

COMMANDO C2000 Managed Switch Web Manual

SoliderOS Version 1.4 Onwards

Copyright © 2020 COMMANDO Networks, All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of COMMANDO Networks Ltd.

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 or representations of any kind, either express or implied.

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

TABLE OF CONTENTS

Introduction

1.COMMANDO Solider OS
1.1 Web Interface
1.2 Menu Description

2. Status

2.1 System Information
2.2 Logging Message
2.3 Port
2.3.1Statistics
2.3.2 Error Disabled
2.3.3Bandwidth Utilization
2.4 Link Aggregation
2.5 MAC Address Table

3. Network

3.1 IP Address
3.2 DNS
3.3 Hosts

4. Port

4.7 Storm Control
4.8 Mirroring

5. VLAN

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

6. MAC Address Table

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

7. Spanning Tree

7.1 Property

7.2 Port Setting
7.3 MST Instance
7.4 MST Port Setting
7.5 Statistics

8. Discovery

8.1 LLDP
8.1.1 Port Setting
8.1.2 MED Network Policy
8.1.3 MED Port Setting
8.1.4 Packet View
8.1.5 Local Information
8.1.6 Neighbor
8.1.7 Statistics

9. DHCP

9.1 Property
9.2 IP Pool Setting
9.3 VLAN IF Address Group Setting
9.4 Client List
9.5 Client Static Binding Table

10. Multicast

10.1 General
10.1.1 Property
10.1.2 Group Address
10.1.3 Router Port
10.1.4 Forward All
10.1.5 Throttling
10.1.6 Filtering Profile
10.1.7 Filtering Binding
10.2 IGMP Snooping
10.2.1 Property

10.2.2 Querier
10.2.3 Statistics
10.3 MLD Snooping
10.3.1 Property
10.3.2 Statistics
10.4 MVR
10.4.1 Property
10.4.2 Port Setting
10.4.3 Group Address

11. Routing

11.1 IPv4 Management and Interfaces
11.1.1 IPv4 Interface
11.1.2 IPv4 Routes
11.1.3 ARP
11.2 IPv6 Management and Interfaces
11.2.1 IPv6 Interface
11.2.2 IPv6 Addresses
11.2.3 IPv6 Routes
11.2.4 IPv6 Neighbors

12. Security

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

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

13. ACL

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

14. QoS

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

15. Diagnostics

14.5 Logging

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

16. Management

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

16.5.1 Statistics
16.5.2 History
16.5.3 Event
16.5.4 Alarm
16.6 Restore Factory Default

17. POE

17.1 PoE Port Setting
17.2 PoE Port Schedule Setting

Chapter 1 Introduction

COMMANDO Soldier 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++ 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 webbased 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 formfactor, 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++ 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 webbased 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 / TeInet/ 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**

🕵 PuTTY Configuration		?	Х
Category:			
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial 	Basic options for your PuTTY se Specify the destination you want to conner- Serial line COM4 Connection type: Raw Telnet Rlogin SS Load, save or delete a stored session Saved Sessions Default Settings Close window on exit: Always Never O Only on c	ession Speed 115200 H Se Loac Save Delet clean exit	erial
About Help	Open	Cano	el

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

Internet Protocol Version 4 (TCP/IPv4) Properties						
General						
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.						
Obtain an IP address automatical	y					
O Use the following IP address:						
IP address:	192.168.0.11					
Subnet mask:	255.255.255.0					
Default gateway:	192.168.0.1					
 Obtain DNS server address autom 	natically					
• Use the following DNS server add	resses:					
Preferred DNS server:						
Alternate DNS server:	· · ·					
Validate settings upon exit	Advanced					
	OK Cancel					

Fig-5. Local Area Connection properties for Web Interface

Now Open any web browser type <u>http://192.168.0.1</u> 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

COMMANDO	Status » System Information	Save Logout Reboot Debug
status System Information System Time Logging Message vert Link Aggregation MAC Address Table vetwork		
v Port		
∨ VLAN	System Information Edit	
V MAC Address Table		
v spanning i ree	MOOH FILSSELI 22	
V DHCP	j Spiten Name Sutch	
 Multicast 	System Location default en	
v Routing	System Contact debut sow	
 Security 	Serial Number 0123457769 47%	
V ACL	27 Tage 1	
v Q0S	MAC Address 00E0 4C 0000 00 27%	
 Diagnostics 	i IPv4 Address = 152:158.0.1	
✓ Management	Bod Lidness 567 99/Littlefon()24	
	system Uptime - v Cogi Ori, 5 min and 5 ee	
	Current Time 2019-12-31 1704-36 UTC-7	
	Loader/Version 10.06	
	Losder Dele Nov 17 2019 - 1817/03	
	Firmware/Version Solie/OS 2X/1/4 5%	
	Firmare Date - Se 02 0201 - 16 28 18 29	
	a a a a a a a a a a a a a a a a a a a	
	Tende Disable 2%	
	SSH Disabed 27	
	HTTPs Disoled	
	SIMP Disable	

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 Access 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).

