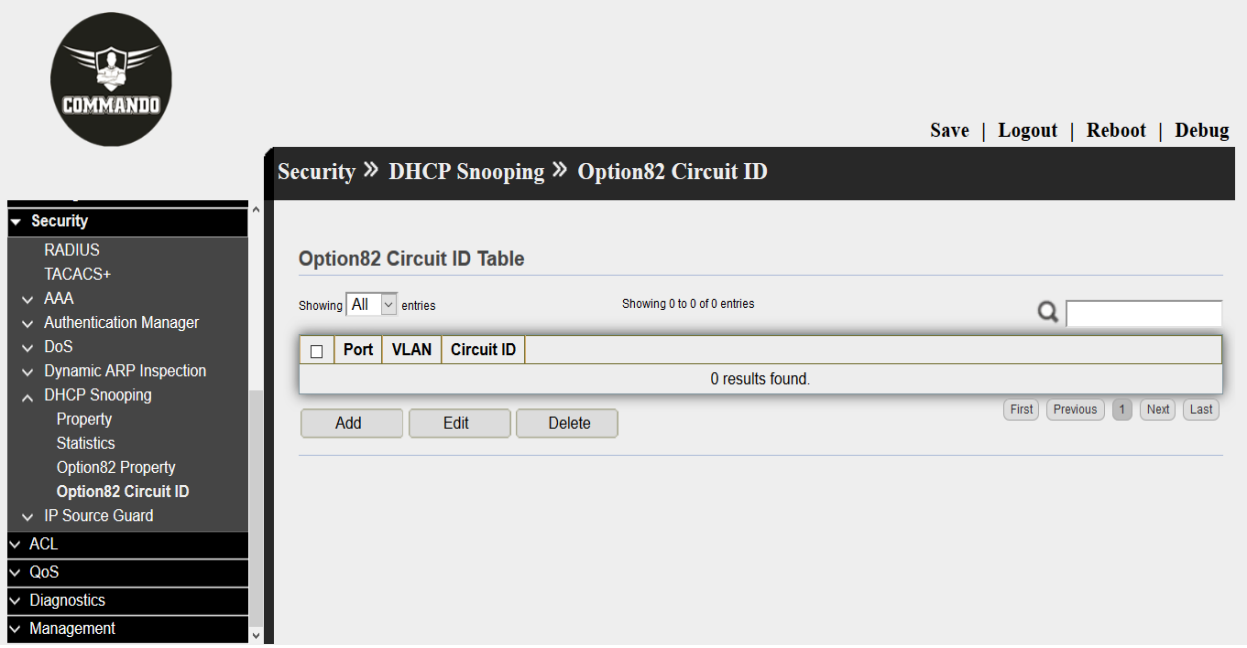


Fig 12.8.10 DHCP Snooping Option82 Circuit ID Table page

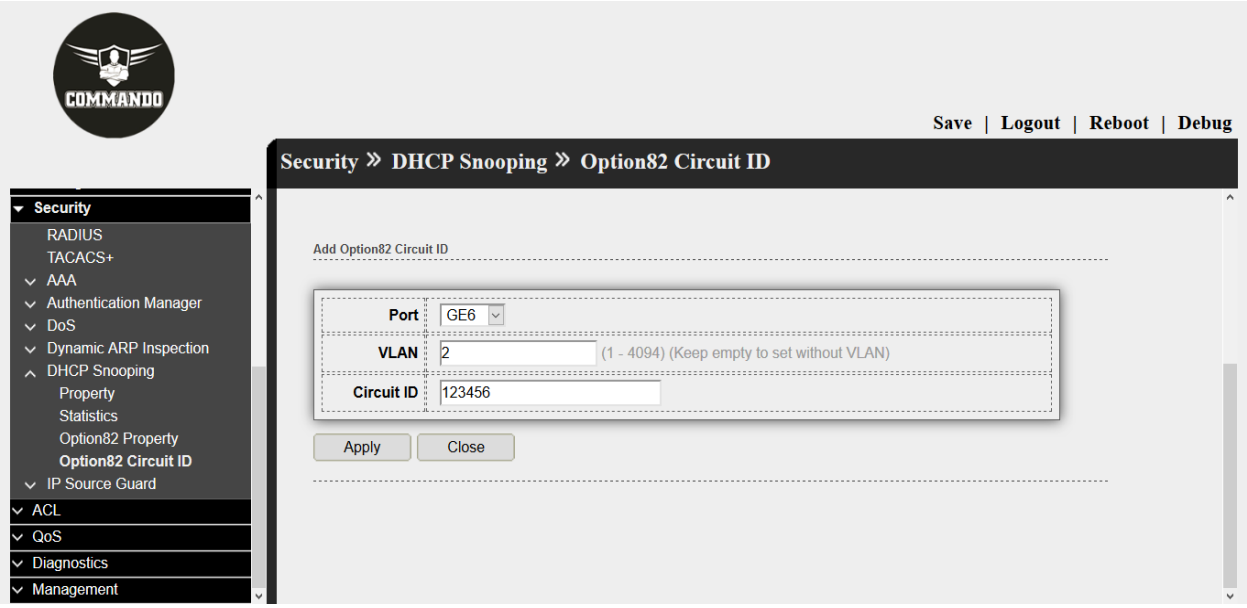


Fig 12.8.11 DHCP Snooping Add Option82 Circuit ID page

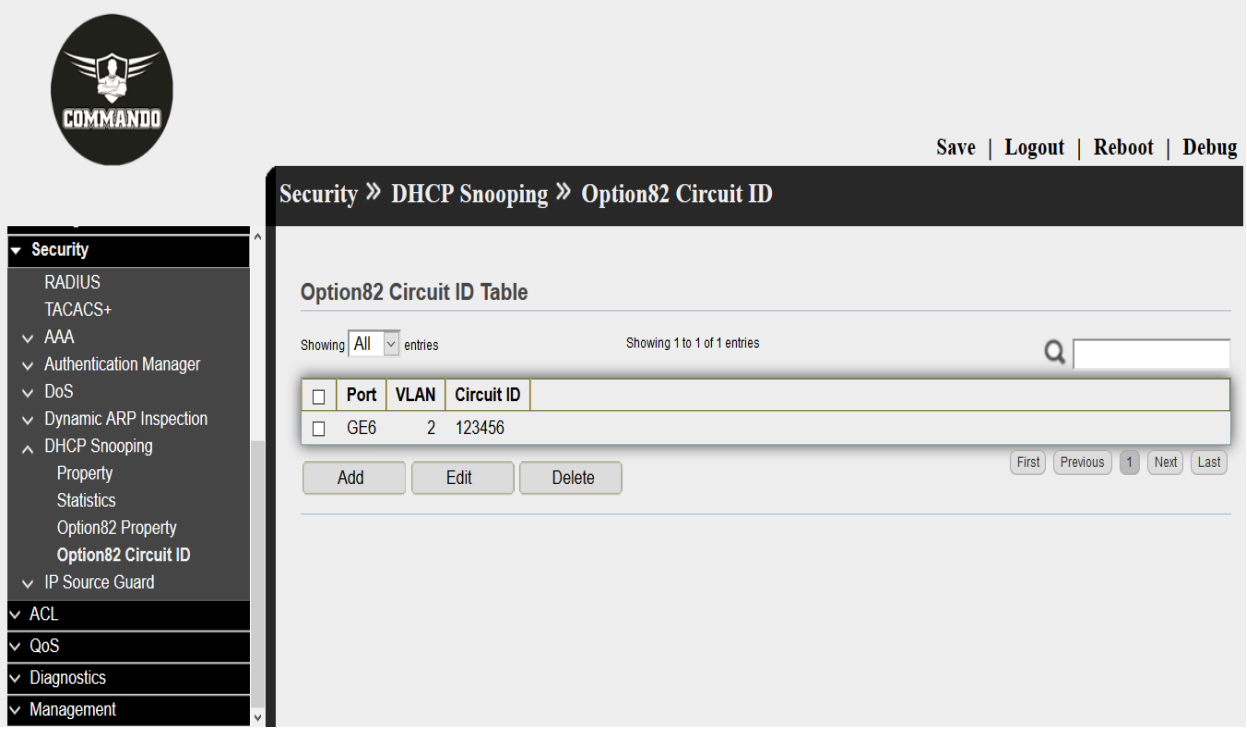


Fig 12.8.12 DHCP SnoopingOption82 Circuit ID Table after enabling GE2 port page

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.

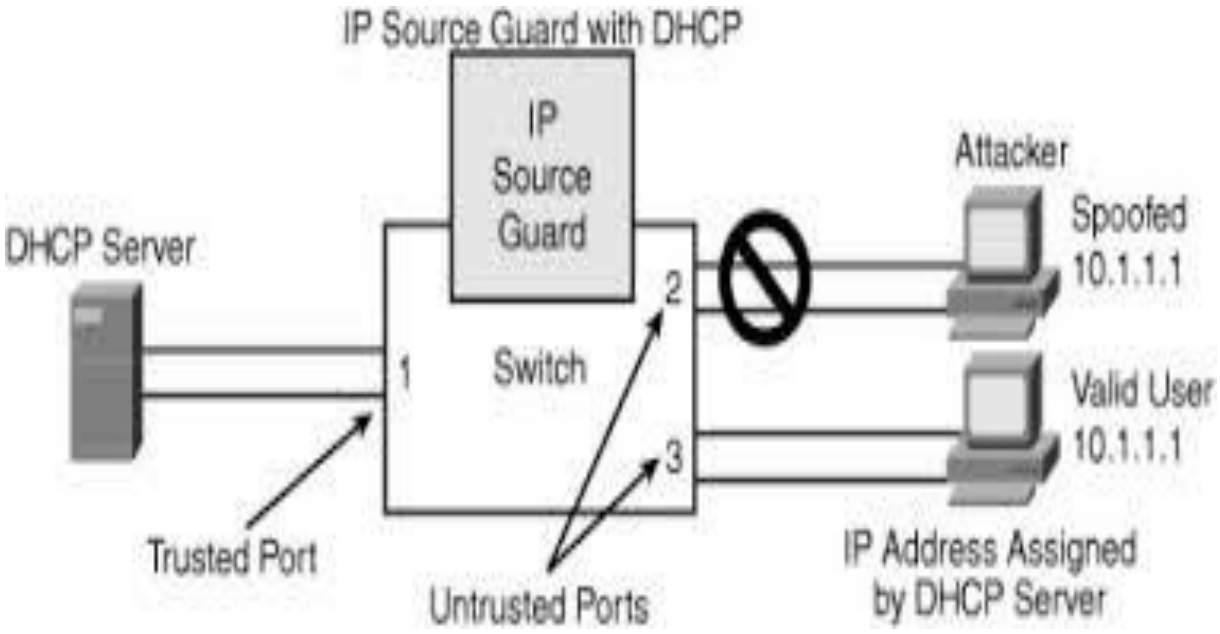


Fig 12.9.1 IP Source Guard concept

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.**

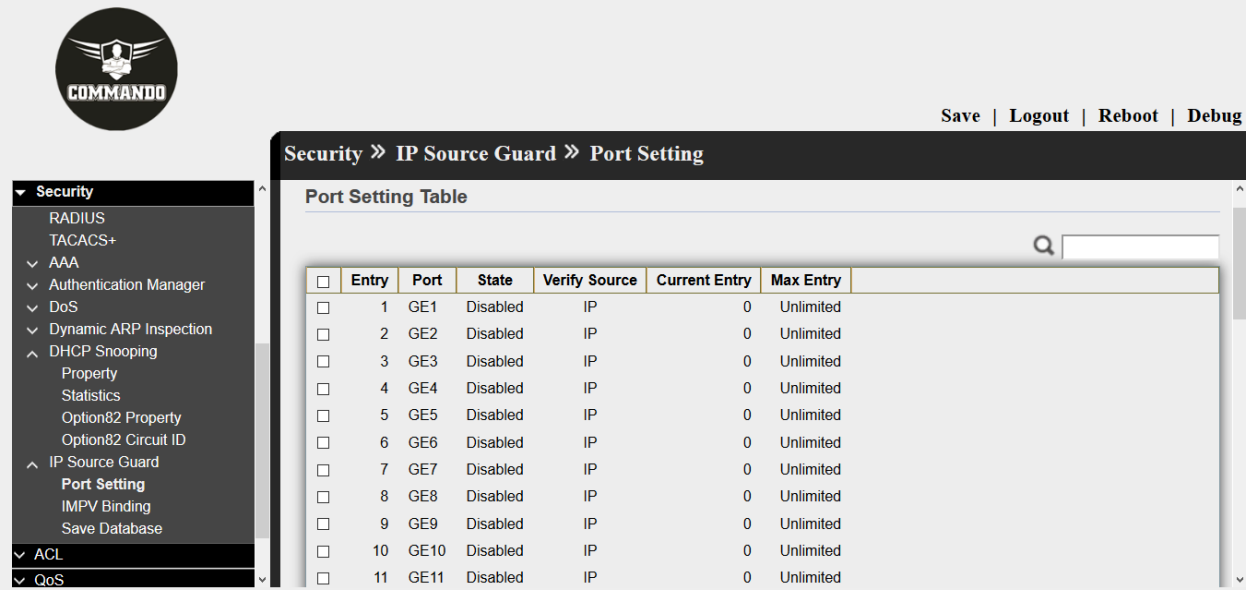


Fig 12.9.2 IP source guard default Port Setting table page

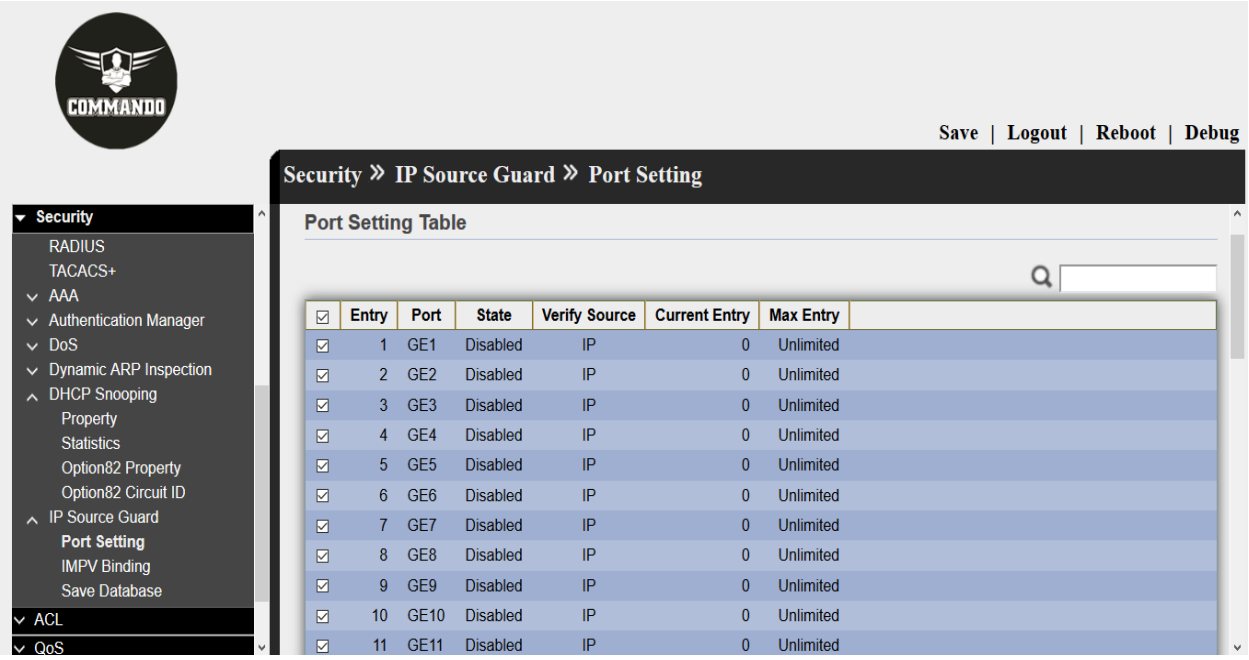


Fig 11.9.2 IP source guard Selecting Ports for Setting page

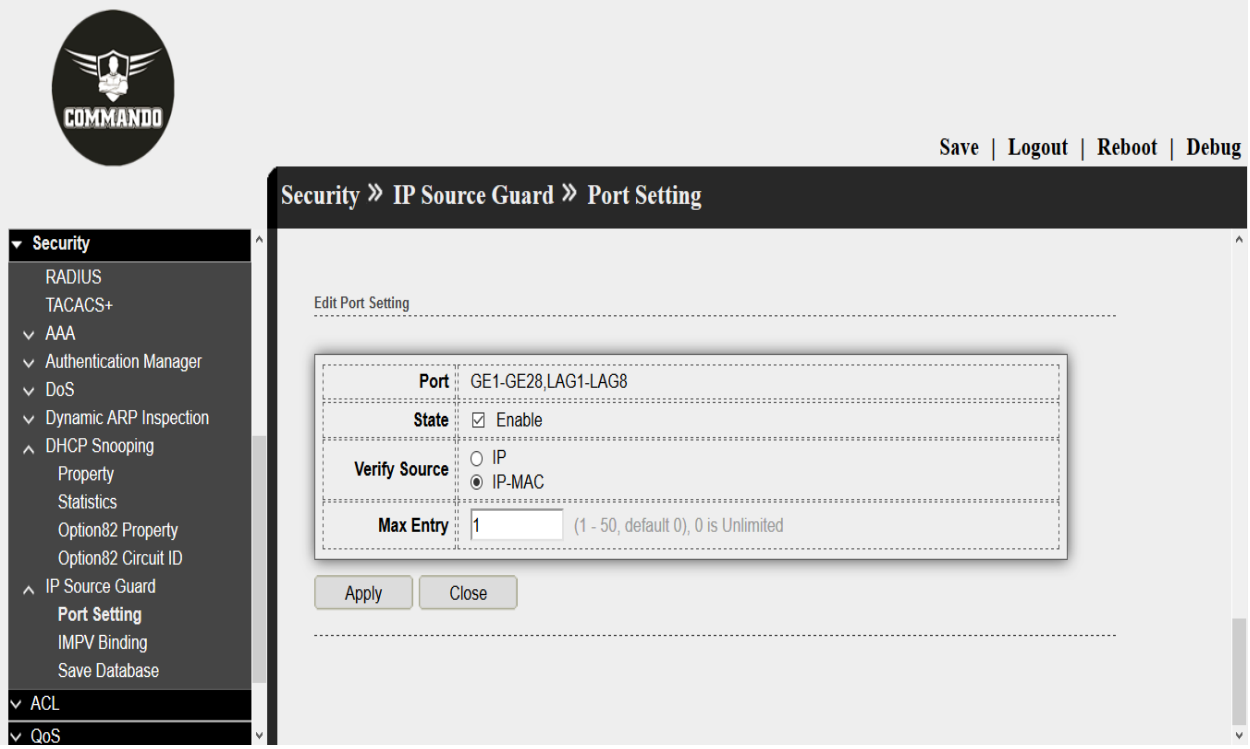


Fig 12.9.3 Edit IP source guard Ports Setting page

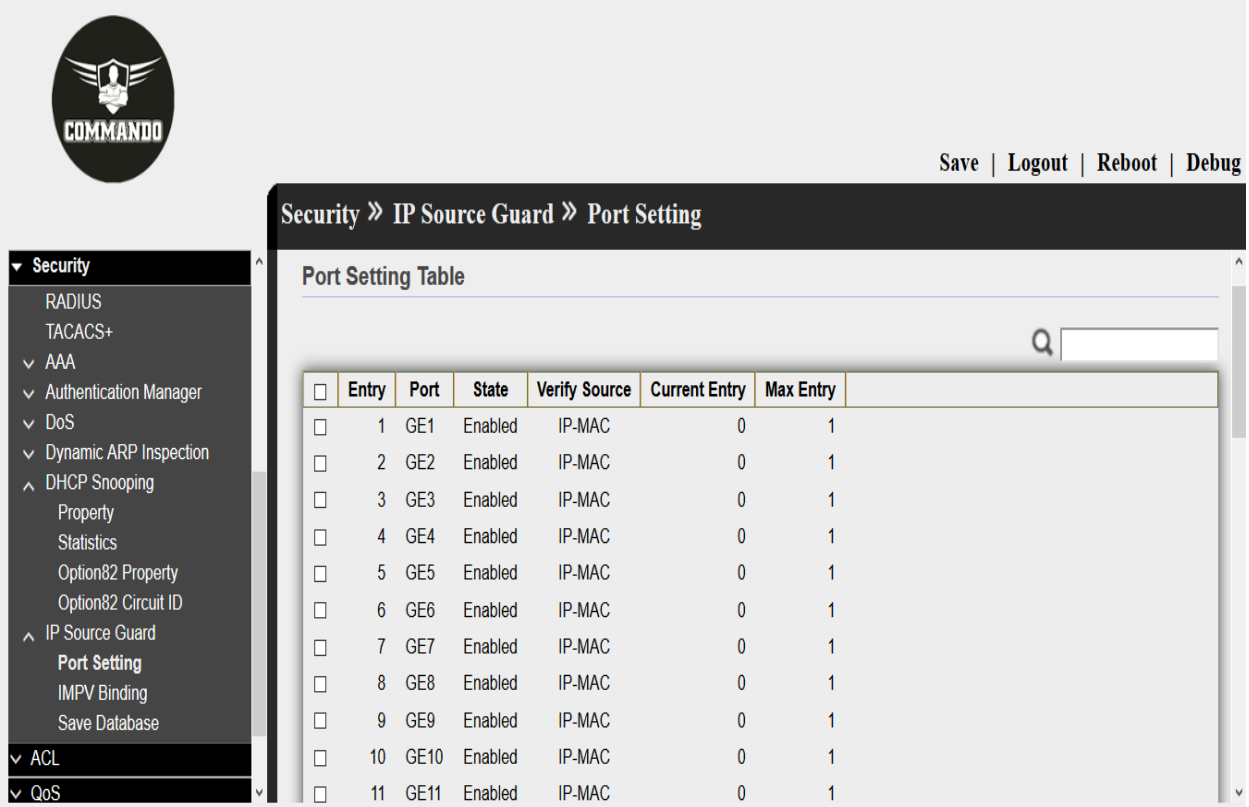


Fig 12.9.4 IP source guard Port Setting table after setting page

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 IPMV Binding , click **Security >> IP Source Guard >> IMPV Binding.**

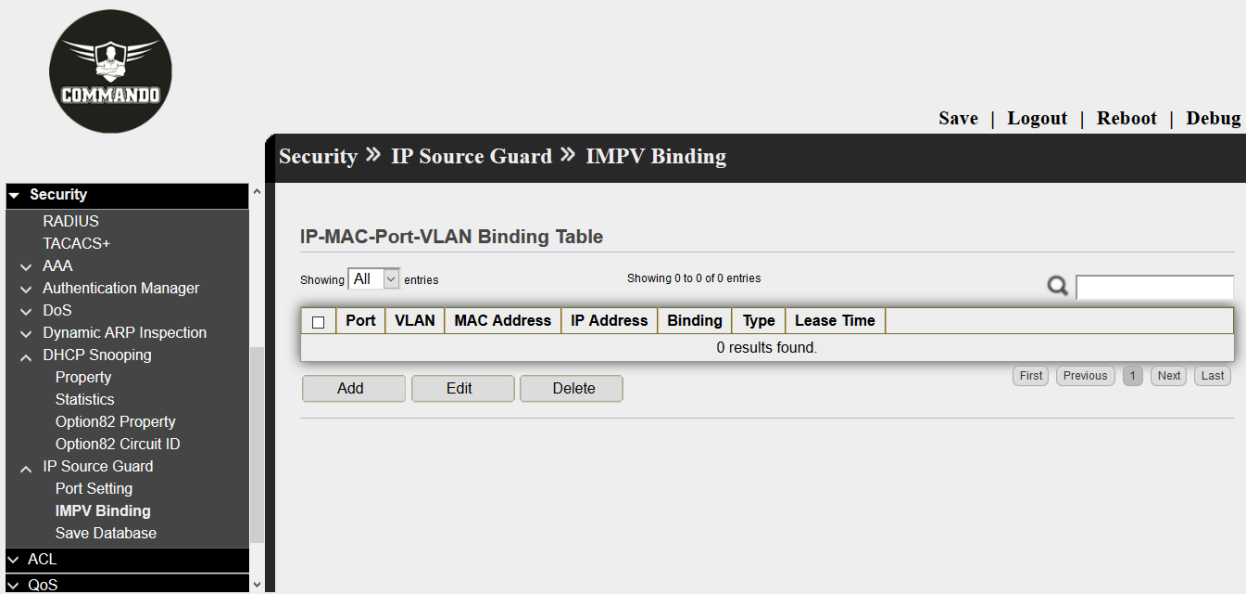


Fig 12.9.5 IP Source Guard Default IMPV Binding Table page

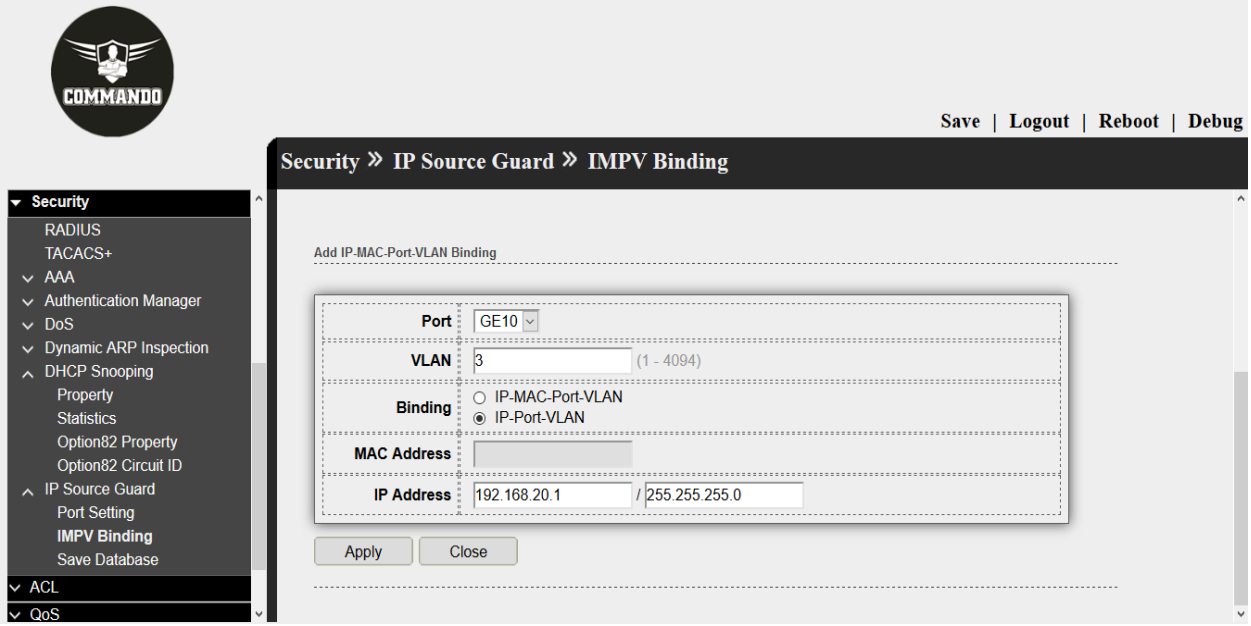


Fig 12.9.6 Add IP Source Guard IP-MAC-Port-VLAN Binding page

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.**

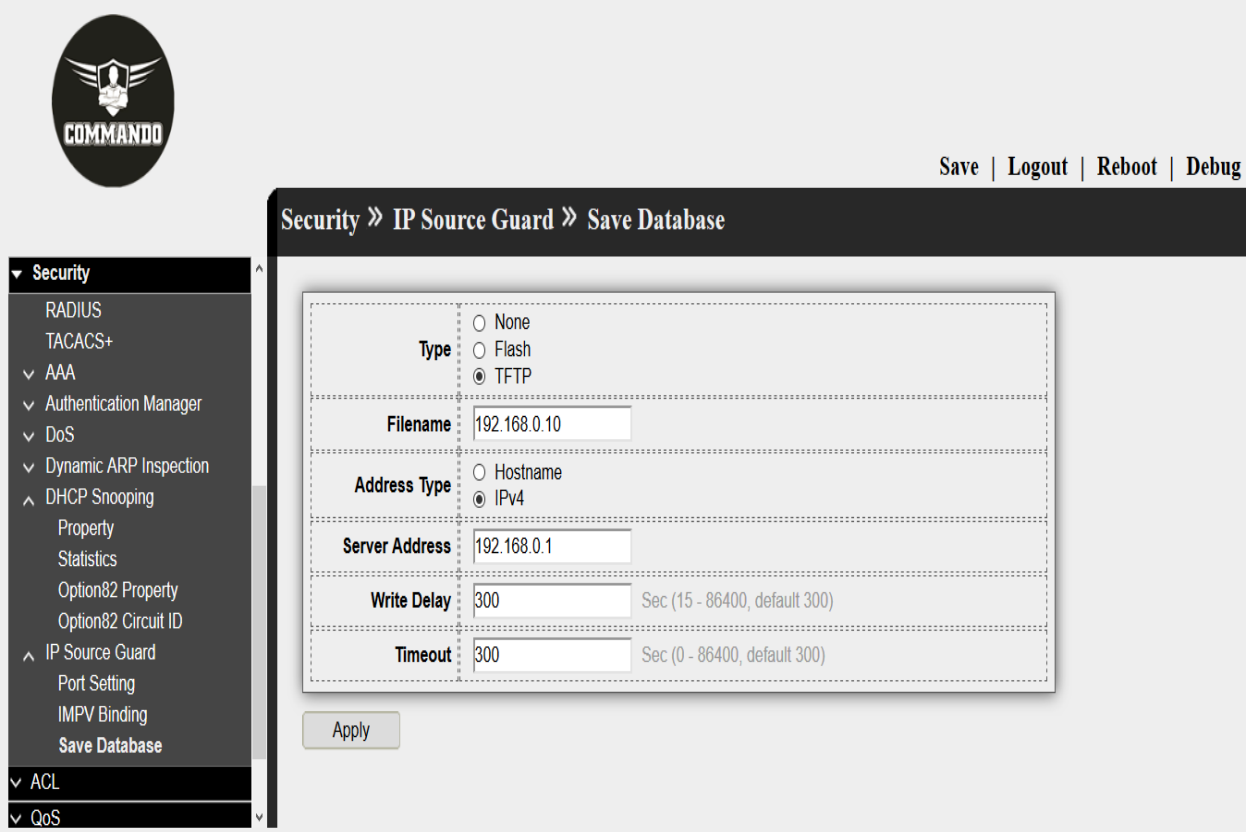


Fig 12.9.7 IP Source Guard Save Database page

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 source 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 criteria 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 criteria 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.**

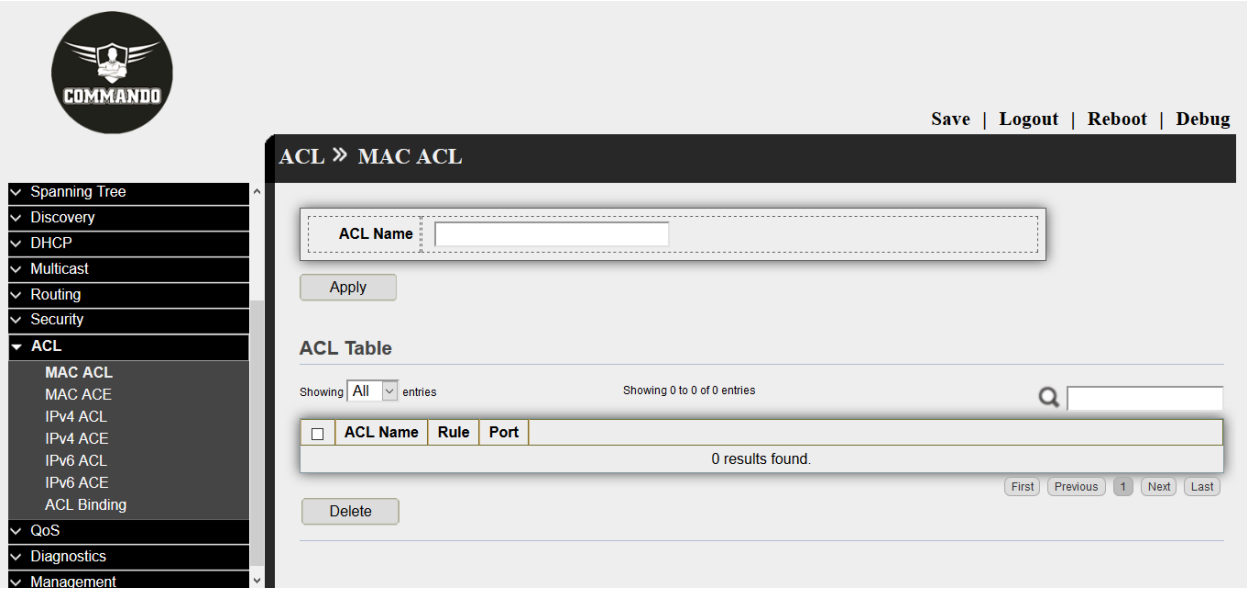


Fig 13.1.1 Default MAC ACL Table page

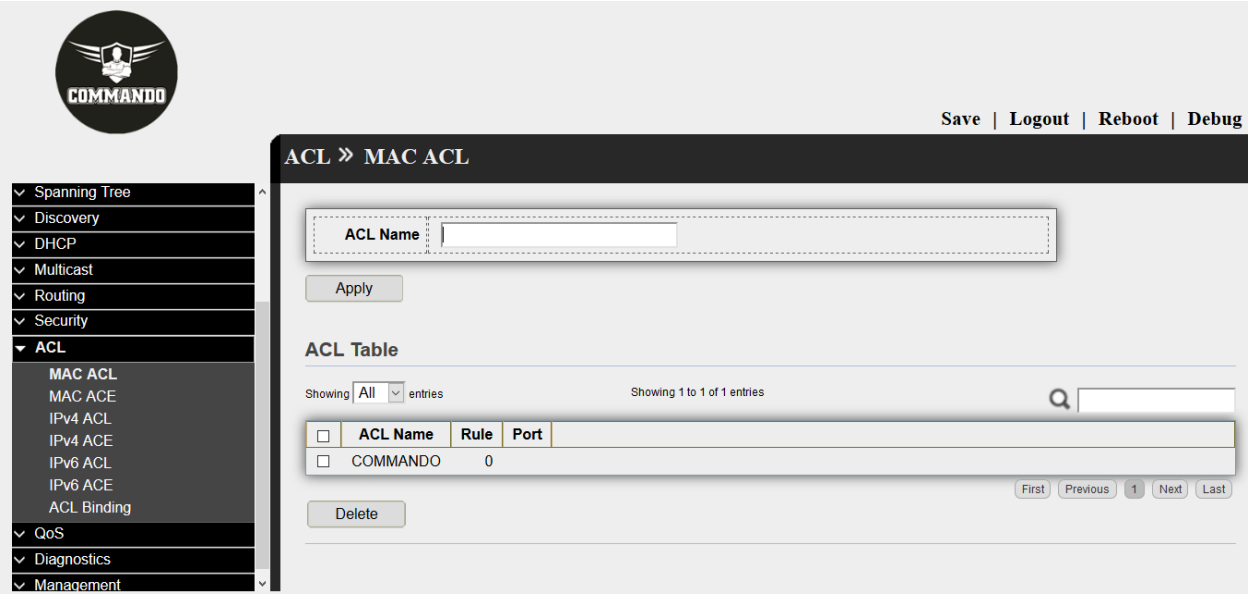


Fig 13.1.2 MAC ACL Table after creating COMMANDO page

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**

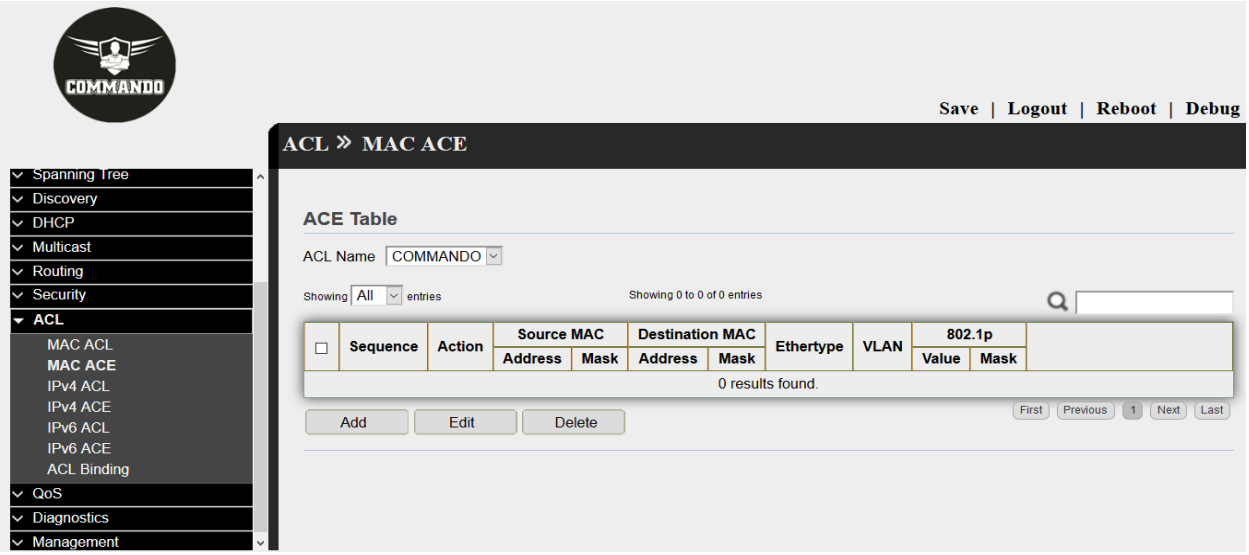


Fig 13.2.1 Default MAC ACE page

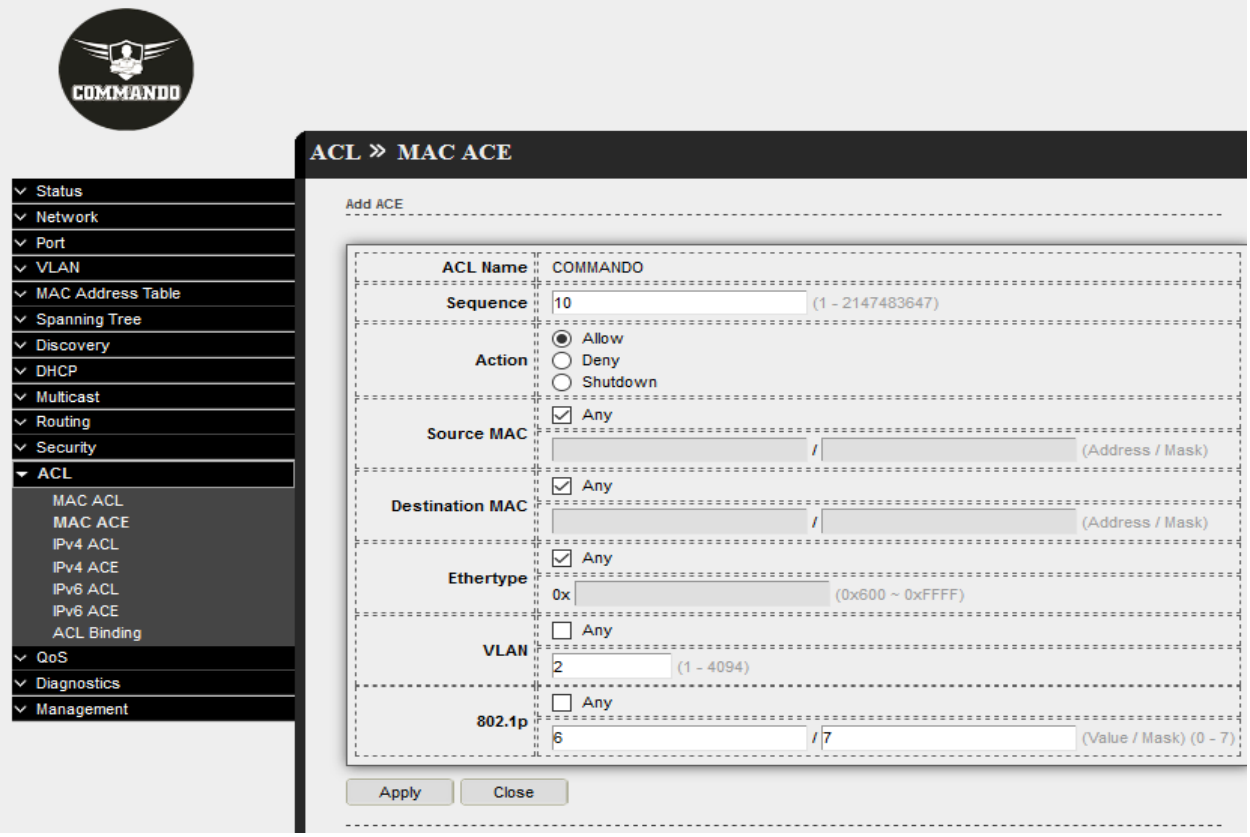


Fig 13.2.2 Add MAC ACE page

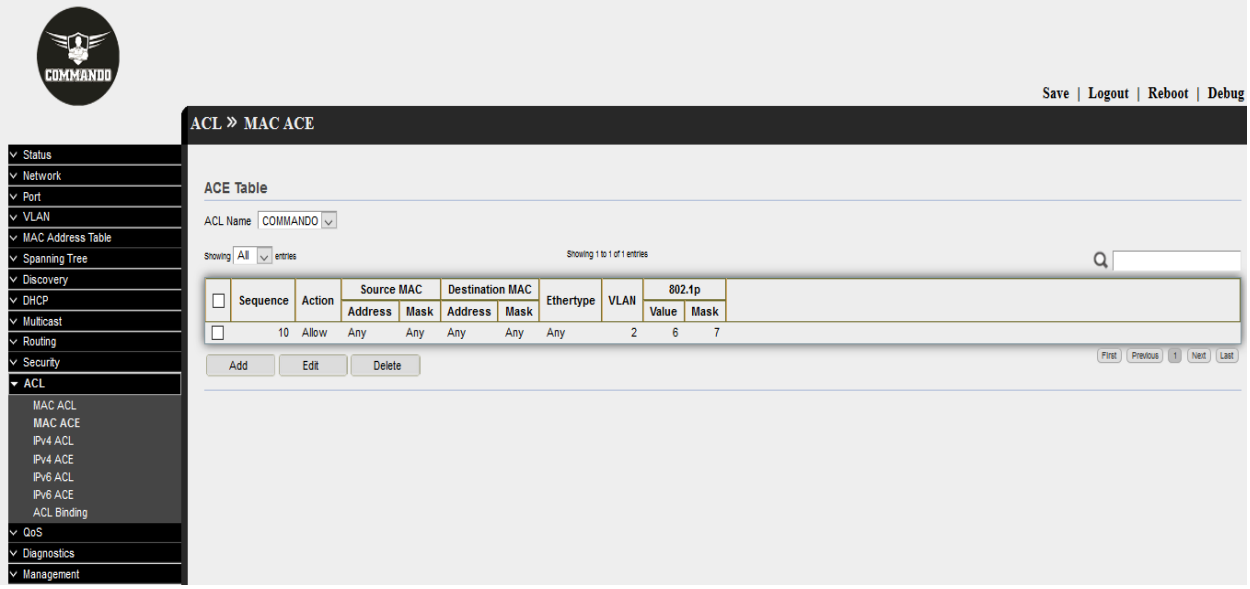


Fig 13.2.3 MAC ACE Table page

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**

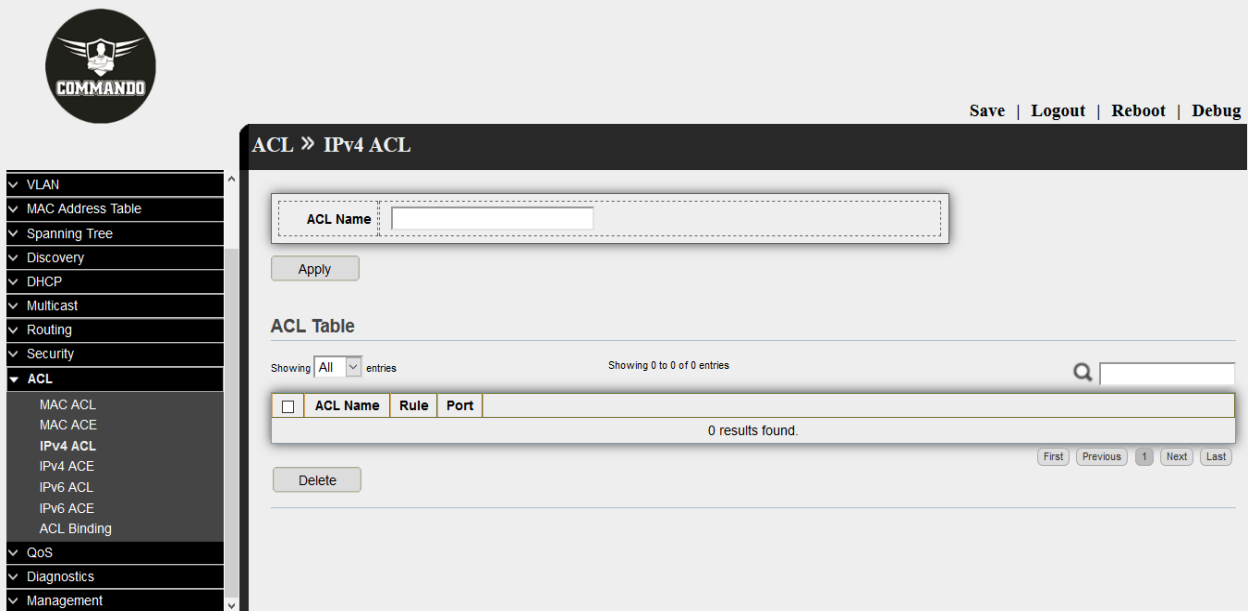


Fig 13.3.1 Default ACL Table page

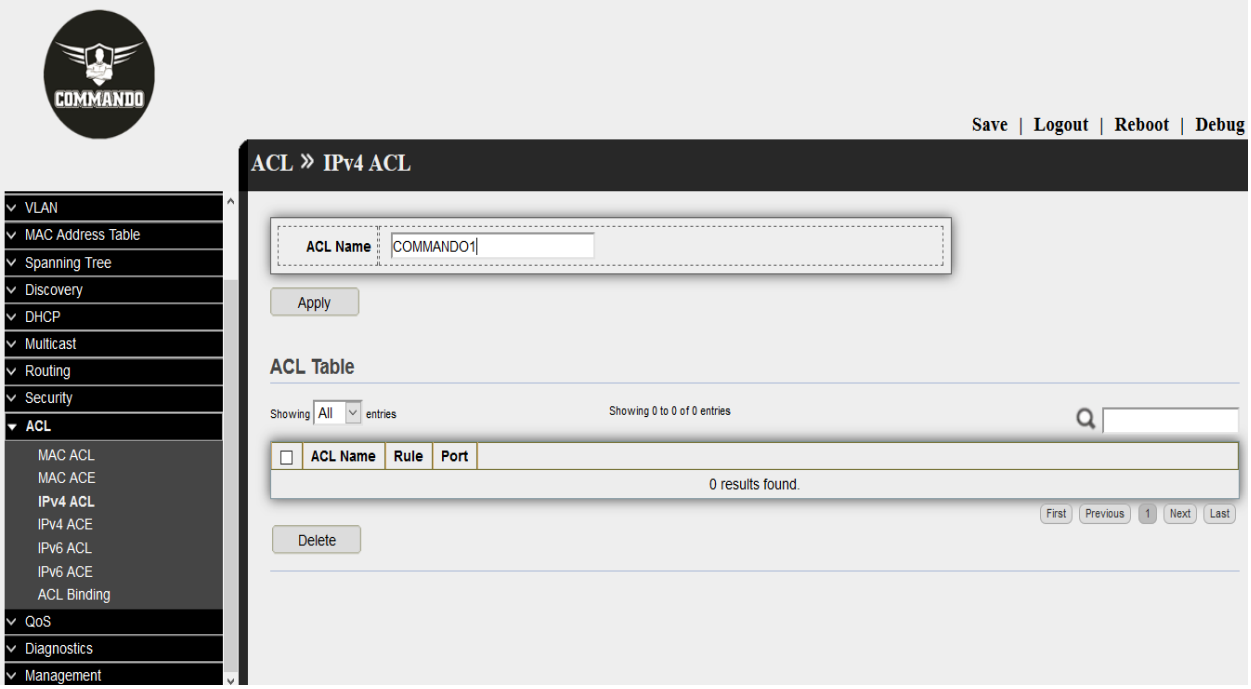


Fig 13.3.2 Edit IPv4 ACL Name page

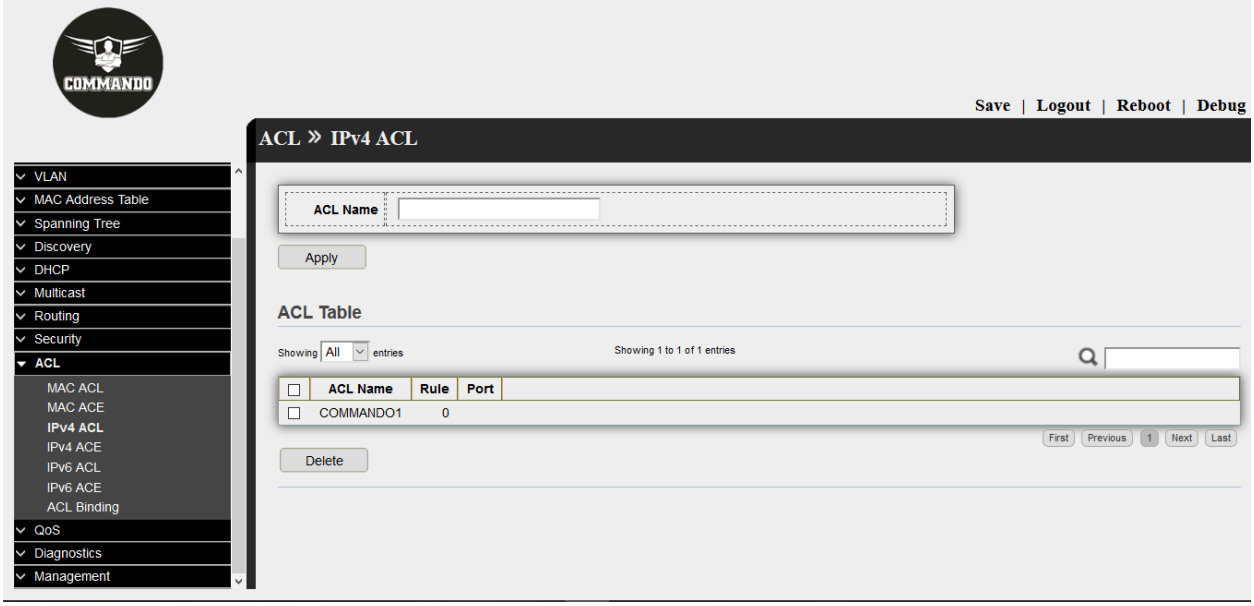


Fig 13.3.2 IPv4 ACL Table after creating COMMANDO1 ACL page

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**

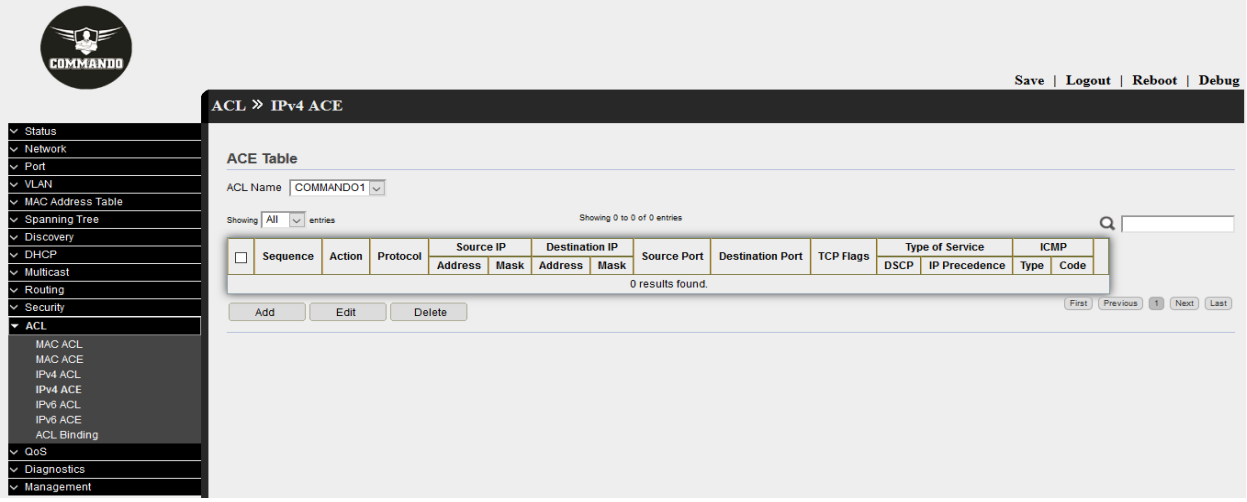


Fig 13.4.1 Default IPv4 ACE Table page

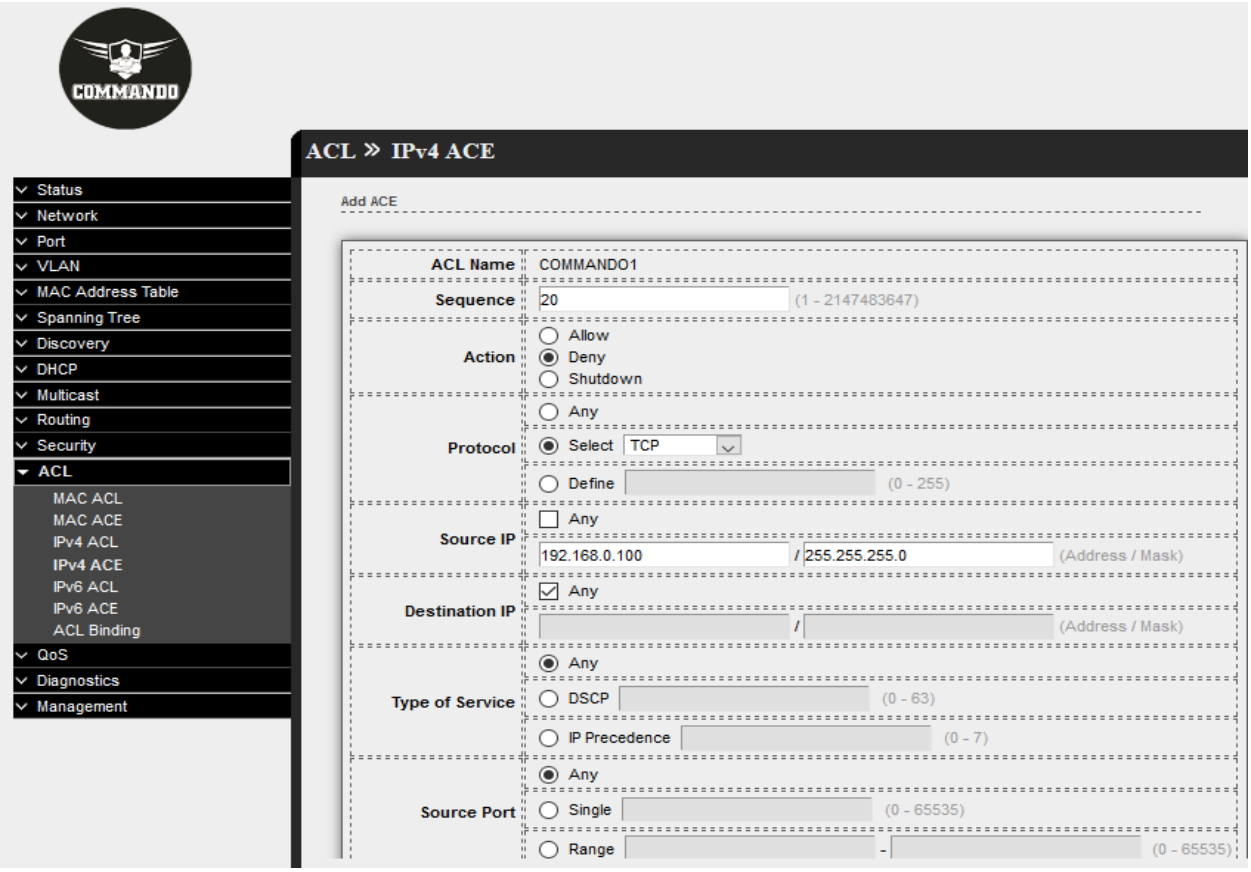


Fig 13.4.2 Add IPv4 ACE page

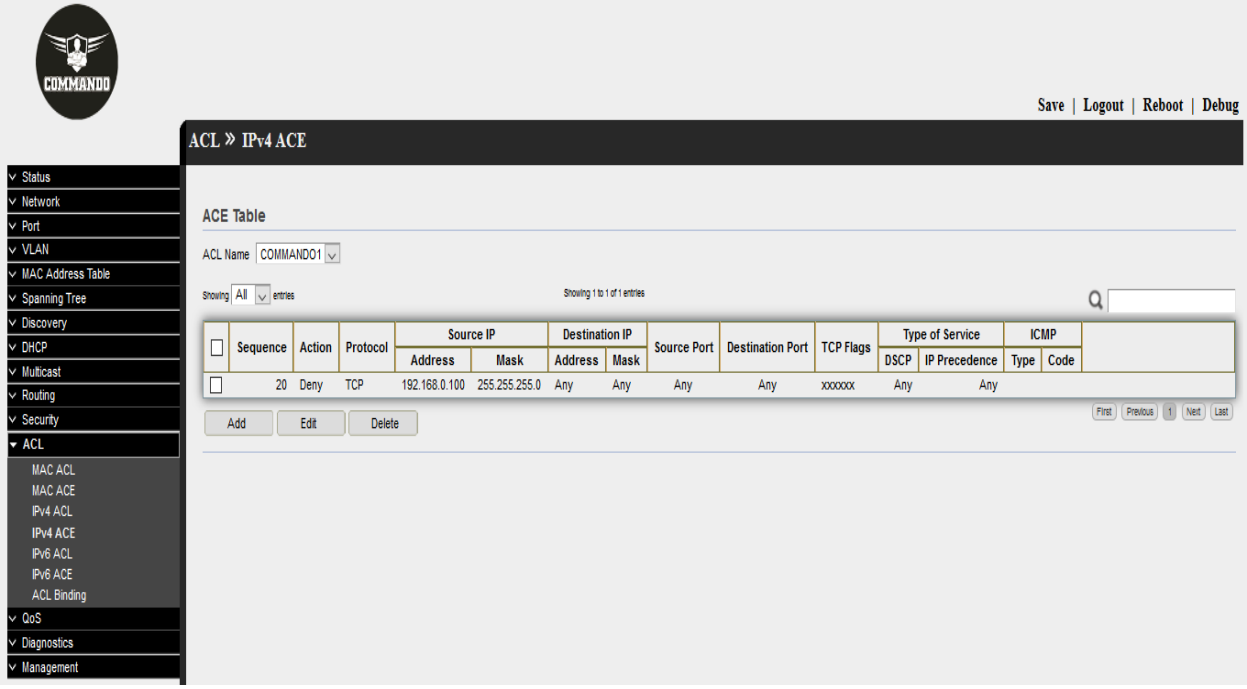


Fig 13.4.3 IPv4 ACE Table page

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**

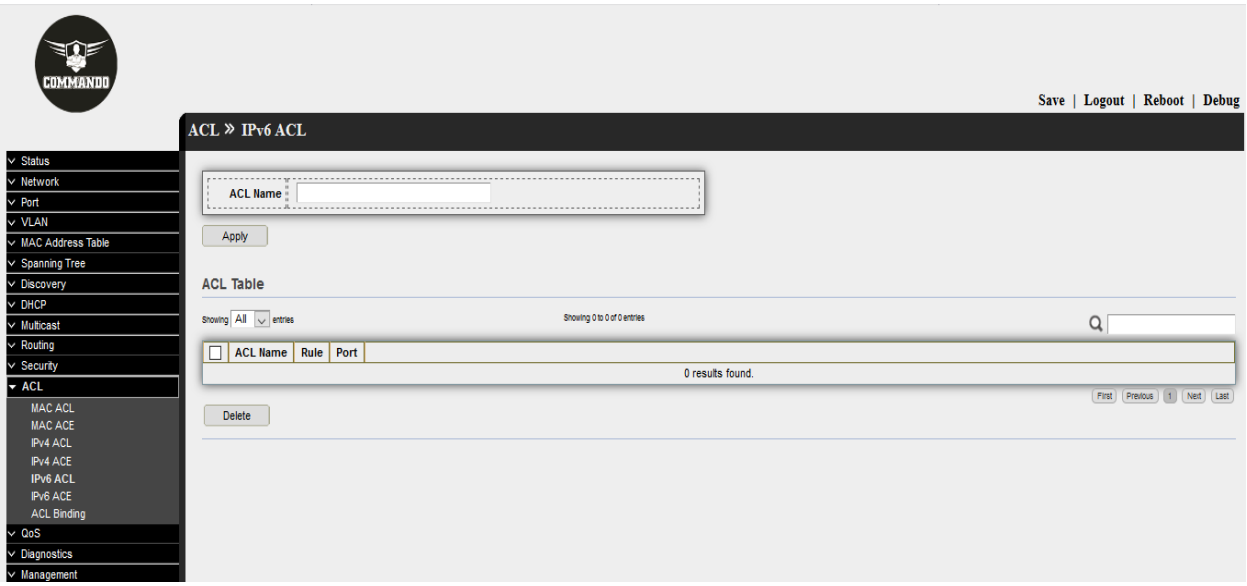


Fig 13.5.1 Default IPv6 ACL Table page

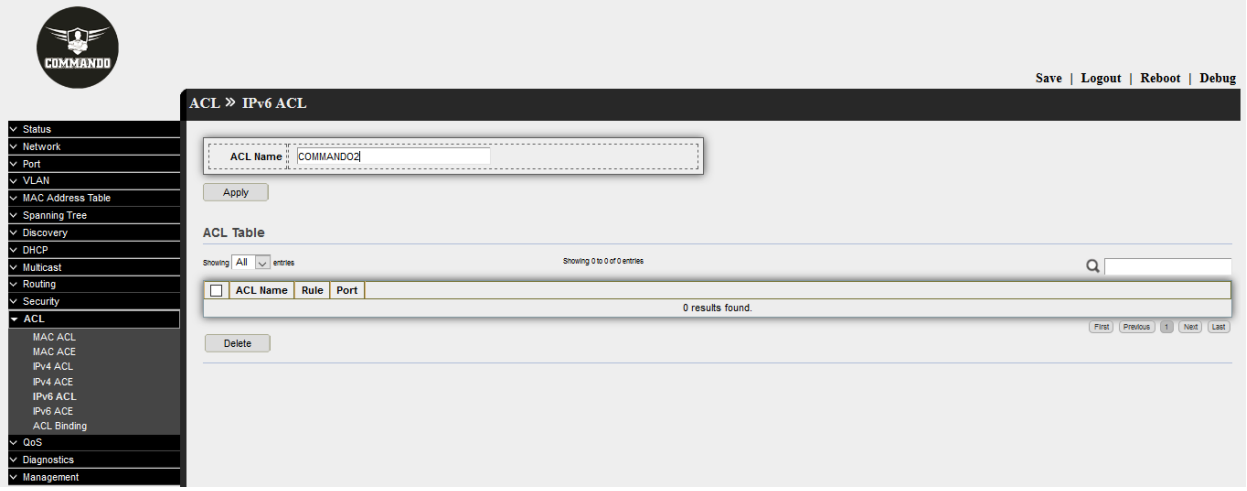


Fig 13.5.2 IPv6 ACL Name page

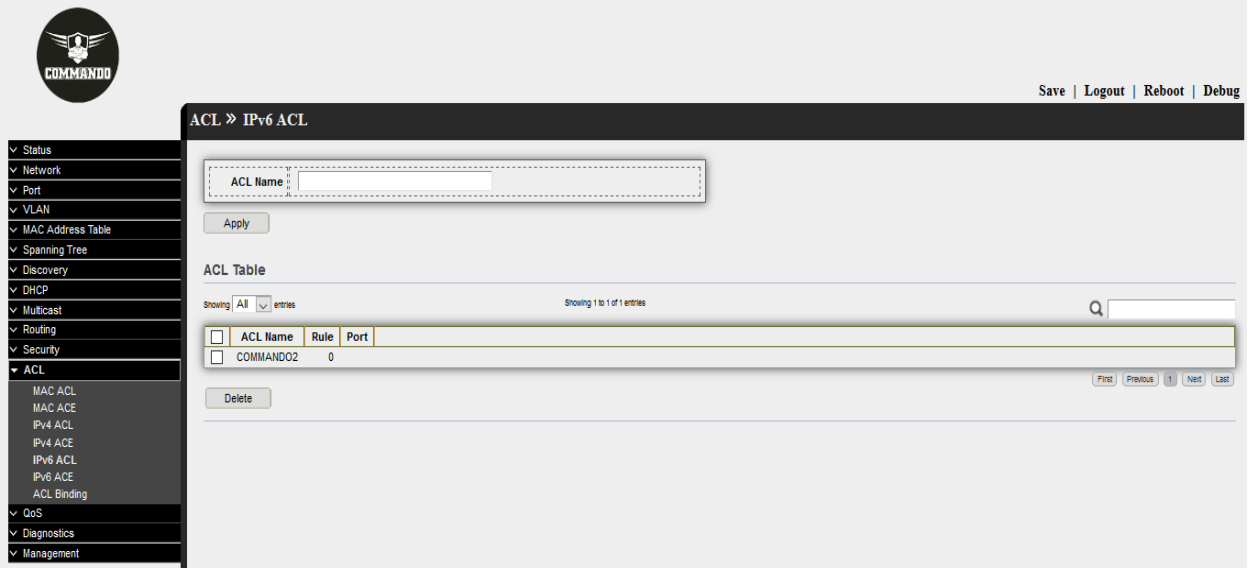


Fig 13.5.3 IPv6 ACLTable after changing page

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**

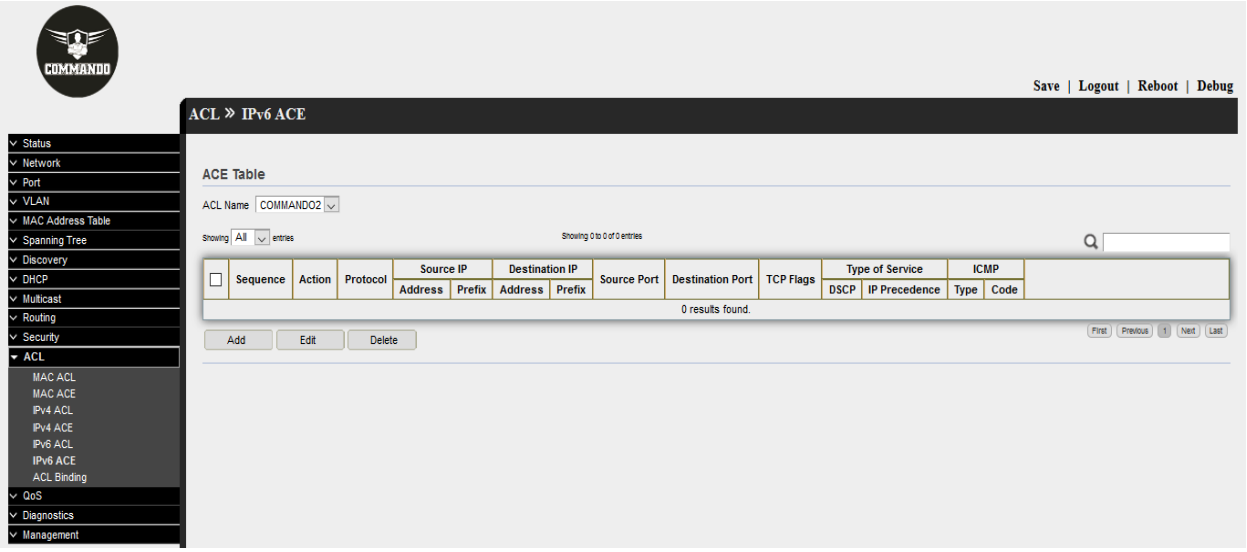


Fig 13.6.1 Default IPv6 ACE Table page

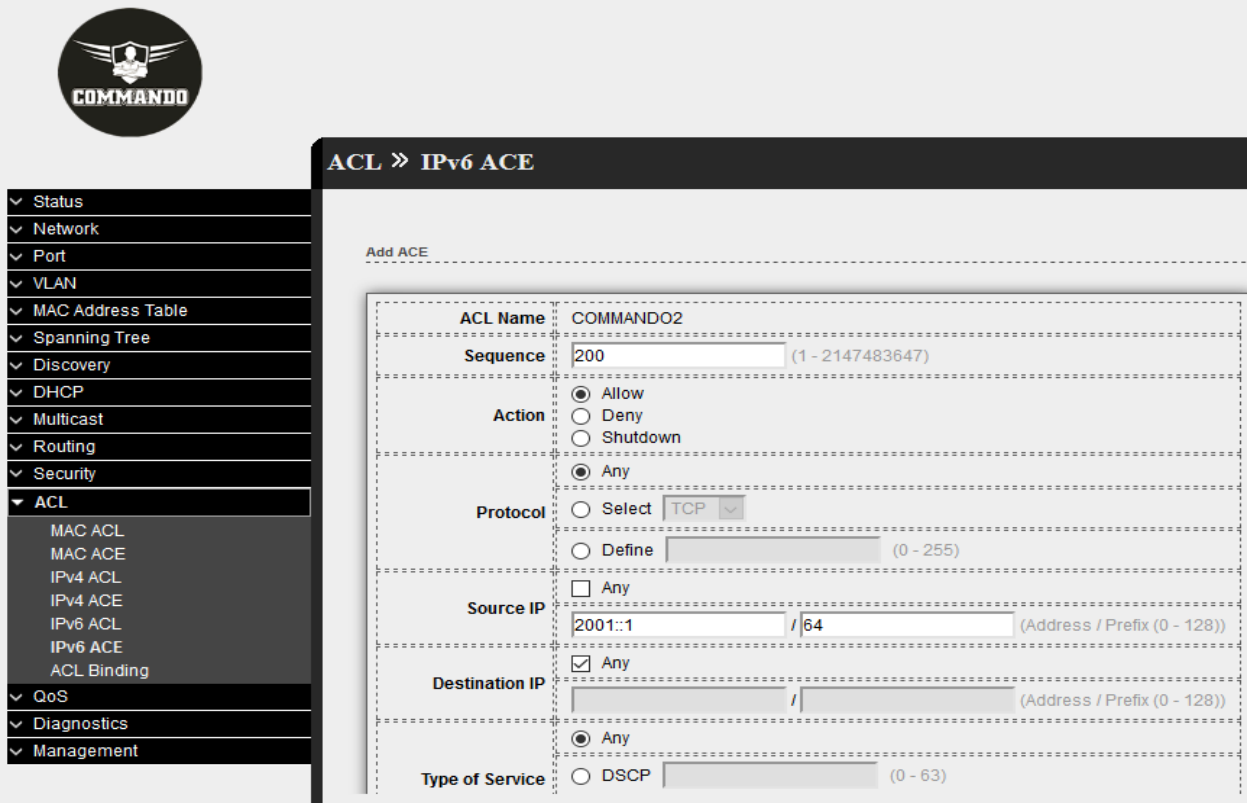


Fig 13.6.2 Add IPv6 ACE page

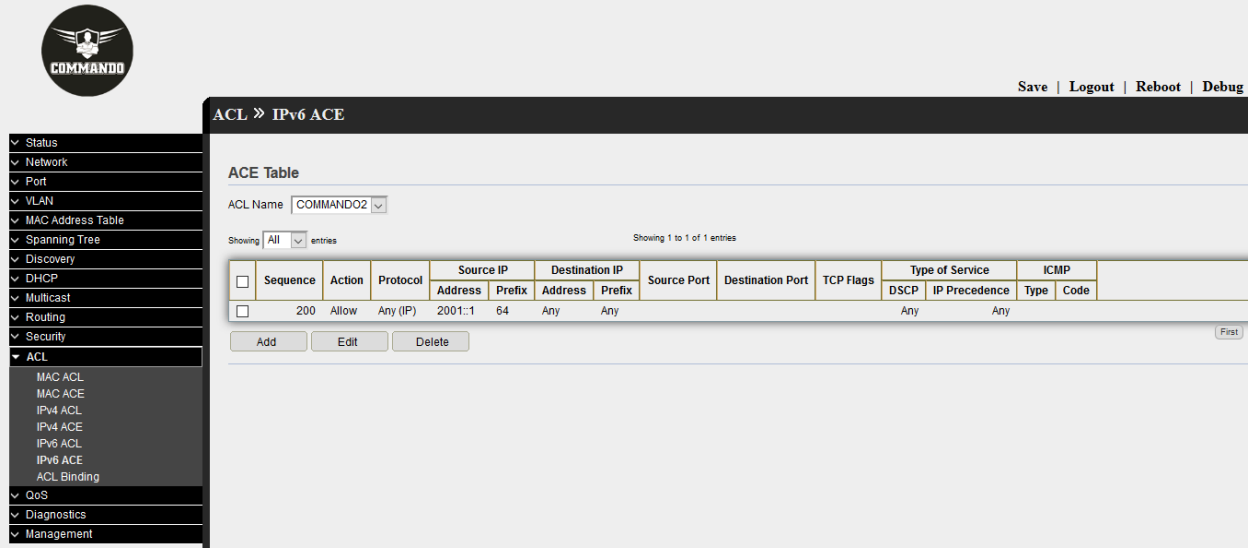


Fig 13.6.3 IPv6 ACE table after adding ACE page

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**

Fig 13.7.1 ACL Binding Table page

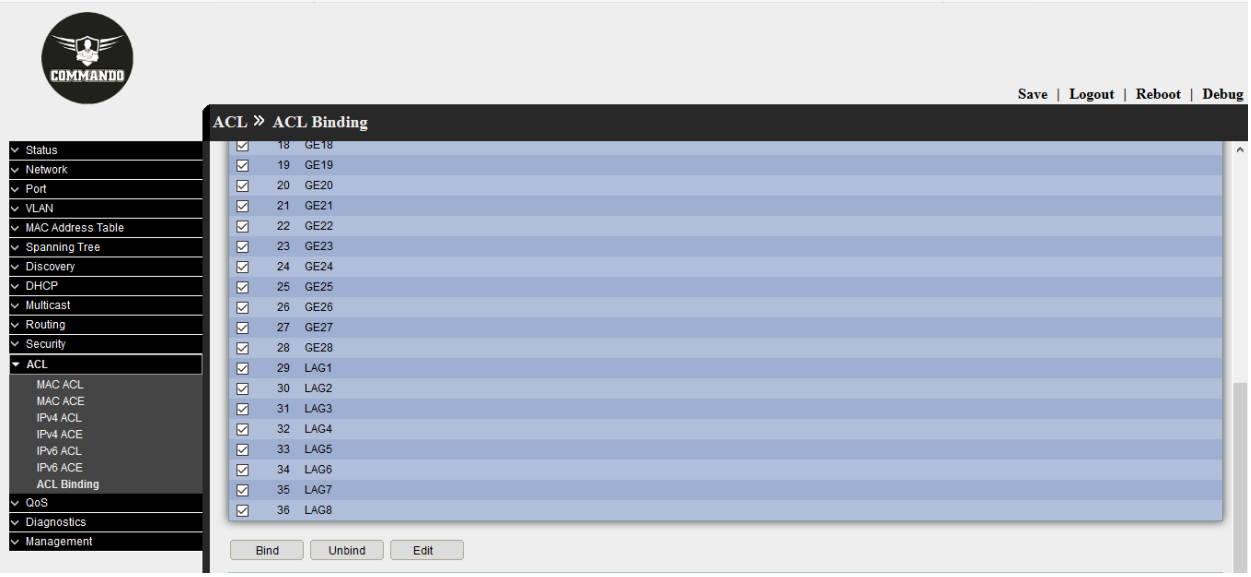


Fig 13.7.2 Selecting port for ACL Binding page

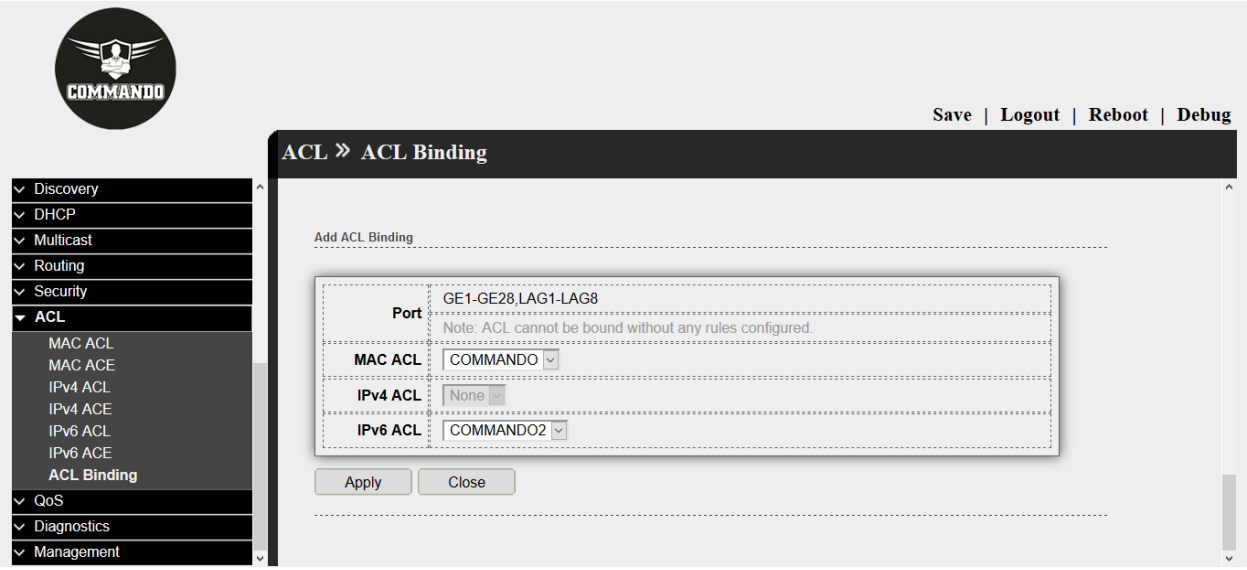


Fig 13.7.3 Add ACL Binding page

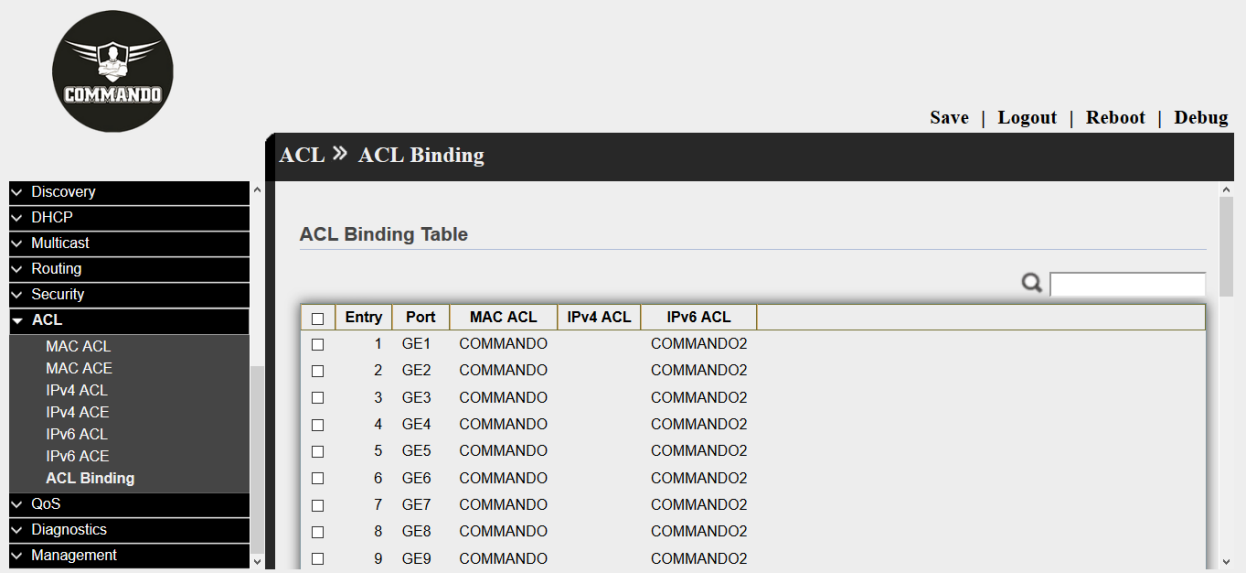


Fig 13.7.4 ACL Binding Table after Enableing GE1 port page

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).

14.1 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. In order 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 located 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. C2000 Series Switches allow setting QoS on per port basis with queueing.