SA-5 SA-5 SA-5 SA-7 AN AC Address Table Sammajor Tree Bookery HCP JICOSST Oxdrag Samsagement Samsagement Xocus Management Access Station Station Management Access Management Access Management Access Management Access Station Management Access
Analysis Management >> Management Access >> Management Service Analysis Imagement Service Analysis Imagement Service Analysis Imagement Service Analysis Imagement Service AccAdress Table State AccAdress Table State AccAdress Table State Scovery Imagement HCP Imagement Management Enable Scovery Imagement HCP Imagement Scovery Imagement HCP Imagement Scovery Enable Scovery Imagement Scovery Enable Scovery Enable<
Management Service Management Service Teinet Teinet Saturation ast Set Set Solution Setsion Timeout
Work t N C Address Table ming Tree Orep HTTP Enable Stast ding Management Access Management Acce Manage
t Management Service NN Teinet [] Enable C Address Table Service sming Tree Service CP HTTP []] Enable HTTP []] Enable Enable CP HTTP []] Enable Micast Enable Signostice Service Inagement Acces Finet [10] Management Acce Min (0 - 65535, default 10) Management Acce Finmware Numagement Acce Finmware Sonduration Simulation MAnagement Acce Min (0 - 65535, default 10) Management Acce Min (0 - 65535, default 10) HTTP [] [0] Min (0 - 65535, default 10) HTTP [] [0] Min (0 - 65535, default 10) HTTP [] [0] Min (0 - 65535, default 10) HTTP [] [0] Min (0 - 65535, default 10) HTTP [] [0] Min (0 - 65535, default 10) HTTP [] [0] Min (0 - 65535, default 10) HTTP [] [0] Min (0 - 65535, default 10) HTTP [] [0] Min (0 - 65535, default 10) HTTP [] [0] Min (0 - 65535, default 10) HTTP
N Teined: Enable Address Table SHI Enable SHI Enable Enable Address Table SHI Enable Address Table SHI Enable Address Table SHI Enable P Cast Enable Ing Enable Enable Mangement Enable Enable Second Teinet 10 Management AcC Min (0 - 65535, default 10) Enable Management AcC SHI 10 Management AcC Min (0 - 65535, default 10) Enable Management AcC SHI 10 Min (0 - 65535, default 10) HTTPS 10 Min (0 - 65535, default 10) Enable Management AcC SHI 10 Min (0 - 65535, default 10) HTTPS 10 Min (0 - 65535, default 10) Enable HTTPS 10 Min (0 - 65535, default 10) Enable HTTPS 10 Min (0 - 65535, default 10) Enable HTTPS 10 Min (0 - 65535, default 10) Enable
Address Table ing Tree exy set set set set set set set se
SSH Enable or Finally or Finally st State state State
MTTE State
Set Image: Simple interview in
Site Image 9 SNMP 9 Enable Session Timeout Console 10 Min (0 - 6533, default 10) anagement Accesss anagement AcL anagement AcL anagement Acc Ap Min (0 - 6533, default 10) ON Enable ON Enable SH 3 SH 3 SH 3 SH 3 Silent Time
SNMP Enable ty SNMP Struct Enable ty Second Total second Total regement Console regement Total stanagement Min (0 - 65535, default 10) regement VLAN State tanagement ACcess State transperent ACL HTTPS tanagement ACC Min (0 - 65535, default 10) tanagement ACC HTTPS transperent ACC Min (0 - 65535, default 10) tanagement ACC HTTPS transperent ACC Min (0 - 65535, default 10) tanagement ACC HTTPS transperent ACC State
Session Timeout Session Timeout Session Timeout Session Timeout Console John (0 Session Timeout Console Tellet 10 Man (0 Session Timeout Console Tellet 10 Man (0 Session Timeout Session Timeout Session Timeout Session Timeout Session Timeout Man (0 Session Timeout Tomagement Acce Mark Mark Session Timeout Session Timeout <tr< th=""></tr<>
Session Timeout sigement er Account sargement Access Management VLAN Management AccL Management AccL
Session Timeout Sessi
console 10 Min (0 - 6533, default 10) agement 4 Teinet 10 Min (0 - 6533, default 10) aragement Access danagement VLAN fanagement ACL fanagement ACL fanagement ACL mware Min (0 - 6533, default 10) Arangement ACL fanagement ACL fanage
Account er Account magement Xocess Xanagement XOLN Aanagement ACL Management ACL Management ACL Management ACL Management ACL Management ACL Management ACL Management ACL Min (0 - 65535, default 10) Min (0 - 65535, default 10) Password Retry Count Min (0 - 65535, default 10) Min (0 - 65535, default 10) Password Retry Count Min (0 - 65535, default 10) Password Retry Count Min (0 - 120, default 3) Store Factory Default Stilent Time
Sgement nagement Access (brangement Access (brangement Access (brangement Access) Imagement in 10 (0 - 6553, default 10) SBH 10 (0 - 6553, default 10) Management Access (brangement Access) Imagement Access (brangement Access) State Factory Default
er Account magement Access tranagement Access tranagement ACL tranagement ACL tranagem
Inagement Access Imagement Access Kanagement VAN Imagement Access Kanagement Acc Imagement Acc Min (0 - 6553, default 10) Kanagement Acc Imagement Acc <tr< th=""></tr<>
anagement VLAN lanagement Service anagement ACL anagement ACL mware miguration MP Kon store Factory Default HTTP [0 Min (0 - 65535, default 10) Password Retry Count MP Kon Store Factory Default Password Retry Count (0 - 120, default 3)
Management Service HTTPS 10 Min (0 - 65535, default 10) Management ACL HTTPS 10 Min (0 - 65535, default 10) Management ACE Password Retry Count Password Retry Count Introduction Introduction Introduction MAR Console 5 (0 - 120, default 3) Mon Introduction Introduction Introduction State Introduction Introduction Introduction Introduction Introduction Introduction Introduction Mon Introduction Introduction Introduction State Introduction Introduction Introduction State Introduction Introduction Introduction State Introduction Introduction Introduction
anagement NCL anagement ACE HTTPS:::::::::::::::::::::::::::::::::::
Password Retry Count Ap Consol 5 (0 - 120, default 3) Silent Time
And guration (A de) ACN ACN NCN Rebore Factory Default Silent Time Silent Time
NM/P Console 3 (0 - 120, default 3) MON
MON Estore Factory Default Silent Time
eetore Factory Default Telnet 3 (0 - 120, default 3) Silent Time
\$\$#1 3 (0 - 120, obtault 3) Silent Time
Silent Time
Silent Time
Silent Time
Console !! 0 Sec (0 - 65535, default 0)
Teinet 0 Sec (0 - 65635, default 0)
SSH Sec (0 - 65535, default 0)