To view and configure QoS Property , click **QoS >> General >> Property.**

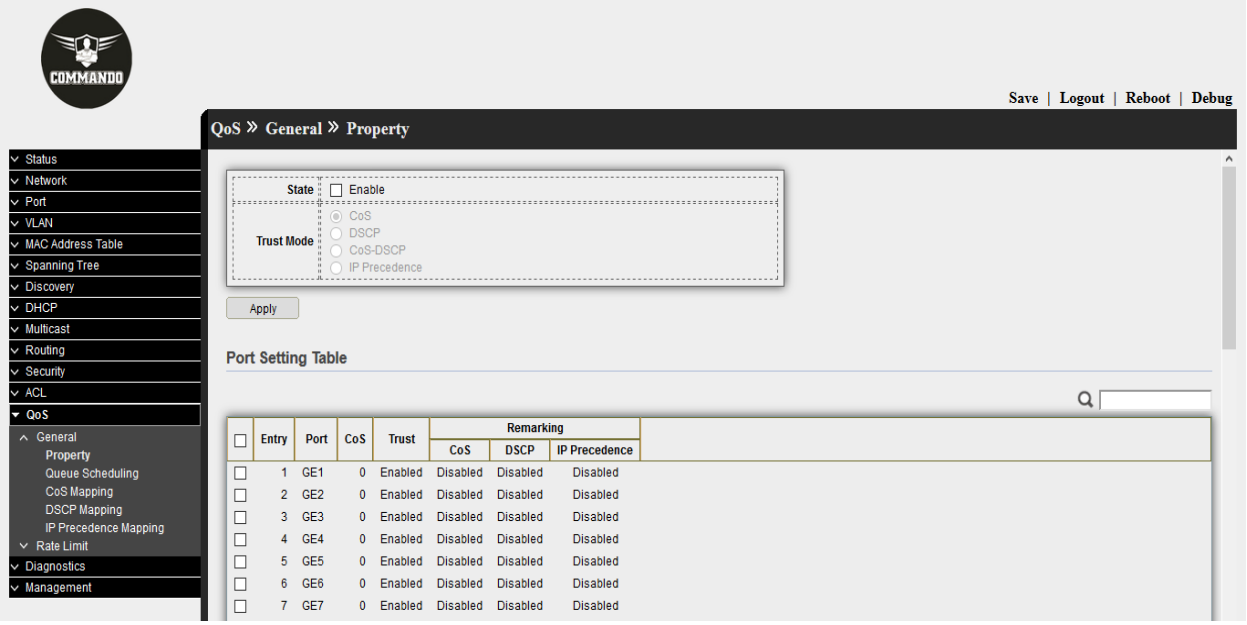


Fig 14.1.1 Default QoS Port Setting table page

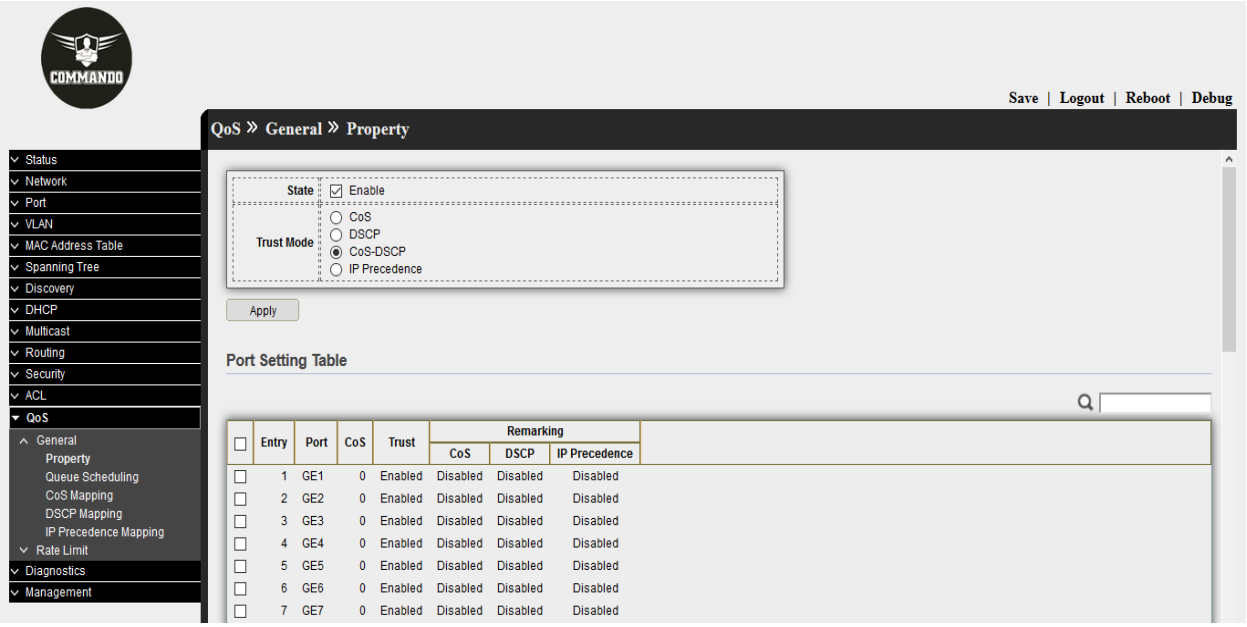


Fig 14.1.2 Enableing QoS on Switch page

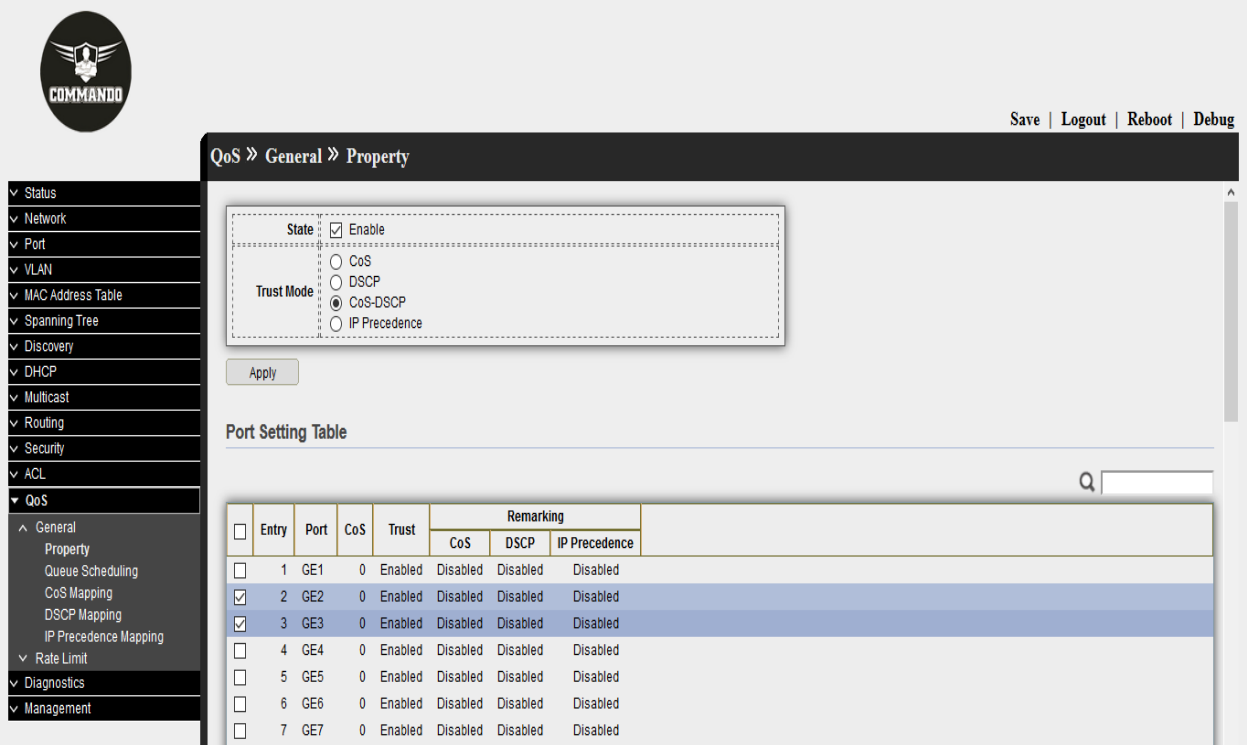


Fig 14.1.3 Selecting Ports for Qos setting page

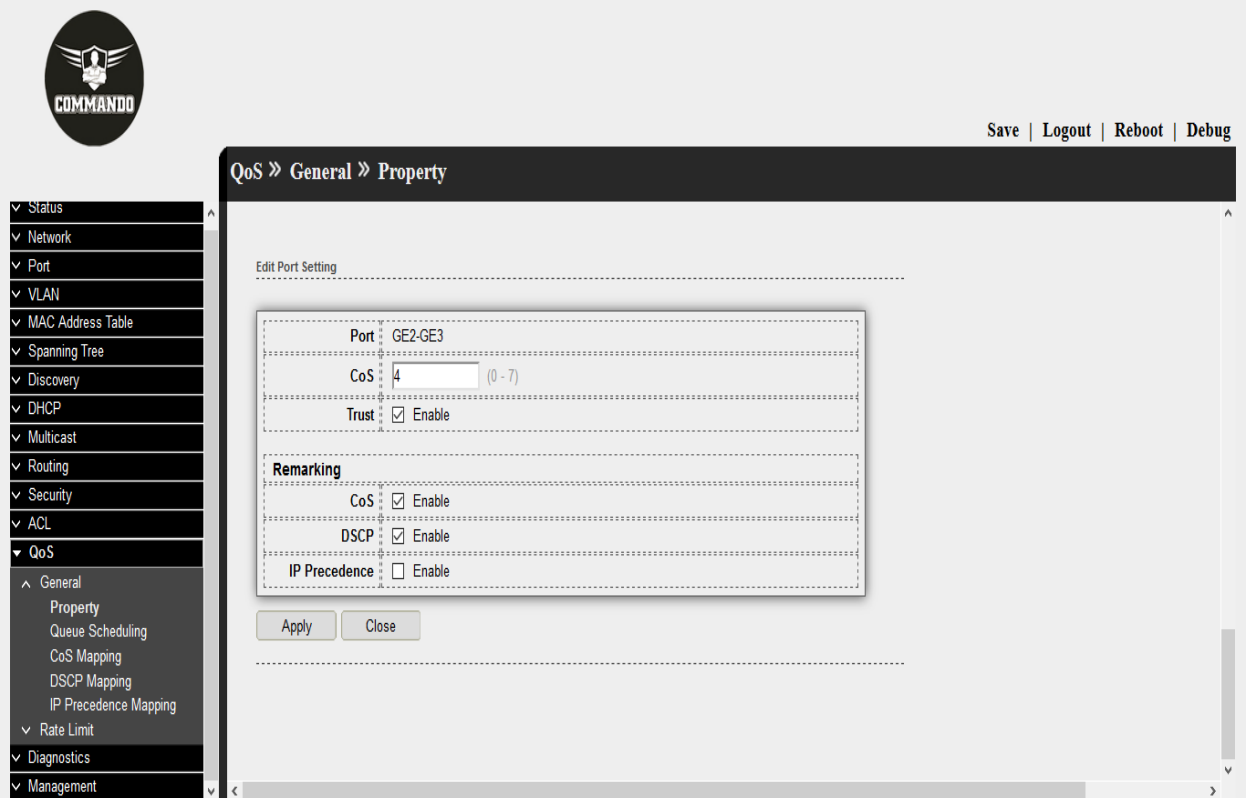


Fig 14.1.4 Edit Ports setting for Qos page

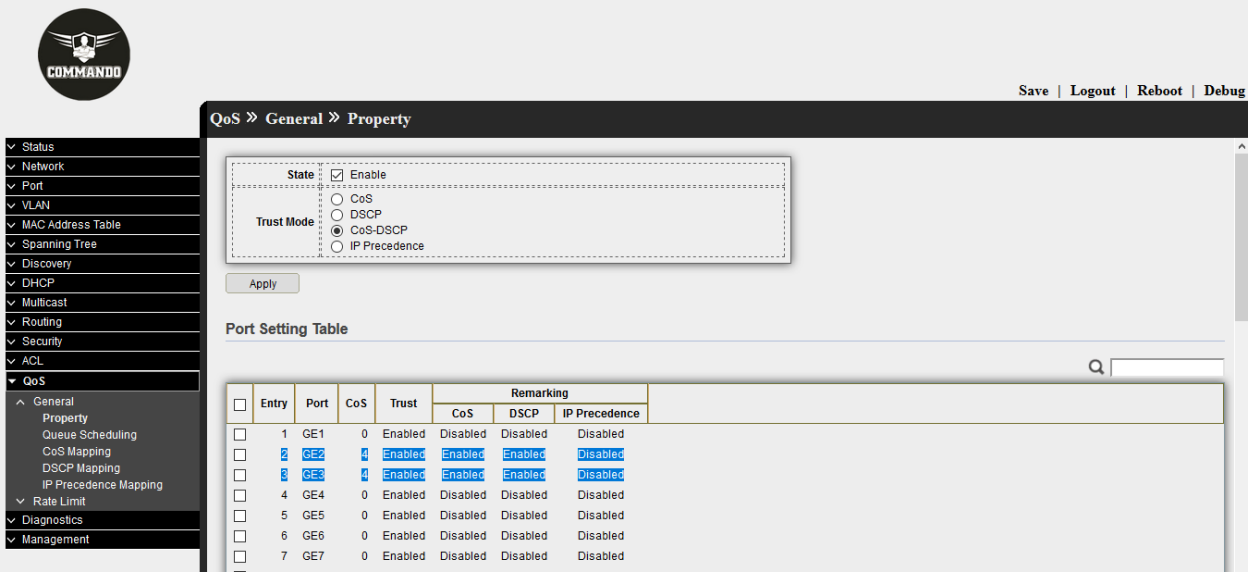


Fig 14.1.5 QoS Port Setting table page

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**

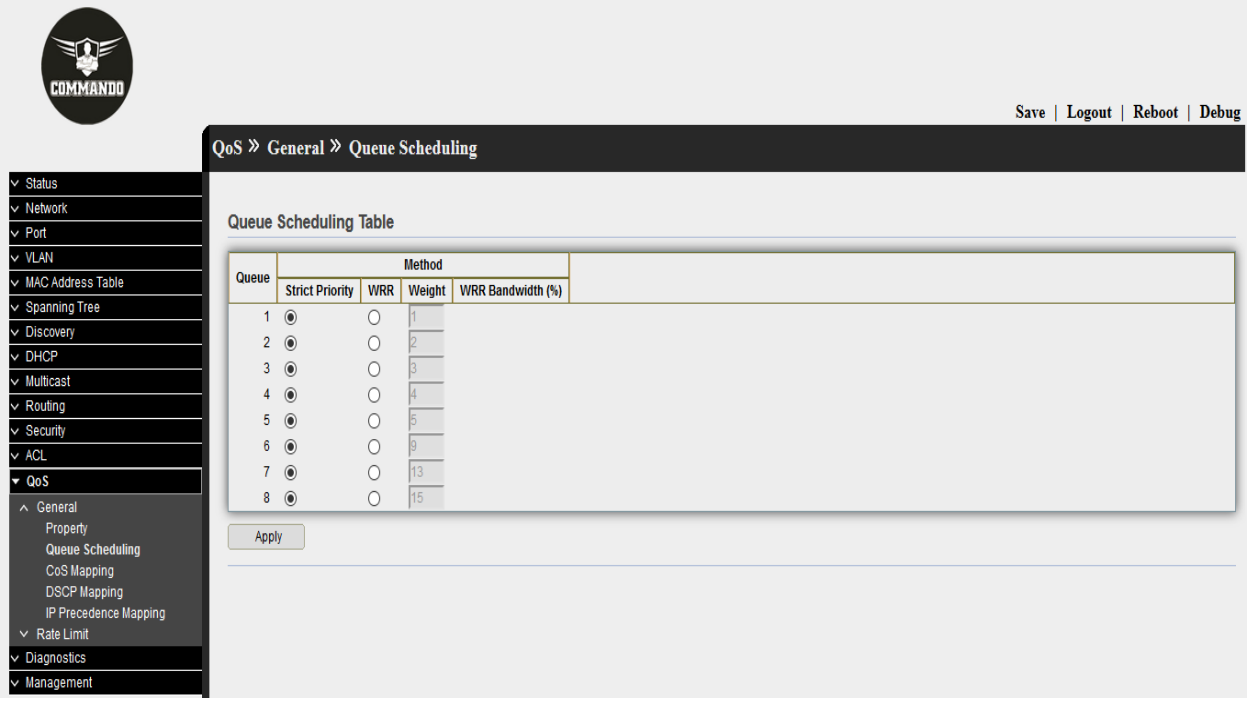


Fig 14.1.6 Default QoS Scheduling table page

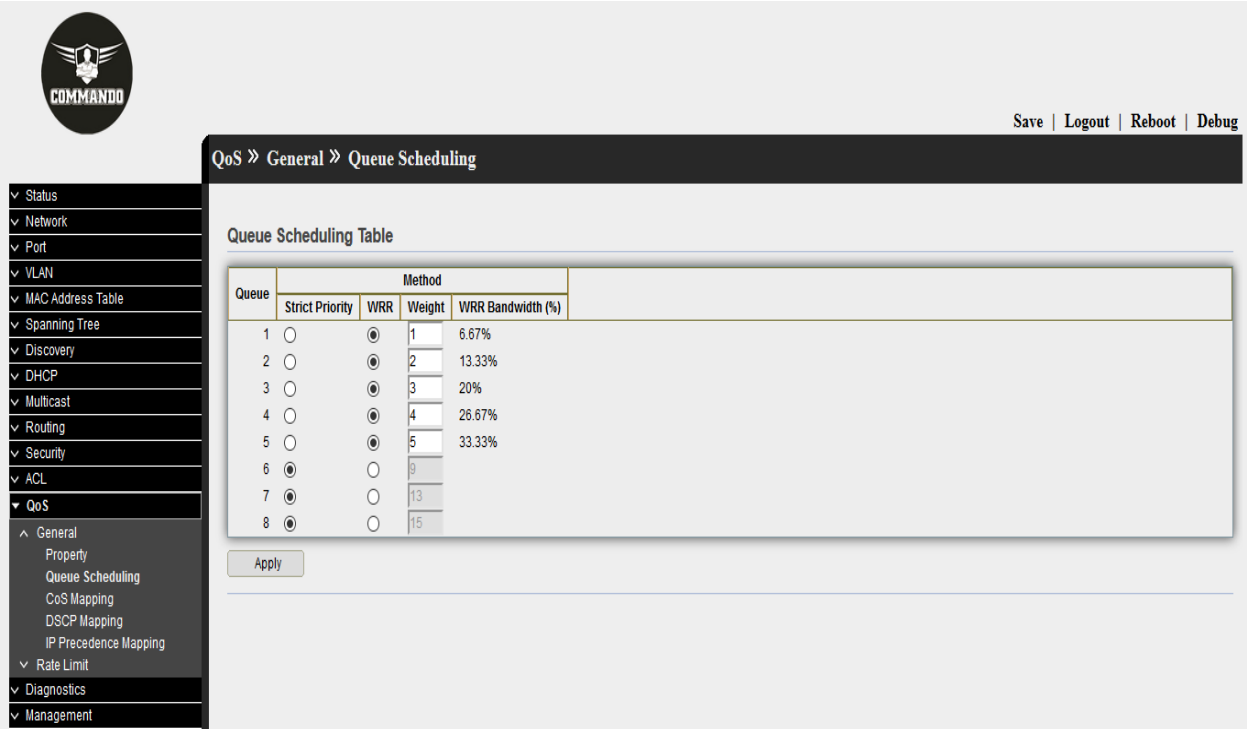


Fig 14.1.7 QoS Scheduling changing Queue Method page

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**

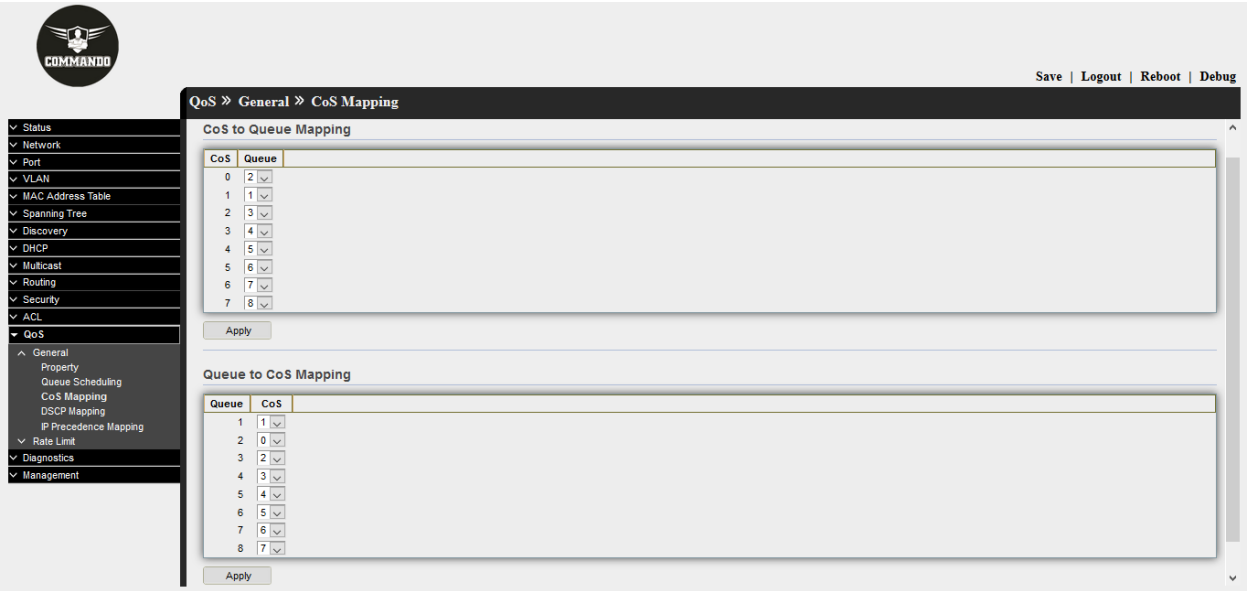


Fig 14.1.8 Default CoS to Queue Mapping page

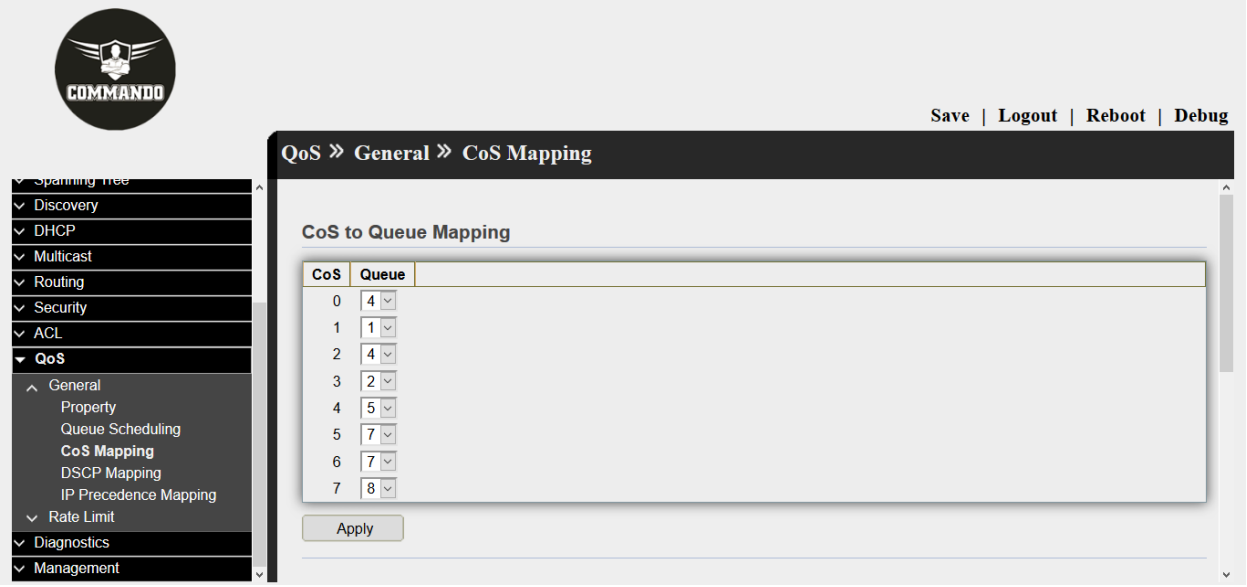


Fig 14.1.9 CoS to Queue Mapping Changing Queue values page

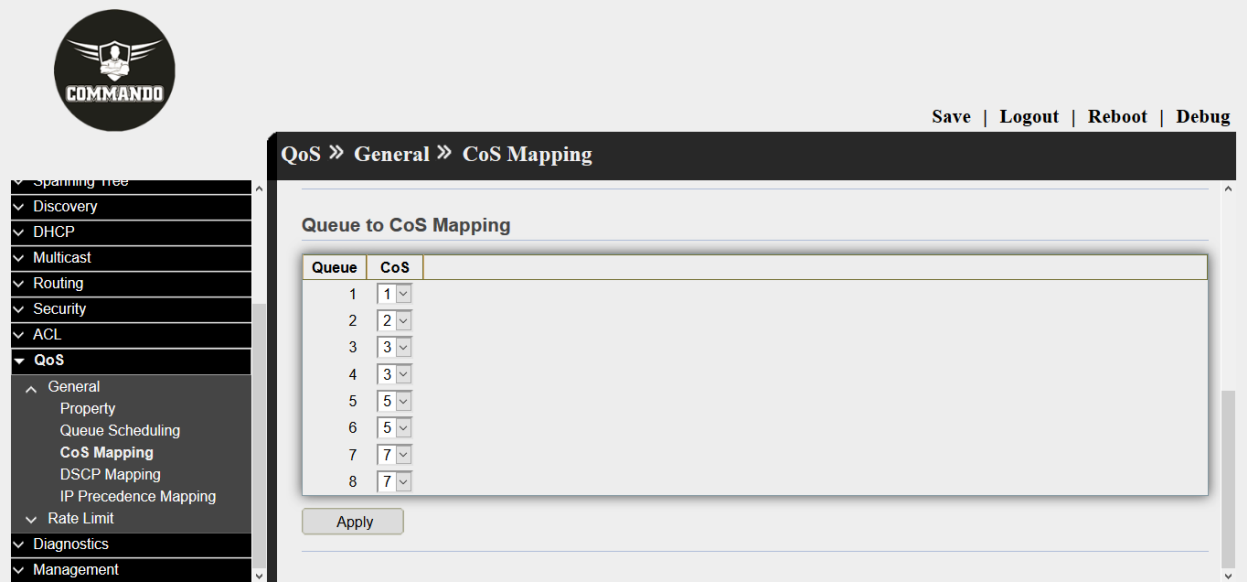


Fig 14.1.10 CoS to Queue Mapping Changing CoS values page

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.**

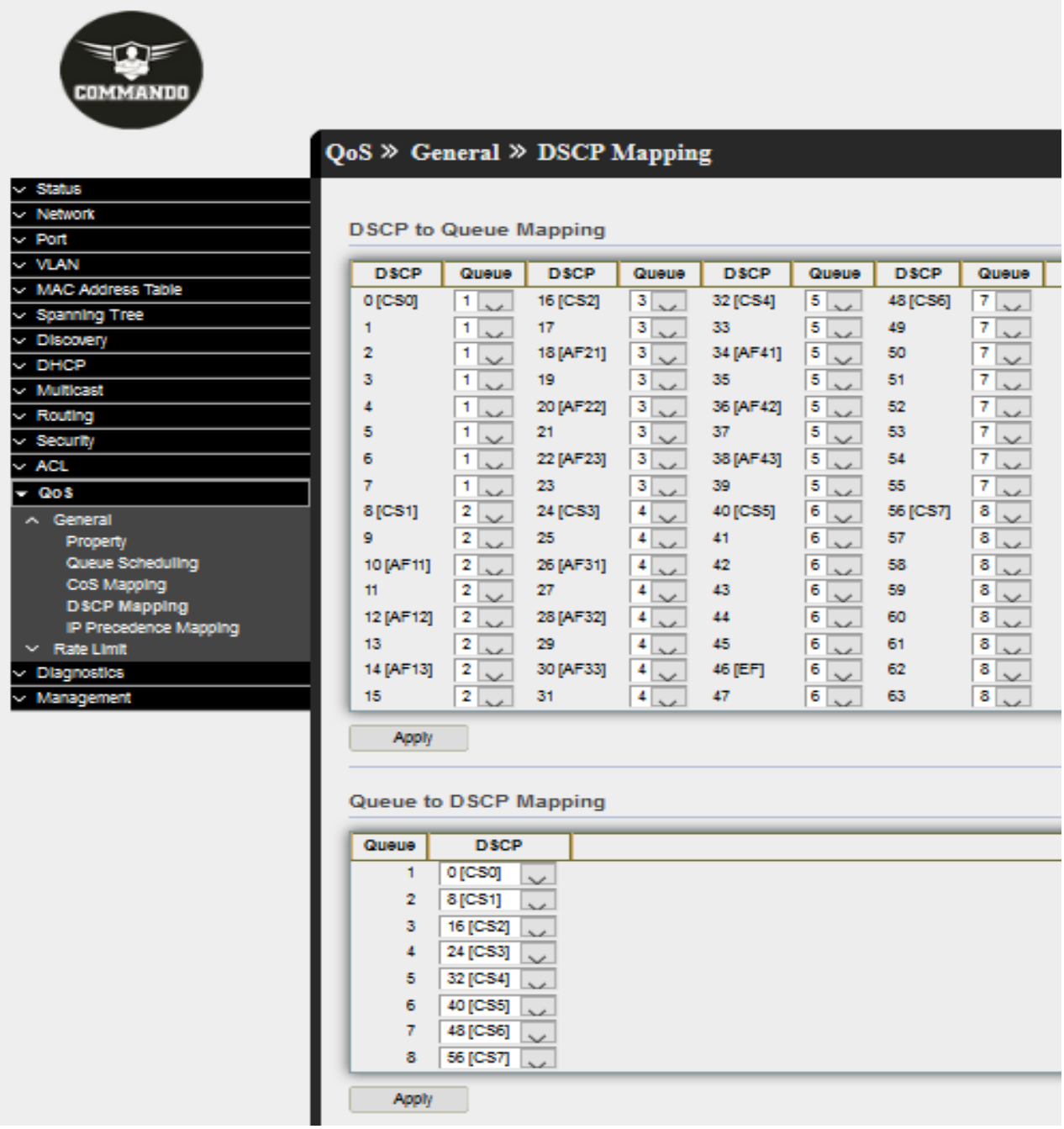


Fig 14.1.11 Default DSCP to Queue Mapping page

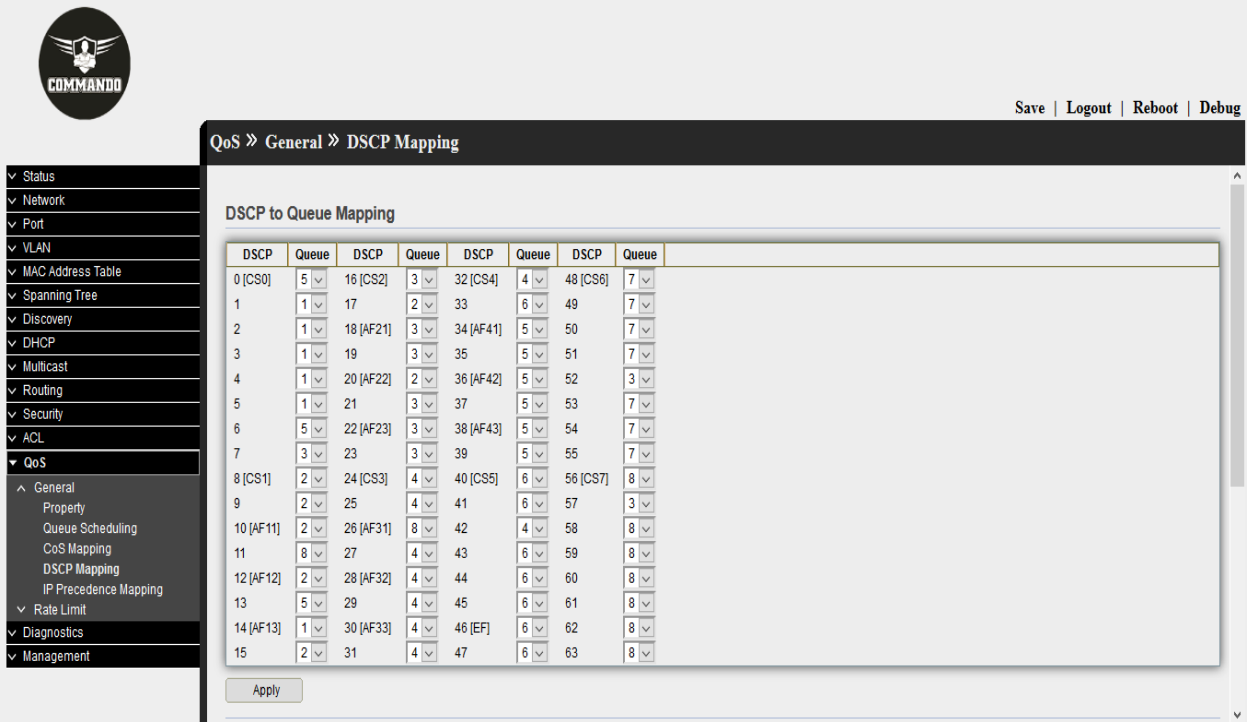


Fig 14.1.12 Changing DSCP to Queue Mapping page

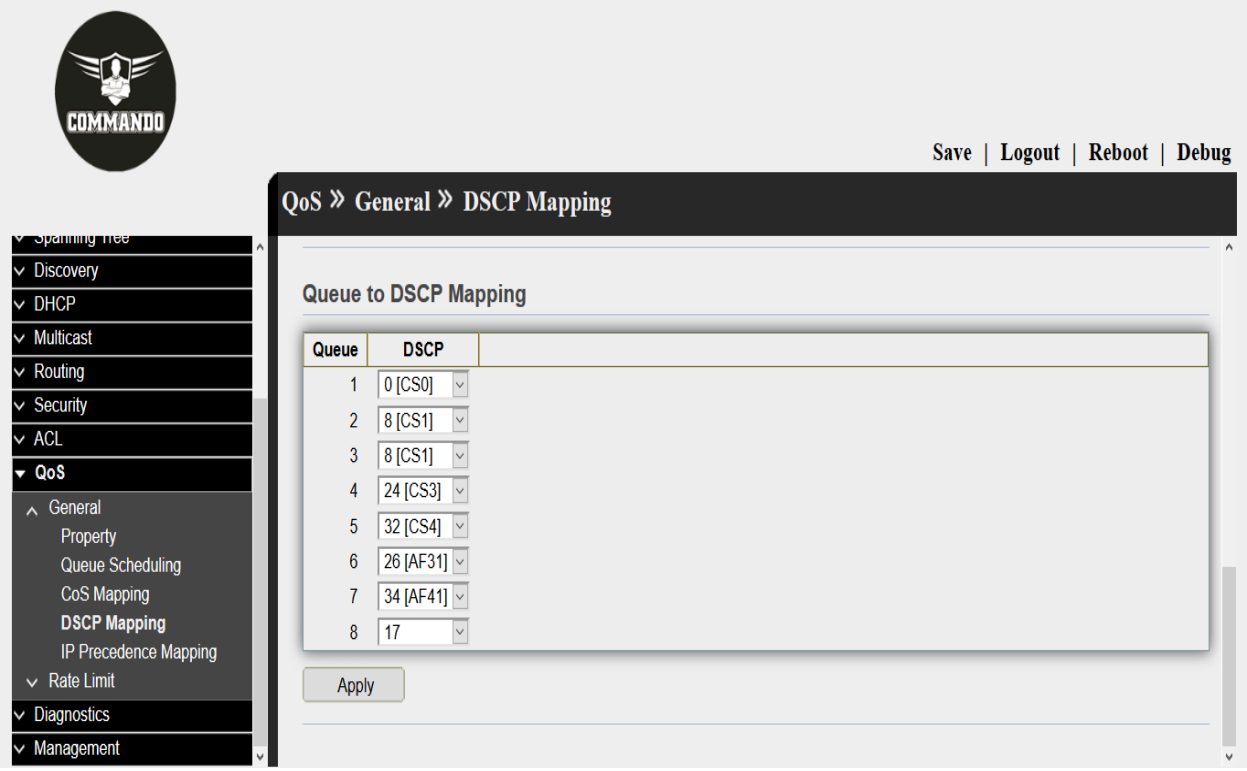


Fig 14.1.13 Changing Queue to DSCP Mapping page

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.**

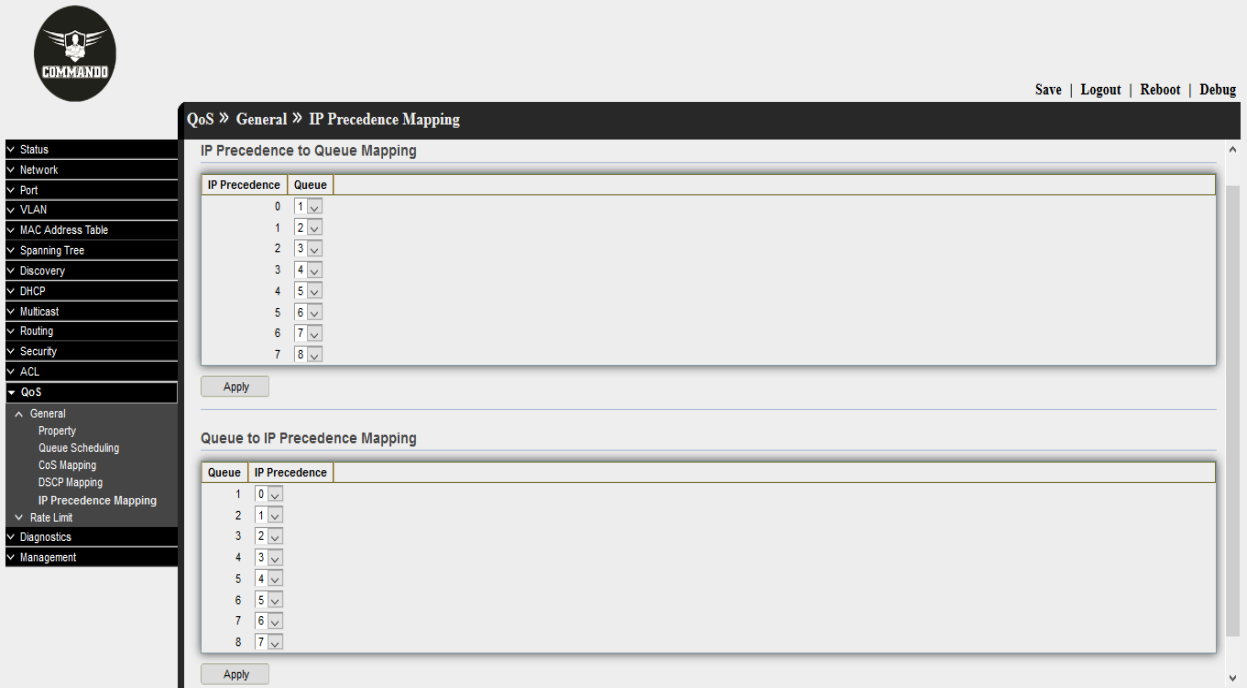


Fig 14.1.15 IP Precedance to queue Mapping page

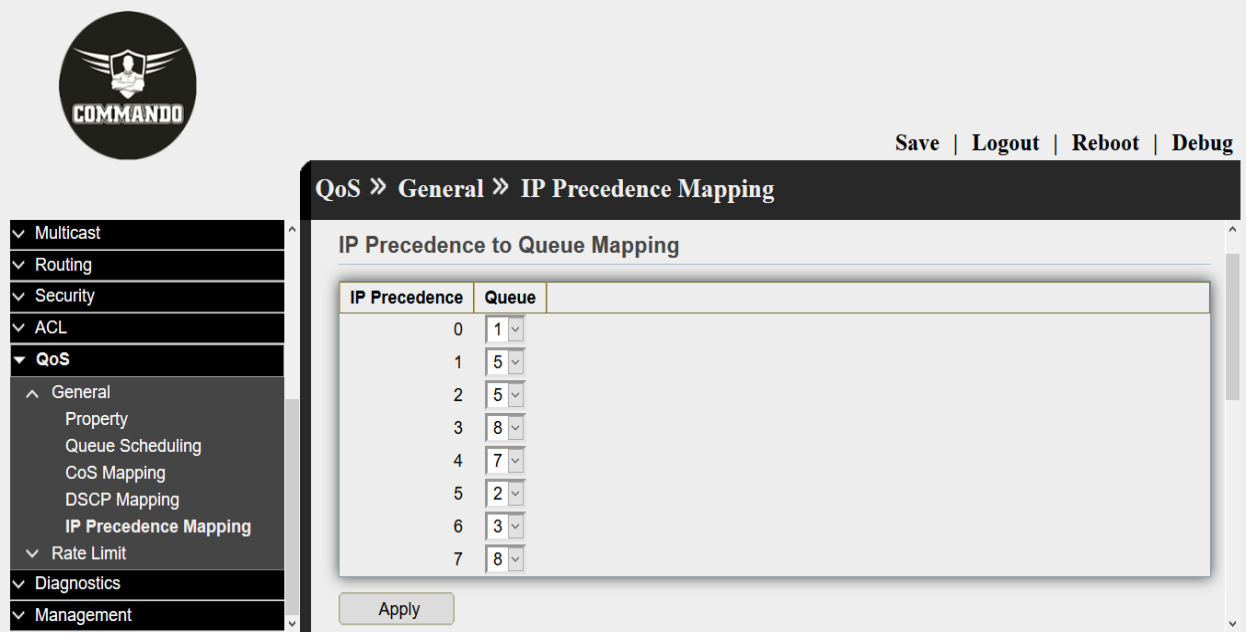


Fig 14.1.16 Changing IP Precedance to queue Mapping values page

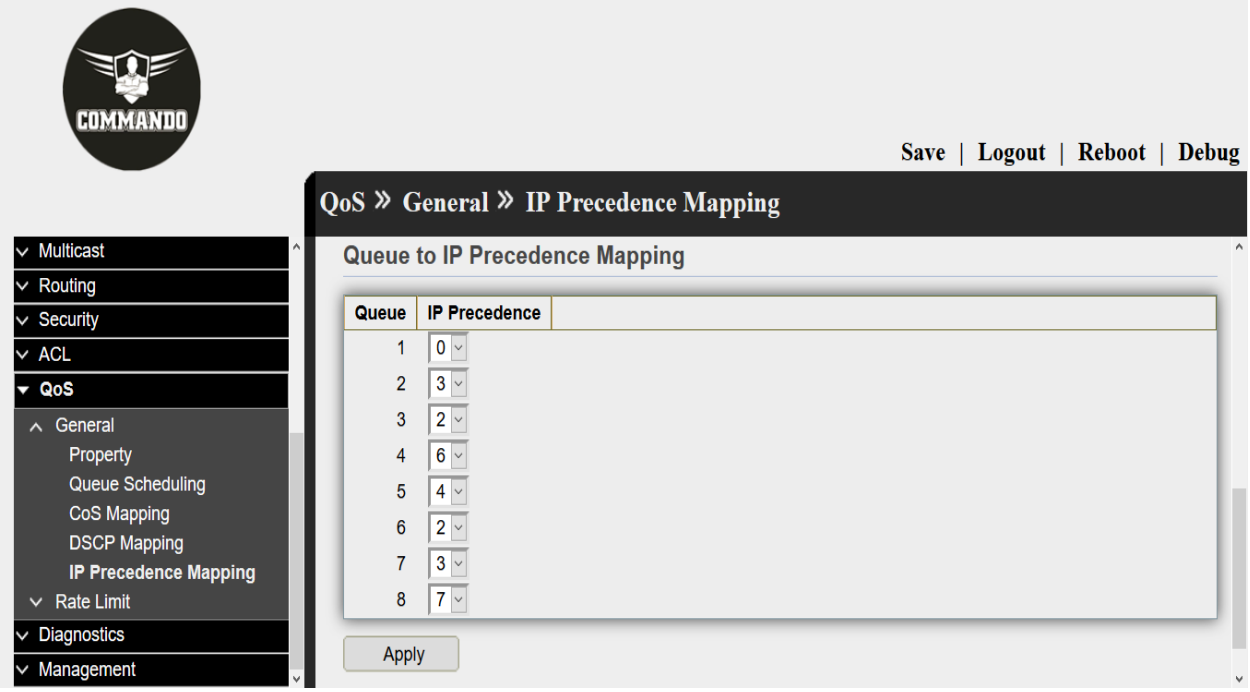


Fig 14.1.17 Changing Queue Mapping to IP Precedence values page

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.

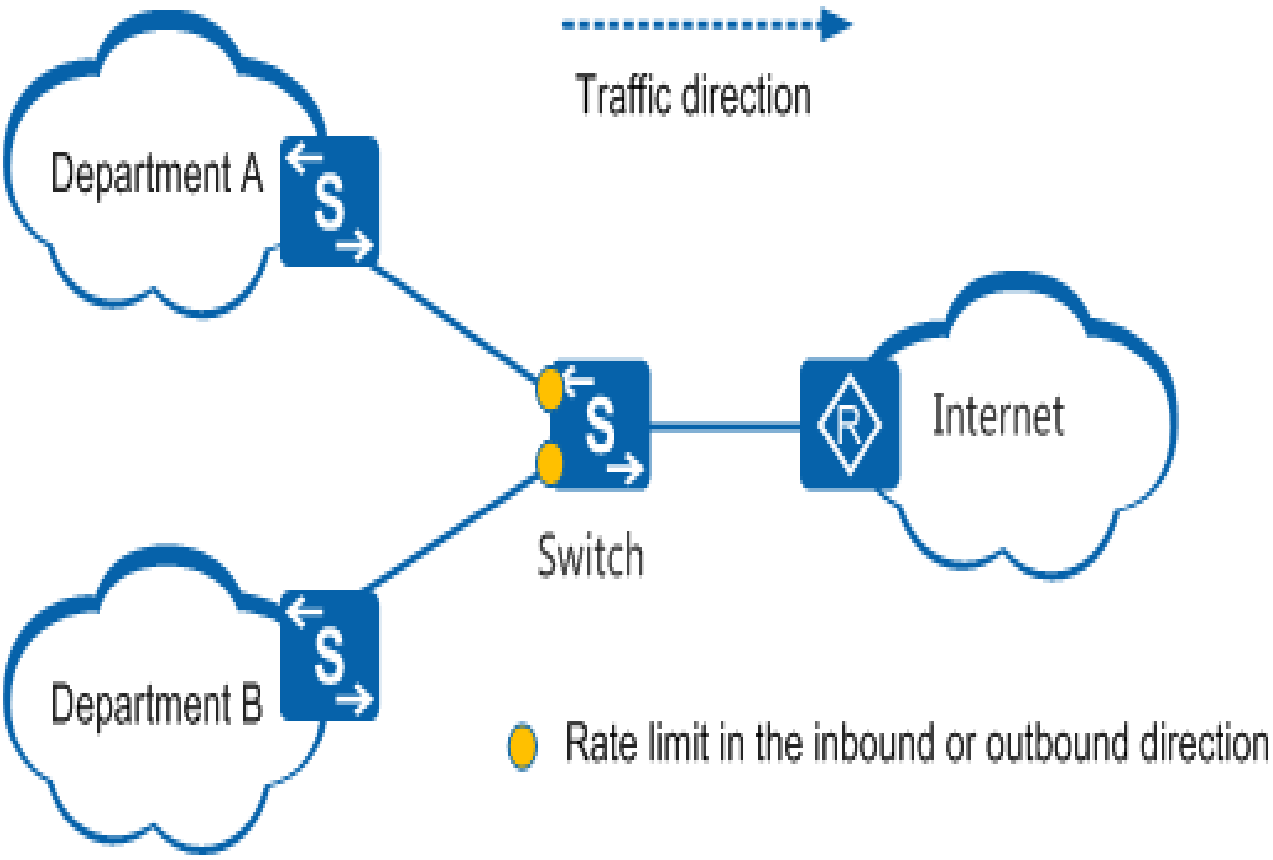


Fig 14.2.1 Rate Limiting concept

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.**

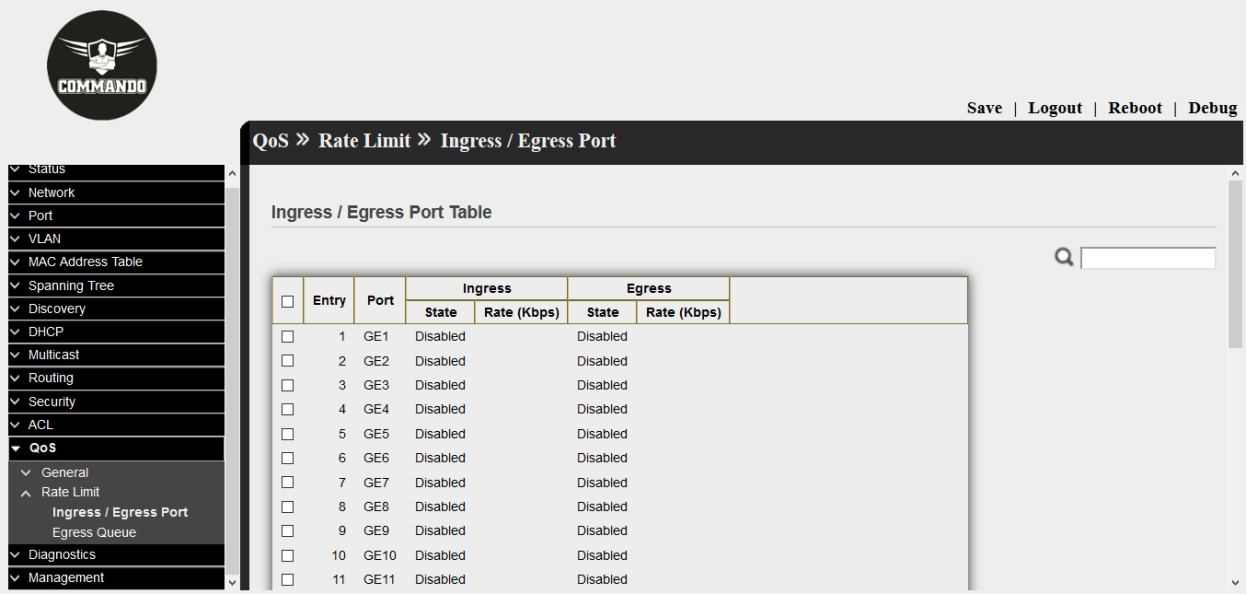


Fig 14.2.2 Ingress / Egress Port Table page

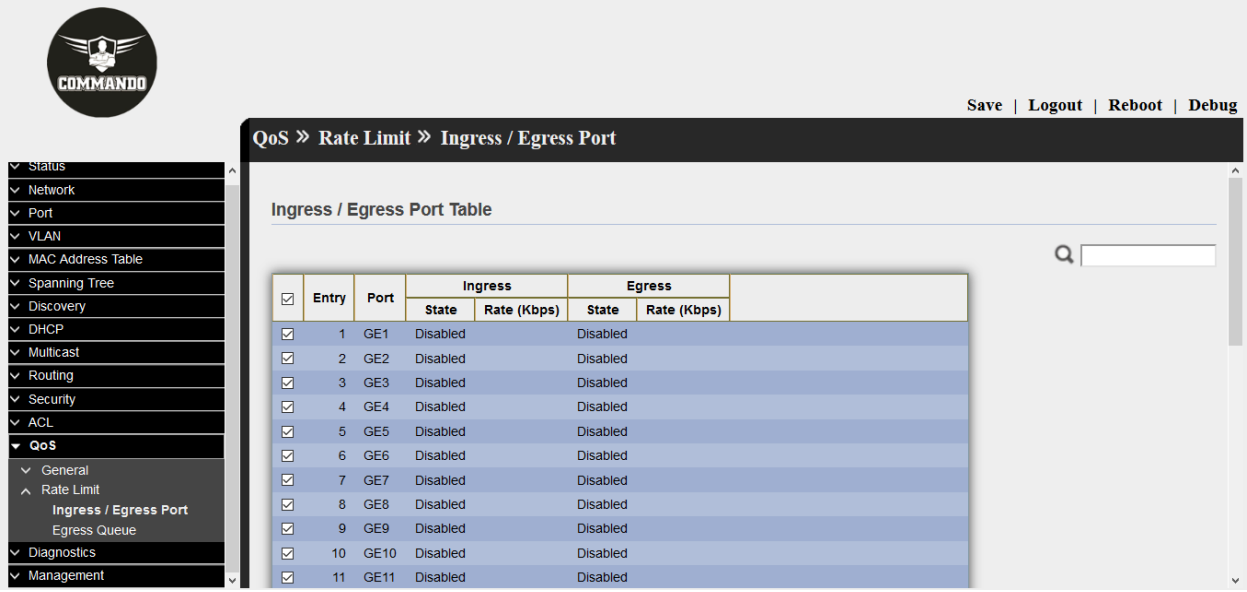


Fig 14.2.4 Selecting Ingress / Egress Port page

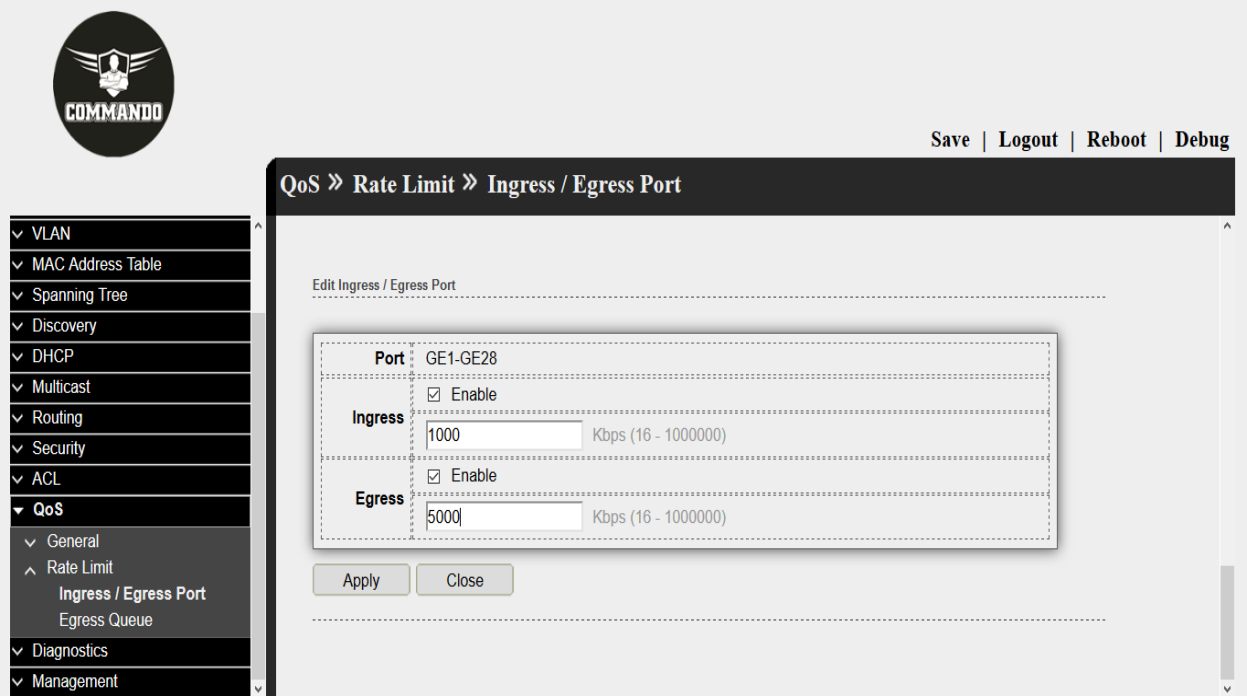


Fig 14.2.5 Edit Rate Ingress / Egress Port page

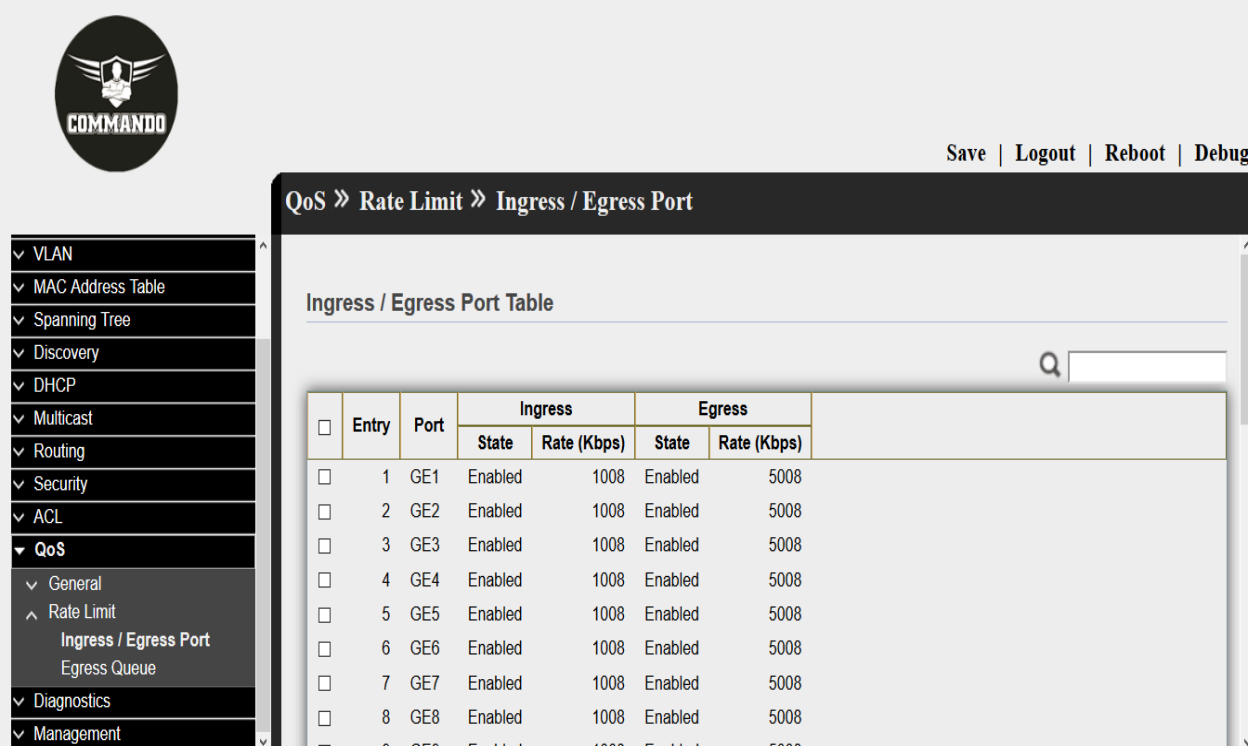


Fig 14.2.6 Selecting Ingress / Egress Port page

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.**

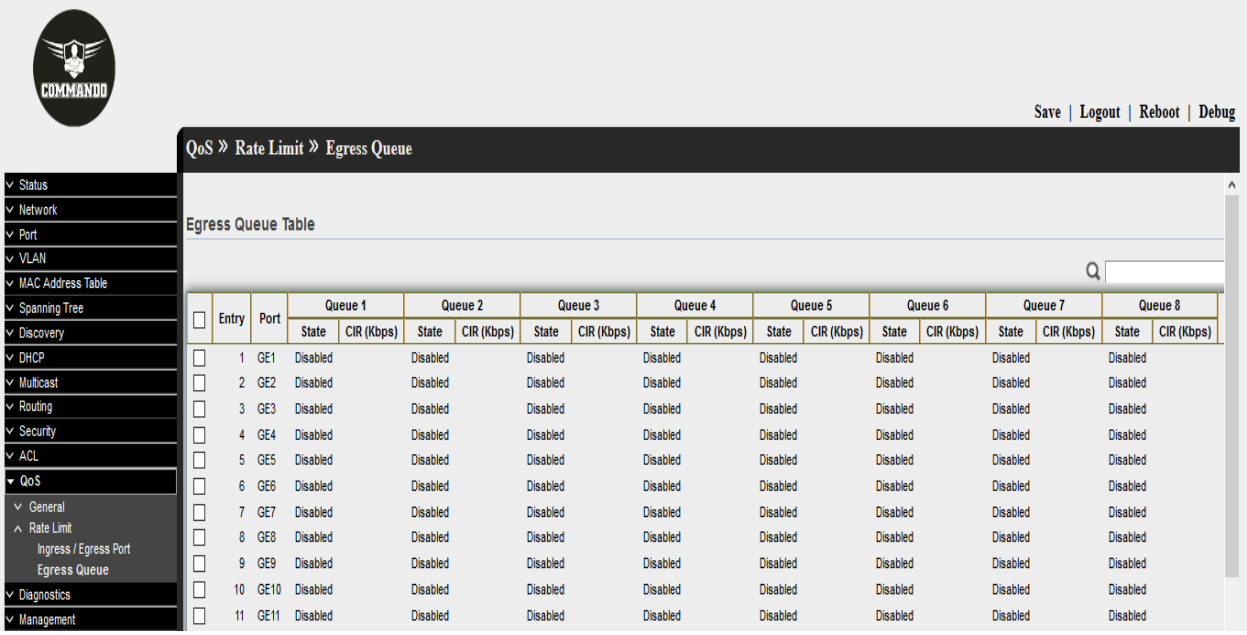


Fig 14.2.7 Default Egress Queue Table page

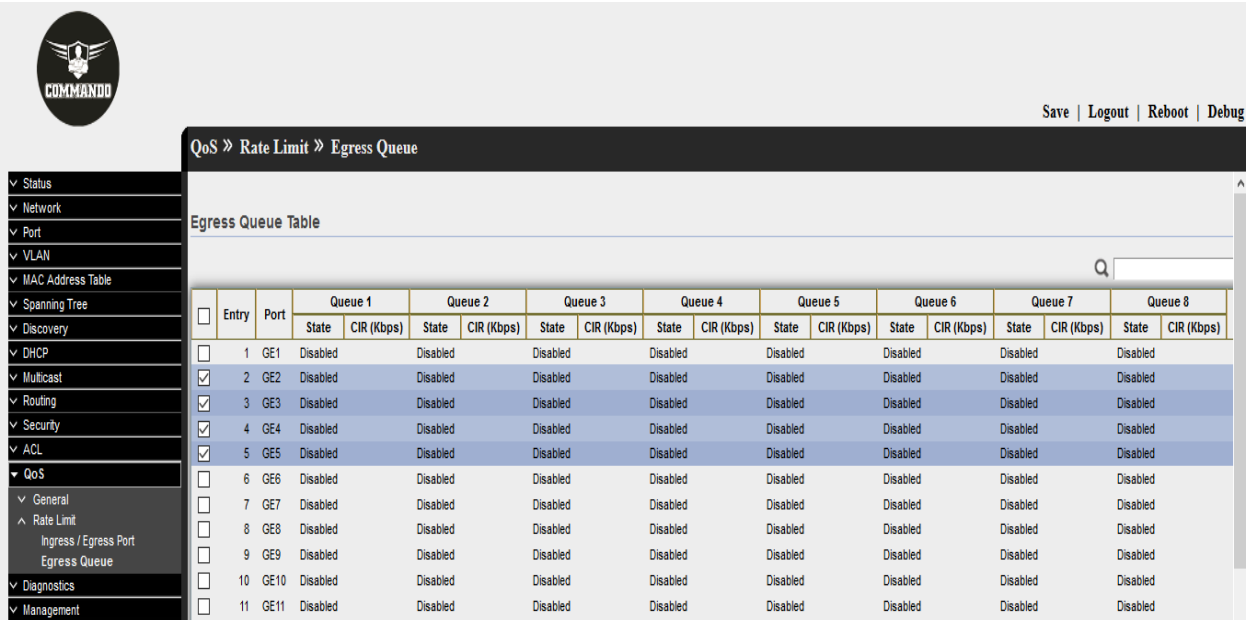


Fig 14.2.8 Selecting Egress Queue ports page

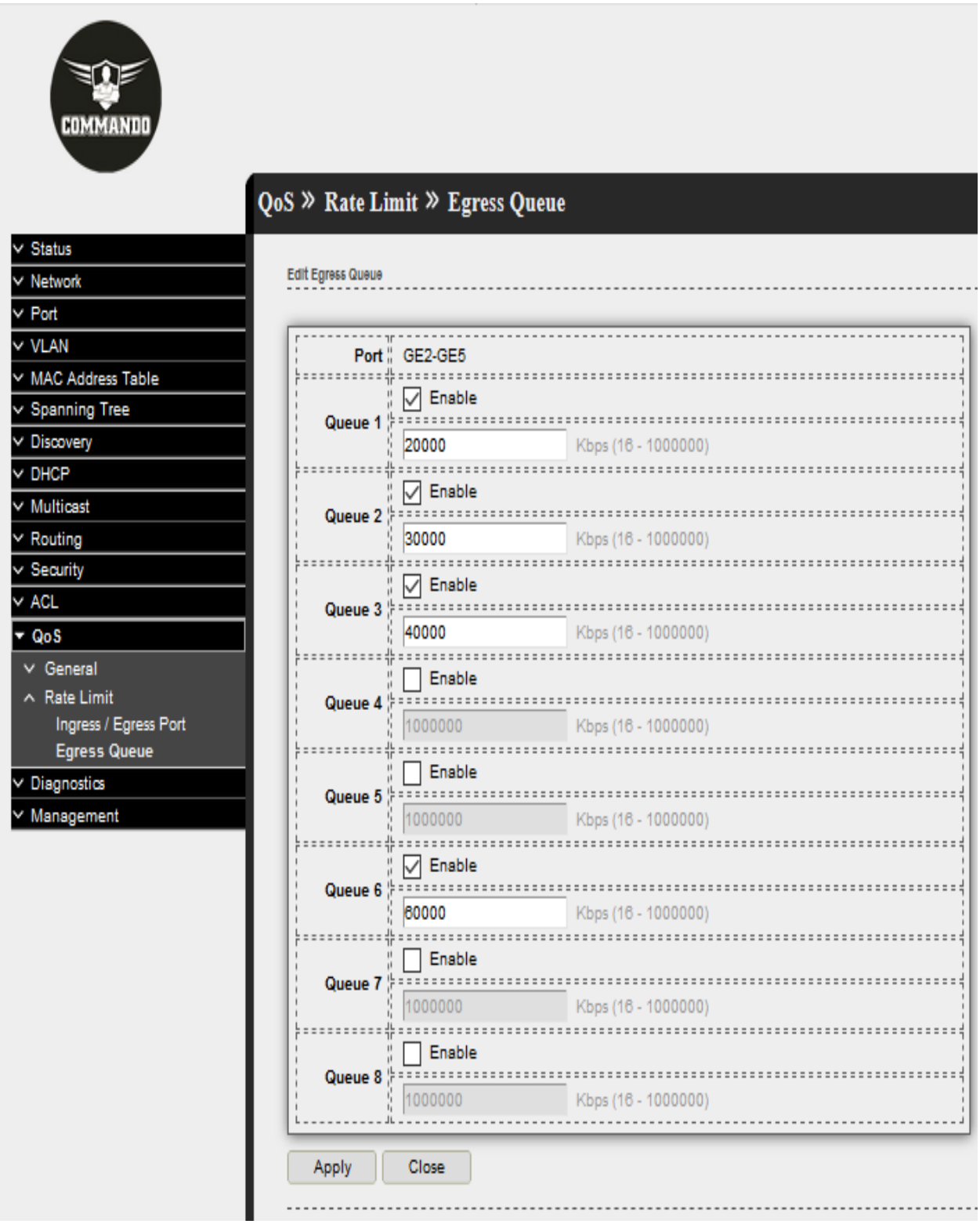


Fig 14.2.9 Edit Egress Queue page

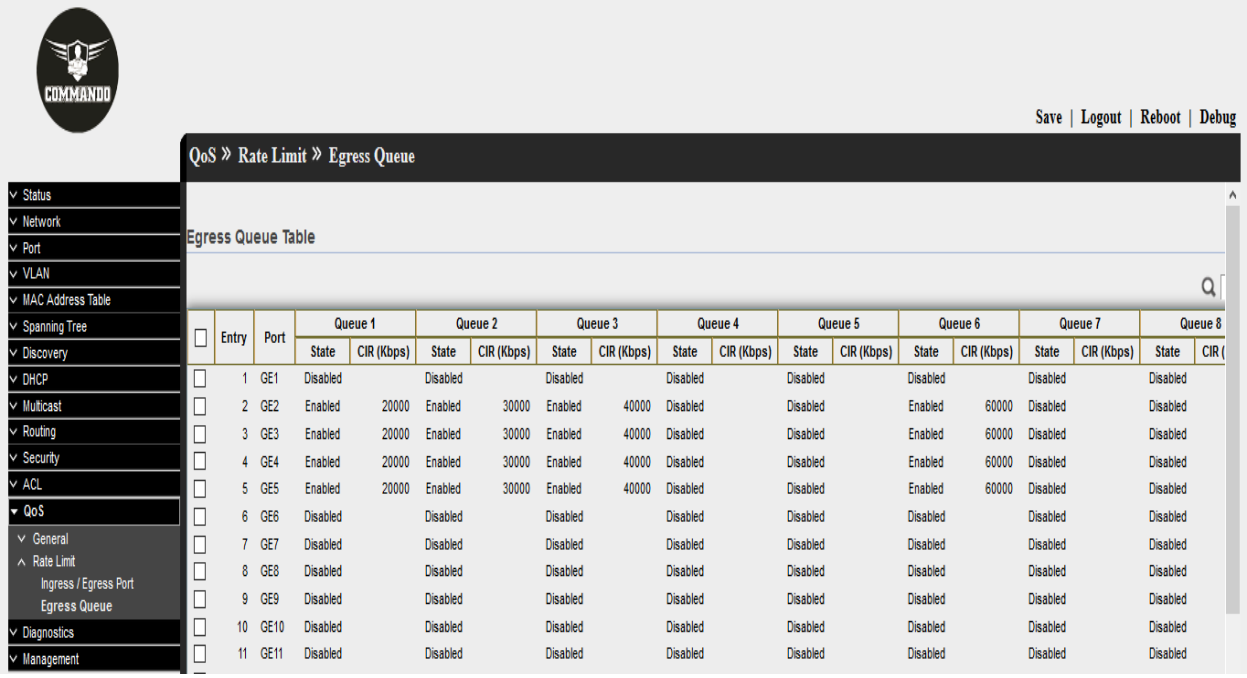


Fig 14.2.10 Egress Queue Table after Editing Queue page

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) your each node has passed to reach the tested host, and measure transit delays of packets across entire path to 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 also 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 C2000 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.

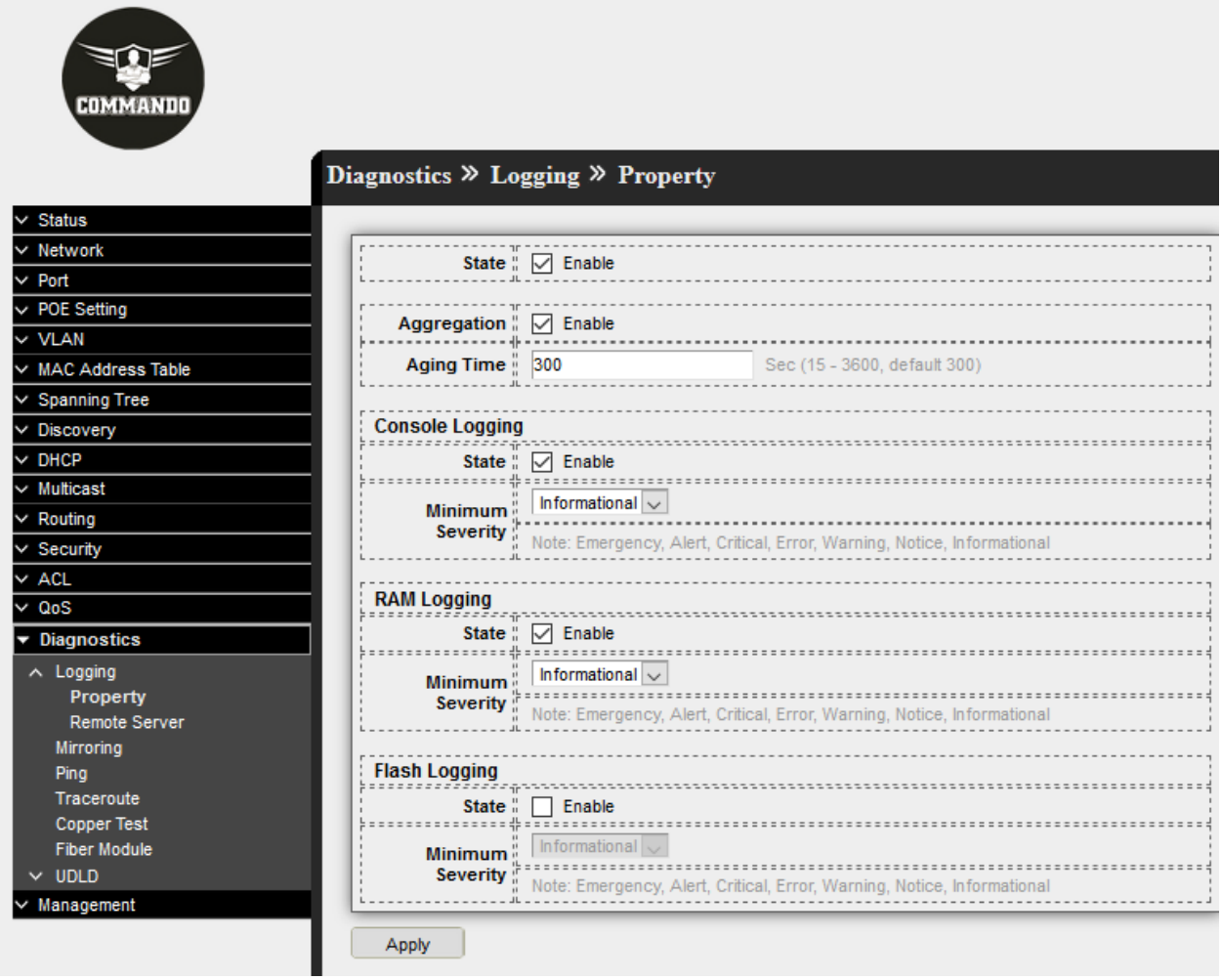


Fig 15.1.1 Diagnostic Logging Property page

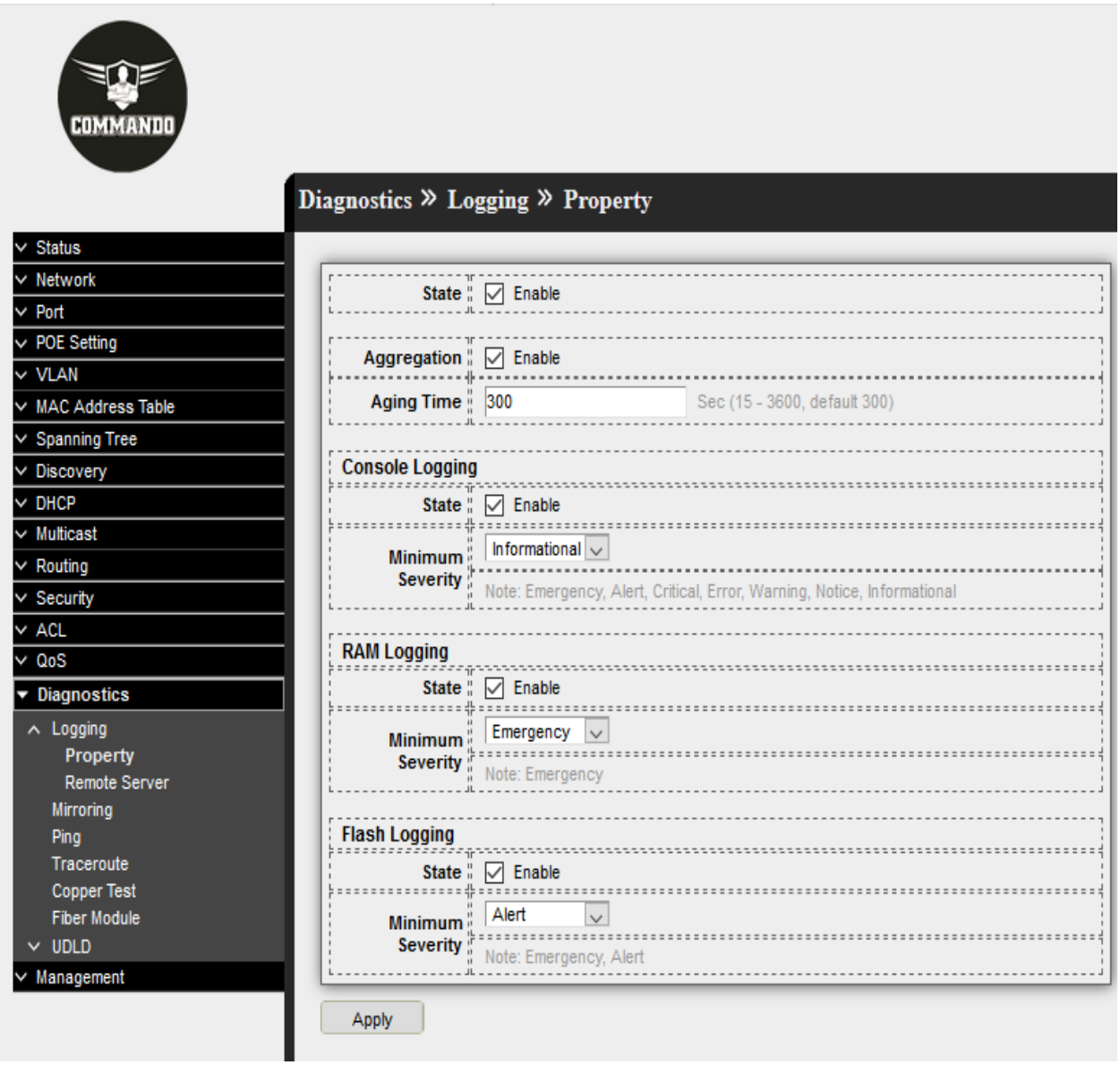


Fig 15.1.2 Changing Diagnostic Logging Property options page

15.1.2 Remote Server

To configure the remote logging server, click **Diagnostic >> Logging >> Remote Server.**

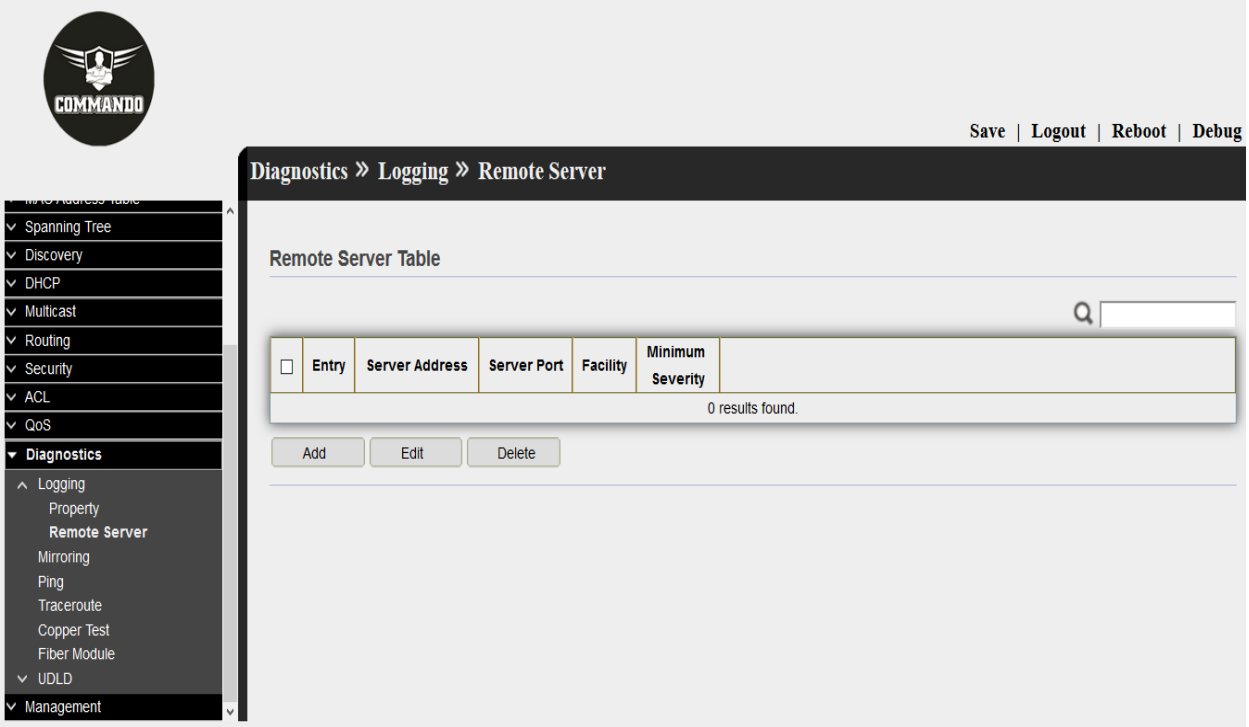


Fig 15.1.3 Diagnostic Logging Deafult remote server page

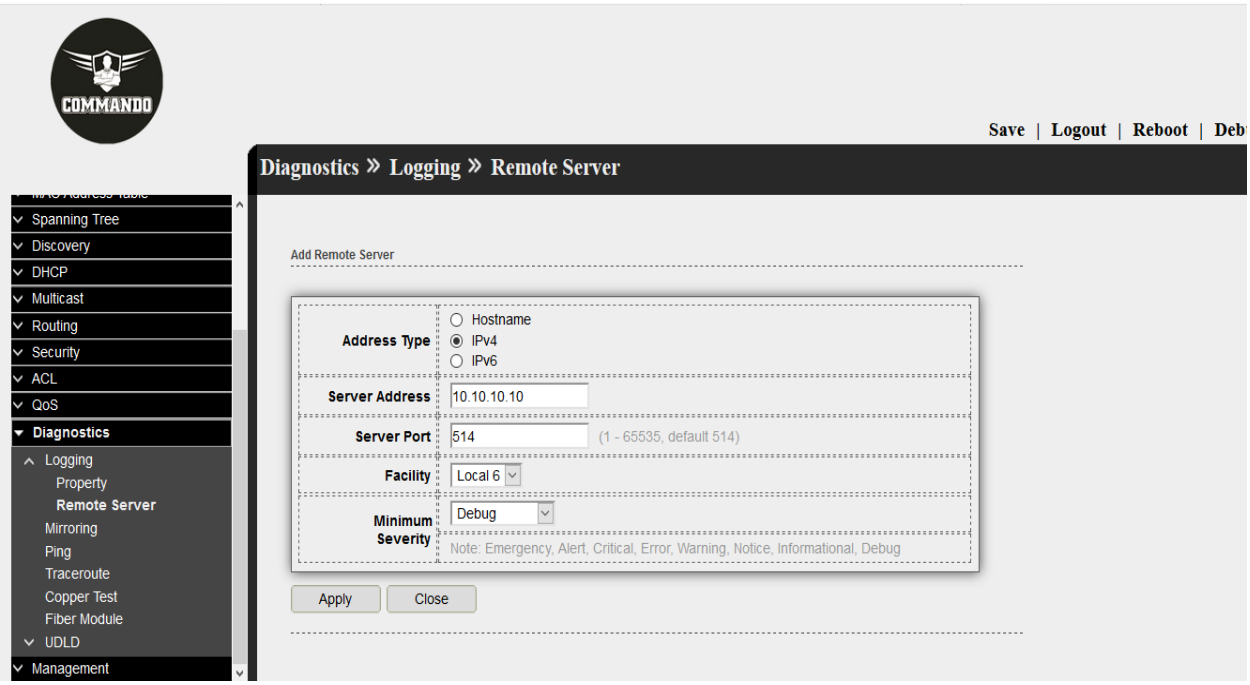


Fig 15.1.4 Diagnostic Logging Add remote server page

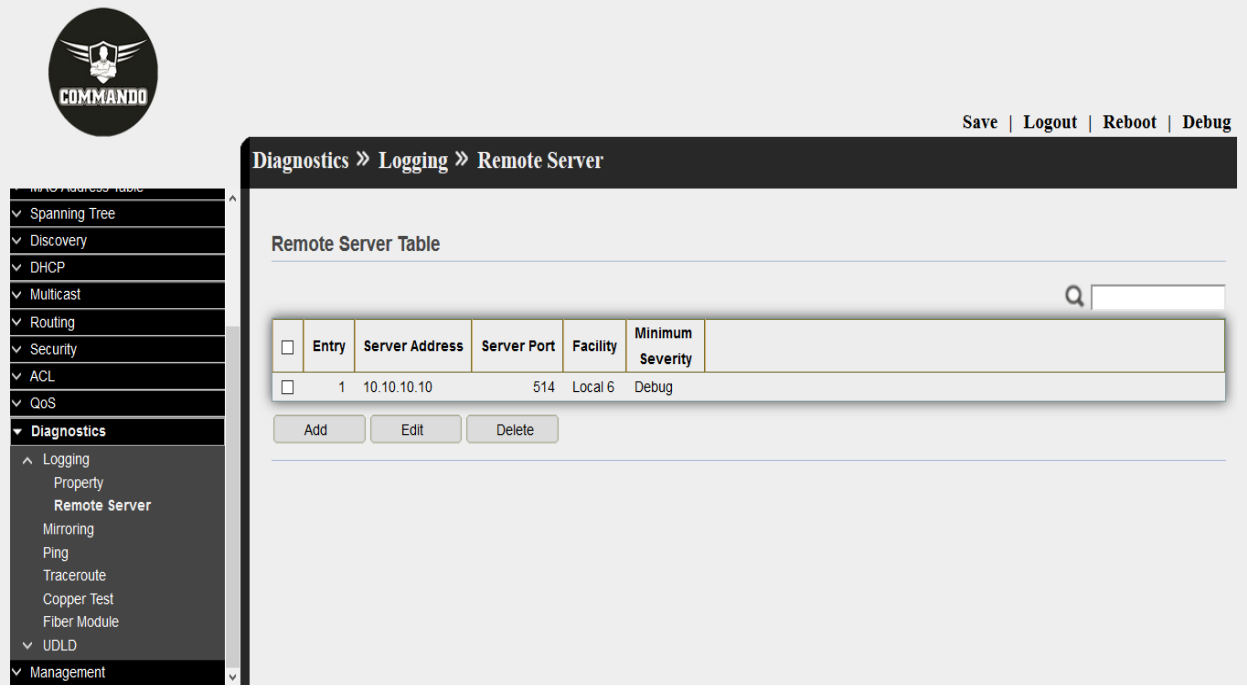


Fig 15.1.5 Diagnostic Logging remote server Table page

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.**

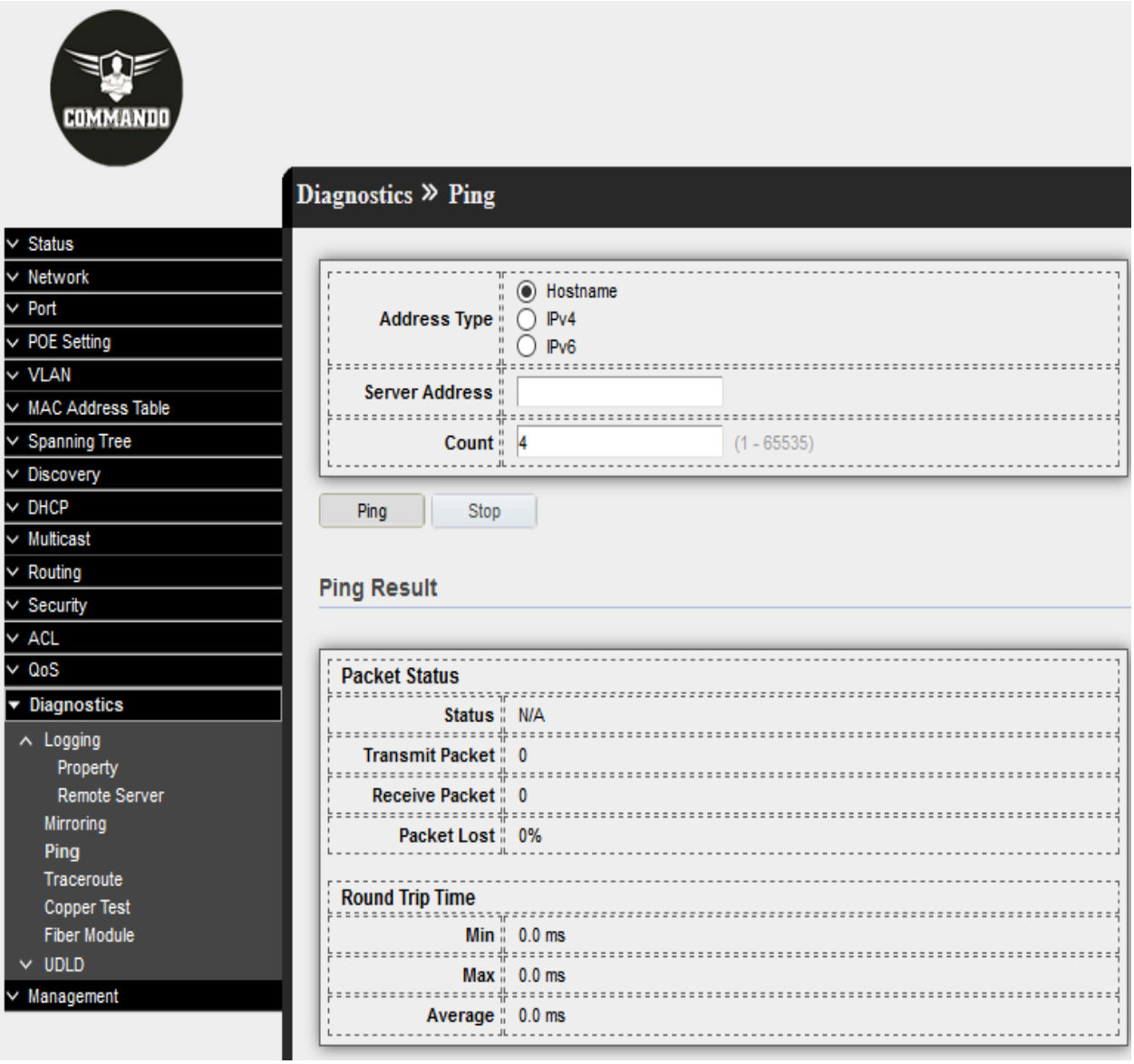


Fig 15.2.1 Diagnostic Default Ping test page

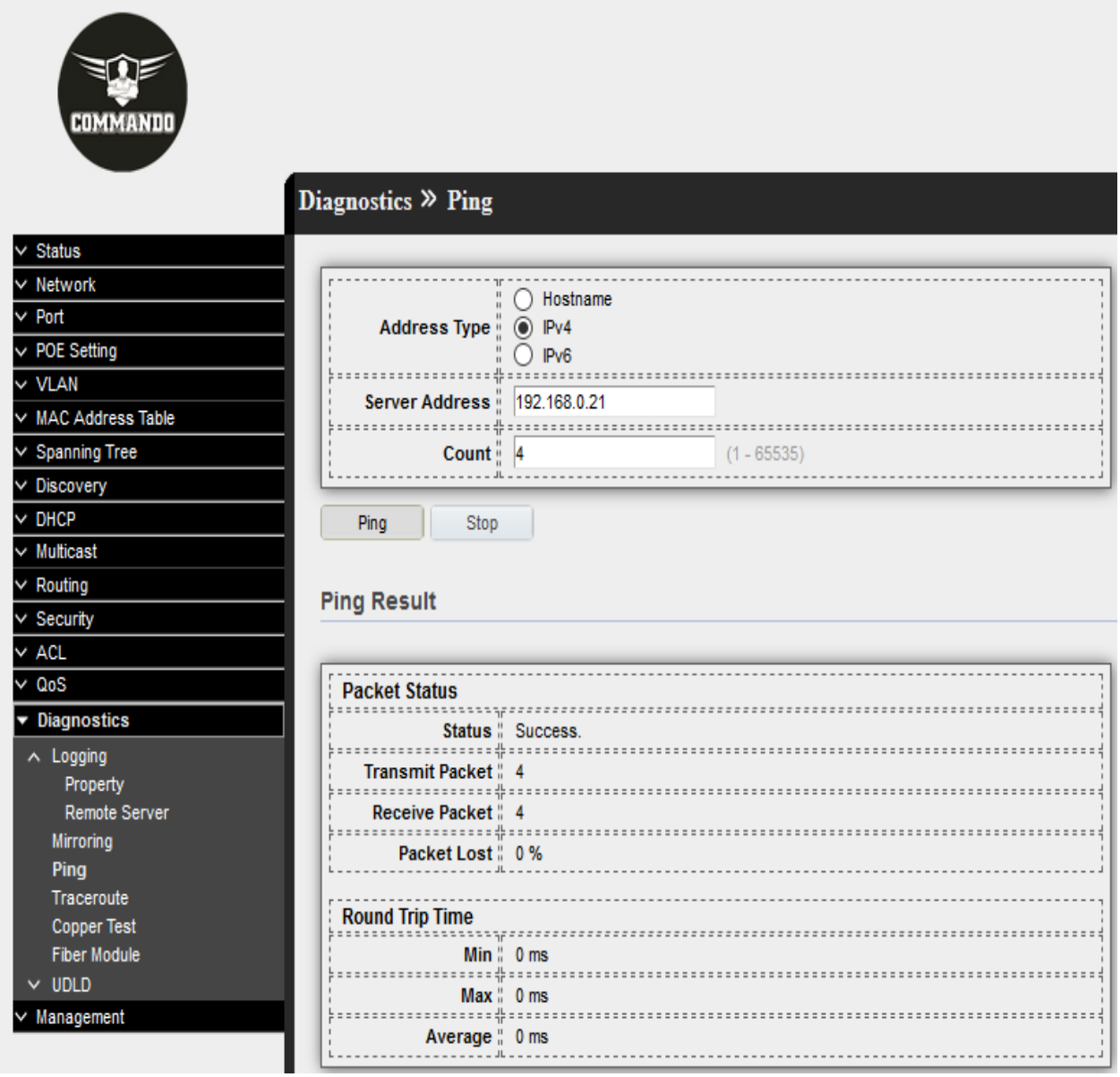


Fig 15.2.2 Diagnostic Ping test result page

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.**

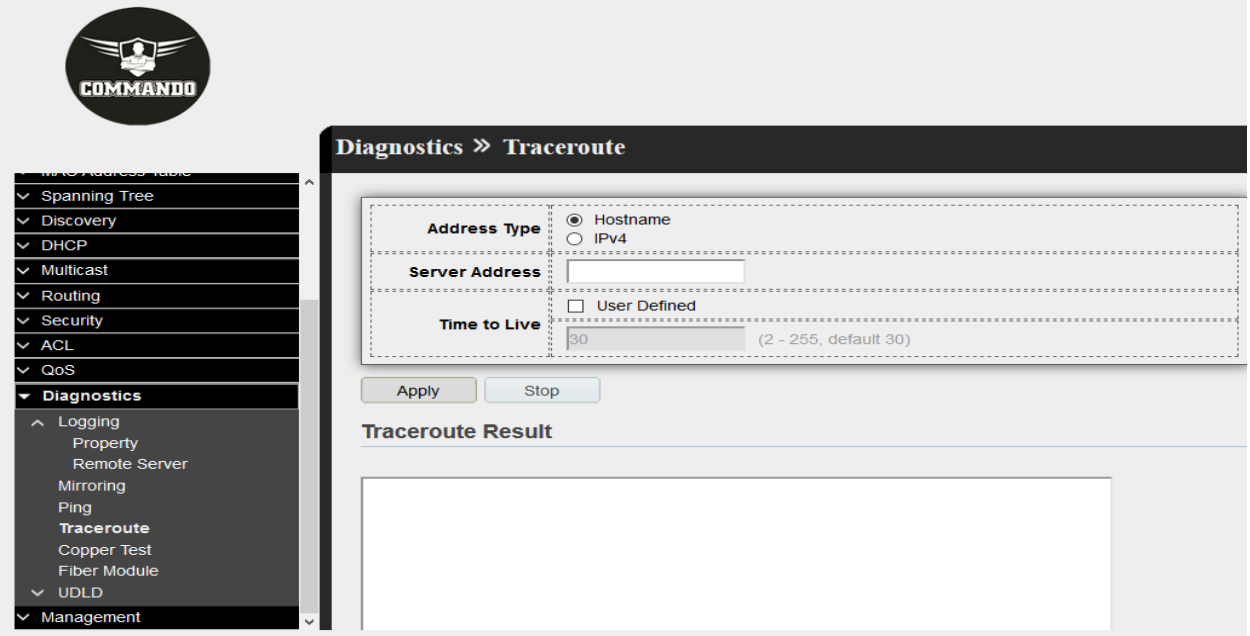


Fig 15.3.1 Diagnostic Traceroute Default test page

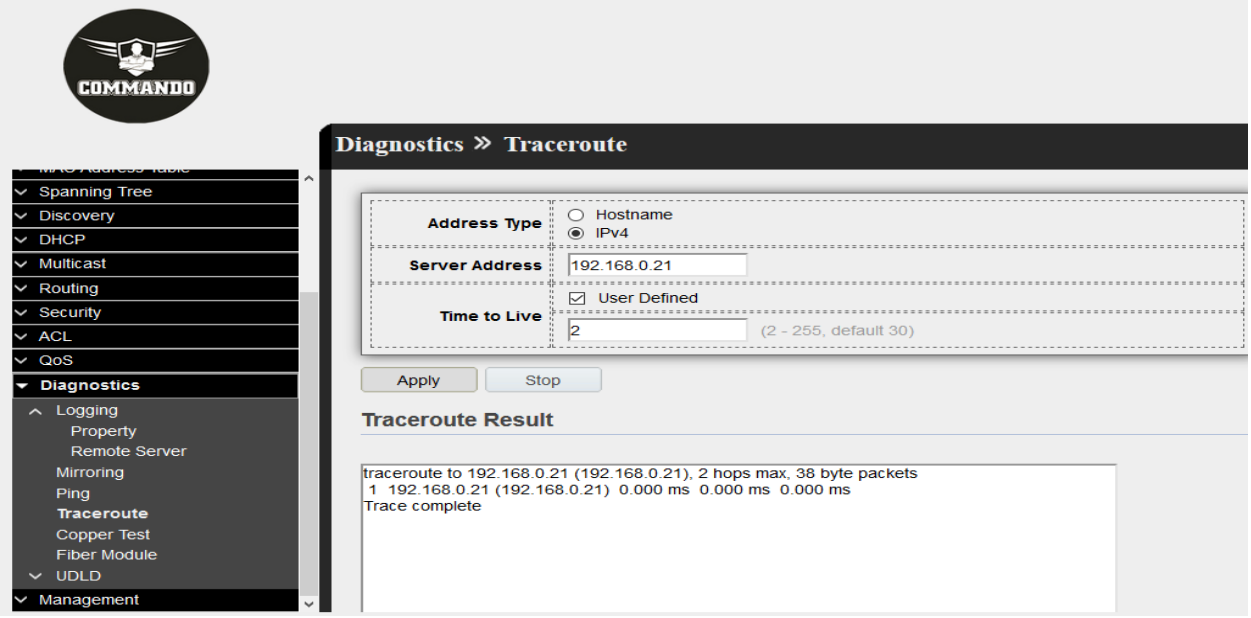
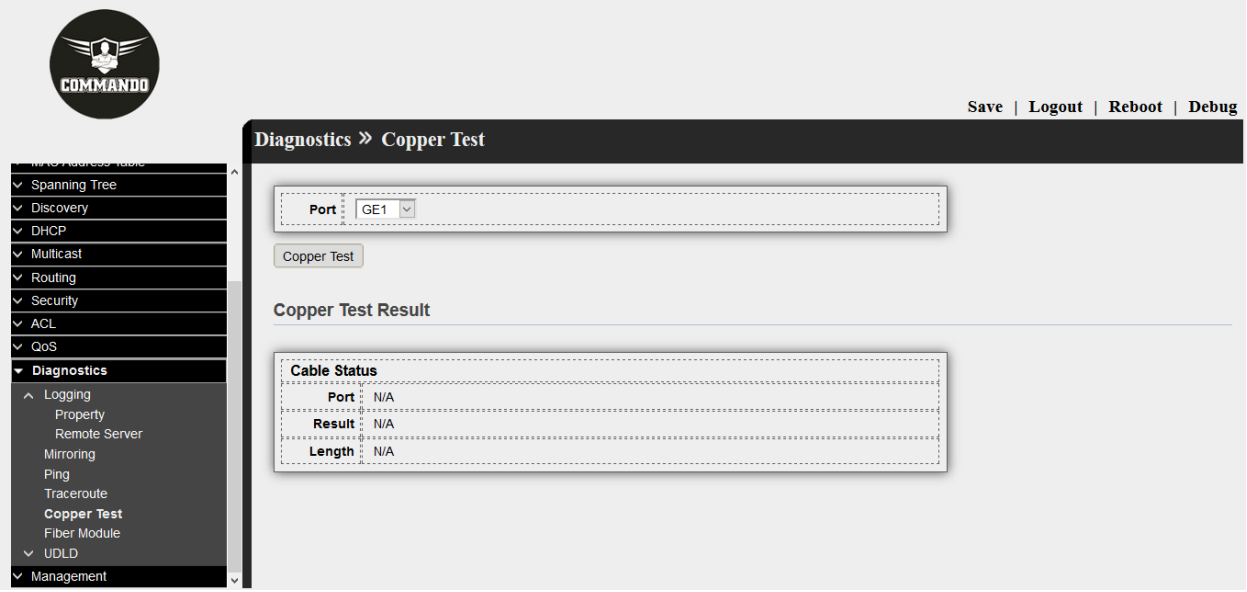