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.

0+ 12

← -	→ C	A	Not secure	e 192	2.168.0.1/home	html																	☆	*	4
		ANDO)																						
				St	atus » Syst	em Inf	ormation													Sa	ve	Logout	Reb	oot	1
v Sta S S U V P Li M	tus ystem Ir ystem Ti ogging N ort ink Aggre IAC Addi	nformat ime Aessage egation ress Tab	lion 9		SOLDIER C2000 L2 Managed Bwit C2000-24G+	BDF O Nexes	E + 48FP Uplink.		61	63 (***) (***) (***)	63	67 (***) (***) (***) (***)	C6	G11 	613	G13	G17	618	031 (***) (***) (***)	633 (***) (***) (***)		•			
< Neb	work																								
Por	1			- 1																					
< VLA	N			- 1	System Info	rmation				E	512	1001	-					-	100						
< MAI	C Addres	ss Table		- 1		Model	DTI 9392M	**********				90	·						CPU						
Spa	nning Tr	66		- 1		history	Cultab					80	۰ <u></u>												
Disc	overy			- 1	Syster	n Name	switch					70													
	utr Konst			- 1	System L	ocation	default					807	•												
- Mul	tina			- 1	System	Contact	default					507	•												
< 800	uny			- 1	Serial	Number	0123456789					40	•												
ACI	uny			- 1								30	•												
2 005	-			- 1	MAC	Address	00:E0:4C:00:0):00				201	•												
Dia	nostics			- 1	IPv4/	ddress	192.168.0.1					101	•												
Mar	anemer	nt .		- 1	IPv6 /	\ddress	fe80_2e0.4cff1	e00:0/64				0		17:07:00	17	08:00	17:09:	0	17:10:00						
				71	Svs	em OID	136141272	82.1.1								Time									
					Sustan	Untime	0 day 0 br 10	min and 44 a																	
					System	opame	0 day, 0 hr, 10	mm and 44 S	ec.																
				1																					
_	-	-						_	-				-	-	-	-	-					-	-	-	-

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 SoliderOS 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.

	COMIMIANDO
٨	Status
\sim	Network
\sim	Port
\sim	VLAN
\sim	MAC Address Table
\sim	Spanning Tree
\sim	Discovery
\sim	DHCP
\sim	Multicast
\sim	Routing
\sim	Security
\sim	ACL
\sim	QoS
\sim	Diagnostics
\sim	Management

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.

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

Table 1.1 C2000 Series Switches SoliderOS Web Software Frameworks.

	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. Intelligent 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

COMIMANDO				Save	Logoi	ıt Re	boot	Debug	
✓ Status ^									^
	SOLDIER C20	C 2405 + 405 + 4050 Halat	G3						
	L2 Managed								
		Save running configuration to startur							
	C2000-24	configuration. Do you want to continue	e?						
			G4						
 ✓ Network ✓ Port 		OK							
	Sustan								
	System								
✓ Spanning Tree		Model RTL8382M							
✓ Discovery	Syst	em Name Switch							
✓ DHCP ✓									

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

COMMANDO					Save	Logou	ıt R	eboot	Debug
▼ Status ^									
System Information	SOLDIER C2000		G1	G3					
System Time	L2 Managed								
 ✓ Port 		Logout will disconnect	your current						
Link Aggregation	C2000-24	session. Do you want to	o continue?						
MAC Address Table				G4					
		OK Canc	el						
✓ VLAN									
✓ MAC Address Table	System I			Ec					
✓ Spanning Tree		Model RTL8382M							
✓ Discovery	System	Name Switch							
✓ DHCP v	<								

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

COMMANDO				Save	Logou	1t R	eboot	Debu
✓ Status ^								
System Information		D Hafak	G1					
System Time	L2 Managed							
Logging Message	Reboot the sys	tem and unsaved cha	anges in					
Link Aggregation	c2000-24 the configuration	on will be lost. Do y	ou want					
MAC Address Table		to continue?						
✓ Network								
✓ Port		OK Cancel						
VLAN	System I							
✓ MAC Address Table								
✓ Spanning Tree								
✓ Discovery	System Name Swite							
✓ DHCP ✓	<							>

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

COMMANDO	Status » System Inform	ation	Save Logo	ut Reboot <mark>Debug</mark>
✓ Status System Information System Time	Debug Messages			
Logging Message Port Link Aggregation	Showing All v entries	Showing 0 to 0 of 0 entries	(۵,
MAC Address Table	Entry	Message		
✓ Network		o results iouria.		
✓ Port	Delete		First	Previous 1 Next Last
VLAN				
✓ MAC Address Table				
✓ Spanning Tree				
✓ Discovery				
✓ DHCP ✓				
Fig 1 2 7 View Dobuc	moccogo on W/ERI	П		

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.

COMMANDO	atus » System Information	Save Logout Reboot
→ Status ^	·	
System Information System Time Logging Message	Edit System Information	
Link Aggregation	System Name COMMANDO	
MAC Address Table	System Location US	
✓ Network		
✓ Port	System Contact 1234567890	
VLAN	L	
✓ MAC Address Table	Apply Close	
✓ Spanning Tree		
✓ Discovery		
✓ DHCP		
✓ Multicast		
✓ Routing		

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.

COMMANDO	Status » System Tim	e	
 Status System Information System Time 	Status # System Tim	O SNTP	uler
Logging Message V Port Link Aggregation MAC Address Table	Time Zone	Manual Time UTC -7:00 UTC -12:00	n
V Network V Port V VLAN V MAC Address Table	SNTP Address Type	UTC -11:00 UTC -10:00 UTC -9:00 UTC -8:00	
v Spanning Tree v Discovery v DHCP v Hollowsk	Server Address Server Port	UTC -7:00 UTC -6:00 UTC -5:00	(1 - 85535, default 123)
v Routing V Security V ACL	Date Time	UTC -4:30 UTC -4:00 UTC -3:30 UTC -3:00	YYYYY4MADD HHIMMISS
∨ QoS ∨ Diagnostics ∨ Nanagement	Daylight Saving Time	UTC -2:00 UTC -1:00 UTC	
	Туре	UTC +1:00 UTC +2:00 UTC +3:00 UTC +3:30	
	Offset	UTC +4:00 From: Day St	Min (1 - 1440, default 60)

Fig 2.4.2 Timezone configuration page

COMMANDO								
	Status » System T	ime						
✓ Status	Time	17:17:	54		HH:MM:SS			
System Information System Time Logging Message	Daylight Saving Ti	me						
✓ Port Link Aggregation MAC Address Table	Туре	No No No No No	ne curring n-recurring					
✓ Network		0 0a	ropen					
∨ Port	0#	<u>co</u>			NA:= /4			
VLAN	Unset	lon			Iviin (1 - 1440,	default 60)		
✓ MAC Address Table		From:	Day Sun	\sim	Week First 🗸	Month Jan 🗸	Time	
✓ Spanning Tree	Recurring	т	Davi			Manth Las	Time	
✓ Discovery		10.	Day		VVeek First	wonth Jan 🗠	rime	
✓ DHCP		From:			YYYY	-MM-DD		HH:MM
✓ Multicast	Non-recurring							
✓ Routing		10:			YYYY			HH:MM
✓ Security	,							
V ACL	Operational Statu	S						
V QoS	Current Time	2019-1	2-31 17:17:5	54 UTC	-7			
✓ Diagnostics								
∽ Management	Apply							

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.

COMMANDO	Status » System T	ime		
✓ Status ^				
System Information System Time Logging Message	Source	 ○ SNTP ● From Compute ○ Manual Time 	r	
Link Aggregation MAC Address Table	Time Zone	UTC -7:00 🗸		·
✓ Network	SNTP			
✓ Port		Hostname		
VLAN	Address Type	O IPv4		
 MAC Address Table 	Server Address			
✓ Spanning Tree	+			
✓ Discovery	Server Port	123	(1 - 65535, default 123)	
✓ DHCP				
✓ Multicast	Manual Time			
✓ Routing	Date	2020-10-05	YYYY-MM-DD	
✓ Security				
V ACL	lime	09:30:28	HH:MM:SS	
✓ QoS	,			
✓ Diagnostics	Daylight Saving Ti	me		
✓ Management		None		

Fig 2.4.4 Time configuration from connected computer page

	Status » System T	ime
✓ Status		
System Information	[]	
System Time		O SNIP
Logging Message	source	From Computer
✓ Port		Manual Time
Link Aggregation	Time Zone "	
MAC Address Table	L	
- Dort	CNITD	
		· · · · · · · · · · · · · · · · · · ·
MAC Address Table	Address Type	Hostname
Separating Tree		IPv4
Spanning mee		
· Discovery		
	Server Port	123 (1 - 65535, default 123)
Multicast Reuties	L	
 Robuing 	Manual Time	
 Security 	here a second a second	
✓ ACL	Date	2020-10-05 YYYY-MM-DD
~ Q65	Time	09:33:31 HH:MM.SS
 Diagnostics 	i	
Management	Davlight Saving	Time
	Daying in Saving	
		None
		O Recurring
	; Type ;	Non-recurring :
		O USA
		Europen
	Offset	60 Min (1 – 1440, default 60)
		From Day Sun Week First Month Jan Time
	Recurring	
		To: Day Sun Week First Month Jan Time
	Non-recurring	TTTT-MM-CD TTT-MM
		To: YYYY-MM-DD HH:MM
	L	
	Operational Stat	us
	Current Time	2000-10-05-02-22-21-117-0-44
	Current Time	2020-10-03 09:33 31 01 044

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.