Fig 15.3.2 Diagnostic Traceroute test page

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 also 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.**



15.4.1 Diagnostic Default Copper Test Result page

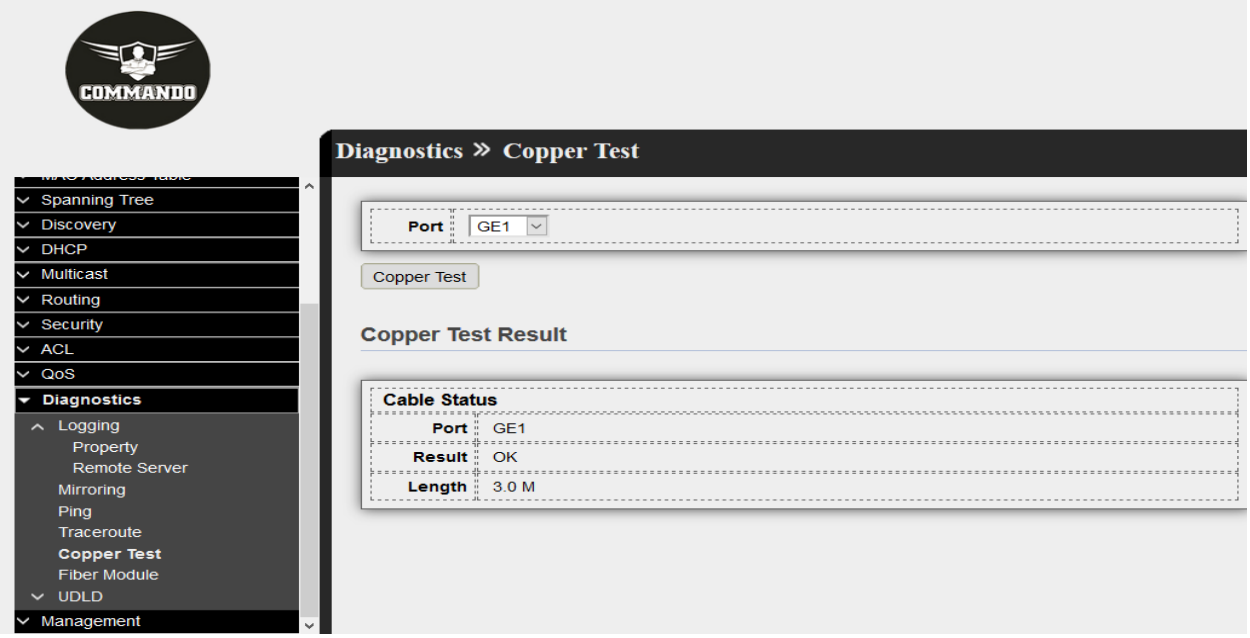


Fig 15.4.2 Diagnostic Copper Test Result page

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.**

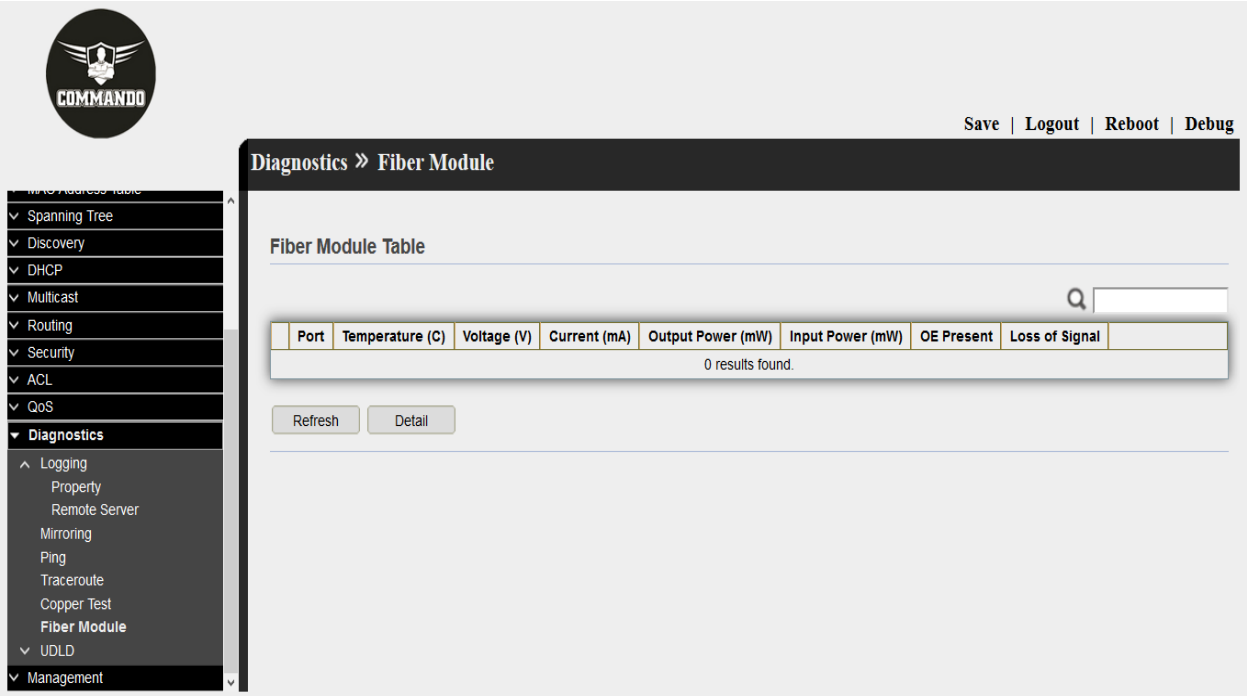


Fig 15.5.1 Diagnostic Default Fiber Module Table page

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.**

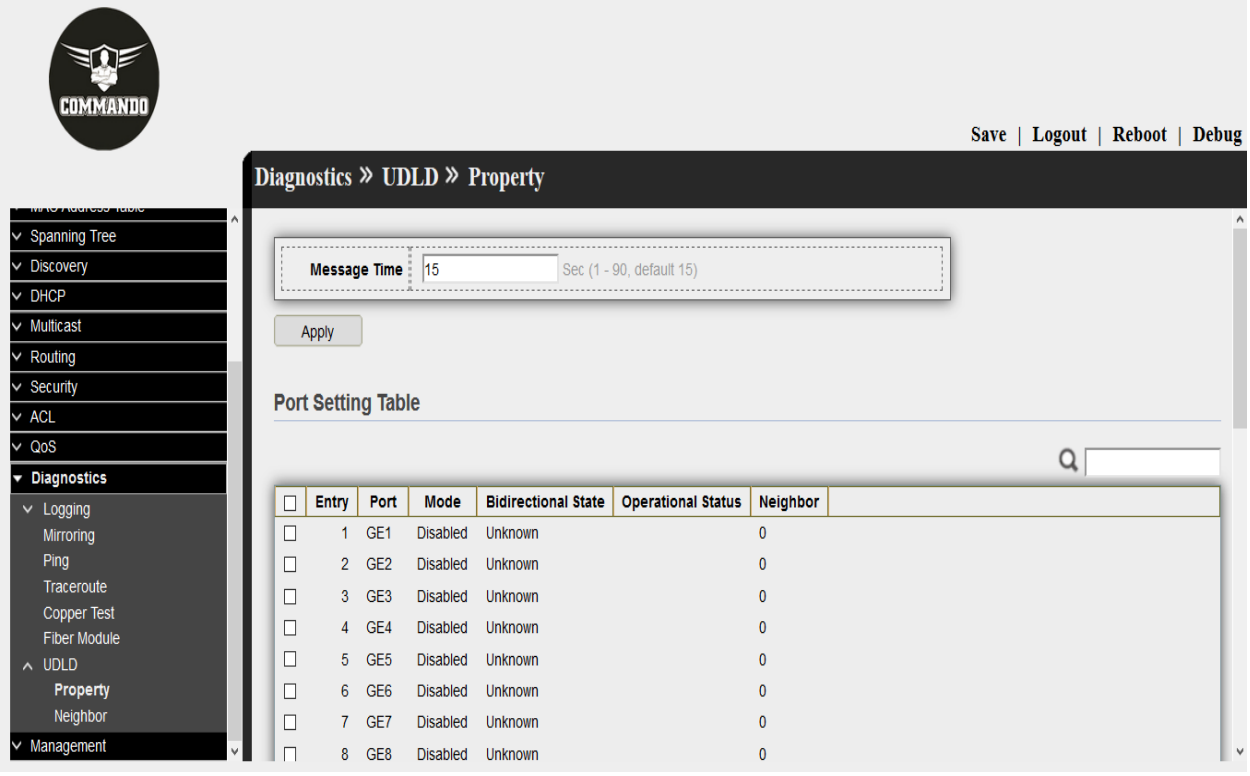


Fig 15.6.1 UDLD Default Port Setting Table page

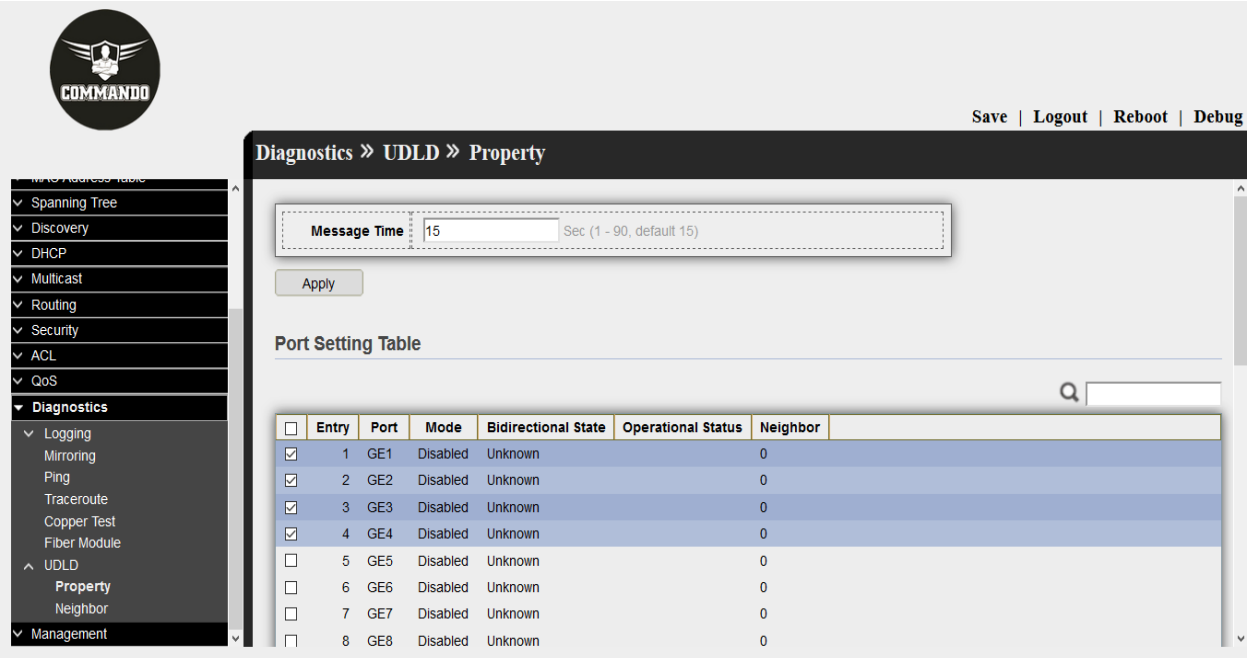


Fig 15.6.2 UDLD Port selection page

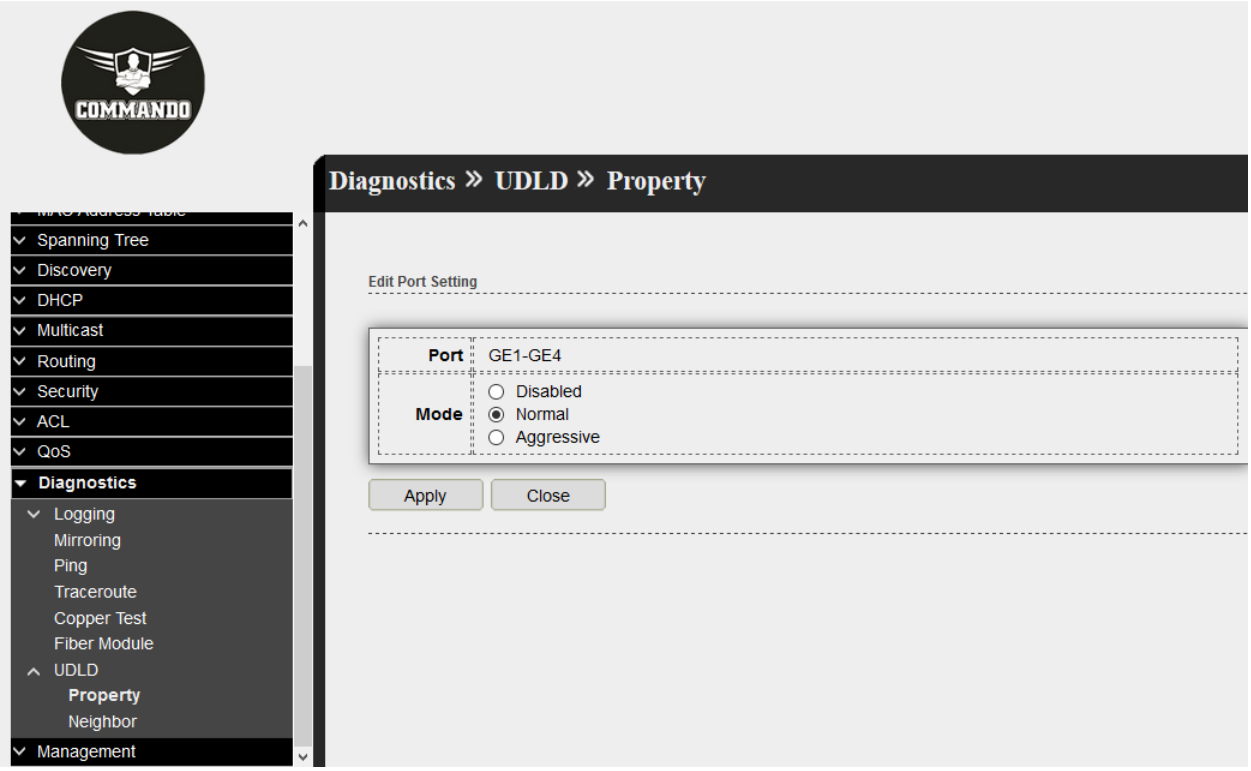


Fig 15.6.3 UDLD Edit Port Setting page

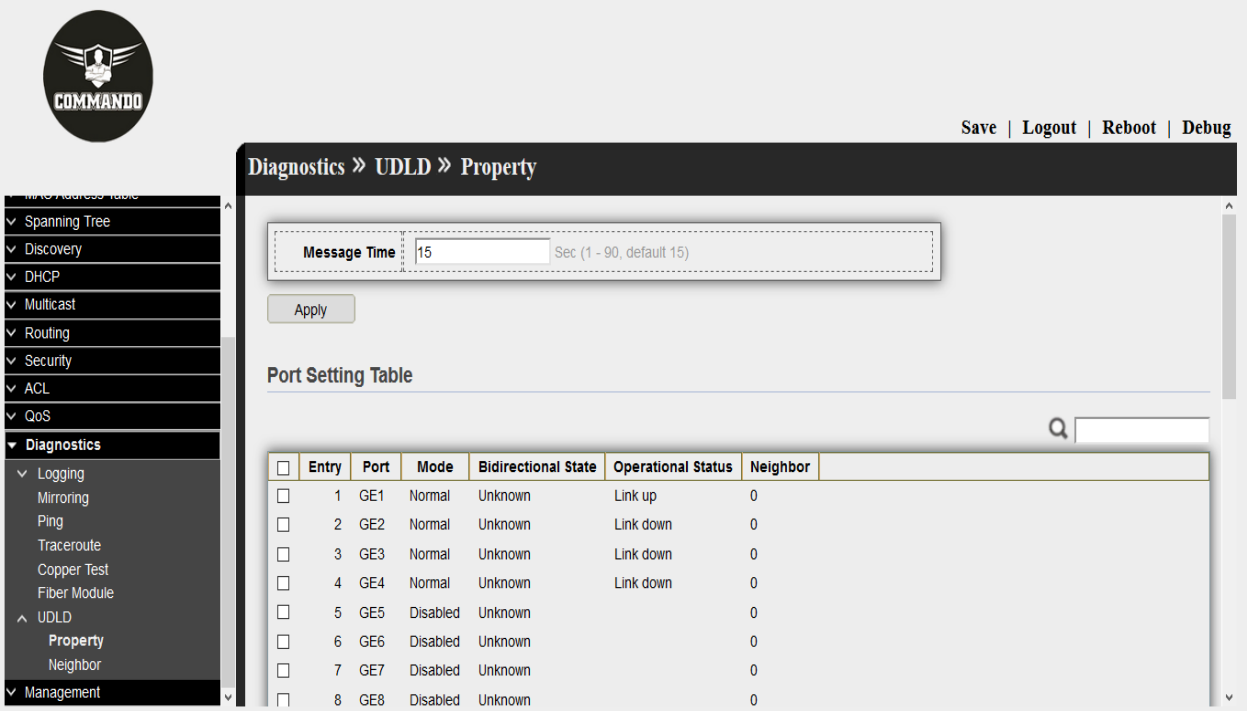


Fig 15.6.4 UDLD Port Setting Table page

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**

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 describes 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 packets.

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: C2000 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 user name 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 an RMON history entry for an interface to gather information about network traffic within that interface.

Event: An 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: An 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 shows tools like SNMP, RMON, Firmware upgrade, user account, save configuration, Alarm, Notification details. To upgrade firmware, User can upgrade firmware thought 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.

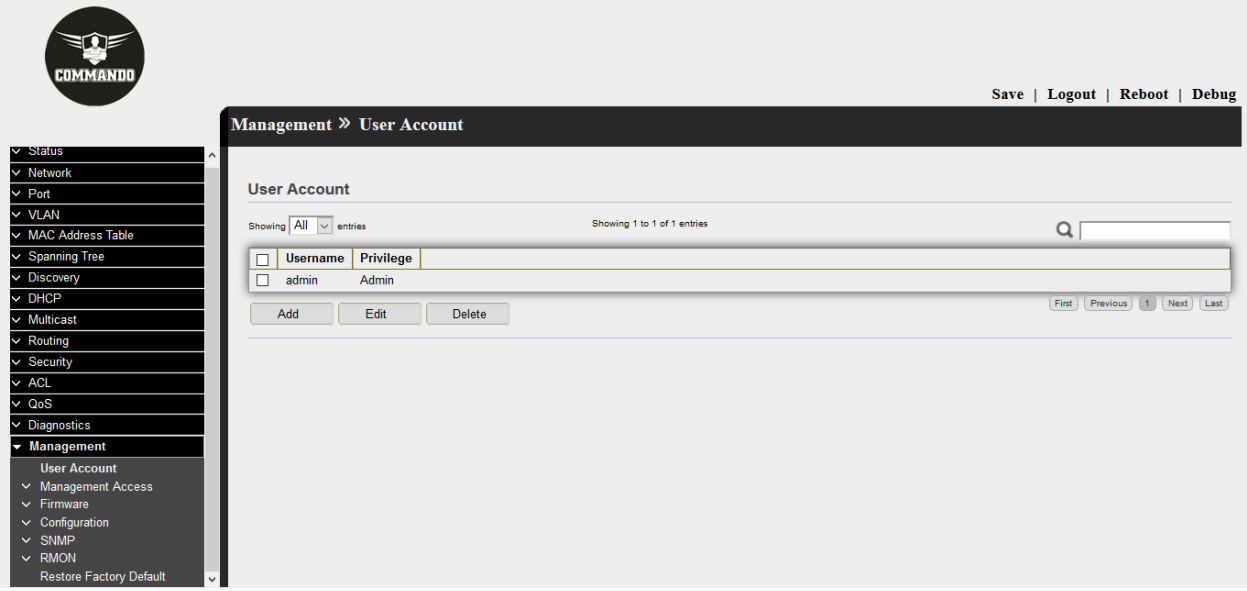


Fig 16.1.1 Default User Account page

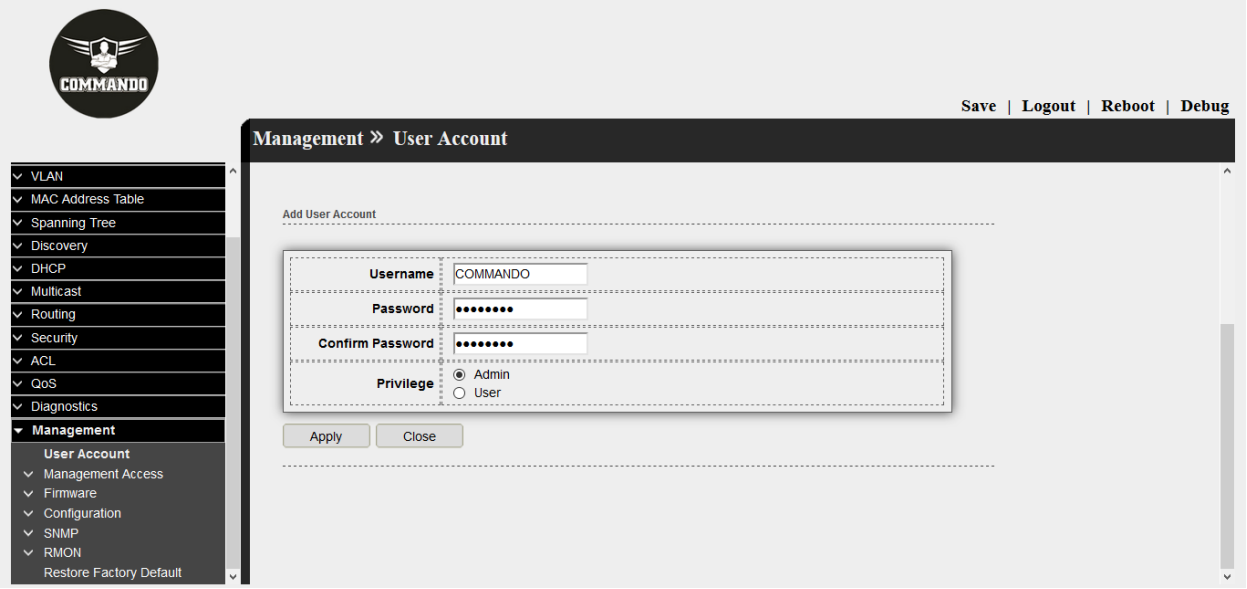


Fig 16.1.2 Add User Account having all privilege page

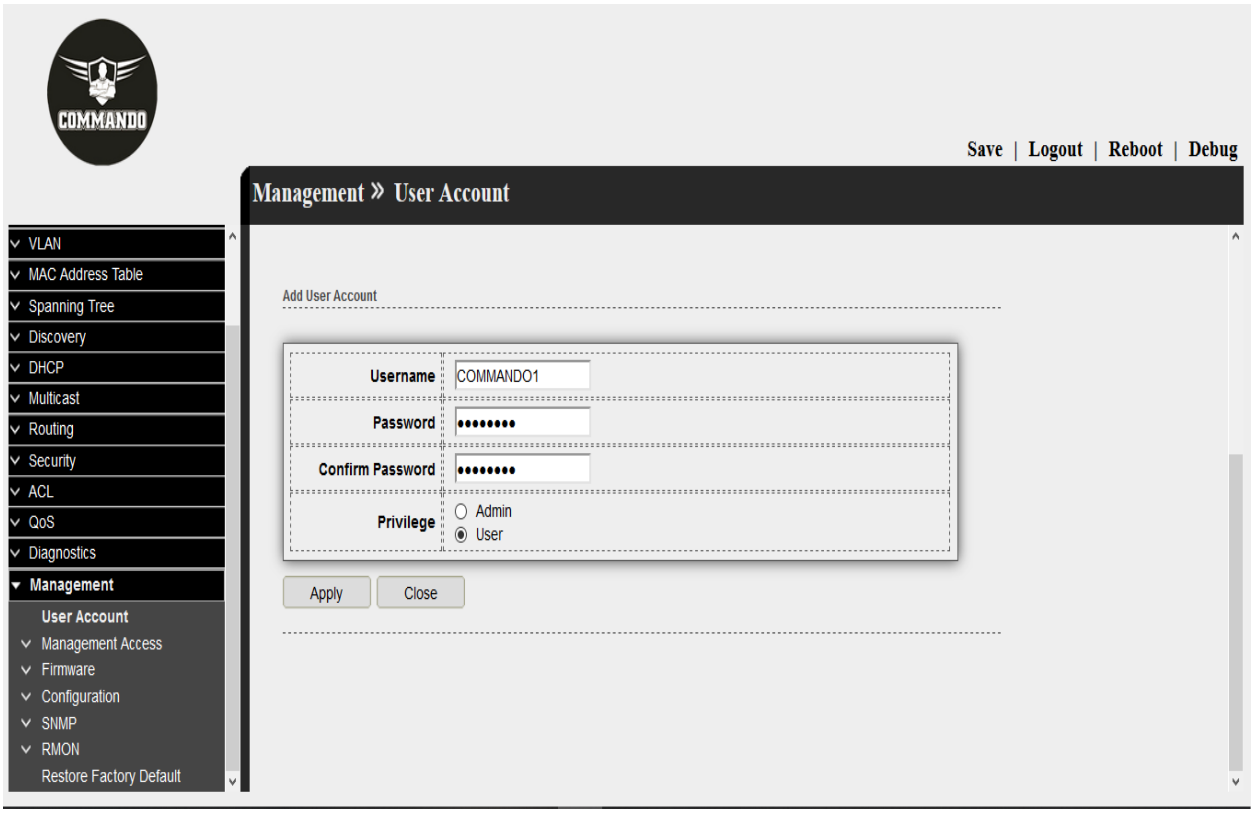


Fig 16.1.3 Add User Account having very limited access page

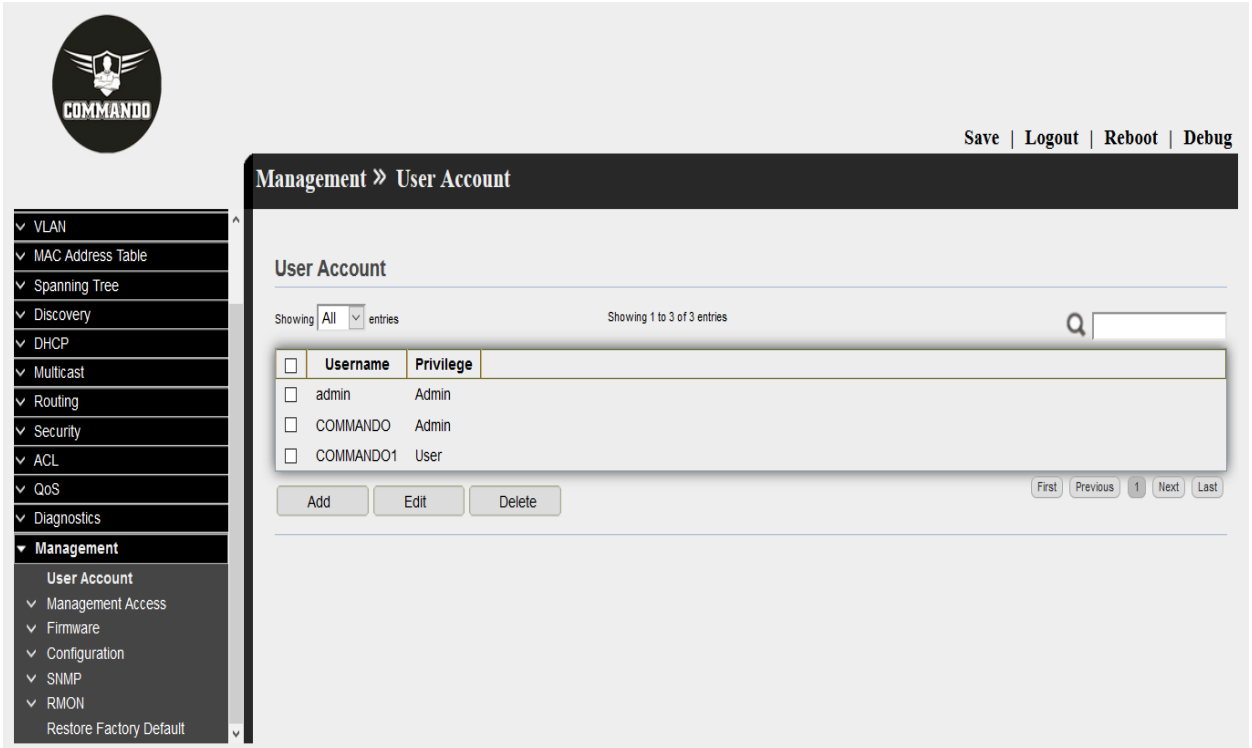


Fig 16.1.4 All User Account page

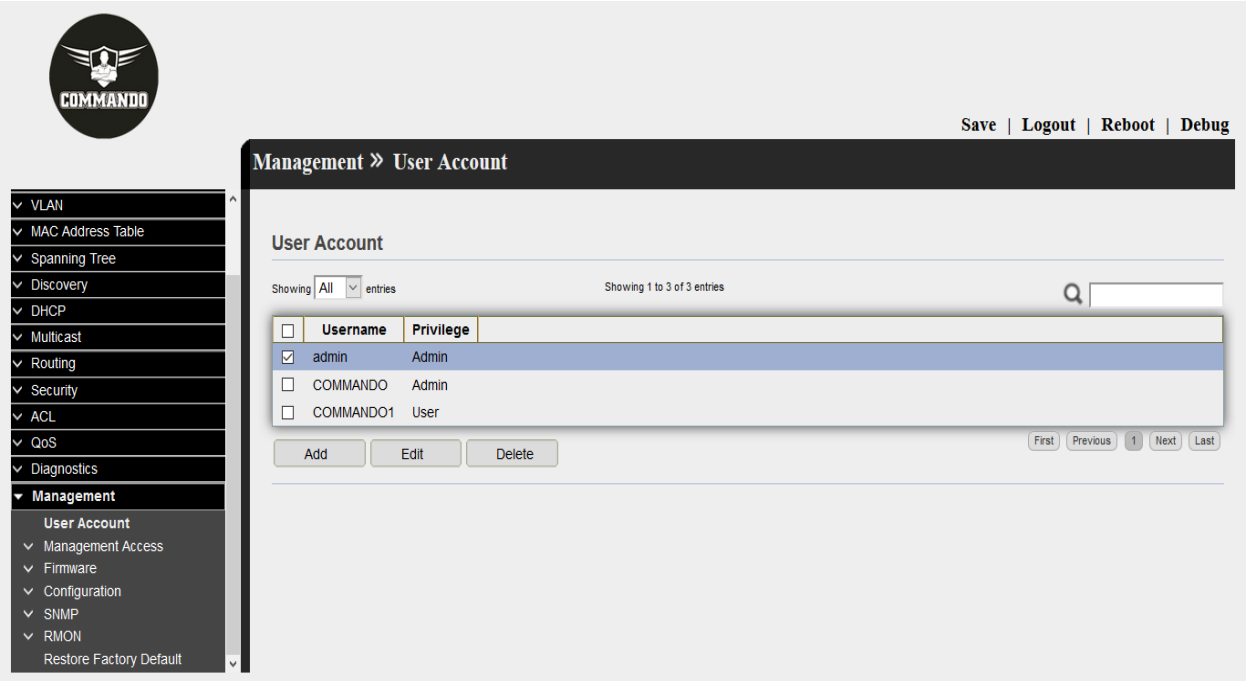


Fig 16.1.5 Selecting and Add/Edit/Delete User Account page

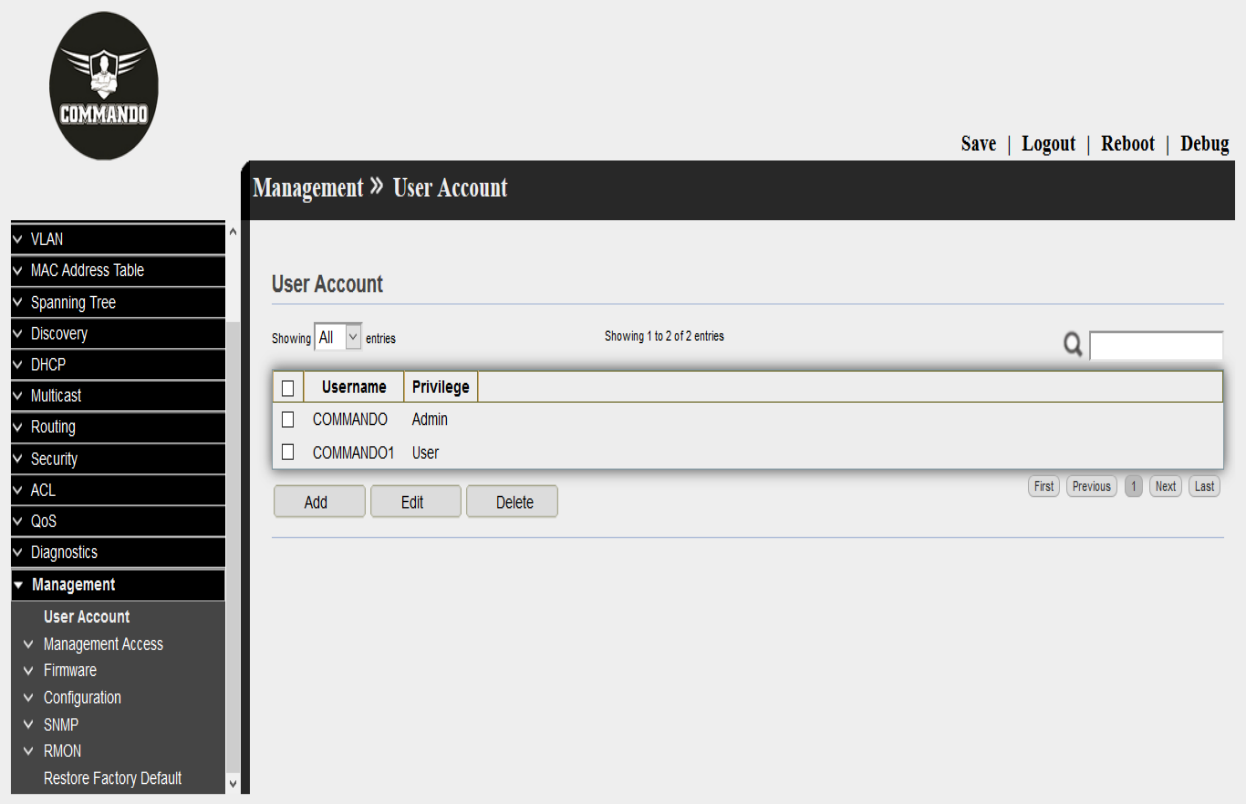


Fig 16.1.6 Deleting default admin account for security purpose page

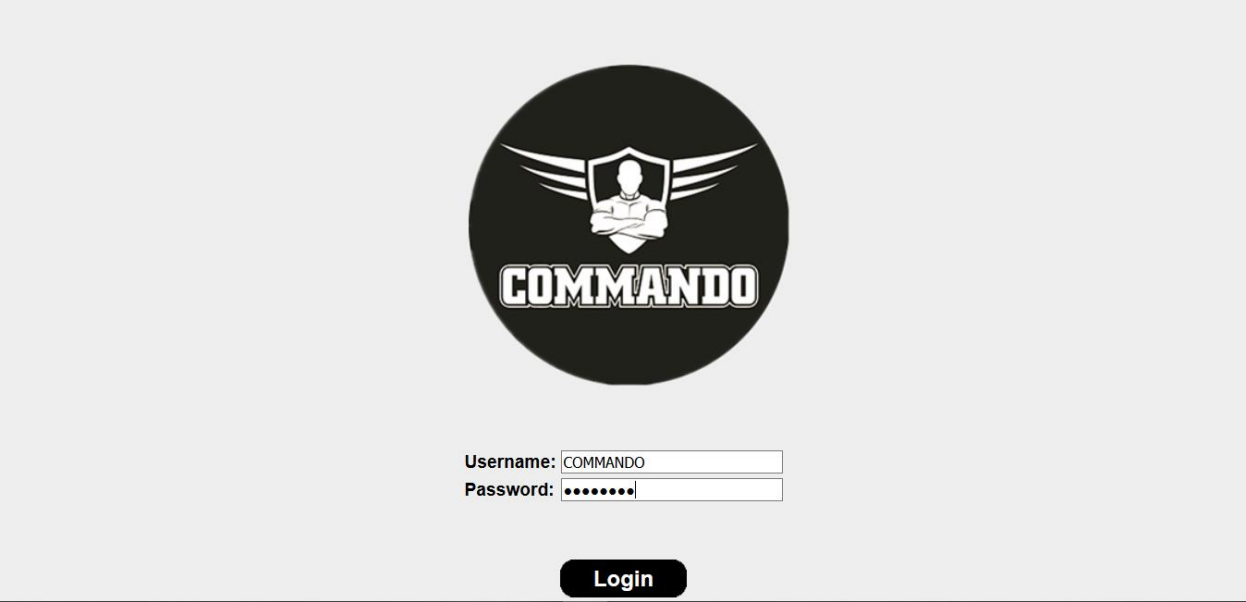


Fig 16.1.7 Login with COMMANDO admin privilege account page

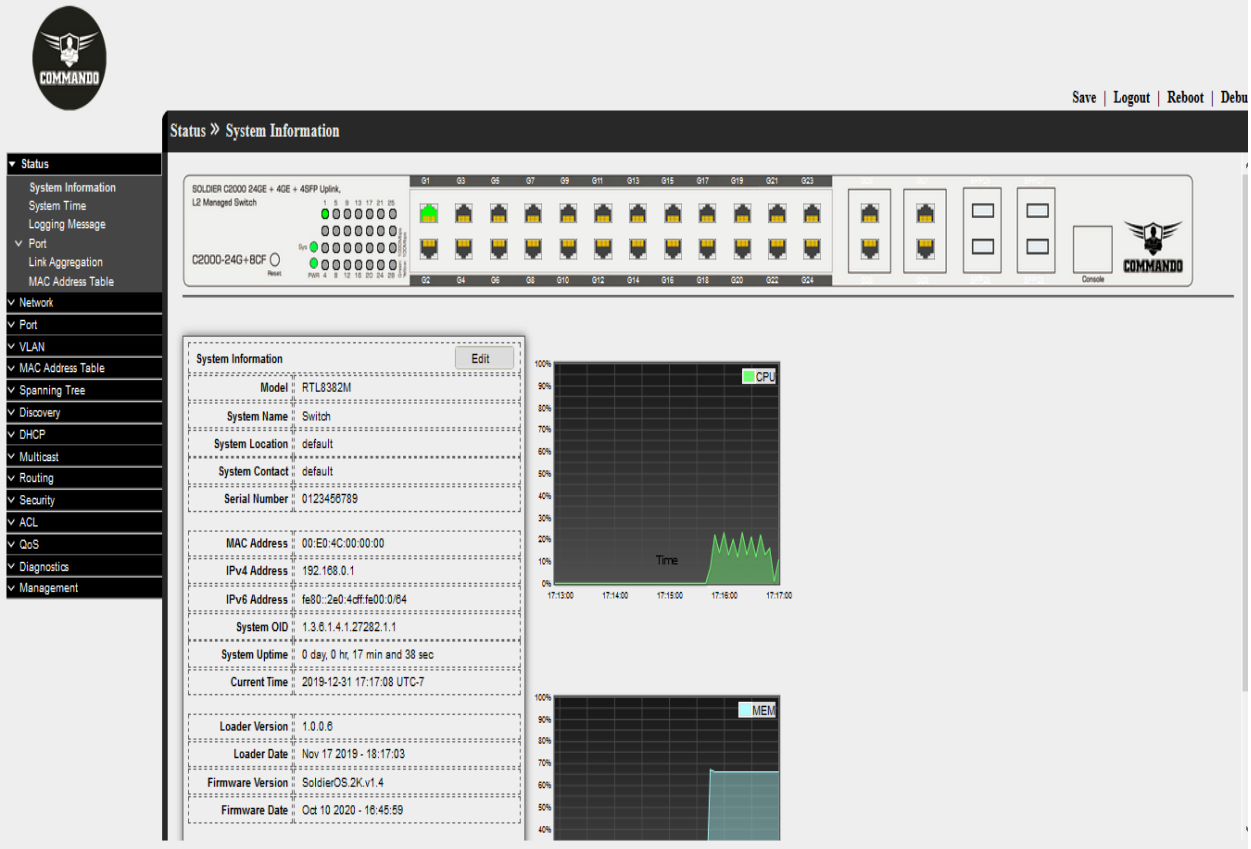


Fig 16.1.8 C2000 Switch access with COMMANDO admin privilege account page

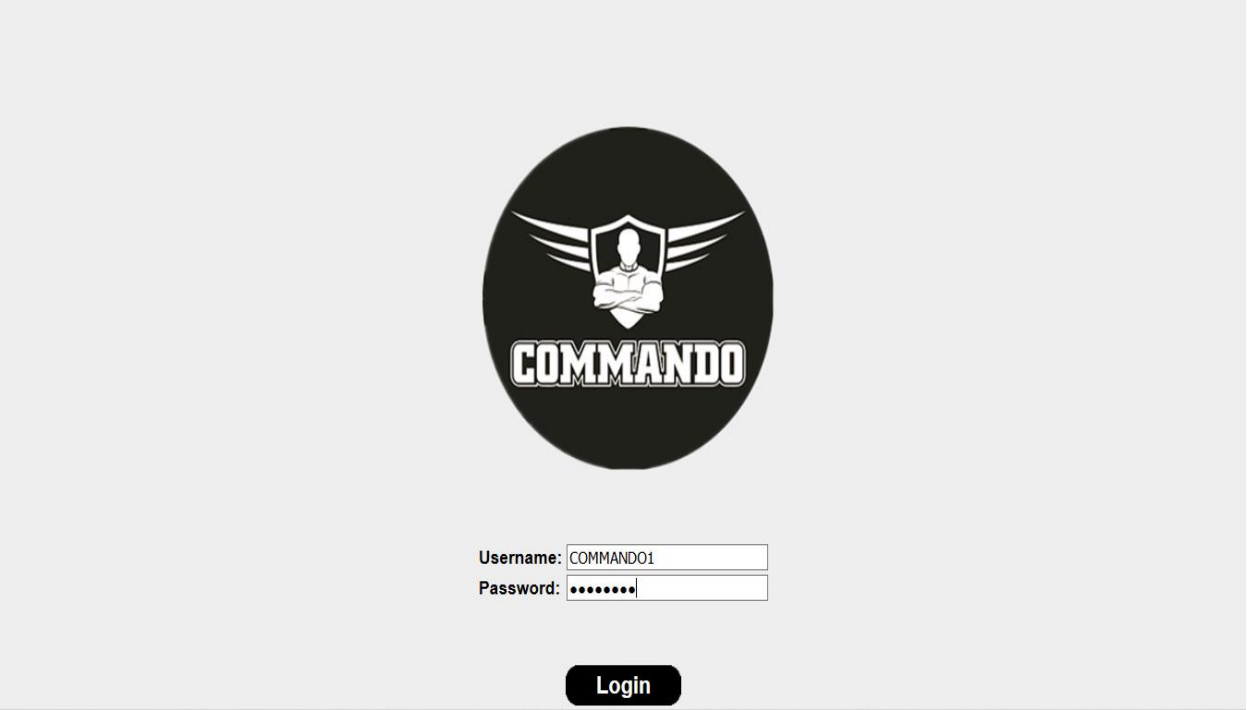


Fig 16.1.9 Login with COMMANDO1 user privilege account page

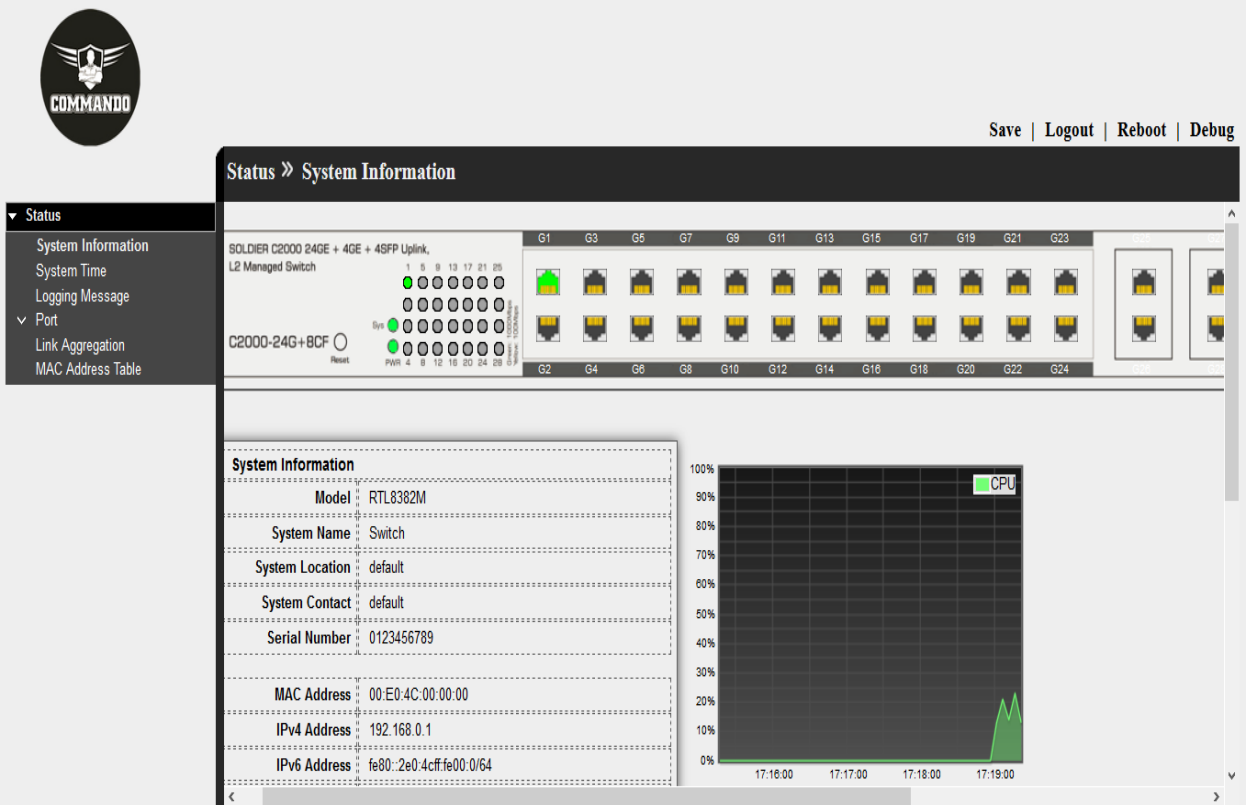


Fig 16.1.10 C2000 Switch access with COMMANDO1 user privilege account page

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 VLAN

Management VLAN is used for managing the switch from a remote location by using protocols such as telnet, SSH, SNMP, syslog etc. Default Management VLAN is VLAN 1. To view and configure Management VLAN page, click **Security >> Management Access >> Management VLAN.**

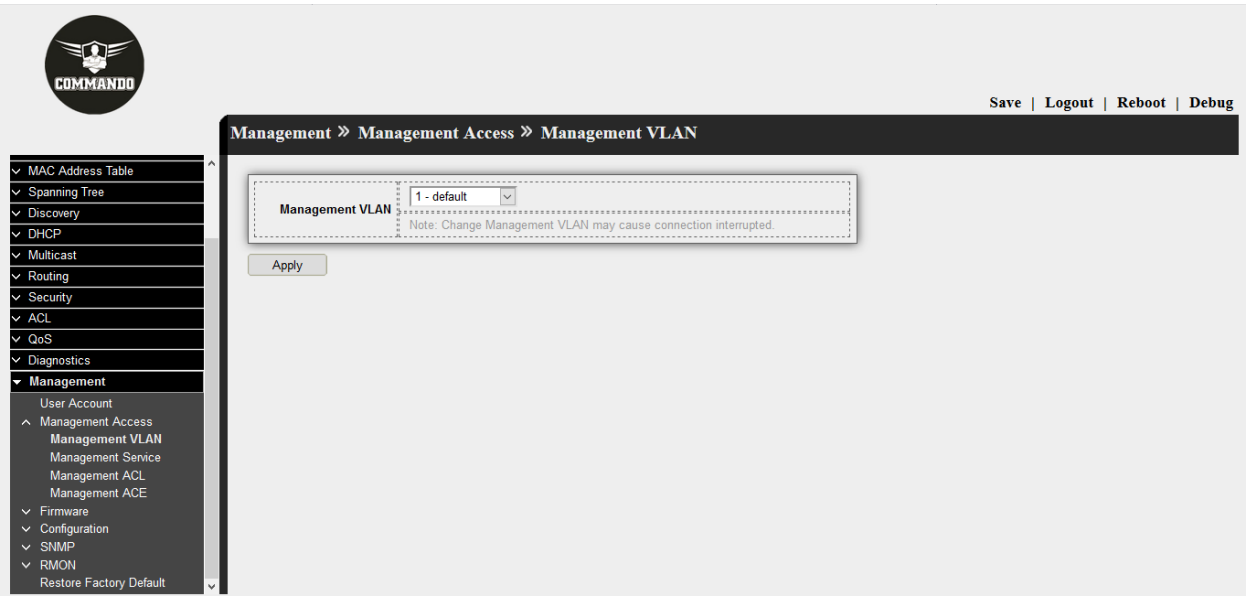


Fig 16.2.1 Default Management Vlan page

16.2.2 Management Service

Methods for accessing for configuration, troubleshooting and managing the C2000 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.