COMMANDO	
	Status » System Time
System information	[]
System Time	● SNTP
Logging Message	Source From Computer
✓ Port	Manual Time
Link Aggregation	
MAC Address Table	
 Network 	
V Port	SNTP
~ VLAN	Hostname
 MAC Address Table 	Address Type
 Spanning Tree 	
 Discovery 	Server Address time1.google.com
V DHCP	· · · · · · · · · · · · · · · · · · ·
 Multicast 	Server Port 123 (1 - 65536, default 123)
✓ Routing	
 Security 	Manual Time
ACI	
· ////	
V GUS	Time 17:21:14 HH:MM:SS
 Diagnostics 	i
 Management 	Devident Service Time
	Daylight saving time
	None
	Recurring
	Type O Non-recurring
	Offset 60 Min (1 - 1440, default 60)
	From: Day Sun week First Month Jan Time
	Recurring
	To: Day Sun 🚬 Week First 🚬 Month Jan 🚬 Time
	YYYY-MM-DD HHIMM
	Non-recurring
	To: YYYY-MM-DD HH:MM
	L
	Operational Status
	Current Time (2019-12-31 17:21:14 UTC-7

Fig 2.4.6 SNTP configuration page

COMMANDO	s » System Inf	ormation
✓ Status	IPv6 Address	fe80::2e0:4cff:fe00:0/64
System Information	System OID	1.3.6.1.4.1.27282.1.1
Logging Message	System Uptime	0 day, 0 hr, 23 min and 41 sec
 ✓ Port 	Current Time	2020-10-05 23:42:37 UTC-7
Link Aggregation	انــــــــــــــــــــــــــــــــــــ	
MAC Address Table	Loader Version	1.0.0.6
V Network	Loader Date	Nov 17 2019 - 18:17:03
	Firmware Version	SoldierOS.2K.v1.4
	Firmware Date	Sep 30 2020 - 16:28:18
	Teinet	Disabled
✓ DHCP	SSH	Disabled
✓ Multicast	HTTP	Enabled
✓ Routing	HTTPS	Disabled
✓ Security		Disabled
✓ ACL	SNMP	Disableu
✓ QoS ✓ <		

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.

COMMANDO				Save	Logout Reboot D	Debug
	Status »]	Logging Message				
Status System Information System Time Logging Message Port	Logging Viewing F	Message Table				
Link Aggregation MAC Address Table	Showing	entries		Showing 1 to 9 of 9 entries	Q	
✓ Network	Log ID	Time	Severity	Description		
✓ Port	1	Dec 31 2019 17:02:32	notice	AAA-0-CONNECT: New http connection for user admin, source 192.168.0.21 ACCEPTED, a	aggregated (1)	
VLAN	2	Dec 31 2019 17:02:32	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.0.21 ACCEPTED		
 MAC Address Table 	3	Dec 31 2019 17:00:36	info	STP-5-PORT_STATE: Port GigabitEthernet5 moving from Learning to Forwarding		
 Spanning Tree 	4	Dec 31 2019 17:00:34	info	STP-6-PORT STATE: Port GigabitEthernet5 moving from Blocking to Learning		
 Discovery 	5	Dec 31 2019 17:00:14	info	STP-6-PORT_STATE: Port GigabitEthernet5 moving from Disabled to Blocking		
V DHCP	6	Dec 31 2019 17:00:14	info	PORT-6-SPEED_DUPLEX: Interface GigabitEthernet5 link speed 1000M duplex full		
 Multicast 	7	Dec 31 2019 17:00:14	notice	PORT-6-I INK LIP: Interface GinabitEthernet5 link un		
 Routing 		Jan 01 2020 00:00:13	notice	SYSTEM-5-COLDSTART: Cold startup		
✓ Security		Jan 01 2020 00:00:13	info	LOGGING & START: Logging is started		
✓ ACL		Jan 01 2020 00.00.15	1110	EOGGING-S-START. Eugging is started		
✓ QoS	Olarea	Defeat			First Previous 1 Next	Last
✓ Diagnostics	Clear	Retresh				
 Management 						

Fig 2.3.1 Logging Message Table of RAM

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

COMMANDO	Status » Logging Message		Save Logout Reboot Debug
Status System Information System Time Logging Message Port Link Aggregation MAC Address Table	Logging Message Table Viewing Flash v Showing All v entries	Showing 0 to 0 of 0 entries	Q
✓ Network	Log ID Time Severity Description	n	
✓ Port		0 results found.	
VLAN			First Previous 1 Next Last
✓ MAC Address Table	Clear Refresh		
✓ Spanning Tree			
✓ Discovery			
✓ DHCP			
✓ Multicast			
✓ Routing			
✓ Security			
✓ ACL			
√ QoS			
✓ Diagnostics			
✓ Management			

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

COMMANDO	Status >	» Log	ging Message	9	Save Lo	ogout	Reboot
Status System Information System Time Logging Message Port Link Aggregation	Loggi Viewing	ng Me	ssage Table		Shoulan 1 to 9 of 9 partice		
MAC Address Table	Showing	All	entries	C 11		ג ו	
× Port	Log I	10	lime	Severity	Description		
		30	31 2019 17:02:32	notice	AAA-0-CONNECT: New http connection for user admin, source 192.168.0.21 ACCEPTED, aggregated (1)		
		50	31 2019 17:02:32	notice	AAA-5-CONNECT: New http connection for user admin, source 192.168.0.21 ACCEPTED		
		100	31 2019 17:00:36	info	STP-5-PORT_STATE: Port GigabitEthernet5 moving from Learning to Forwarding		
		+ Dec	31 2019 17:00:34	info	STP-6-PORT_STATE: Port GigabitEthernet5 moving from Blocking to Learning		
		5 Dec	31 2019 17:00:14	info	STP-6-PORT_STATE: Port GigabitEthernet5 moving from Disabled to Blocking		
Multicast		6 Dec	31 2019 17:00:14	info	PORT-6-SPEED_DUPLEX: Interface GigabitEthernet5 link speed 1000M duplex full		
		7 Dec	31 2019 17:00:14	notice	PORT-6-LINK_UP: Interface GigabitEthernet5 link up		
✓ Routing		8 Jan (01 2020 00:00:13	notice	SYSTEM-5-COLDSTART: Cold startup		
✓ Security		9 Jan (01 2020 00:00:13	info	LOGGING-5-START: Logging is started		
V ACI							

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

COMMANDO Status » Port >	Statistics
▼ Status	
System Information System Time	t GE1 🗸
Logging Message Port Statistics Error Disabled	All Interface Etherlike RMON
Bandwidth Utilization Link Aggregation MAC Address Table	 ○ None ○ 5 sec ● 10 sec ○ 0 sec
✓ Network	
✓ Port	
V VLAN	
V MAC Address Table	
✓ Spanning Tree	
✓ Discovery iflr	OCtets 0
V DHCP ifInUc	astPkts 0
V Multicast ifInNUc	astPkts 0
✓ Routing if InD	iscards 0

Fig 2.4.1 Port selection for MIB Counter Statistics

COMMANDO		
St	atus » Port » Stat	istics
✓ Status		
System Information System Time	Port	5 🗸
Logging Message Port Statistics Error Disabled	MIB Counter O II O E O F	ul nterface Etherlike RMON
Bandwidth Utilization Link Aggregation MAC Address Table	Refresh Rate	lone isec 0 sec
V Network	O 3	l0 sec
	Clear	
		1
	Interface	
	ifInOctets	982661
	ifInUcastPkts	5387
V Routing	ifInNUcastPkts	633
	ifinDiscords	0
	InnDiscards	0
V 00S	ifOutOctets	2346667
	ifOutUcastPkts	5865
 Management 	ifOutNUcastPkts	1302
	ifOutDiscards	n

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.

COMM	ANDO

Status » Port » Statistics RMON Status System Information etherStatsDropEvents 0 System Time etherStatsOctets 316700 Logging Message ether StatsPkts 2146 Port Statistics etherStatsBroadcastPkts 146 Error Disabled etherStatsMulticastPkts Bandwidth Utilization 581 Link Aggregation etherStatsCRCAlignErrors 0 MAC Address Table etherStatsUnderSizePkts 0 Network etherStatsOverSizePkts ✓ Port 0 VLAN ether Stats Fragments 0 MAC Address Table etherStatsJabbers 0 Spanning Tree etherStatsCollisions 0 Discovery etherStatsPkts64Octets 1008 DHCP Multicast etherStatsPkts65to127Octets 748 ✓ Routing etherStatsPkts128to255Octets 38 Security etherStatsPkts256to511Octets 210 ✓ ACL etherStatsPkts512to1023Octets 142 ✓ QoS Diagnostics 0 etherStatsPkts1024to1518Octets ✓ Management

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**.

COMMANDO	Status	» Po	ort » Ei	ror Disabled	
 Status System Information System Time Logging Message Port 	Erro	r Disa	bled Tab	le	
Statistics Error Disabled		Port	Reason	Time Left (sec)	
Bandwidth Utilization		GE1			
Link Aggregation		GE2			
MAC Address Table		GE3			
✓ Network		GE4			
✓ Port		GE5			
VLAN		GE6			
 MAC Address Table 		GE7			
 Spanning Tree 		GE8			
 Discovery 		CEQ			
✓ DHCP		CE10			
✓ Multicast		GE 10			
✓ Routing		GETT			
✓ Security		GE12			
V ACL		GE13			
V QoS		GE14			
 Diagnostics 		GE15			
✓ Management		GE16			
		GE17			



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.

	Status	» Po	rt » Eri	ror Disabled	
✓ Status		GE18			
System Information		GE19			
System Time		GE20			
Logging Message		GE21			
∧ Port		GE22			
Statistics Error Disabled		GE23			
Bandwidth Utilization		GE24			
Link Aggregation		GE25			
MAC Address Table		GE26			
✓ Network		GE27			
✓ Port		GE28			
VLAN		LAG1			
V MAC Address Table		LAG2			
 Spanning Tree 		LAG3			
✓ Discovery		LAG4			
		LAG5			
V Multicast		LAG6			
		LAG7			
		LAG8			
	_	_			_
 ✓ Diagnostics 	R	efresh	Recover		
✓ Management					

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**.