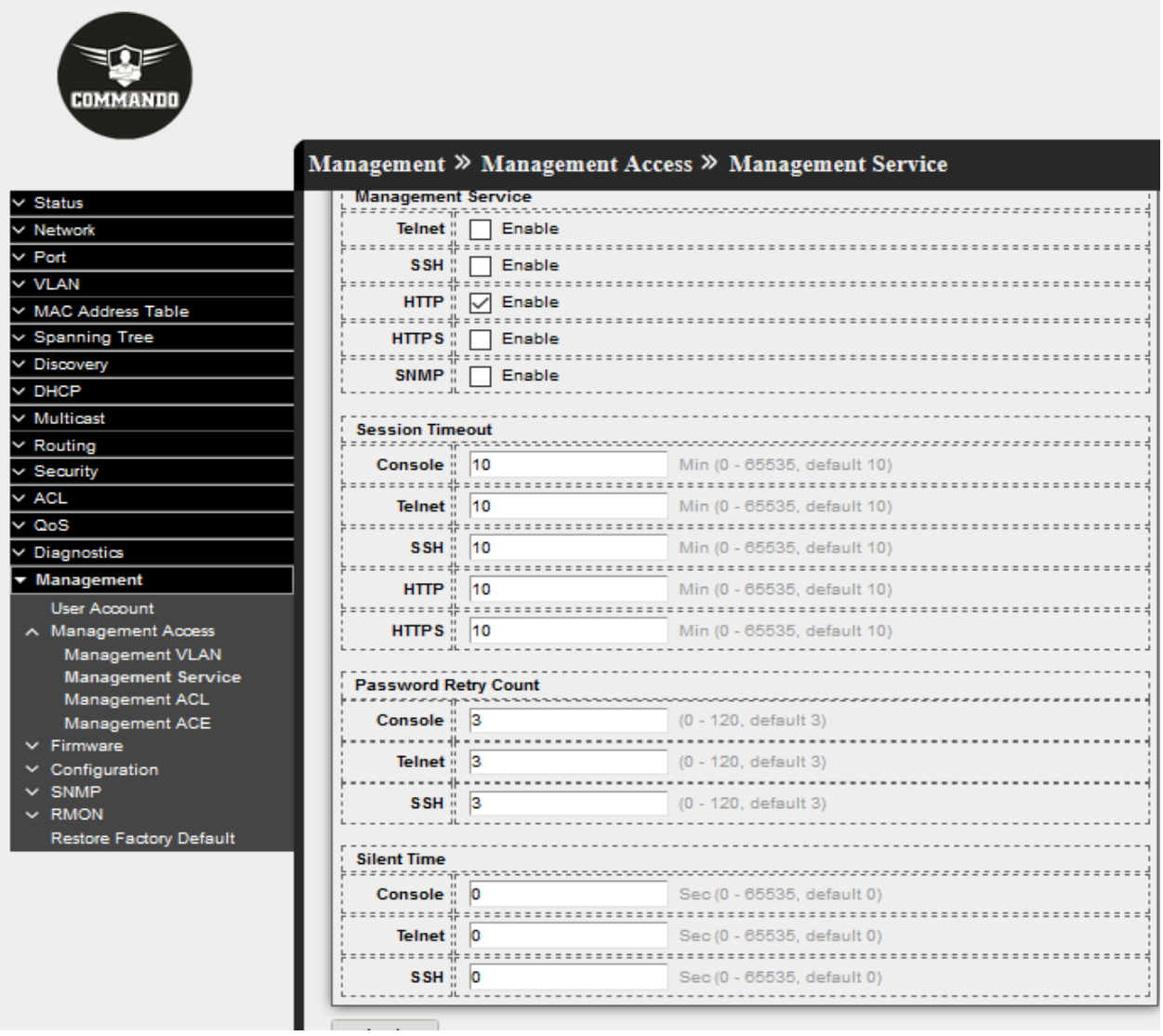


Fig 16.2.2 Management services page

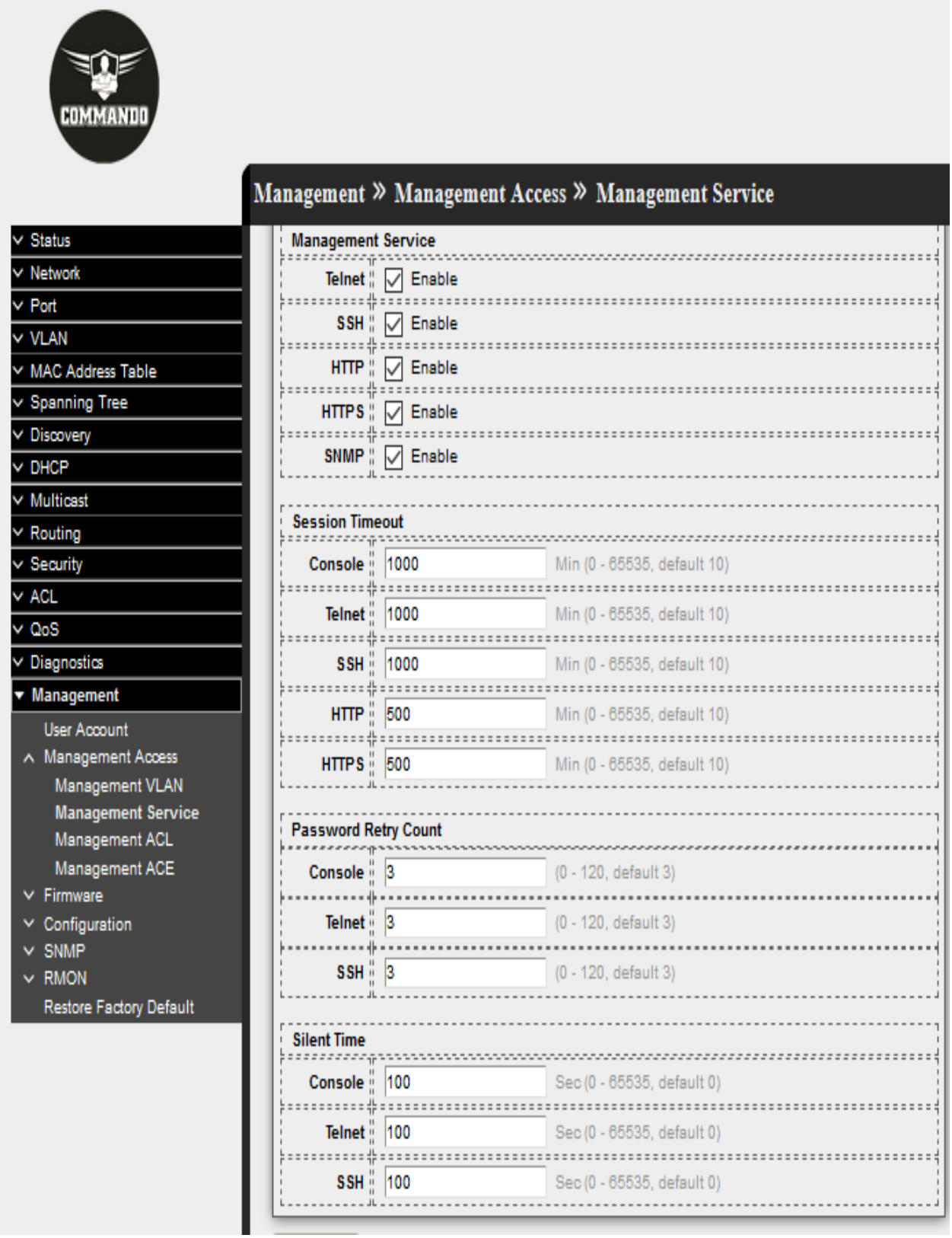


Fig 16.2.3 Enabling Management services page

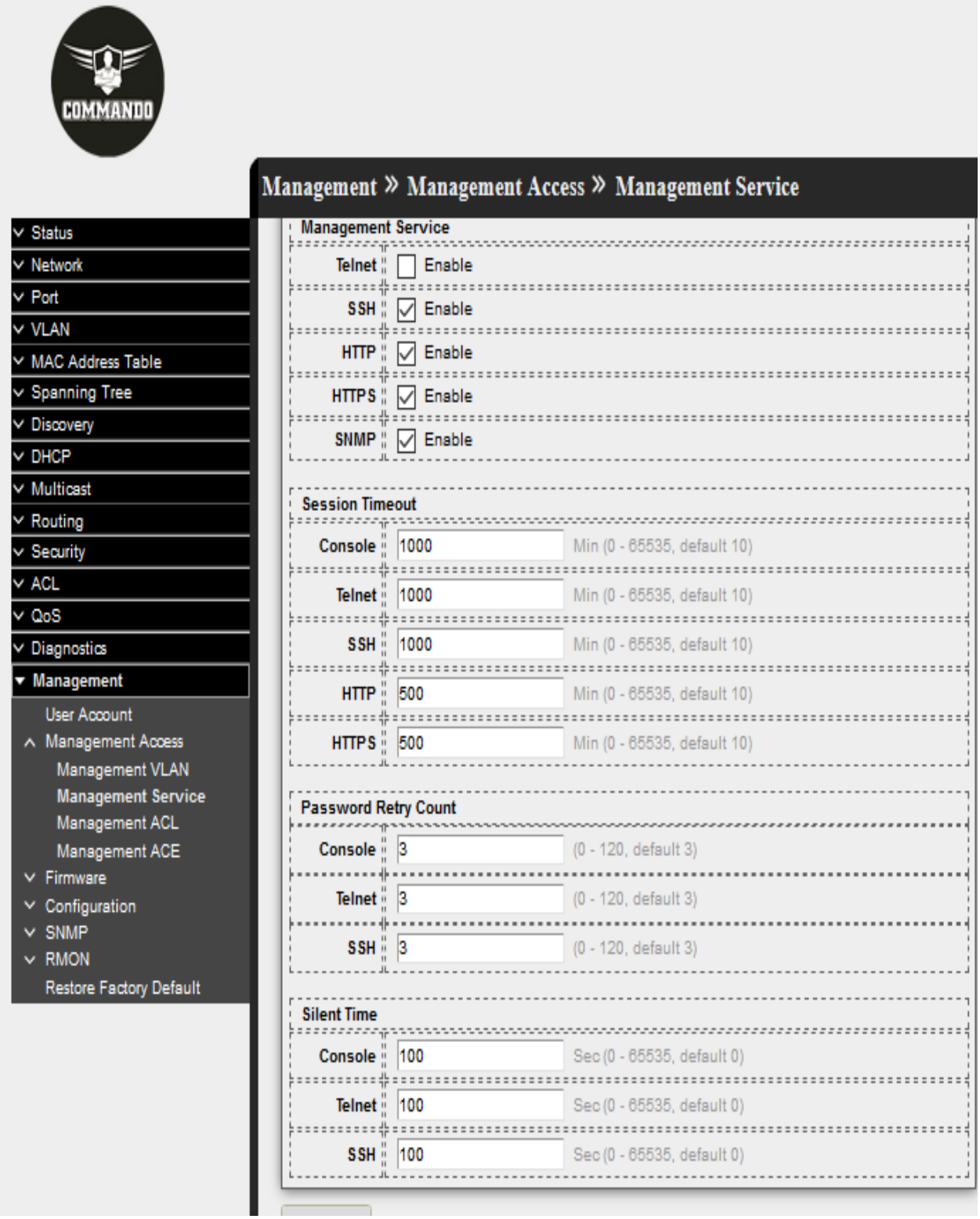


Fig 16.2.4 Disabling telnet Management services page

16.3 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.**

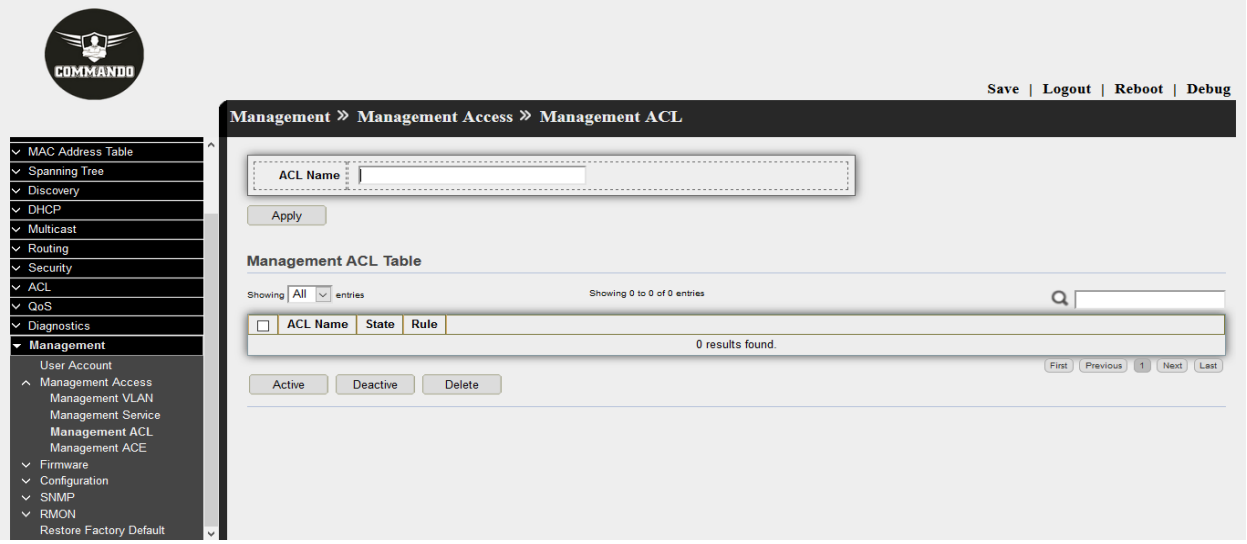


Fig 16.3.1 Default Management ACL Table page

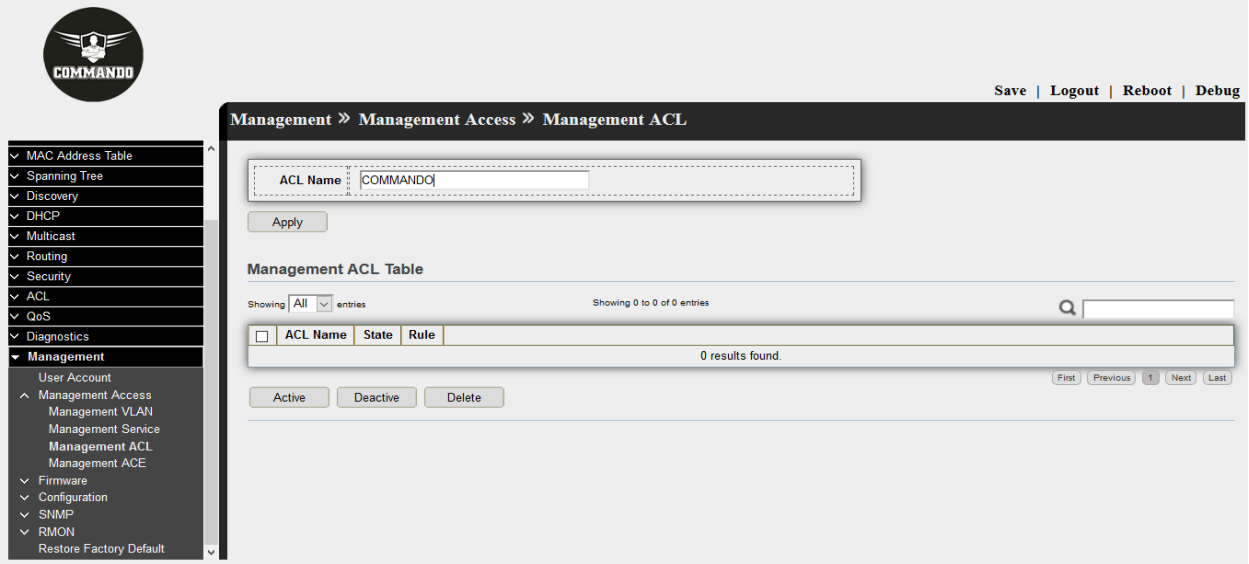


Fig 16.3.2 Adding Management ACL Name page

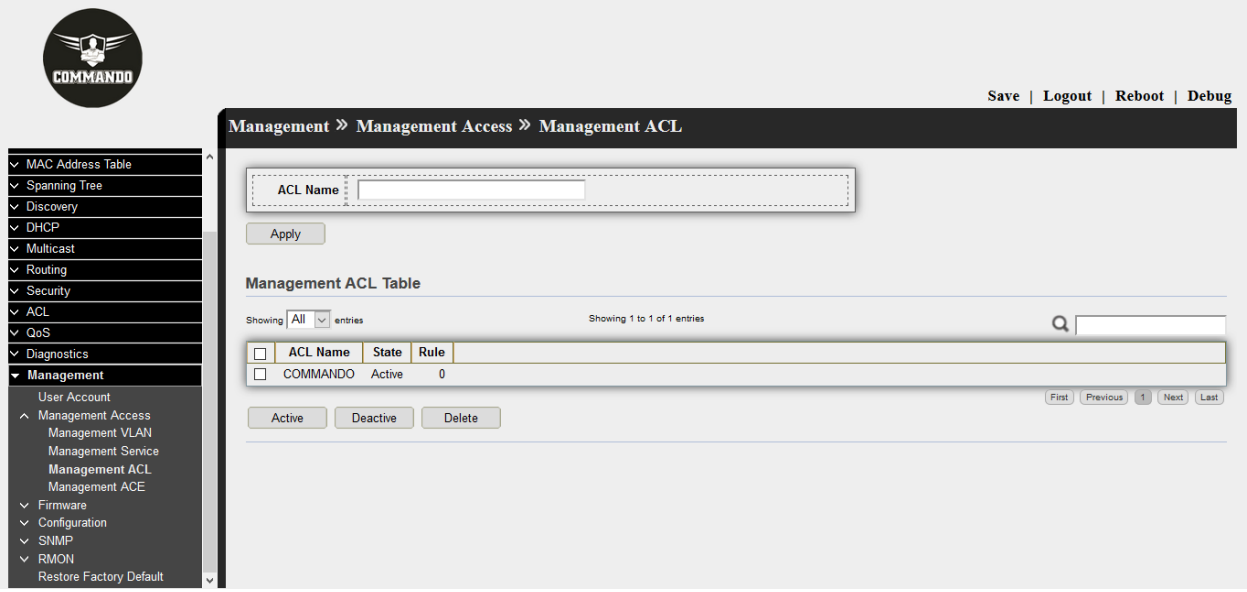


Fig 16.3.3 Activating Management ACL Table page

16.4 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.**

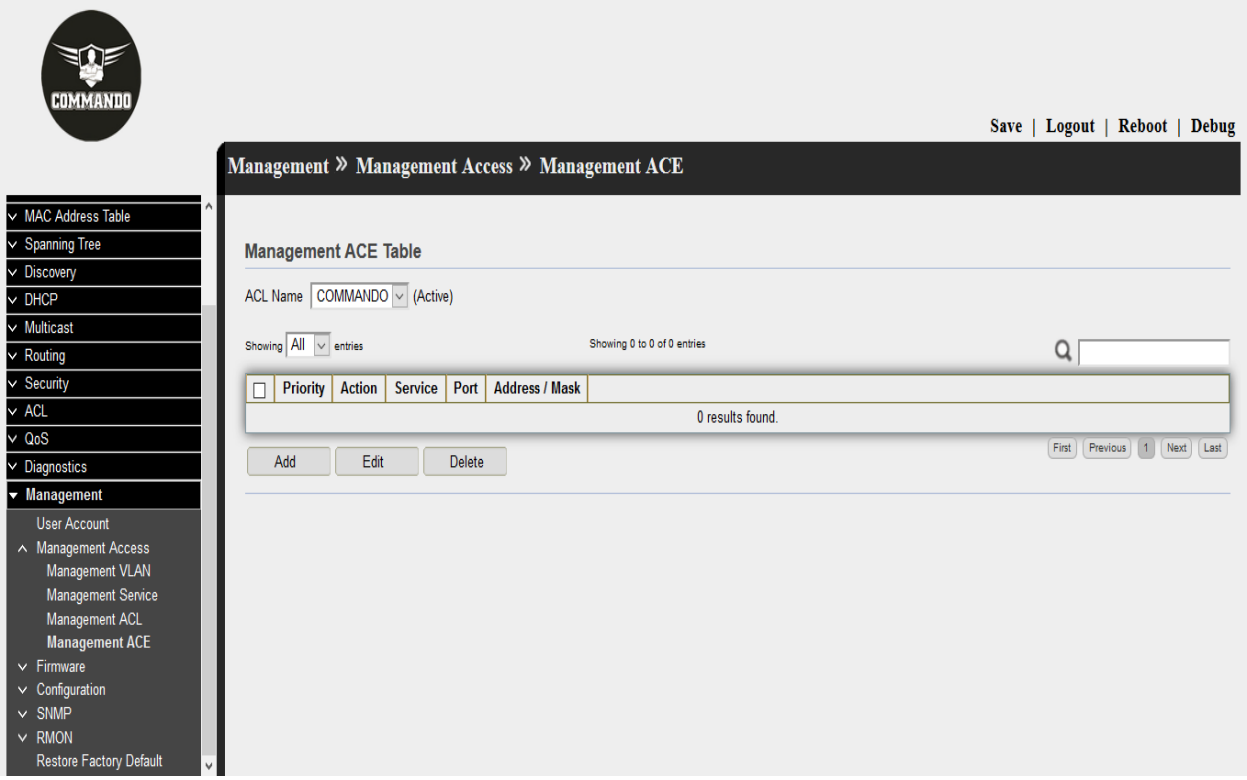


Fig 16.4.1 Default Management ACE Table page

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.

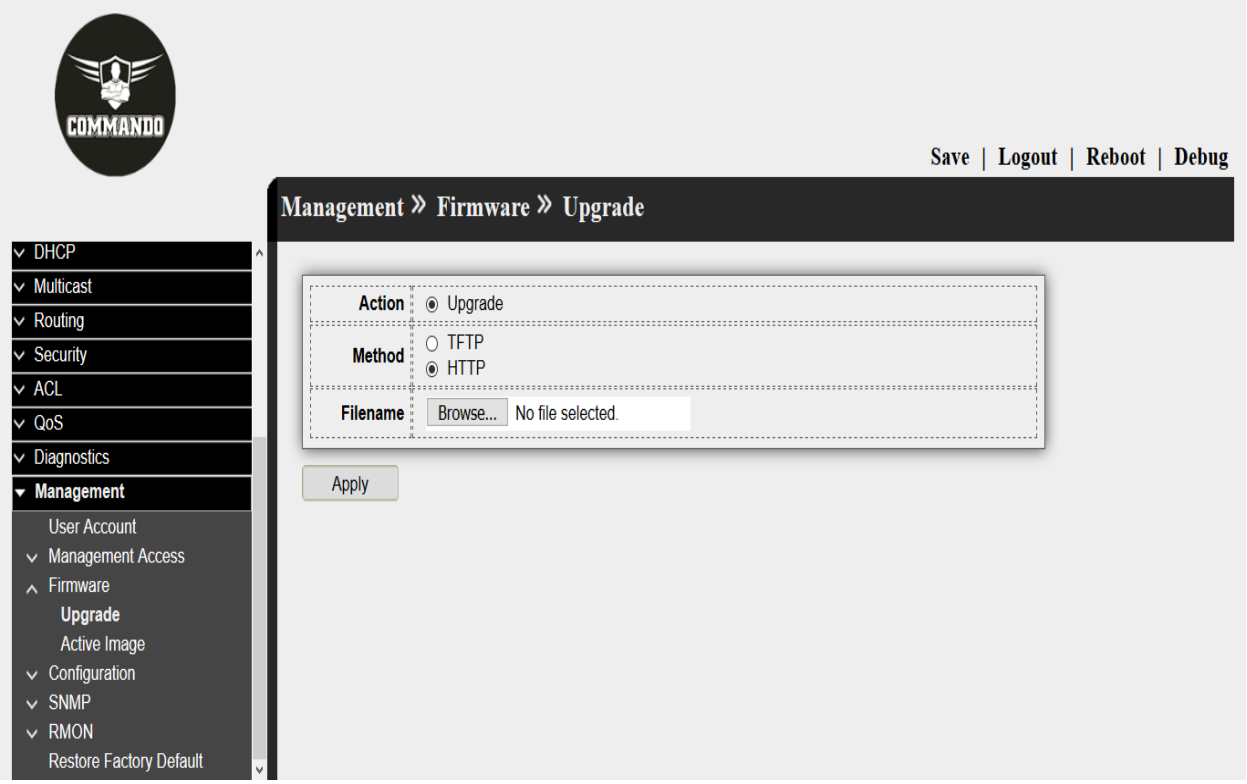


Fig 16.3.1 Default Firmware Upgrade page

Firmware Update Procedure to Firmware Version SoldierOS

Step 1 : Preparing firmware file to be upgrade the switch by 7z unzip software.

Step 2 : For Uploading prepared firmware file to COMMANDO Series C2000 by WEBUI 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.

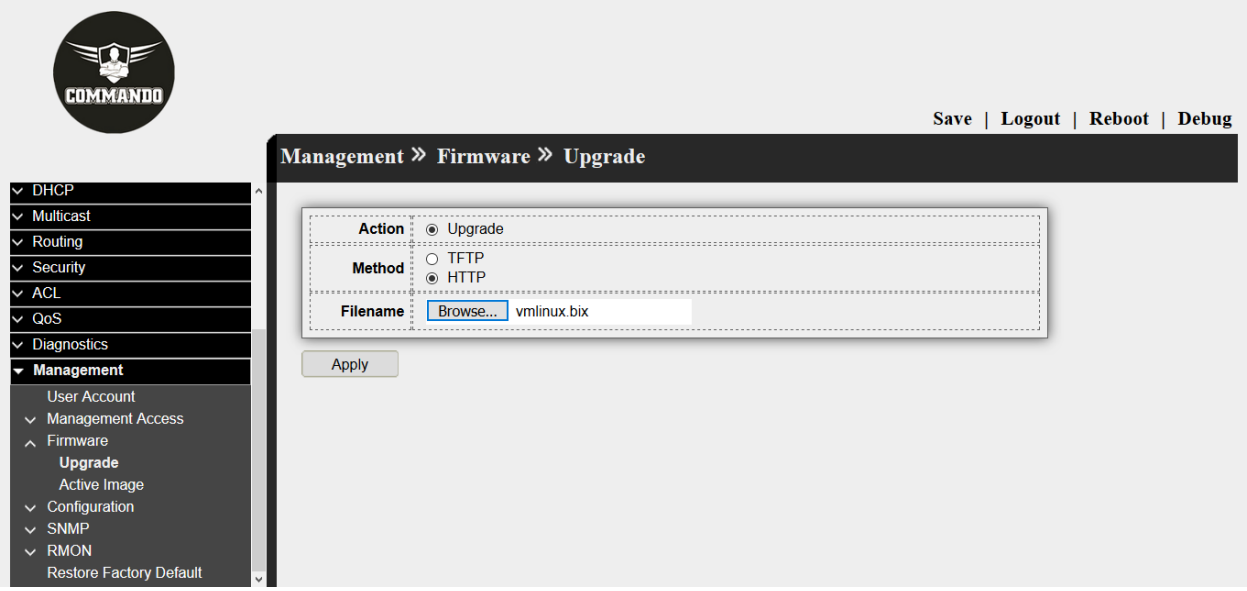


Fig 16.3.2 Firmware Upgrade page

16.3.2 Active Image

In all C2000 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 C2000 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 C2000 series Switches. No saved configuration is lost while changing images.

To view and configure Active Image, Click Management>>Firmware>>Active Image

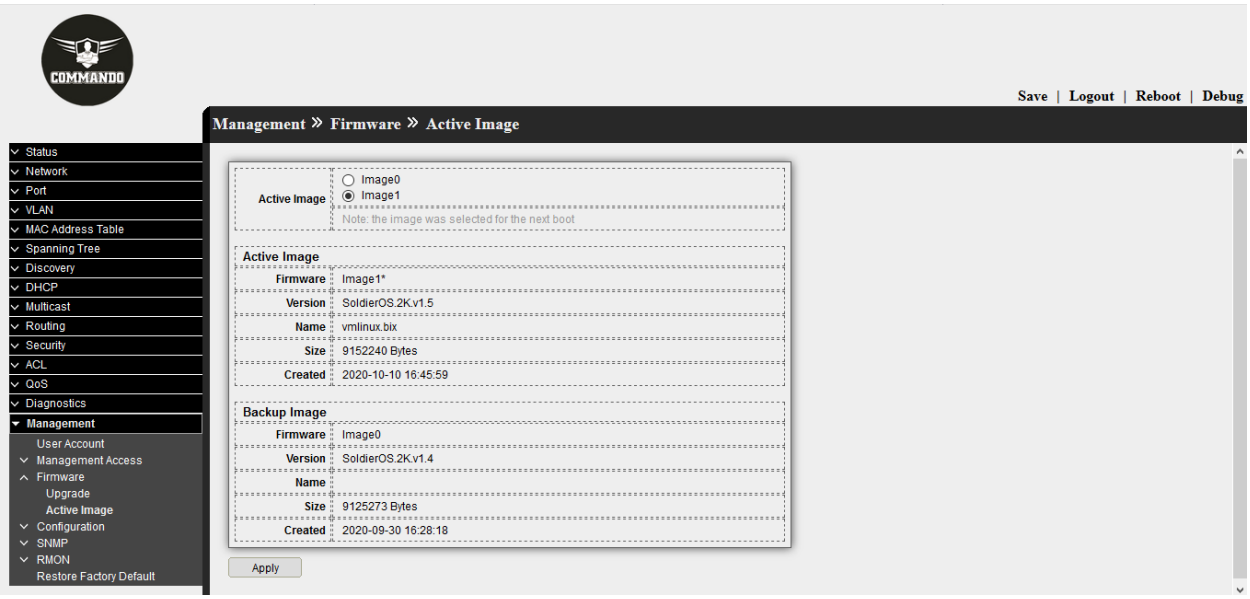


Fig 16.3.3 Firmware Active Image page

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

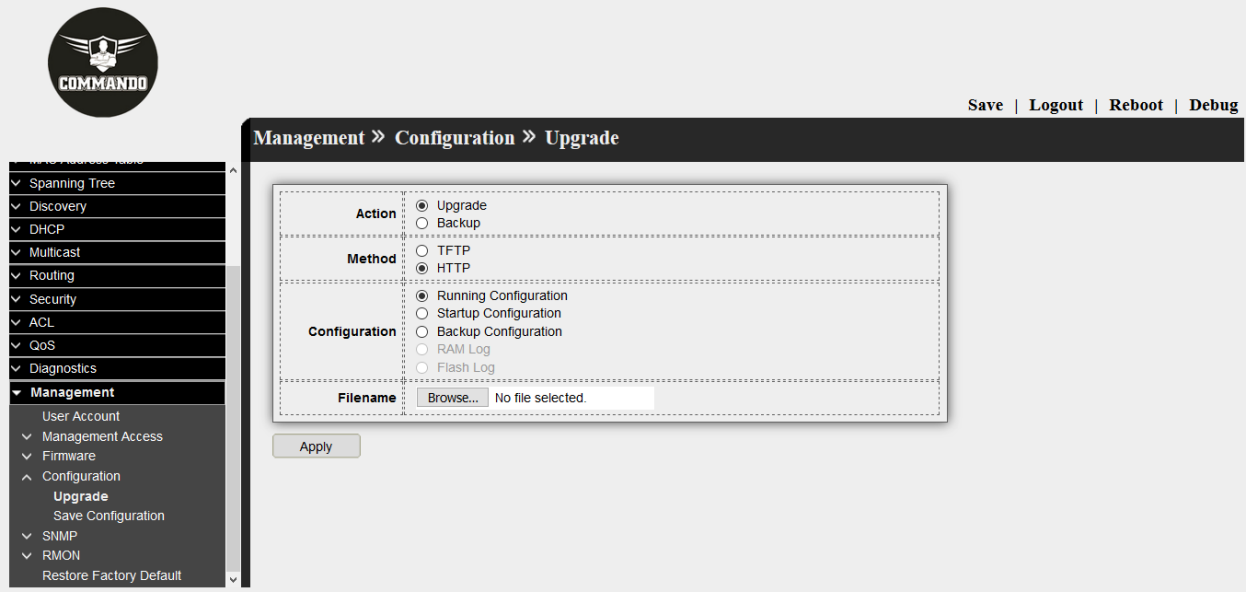


Fig 16.4.1 Configuration default update page

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.

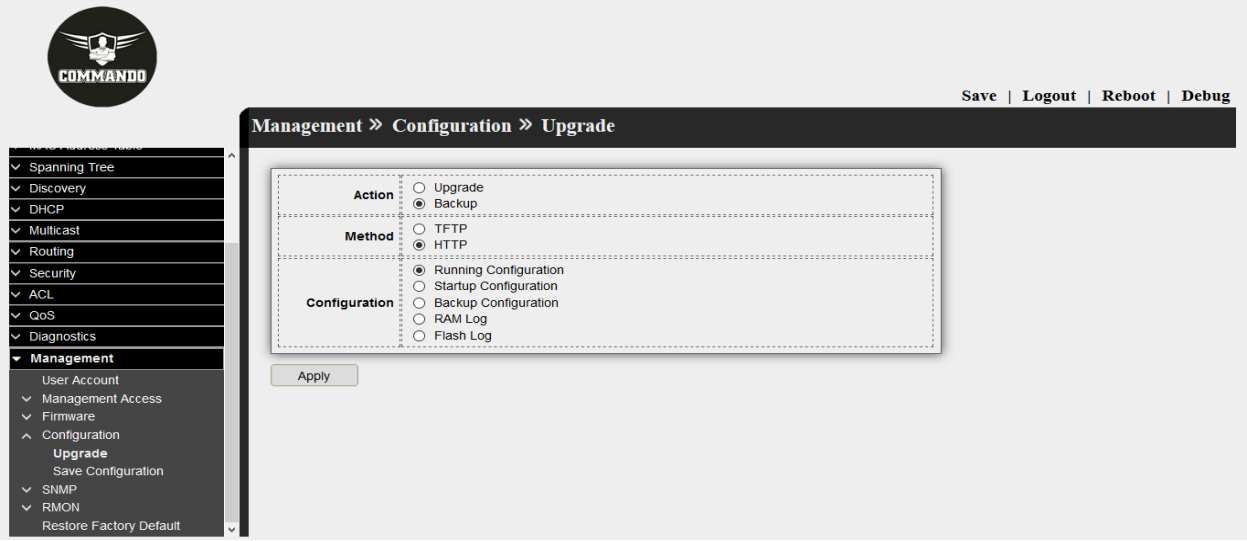


Fig 16.4.2 Backup of Configuration from running configuration page

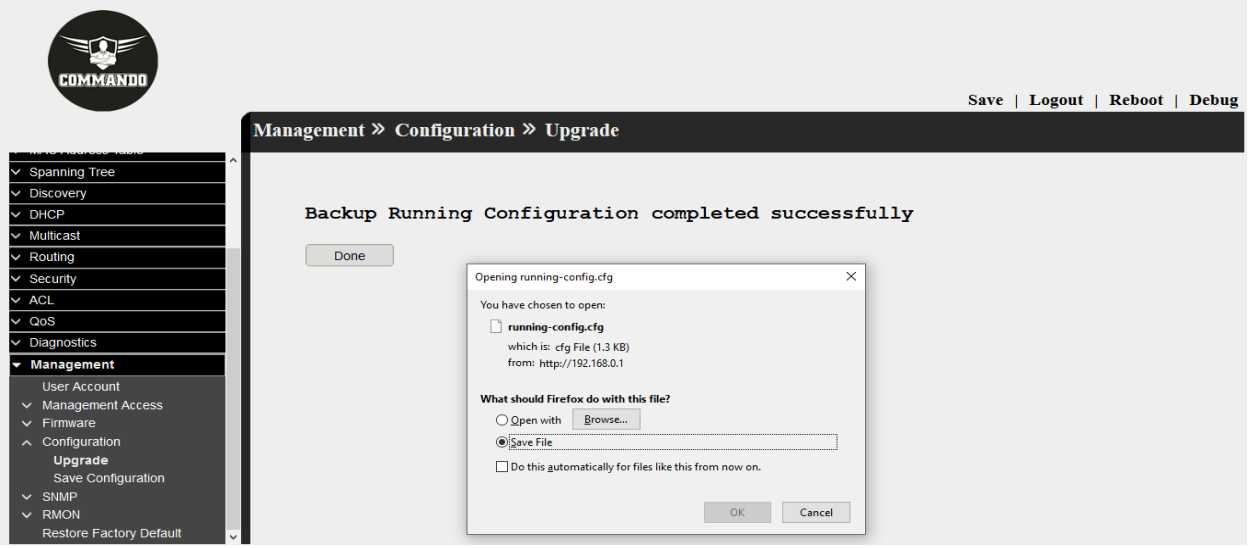


Fig 16.4.3 Backup running configuration page

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 back to the current state if changes lead to an undesirable configuration. All of 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.**