COMMANDO								Save	Logout	Reboot	Debug
	Status »	Link	Aggre	gation							
	Link A	ggrega	tion Ta	ible					٩٢		
Link Aggregation MAC Address Table	LAG	Name	Type	Link Status	Active Member	Inactive Member		 			-
 Network 	LAG 1		Static	Up	GE1-GE2						
IP Address DNS Hoots System Time A Port Port Setting	LAG 2 LAG 3 LAG 4 LAG 5 LAG 6			-							
Link Agregation Group Port Setting LACP EEE Jumbo Frame Port Security Protected Port Stam Control Mirroring VIAN MAC Address Table +	LAG 8										

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.

COMMANDO					Save Logout Reboot 1	Debug
	Status »	MAC Address	Table			
System Information System Time	MAC A	ddress Table				
Logging Message	Showing	II 🗸 entries		Showing 1 to 2 of 2 entries	Q	
Statistics Error Disabled	VLAN	MAC Address	Туре	Port		
Bandwidth Utilization	1	00:E0:4C:00:00:00	Management	CPU		
Link Aggregation	1	28:D2:44:0A:7E:9C	Dynamic	GE5		
MAC Address Table					First Previous 1 Next	Last
✓ Network	Clea	r Refresh				

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.



Network » IP Address

∧ Status			
System information	IPv4 Address		
System Time	Firve Address		
Logging Message		Static	
∧ Port	Address Type		
Statistics			
Error Disabled	IP Address	192.168.0.1	
Bandwidth Utilization	+		
Link Aggregation	Subnet Mask	255.255.255.0	
MAC Address Table			
 Network 	Default Gateway	192.168.0.254	
IP Address			
DNS	Sub IPv4 Address		
Hosts	Enshied "	Enable	
✓ Port			
VLAN	IP Address	0.0.0.0	
 MAC Address Table 			
 Spanning Tree 	Subnet Mask ;;	0.0.0.0	
 Discovery 			
V DHCP	Pv6 Address		
V Multicast	Auto Configuration	Enable	
V Routing	DHCPv6 Client !!	Enable	
Security	·		i
~ ACL	IPv6 Address		
V QUS	Prefix Length	0	(0 - 128)
v Management			
The second s	IPv6 Gateway		
	Operational Status		
	IPv4 Address	192.168.0.1	
	IPv4 Default Gateway	192.168.0.254	
	Sub IPv4 Address	0.0.0.0	
	IDvC Address		
	IF VS AUUIOSS	-	i
	IPv6 Gateway		
	Link Local Address	fe80::2e0:4cff fe00:0/64	i
	Apply		

Fig 3.1.1 Default Management IP address showing 192.168.0.1 page

\leftarrow \rightarrow C' \textcircled{a}	🔽 🖋 🗝 192.168.0.2/hc	ome.html
LUMMANIU		
	Network » IP Address	
✓ Status		
✓ Network	IPv4 Address	
IP Address	Address Torrest	Static
DNS Hosts	Address lype	O Dynamic
✓ Port	IP Address	192.168.0.2
VLAN		
V MAC Address Table	Subnet Mask	255.255.255.0
✓ Spanning Tree	Default Gateway	192.168.0.254
✓ Discovery	L	
V DHCP	Sub IPv4 Address	
✓ Multicast	Enabled	Enable
✓ Routing	IP Address	0 0 0 0
✓ Security		
	Subnet Mask	0.0.0.0
		,
	IPv6 Address	
• Management	Auto Configuration	Enable
	DHCPv6 Client	Enable
	IPv6 Address	
		(0.100)
	Prefix Length	0 (0 - 128)
	IPv6 Gateway	

Fig 3.1.2 Changing Management IP address page

$\overleftarrow{\bullet}$ \rightarrow $\overleftarrow{\bullet}$	😈 🔏 🗝 192.168.0.2/home.html	
COMMANDO	Status » Syste	tem Information
✓ Status	· ·····	
System Information	MAC A	Address 00:E0:4C:00:00:00
System Time	IPv4 A	Address 192.168.0.2
 ✓ Port 	IPv6 A	Address fe80::2e0:4cff:fe00:0/64
Link Aggregation	Syste	tem OID 1.3.6.1.4.1.27282.1.1
MAC Address Table	System	Uptime 0 day, 0 hr, 31 min and 56 sec
✓ Network ✓ Port	Currer	nt Time 2019-12-31 17:31:26 UTC-7
VLAN		
✓ MAC Address Table	Loader V	Version 1.0.0.6
✓ Spanning Tree	Loade	ler Date Nov 17 2019 - 18:17:03
✓ Discovery	Firmware V	Version SoldierOS.2K.v1.4
N DHCP		<u> </u>

Fig 3.1.3 Verification of Changed Management IP address page

COMMANDO	Network » IP Address	Save Logout Reboot Debug
∧ Status ^		
System Information	IPv4 Address	
System Time Logging Message ✓ Port	Address Type	● Static○ Dynamic
Link Aggregation MAC Address Table	IP Address	192.188.0.2
✓ Network	Subnet Mask	255.255.255.0
IP Address DNS	Default Gateway	<u>192.168.0.100</u>
Hosts	Sub IPv4 Address	
	Enabled	Enable
 MAC Address Table 	IP Address	<u>p.o.o.</u>