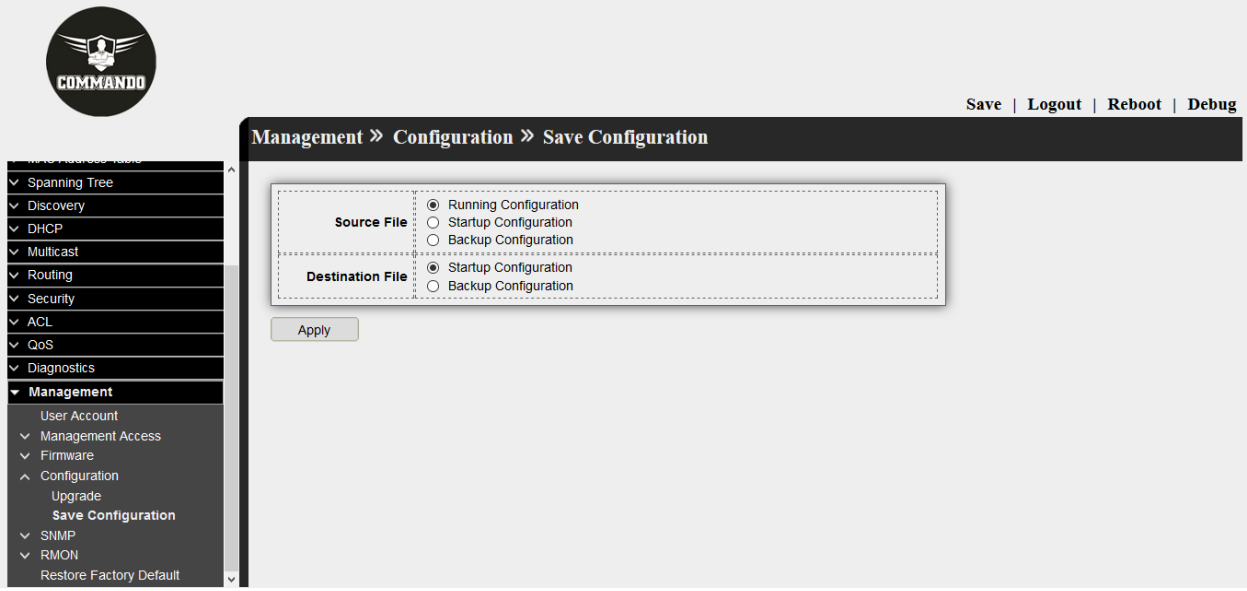


Fig 16.4.4 Save running Configuration to Startup Configuration page

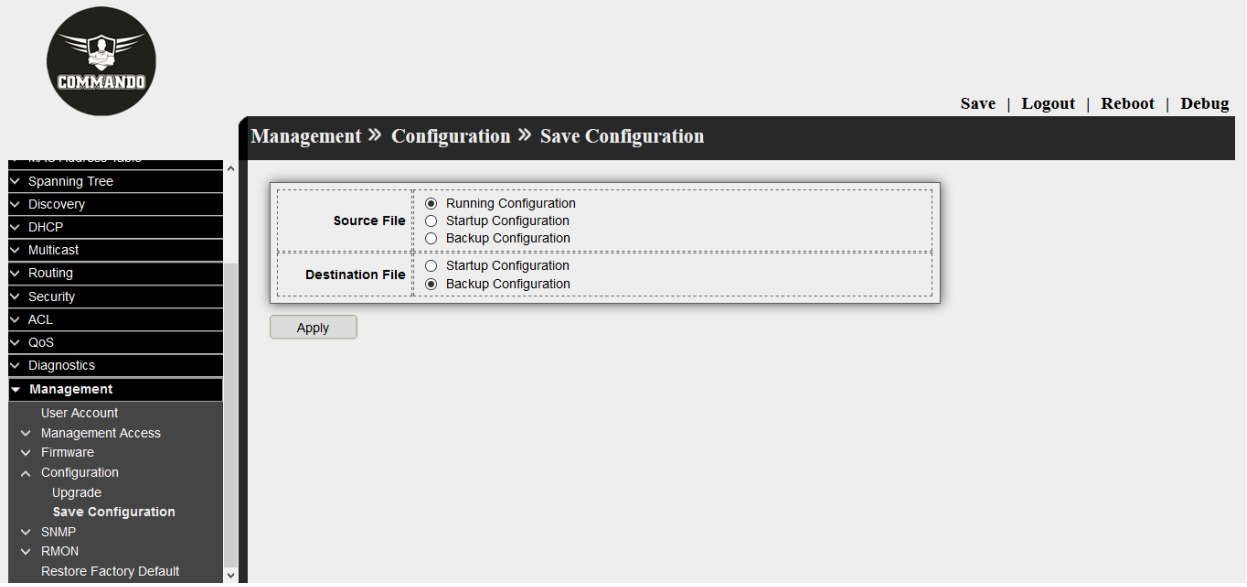


Fig 16.4.5 Save running Configuration to Backup Configuration page

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.**

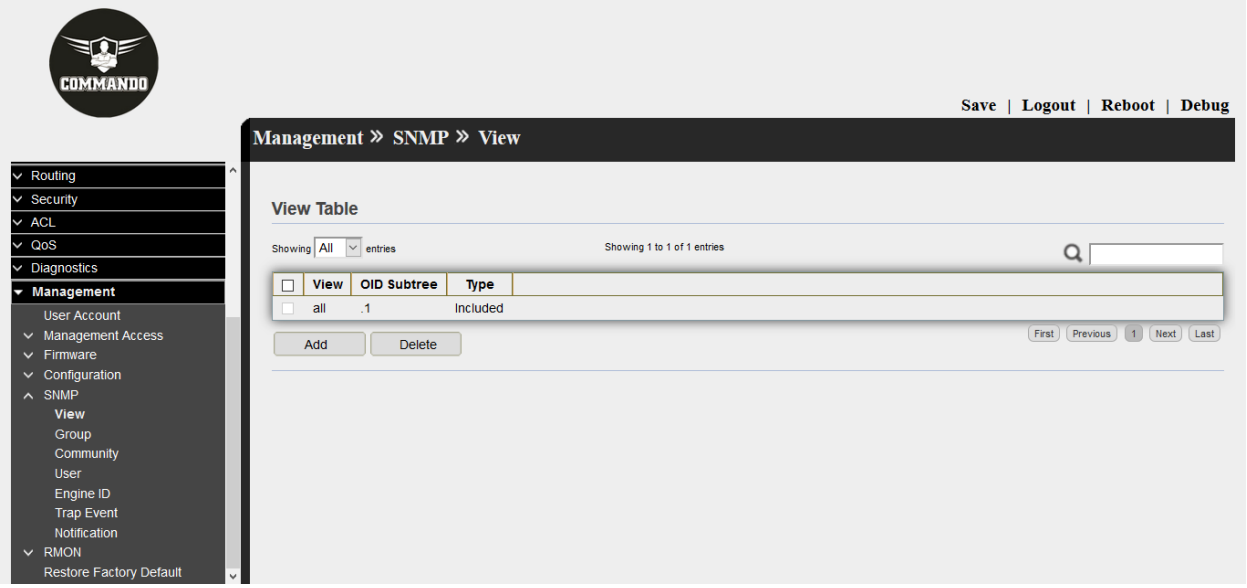


Fig 16.5.1 Default SNMP View Table page

Fig 16.5.2 SNMP add View page

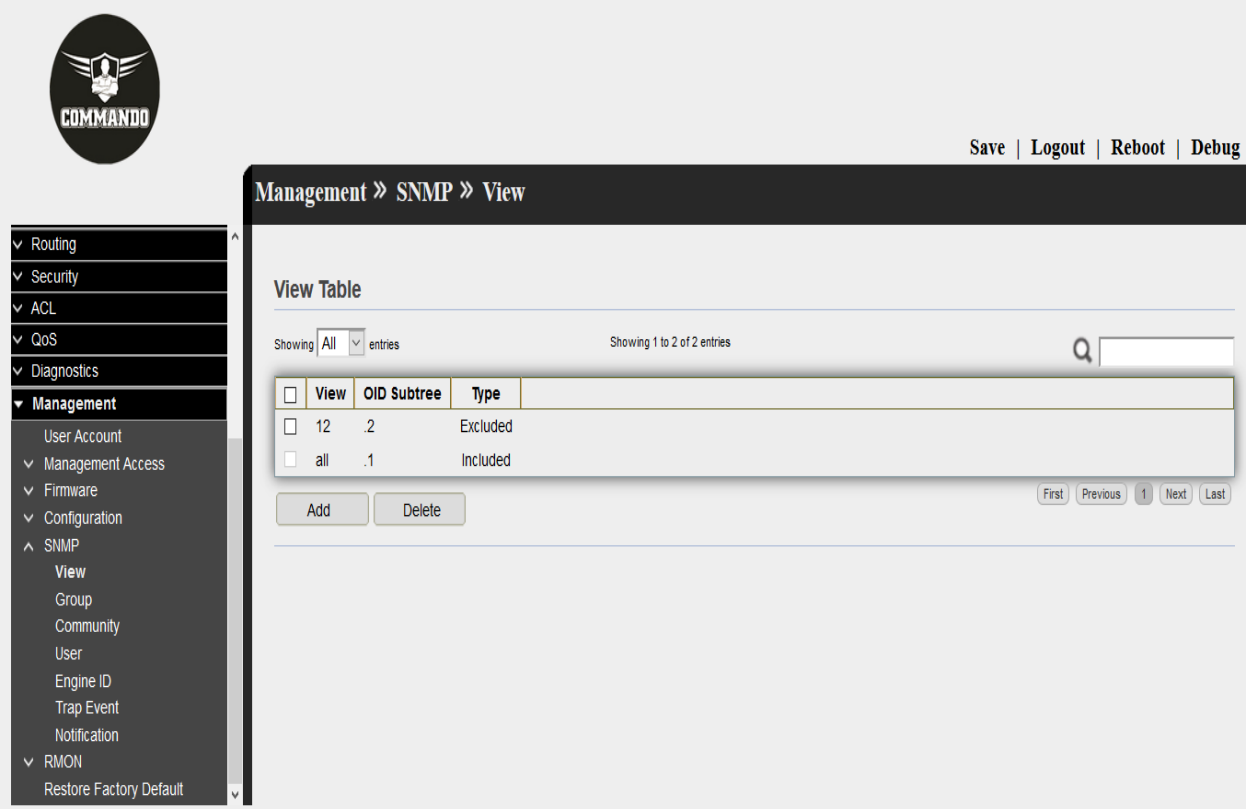


Fig 16.5.3 SNMP View Table page

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.**

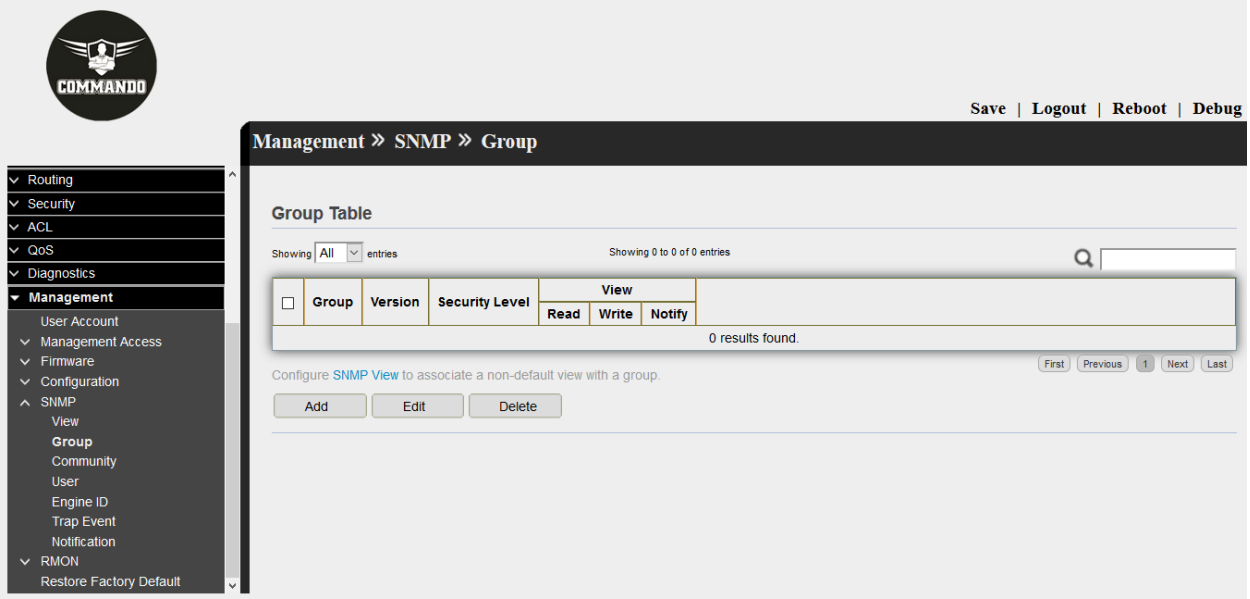


Fig 16.5.4 SNMP Default Group Table page

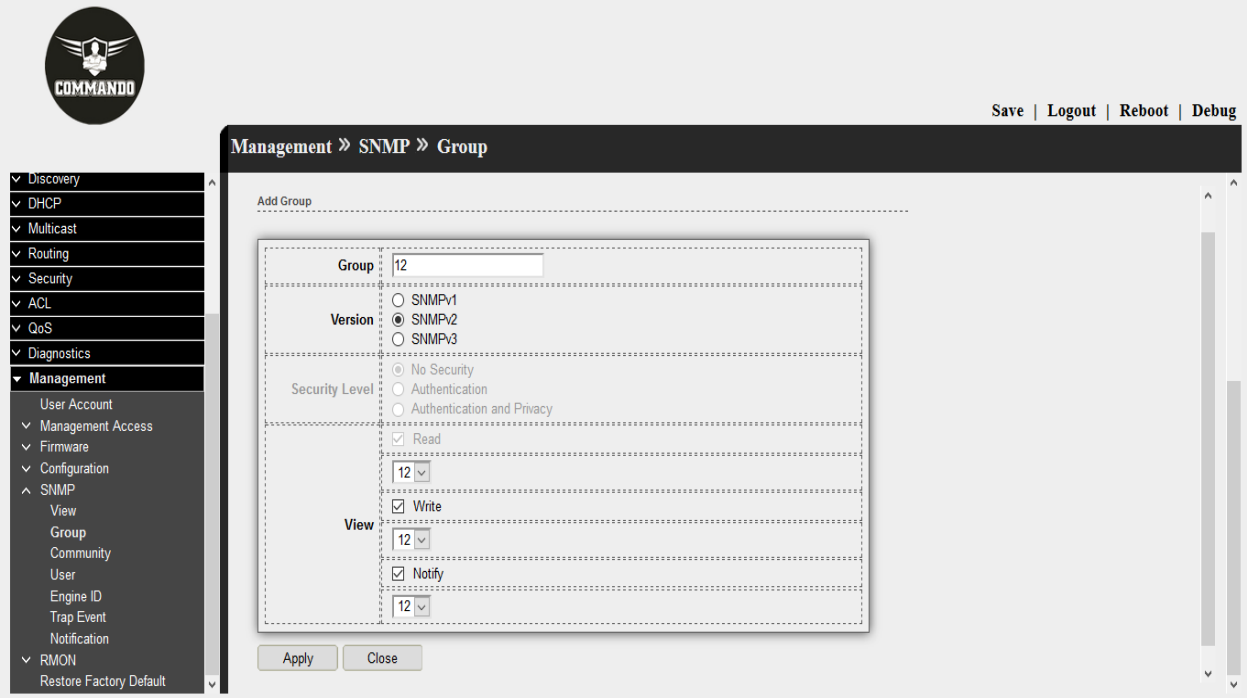


Fig 16.5.5 SNMP Add Group page

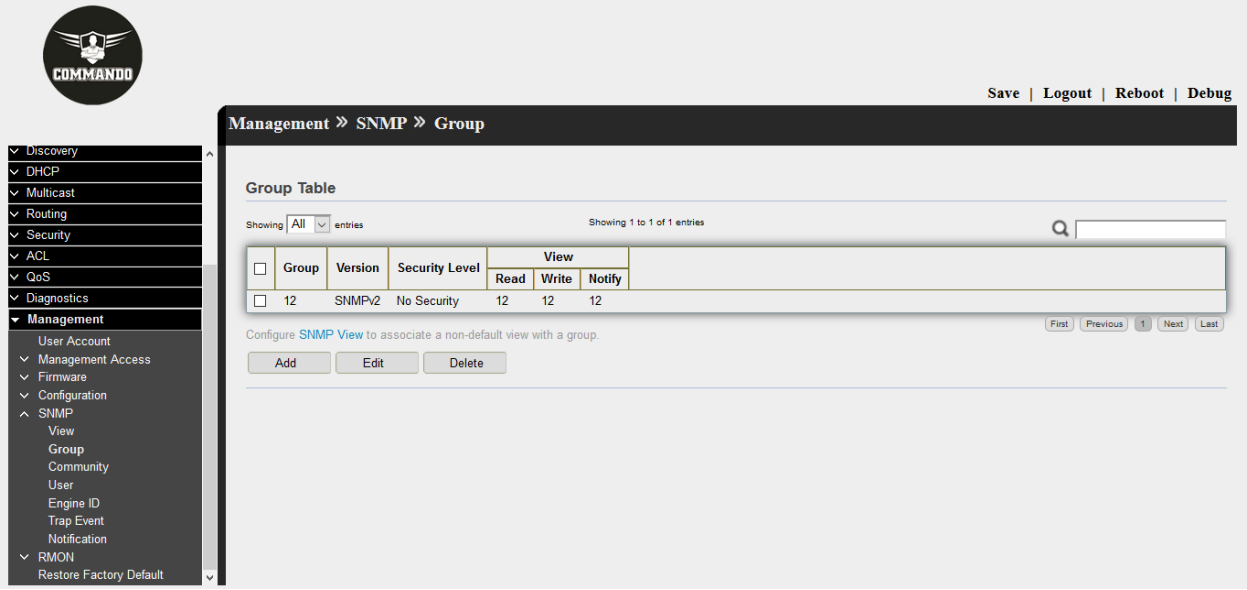


Fig 16.5.6 SNMP Group Table after adding group page

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.**

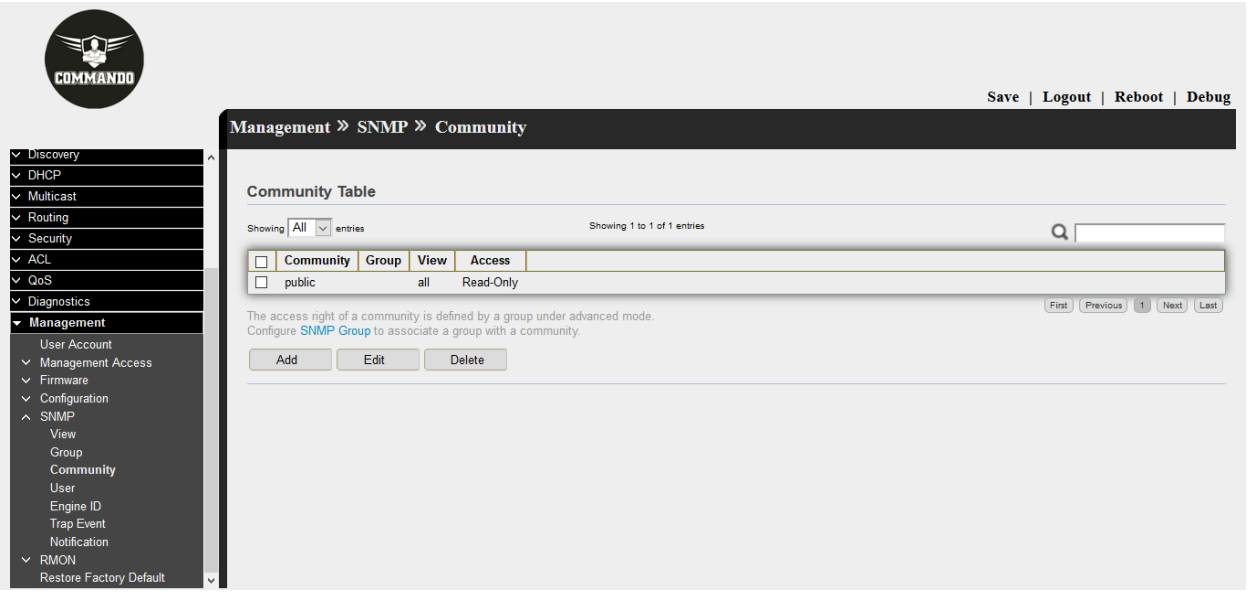


Fig 16.5.7 SNMP Community Table page

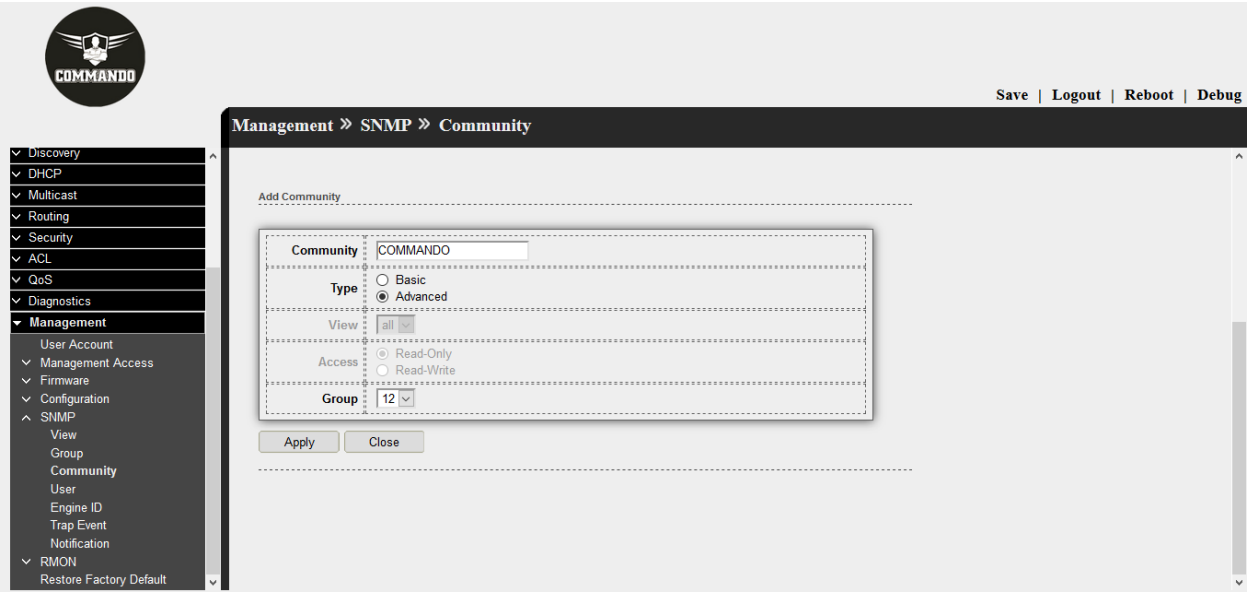


Fig 16.5.8 Add SNMP Community page

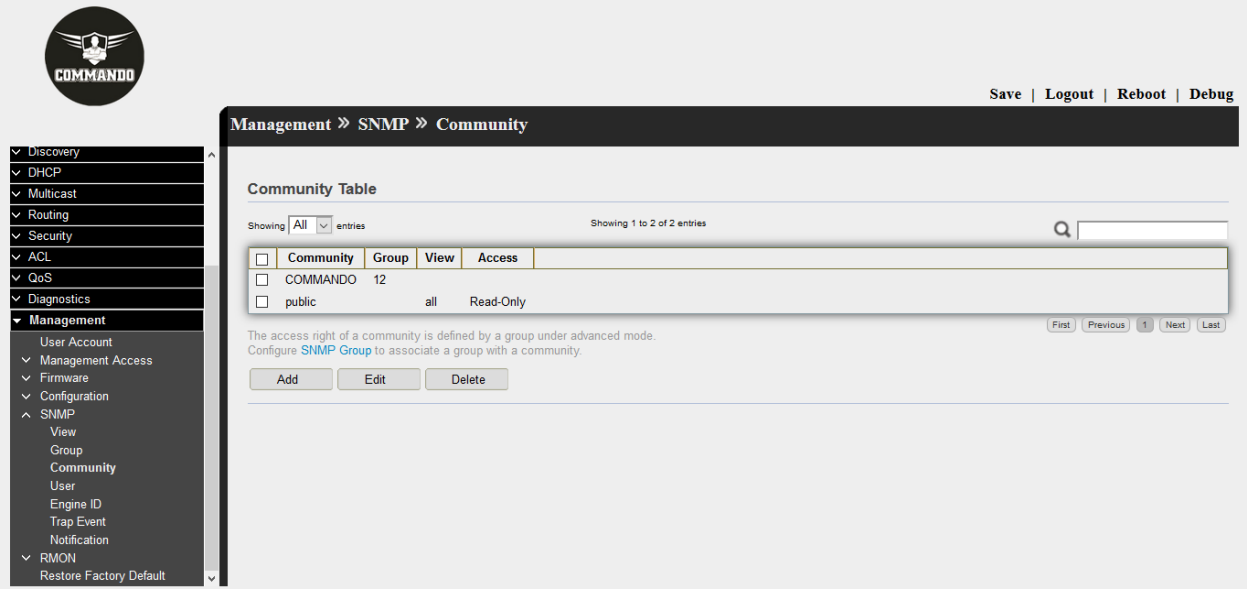


Fig 16.5.9 SNMP Community Table after adding community page

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.**

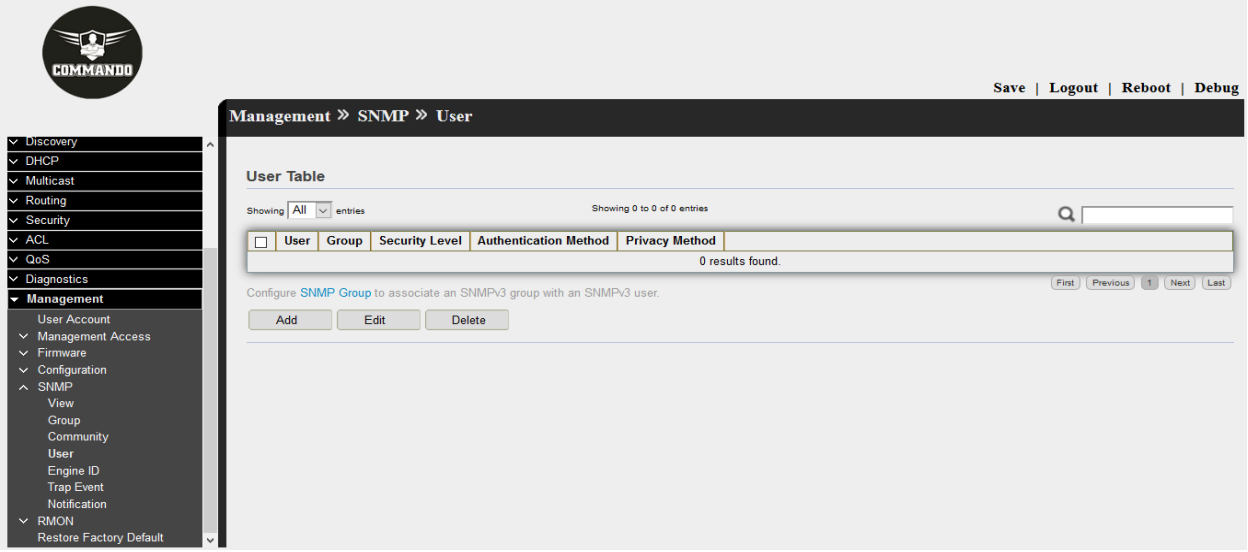


Fig 16.5.10 SNMP Default user Table page

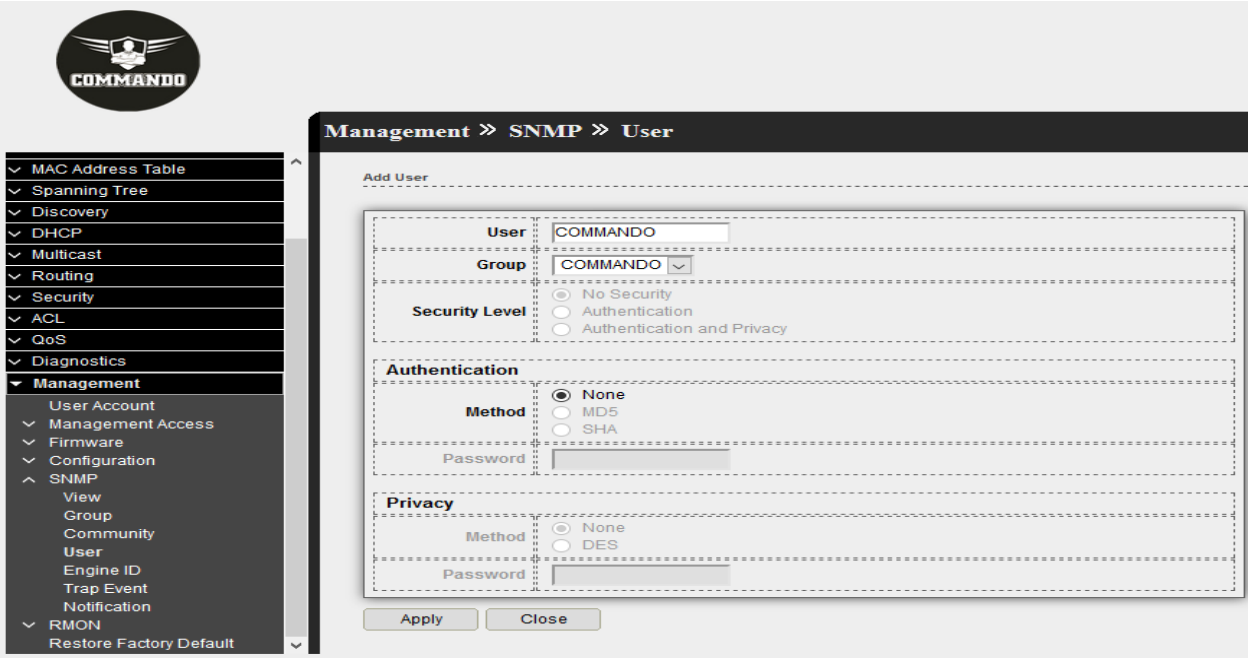


Fig 16.5.11 SNMP Add user page

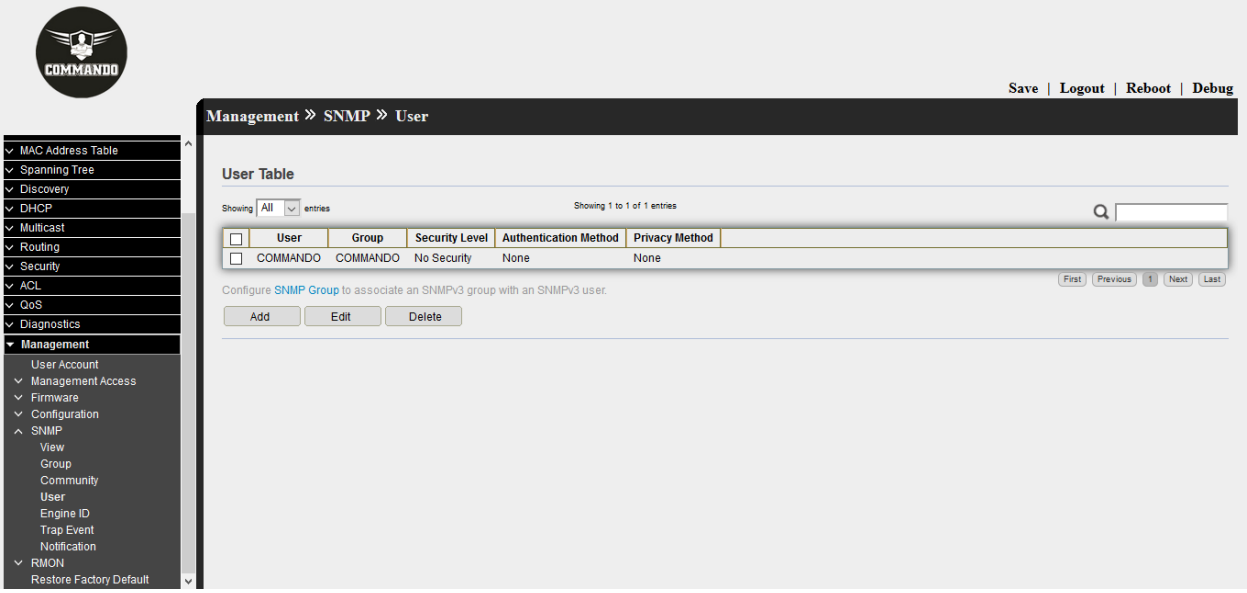


Fig 16.5.12 SNMP user Table after adding User page

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.**

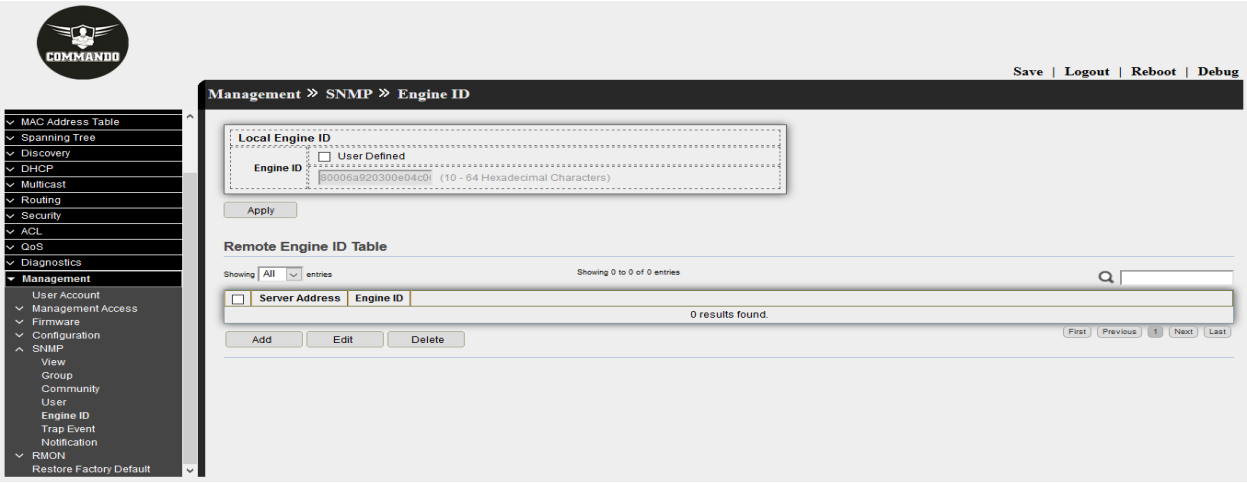


Fig 16.5.13 SNMP Default Remote Engine ID Table page

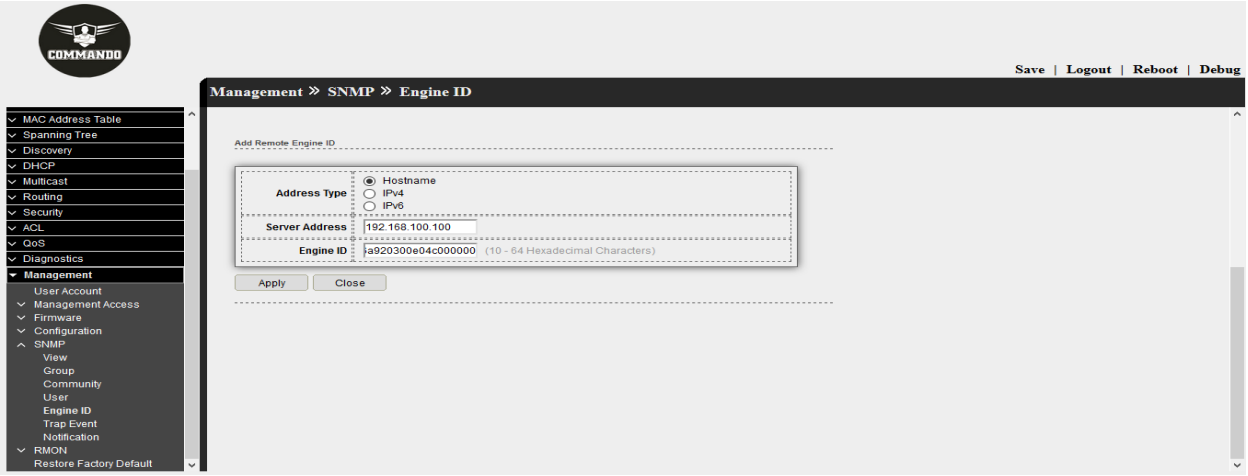


Fig 16.5.14 SNMP Add Remote Engine ID page

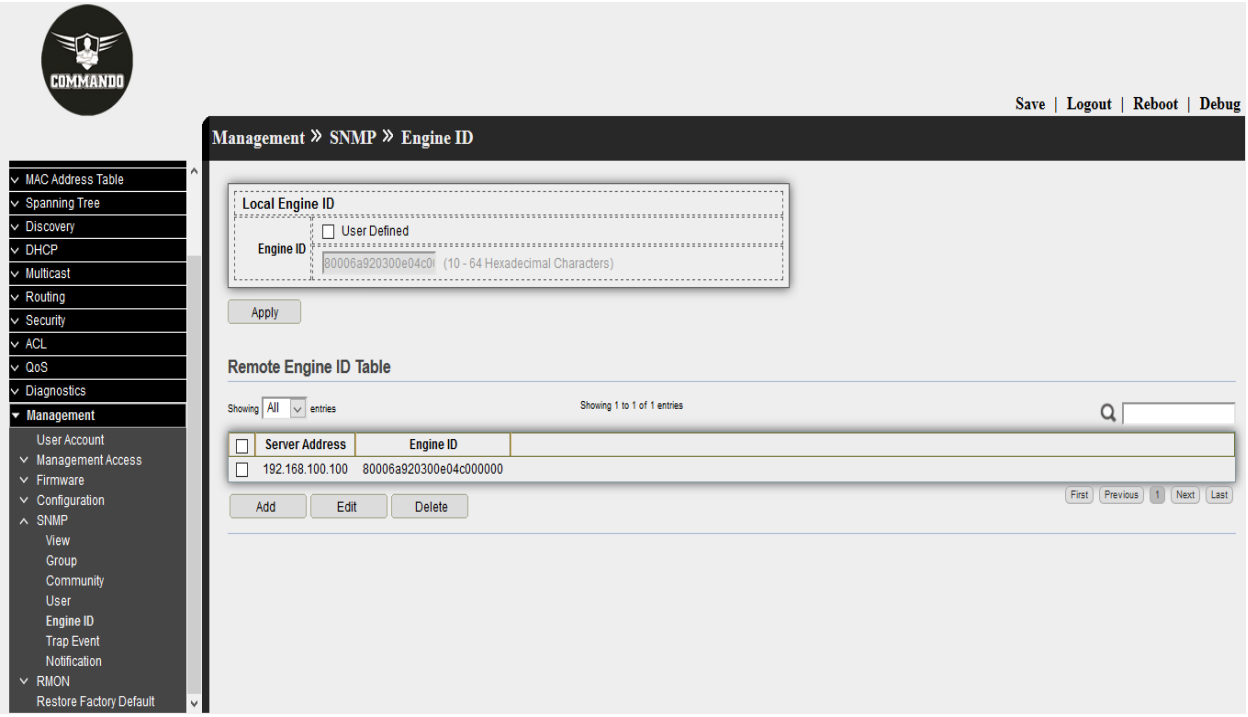


Fig 16.5.15 SNMP Add Remote Engine ID page

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.**

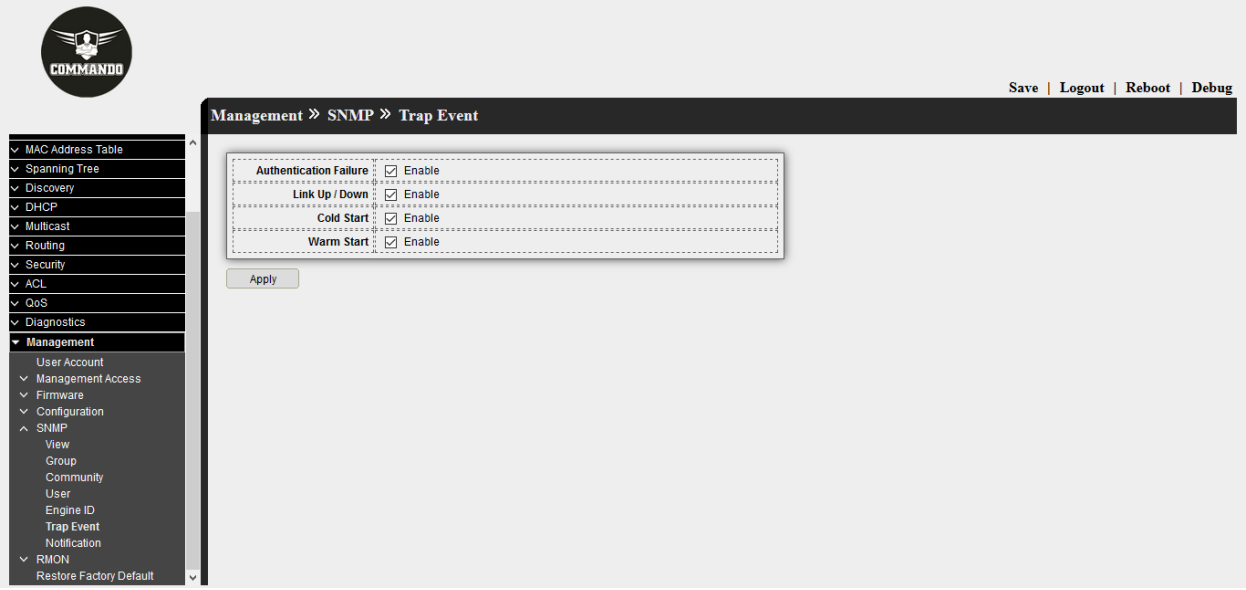


Fig 16.5.16 SNMP Trap Event page

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.**

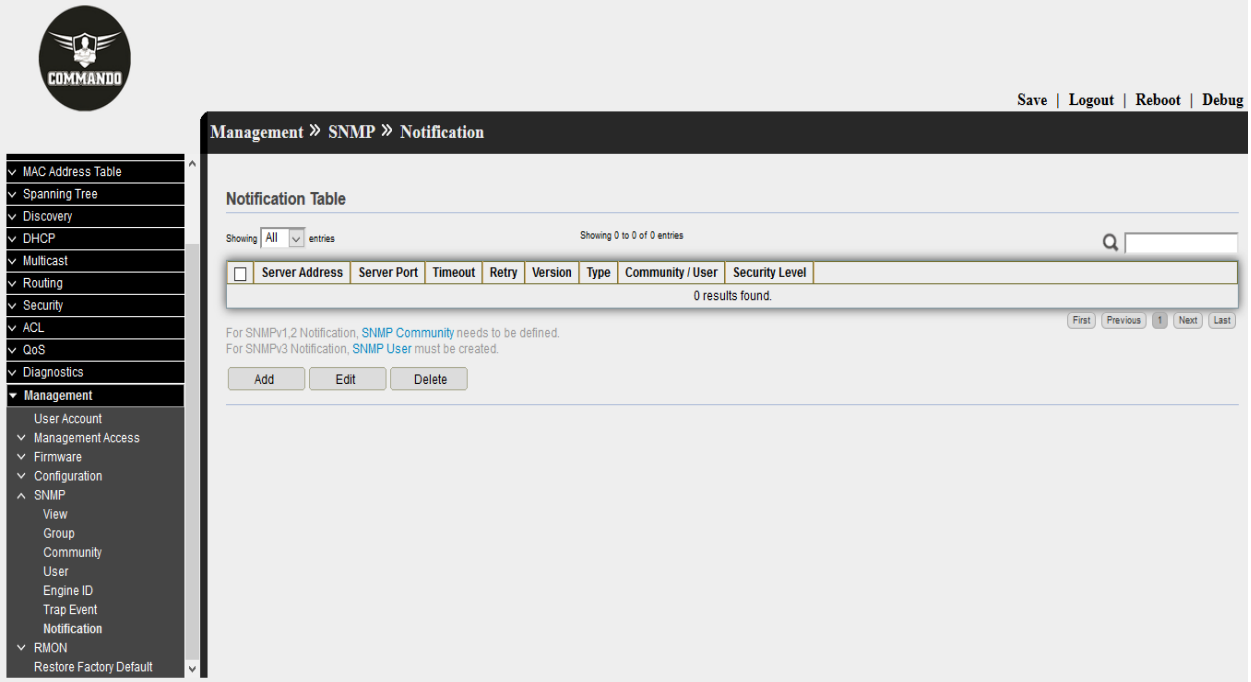


Fig 16.5.17 SNMP Default Notification Table page

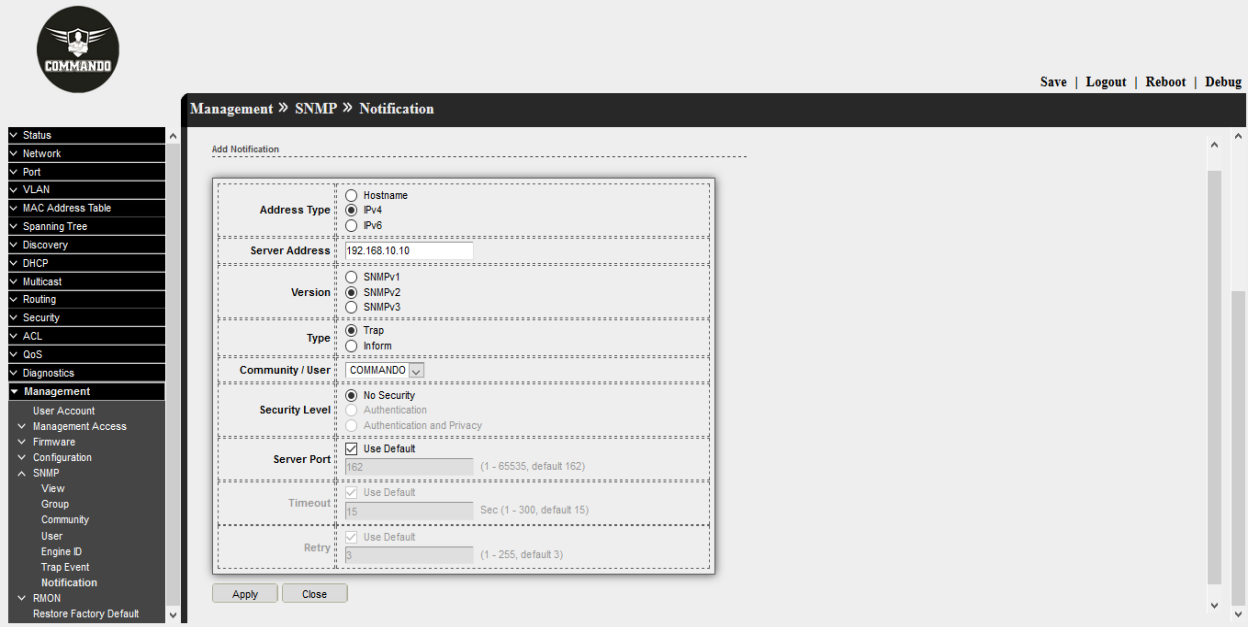


Fig 16.5.18 SNMP Add Notification page

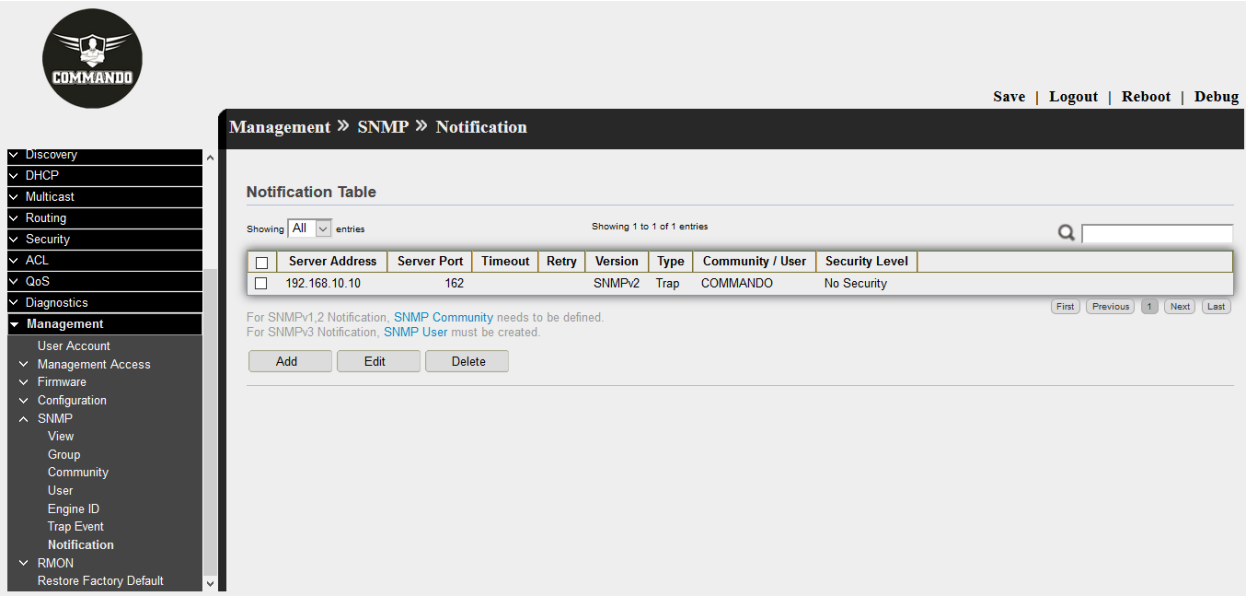


Fig 16.5.19 SNMP Notification Table page

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.**

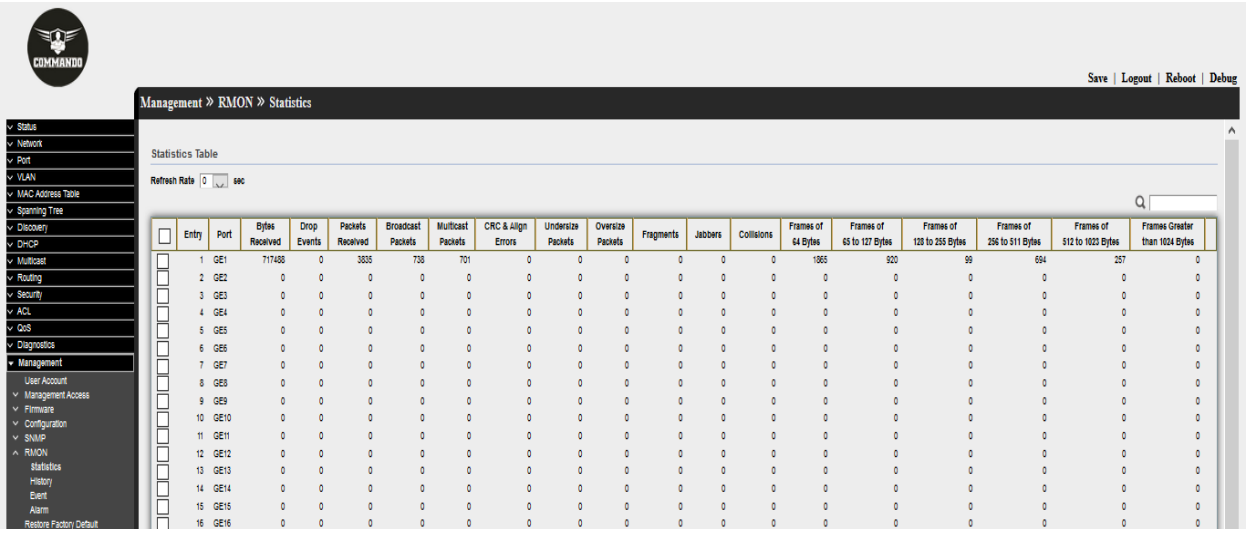


Fig 16.6.1 RMON Statistics Table page

15.5.2 History

The History Table page defines the sampling frequency, amount of samples to store and the port from where to gather the data.

To view and configure RMON history, click **Management >> RMON >> History.**

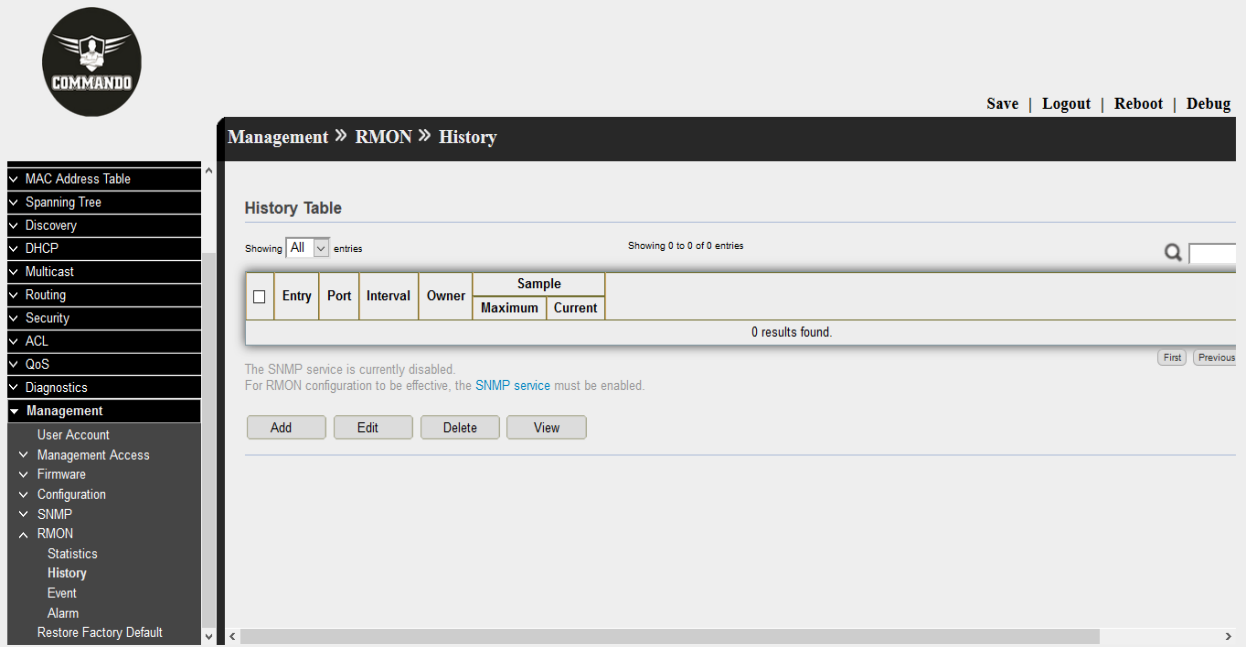


Fig 16.6.2 RMON Default History Table page

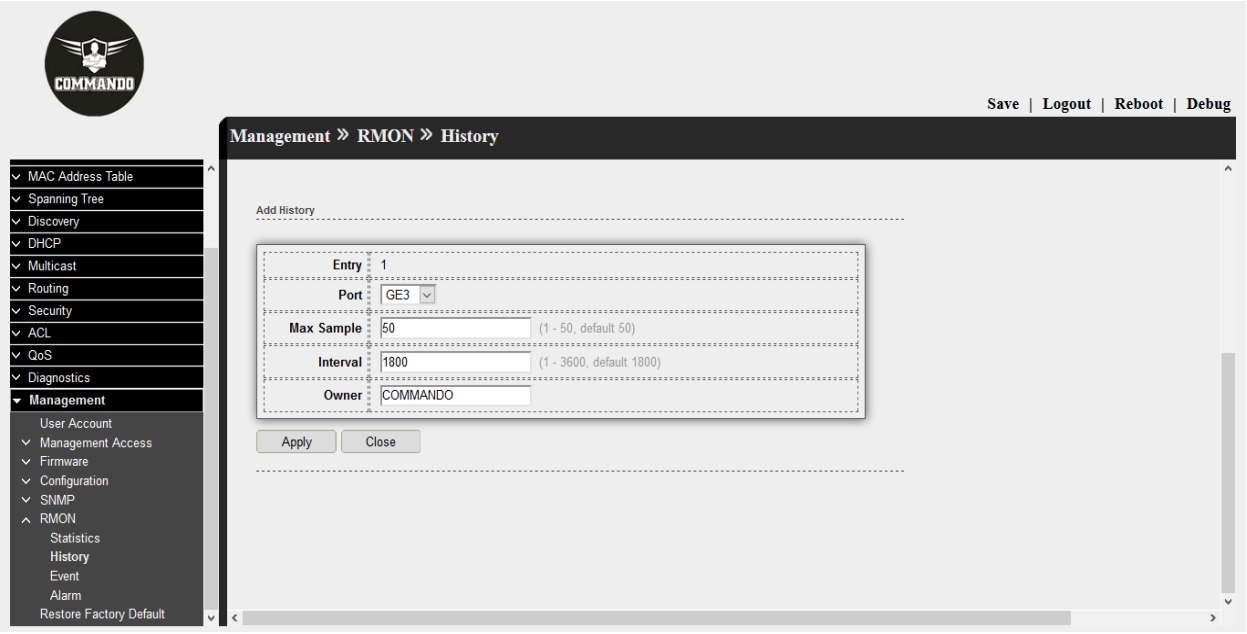


Fig 16.6.3 RMON Add History page

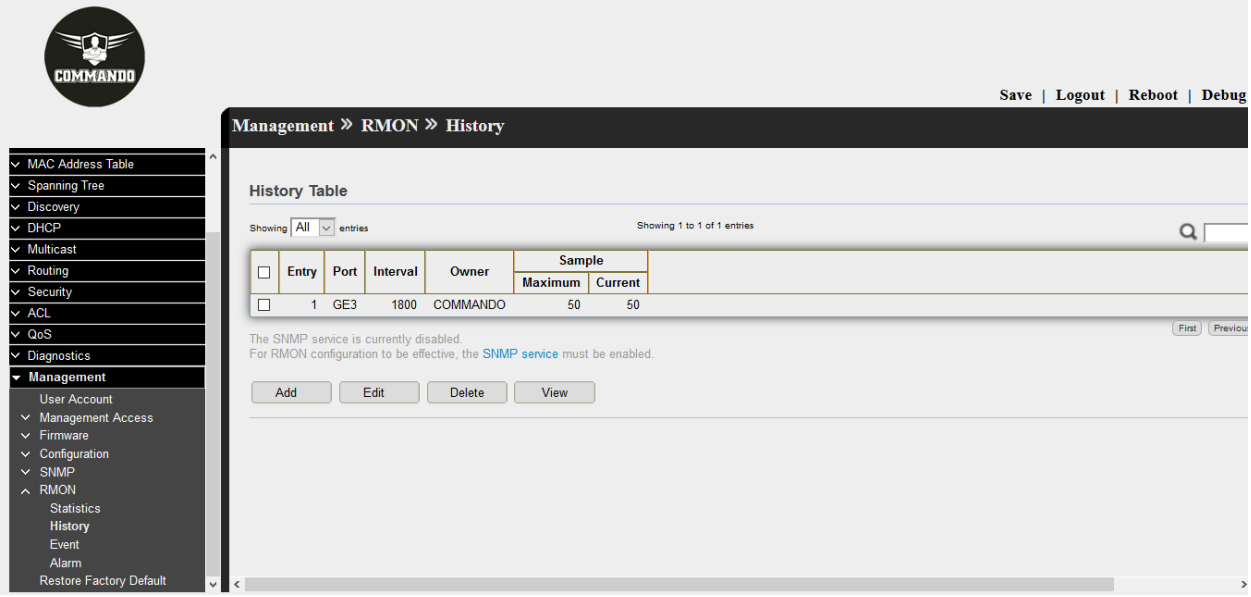


Fig 16.6.4 RMON History Table page

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.**

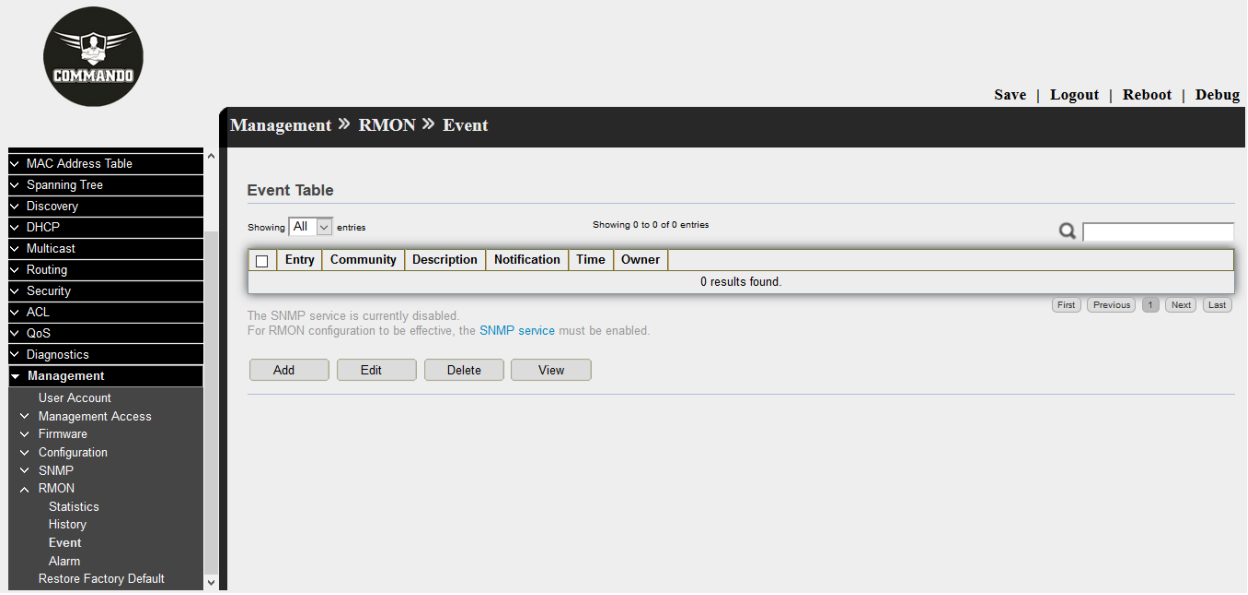


Fig 16.6.5 RMON Default Event Table page

Fig 16.6.6 RMON Add Event page

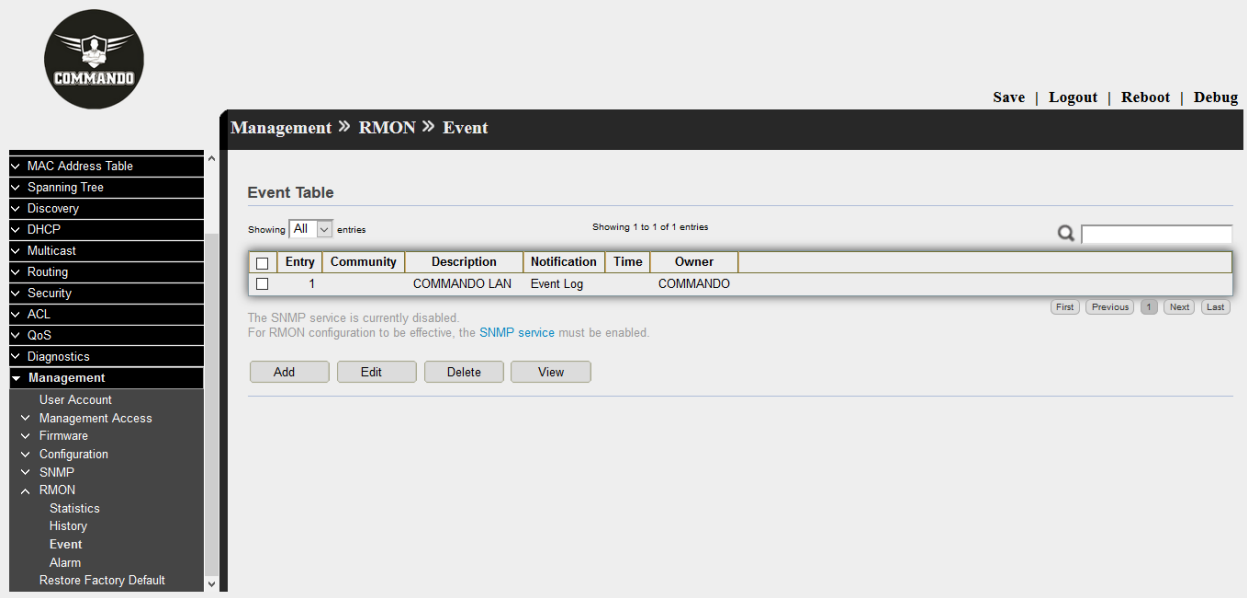


Fig 16.6.7 RMON Event Table page

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.**

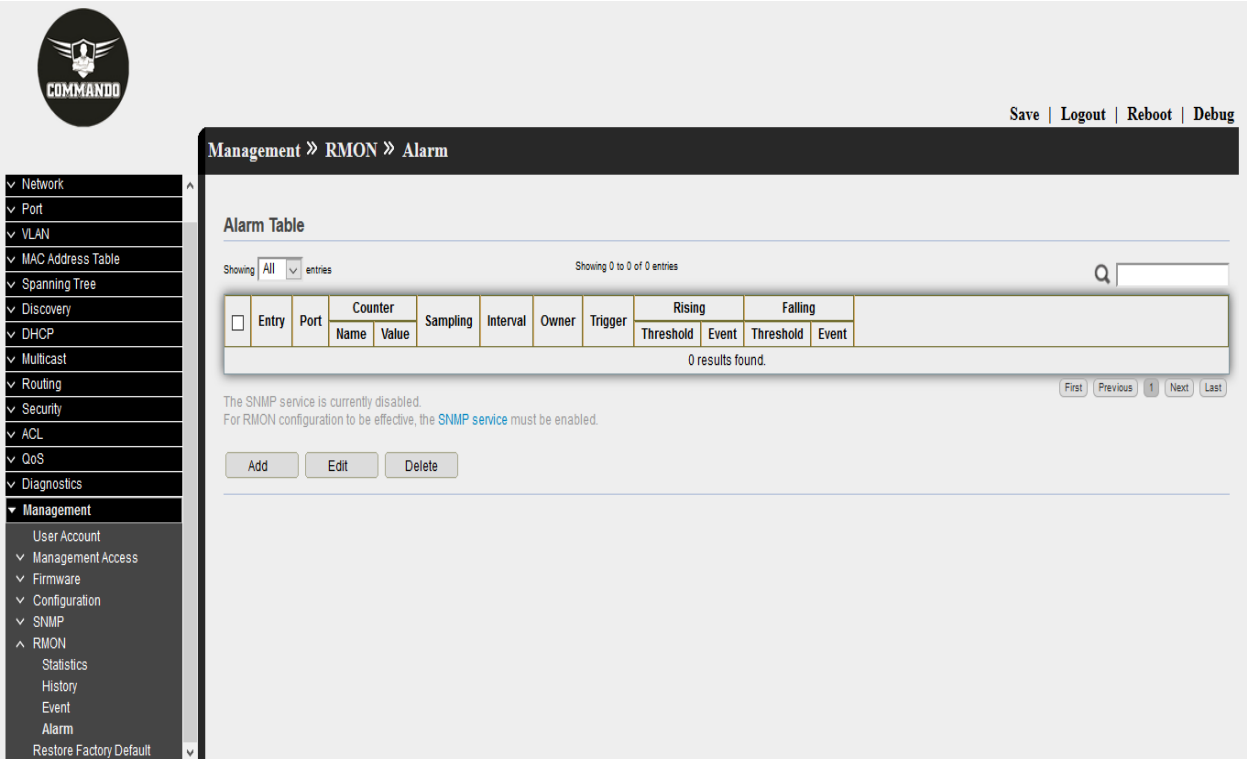


Fig 16.6.8 RMON Default Alarm page

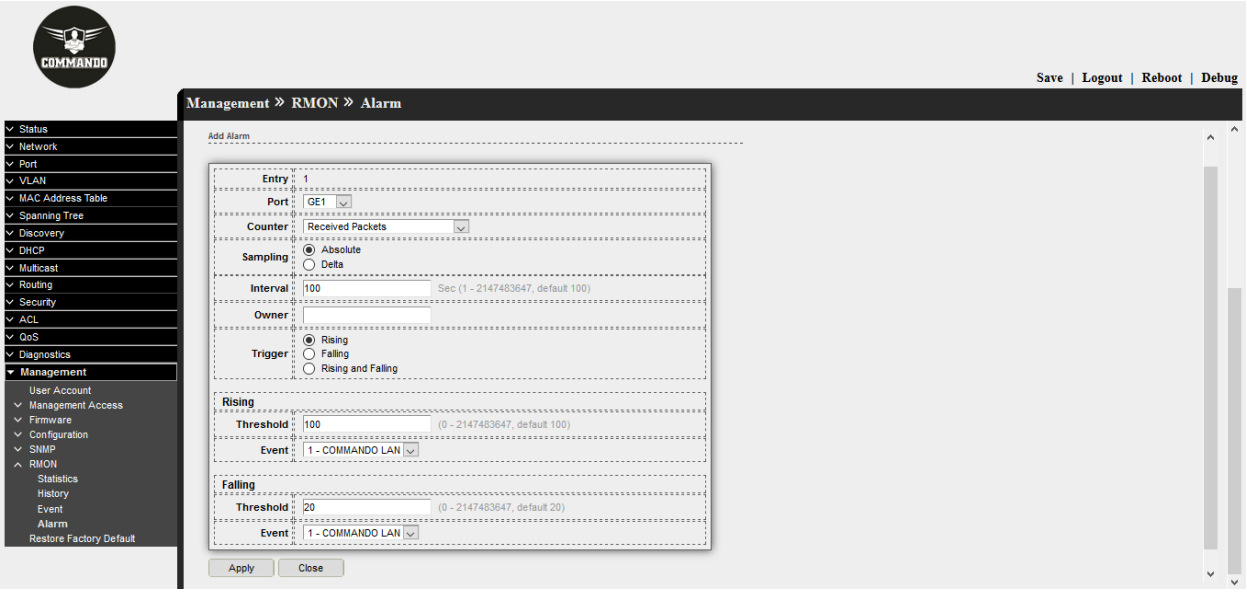


Fig 16.6.9 RMON Add Alarm Counter page

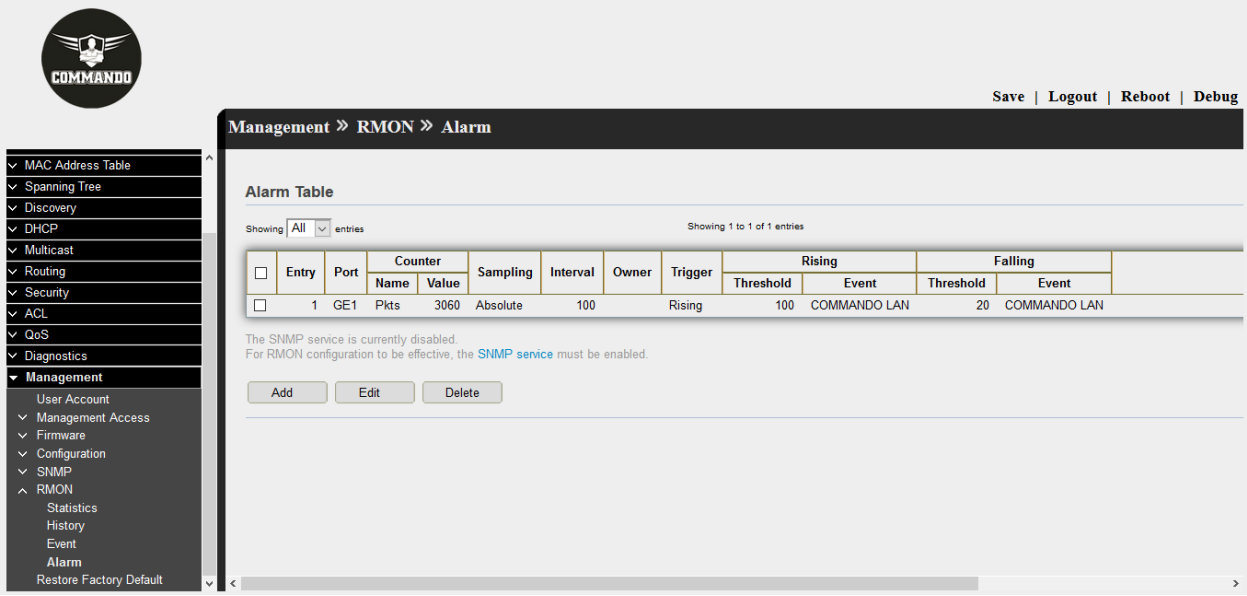


Fig 16.6.10 RMON Alarm Table page

16.7 Restore Factory Default

Hardware also you can factory reset the C2000 Switch by Press and hold the reset button on the front panel with a pin, while holding down the reset button turn on the switch (plug the power back into the device), please keep on holding down the reset button for approximately 10 seconds. Release the reset button and wait for the device to reboot.

For Software reset use Restore Factory Default, Click **Management>>Restore Factory Default** and again reboot the Switch to get factory default configuration in C2000 Series Switches.

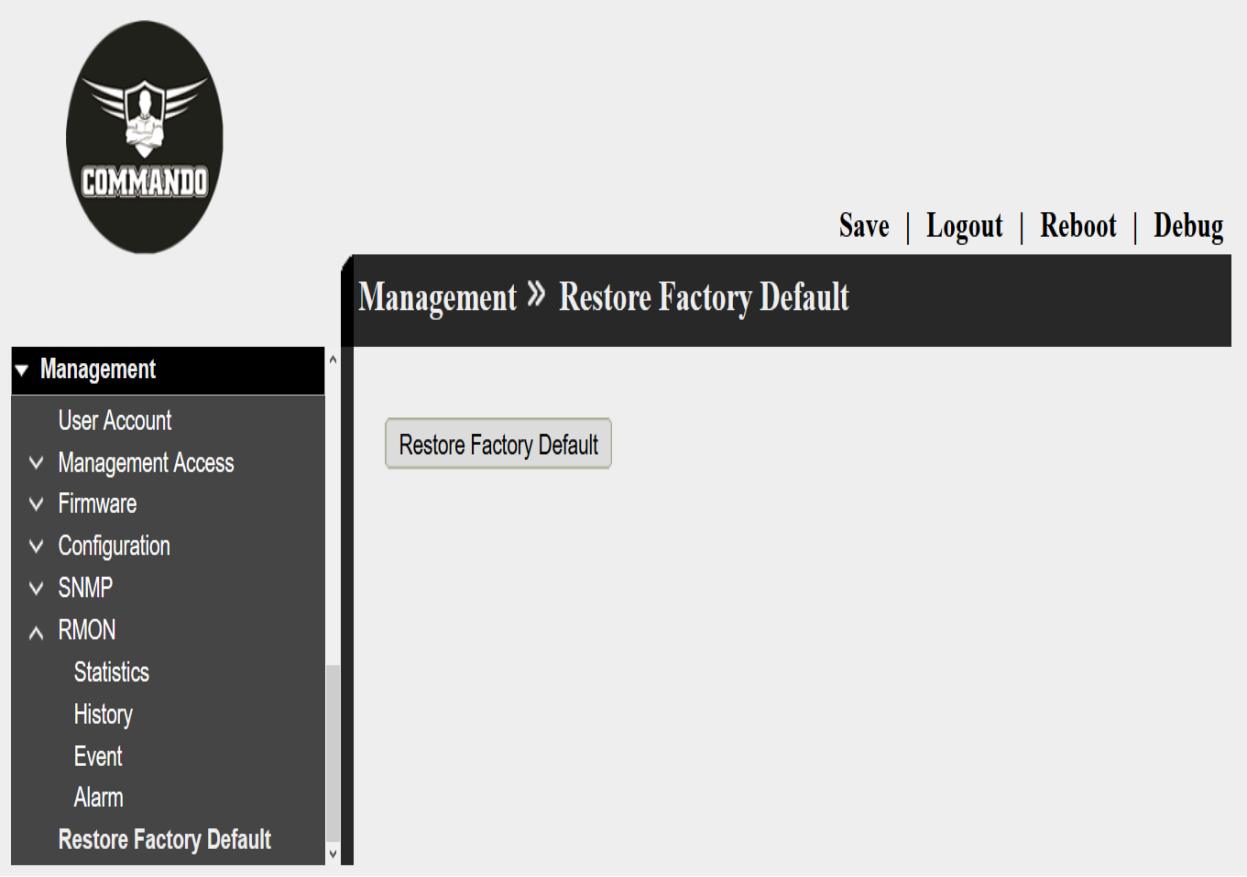


Fig 16.7.1 Restore Factory Default page

17. PoE/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 and IEEE802.3bt. Currently, the max amount of power provided over Cat5 cabling is 15.4 watts for PoE, 25.5 watts for PoE+ and up to 90Watt for PoE++ supported by C2000 series Switches.
Note:- This topic is applicable only for PoE/PoE+/PoE++ C2000 Series PoE Switches Only.

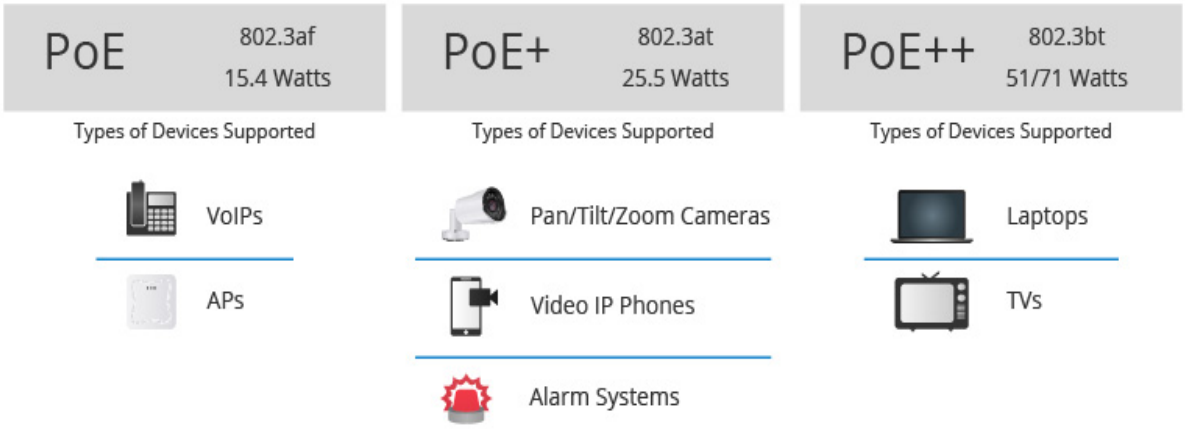


Fig 17.1 C2000 Series PoE/PoE+/PoE++ Switches Concept

16.1.1 POE Port Setting

The PoE/PoE+/PoE++ Settings page displays system PoE/PoE+/PoE++ information for auto enabling PoE/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.**

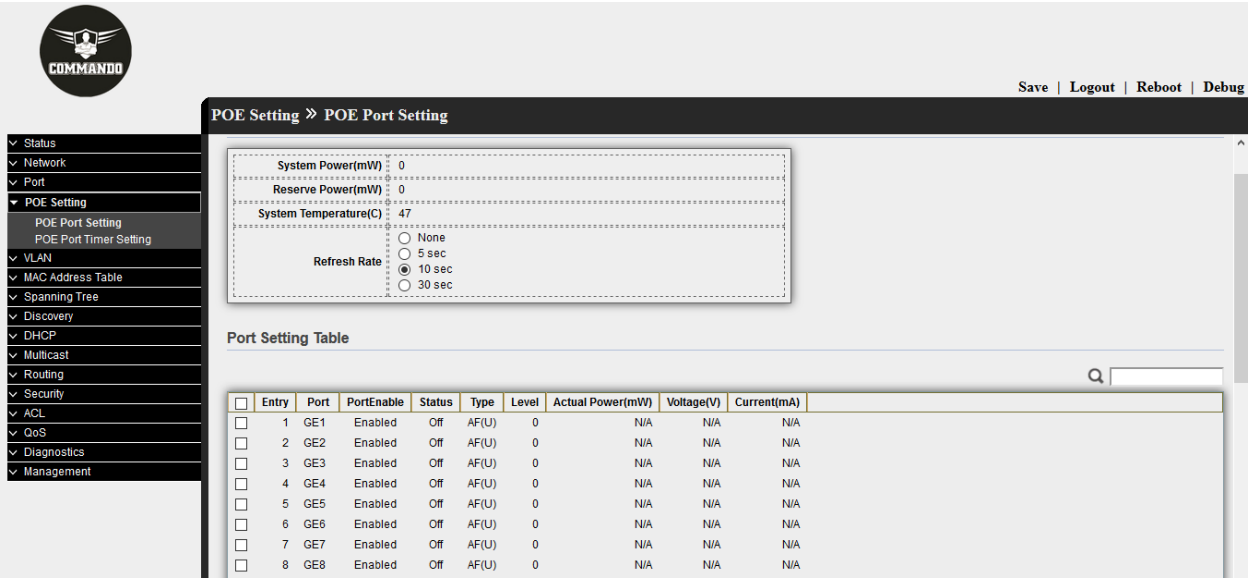


Fig 17.1.2 PoE Port Setting System Default Info page

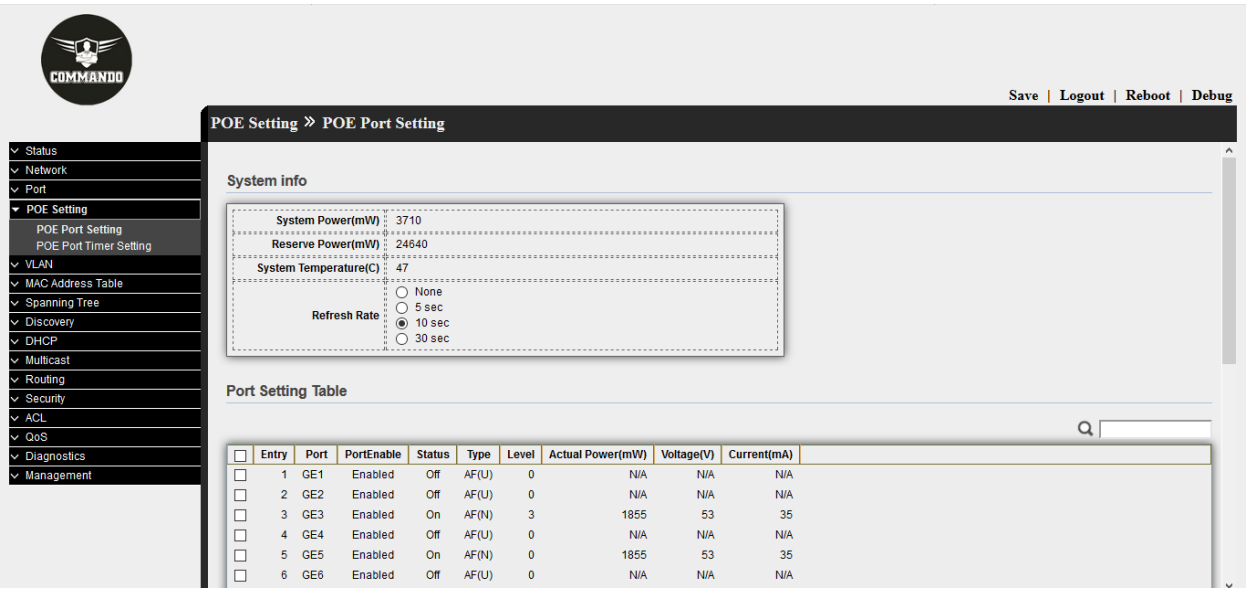


Fig 17.1.2 PoE Port Setting System Info after adding PoE devices page

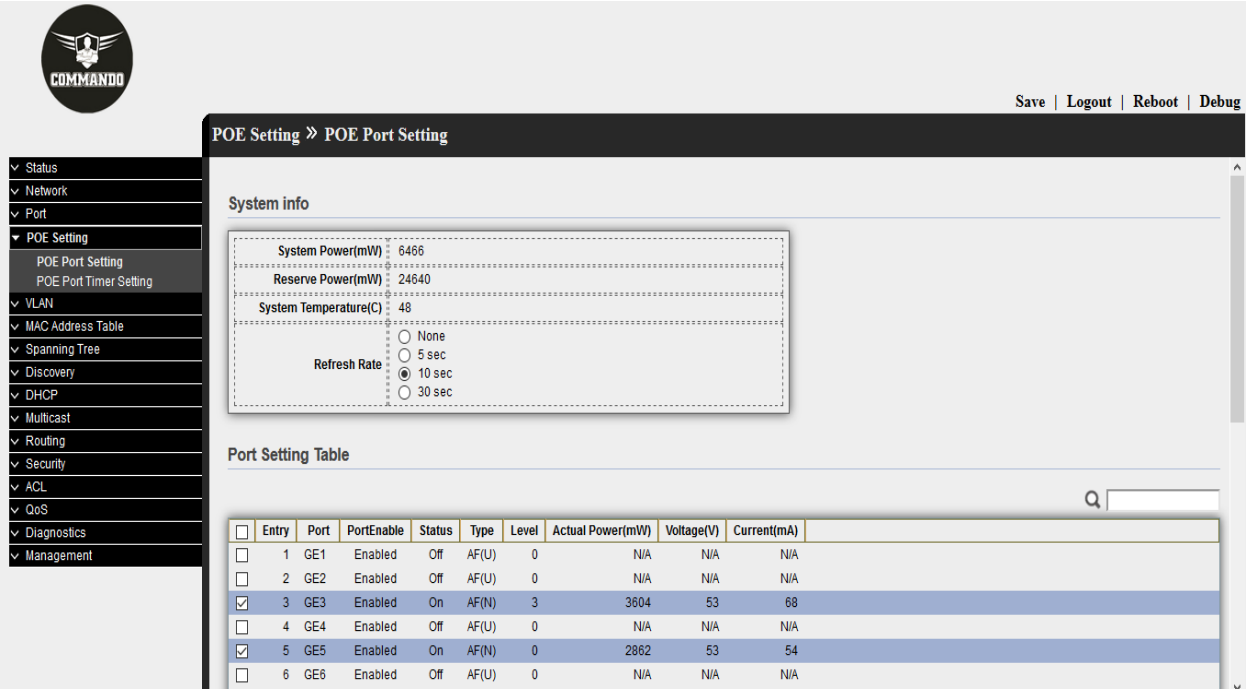


Fig 17.1.3 Selecting PoE Port for Setting page

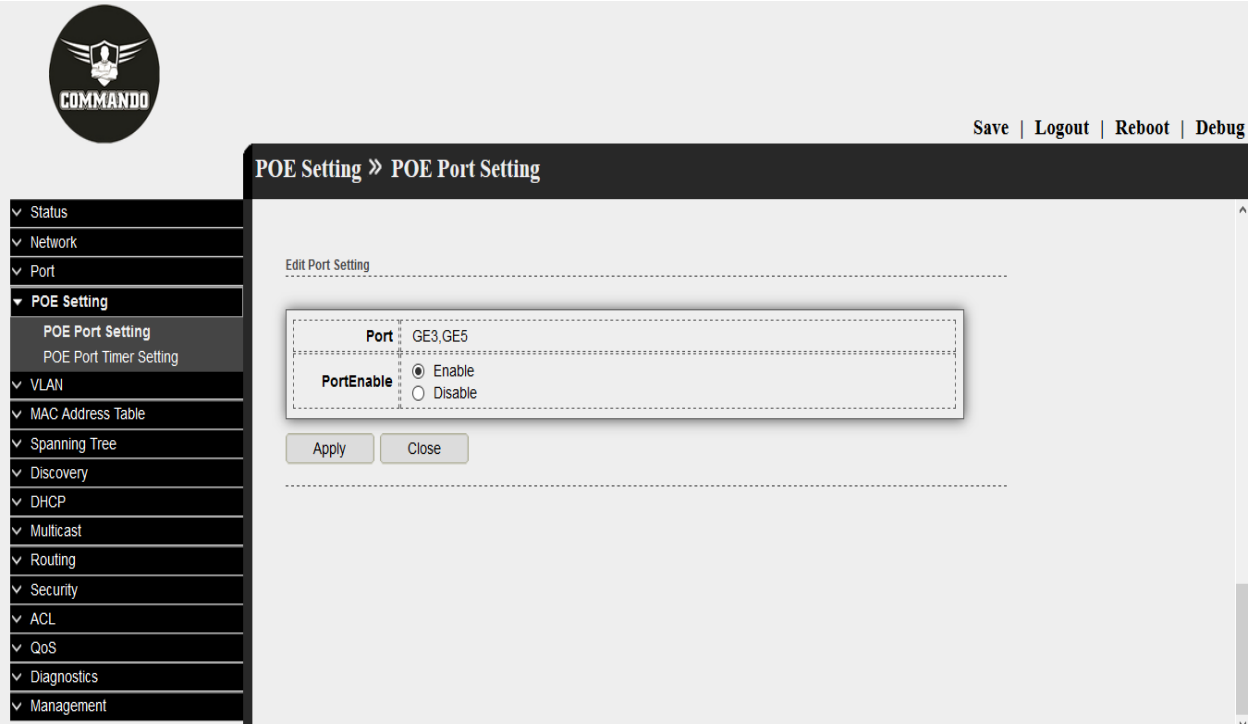


Fig 17.1.4 Edit PoE Port Setting page

17.2 POE Port Timer Setting

PoE/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+/PoE++ power continuously. C2000 Series Switches auto ON/OFF PoE/PoE+/PoE++ as per Scheduled time which makes them intelligent. PoE/PoE+/PoE++ Scheduling is a feature which allows you to specify the amount of time that power is delivered to a PoE/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.**

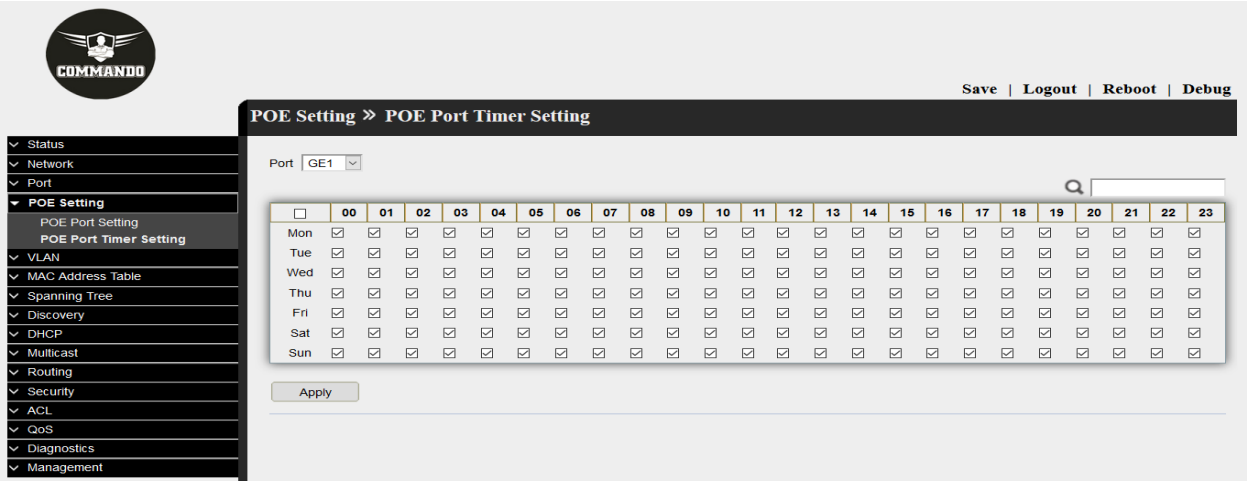


Fig 17.2.1 Default PoE Port Timer Setting for GE1 page

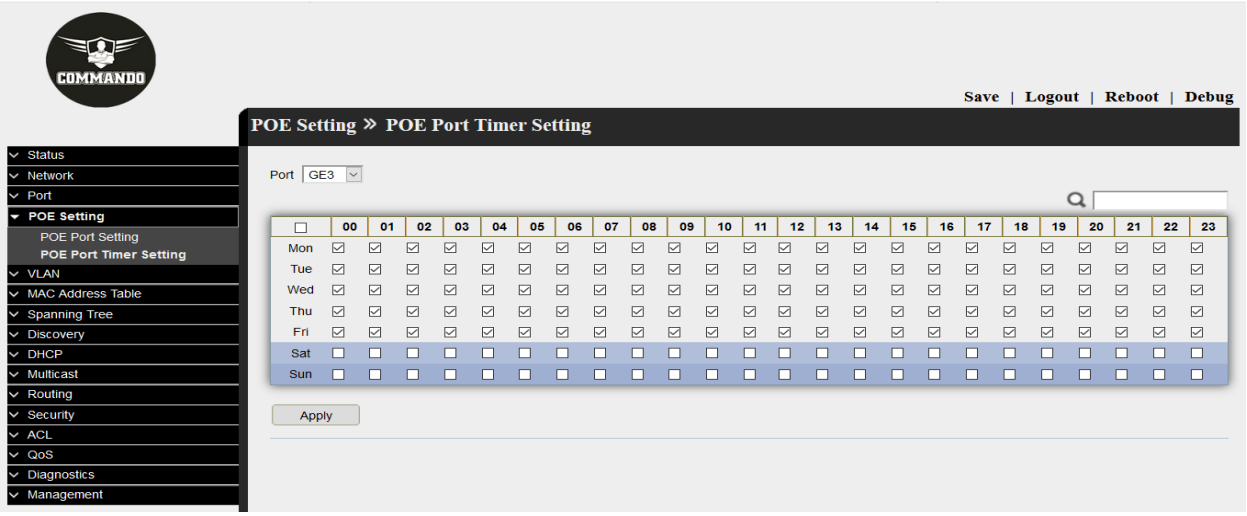


Fig 17.2.2 Turning Off PoE Port Timer Setting for GE3 for Saturday and Sunday page