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**

COMMANDO	Network » DNS	Save Logout Reboot Debug
∧ Status ^		^
System Information System Time	DNS Configuration	
 ✓ Port 	Duc status O Disable	
Link Aggregation	Enable	
NAC Address Table Network	DNS Default Name minimandonetworks.com (1 to 255 alphanumeric characters)	
IP Address DNS Hosts	Apply	
✓ Port	DNS Server Configuration	
VLAN		
 MAC Address Table 		Q
 Spanning Tree 	Preference DNS Server	
Discovery		
· Discovery	() results tound	
✓ DHCP	0 results found.	
DHCP Multicast	Add Delete	

Fig 3.2.1 DNS configuration page

COMIMANDO		Save	Logout	Reboot	Debt
N	etwork » DNS				
 ▲ Status ▲ System Information System Time Logging Message ✓ Port Link Aggregation 	Add DNS Server IPv4/IPv6 Address 10.10.10.10				
MAC Address Table					
IP Address DNS Hosts V Port V VLAN V MAC Address Table V Spanning Tree					
 ✓ Discovery ✓ DHCP 					
ा २ 🧿 🖬 🗂 🛛	2 🕹 🧟 🧿 🖬 🔌		Lii	nks [»] ^ <i>(i</i> r	17:22 10/6/2020

Fig 3.2.2 Add DNS Server page

COMMANDO	Save	Logout	Reboot	Debug
Network » DNS				
Status System Information System Time Longing Message	_			
V Port Link Aggregation MAC Address Table DNS Default Name Commandonetworks co (1 to 255 alohanumeric characters)	1			
Network IP Address DNS Hosts Apply A	<u>.</u>			
Port DNS Server Configuration				
VLAN				
V MAC Address Table		Q		
Spanning Tree Preference DNS Server				
✓ Discovery				
✓ DHCP				_
V Multicast Add Delete				
V Routing				~

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 configuration, click **Network >>Hosts**

COMMANDO		Save Logout Reboot Debug
	Network » Hosts	
Status System Information System Time Logging Message	DNS Host Configuration	
 ✓ Port 		Q
Link Aggregation MAC Address Table	Host IPv4/IPv6 Address	
✓ Network	0 results found.	
IP Address DNS Hosts	Add Delete	
✓ Port	Dynamic Host Mapping	
VLAN		
 MAC Address Table 		Q
 Spanning Tree 	Host Total Elapsed Type IPv4/IPv6 Address	
 Discovery 	0 results found.	
✓ DHCP		
✓ Multicast	Clear	
✓ Routing		

Fig 3.3.1 DNS Host blank configuration page

COMMANDO	Same	Lingent	Debest	Debug
	Save	Logout	Reboot	Debug
	Network » Hosts			
Status System Information System Time Logging Message Port Link Aggregation MAC Address Table Network	Add Host Host I (1 to 255 alphanumeric characters) IPv4/IPv6 Address I0 10.10.10			^
IP Address DNS Hosts	Apply Close			
✓ Port				
V VLAN				
 MAC Address Table 				
✓ Spanning Tree				
✓ Discovery				
✓ DHCP				
✓ Multicast				
V Routing				*

Fig 3.3.2 Add DNS Host and IP address configuration page

× Status ^ System Information	COMMANDO		Save Logout Reboo	ot Debug
 Status System Information System Time Logging Message Port In Address Table I 10.10.10 Add Delete Dynamic Host Mapping VLAN MAC Address Table Inst Mapping VLAN MAC Address Table Clear Routing 		Network » Hosts		
System Information System Time Logging Message P ort Link Agregation MAC Address Table IP Address DNS Hosts V Port V VLAN V VLAN V MAC Address Table Optimic Host Mapping V VLAN V Discovery O Discovery O Discovery O Discovery V DHCP V Multicast Clear	∧ Status ^			~
Logging Message ✓ Port Link Aggregation MAC Address Table ✓ Network IP Address DNS Hosts ✓ Port ✓ Not ✓ VLAN ✓ MAC Address Table ✓ VLAN ✓ MAC Address Table ✓ VLAN ✓ Spanning Tree ✓ biscovery ✓ DHCP ✓ Multicast ✓ Routing	System Information System Time	DNS Host Configuration		
Link Aggregation MAC Address Table Vervork P Address DNS Hosts Vort Vervork Mac Address Table Dynamic Host Mapping Vervory Vervor	Logging Message		0	
 Network IP Address DNS Hosts V Port VLAN VLAN VAddress Table V Spanning Tree V Discovery Discovery O results found. Clear 	Link Aggregation MAC Address Table	Host IPv4/IPv6 Address	~	
IP Address DNS Hosts V Port V VLAN V MAC Address Table V Spanning Tree V DIScovery 0 Discovery 0 Host Total Elapsed Type IPV4/IPv6 Address 0 results found. Clear	✓ Network	1 10.10.10		
V Port Dynamic Host Mapping V VLAN Q V MAC Address Table Q V Spanning Tree Host V Discovery 0 results found. V DHCP Clear V Multicast Clear	IP Address DNS Hosts	Add Delete		
V VLAN V VLAN V VLAN V MAC Address Table V Spanning Tree Host Total Elapsed Type IPV4/IPv6 Address Uscovery Uscovery Clear Clear	✓ Port	Dynamic Host Mapping		
 ✓ MAC Address Table ✓ Spanning Tree ✓ Discovery ✓ DHCP ✓ Multicast ✓ Routing 	VLAN	-1		
Spanning Tree Most Total Elapsed Type IPv4/IPv6 Address Discovery DHCP Multicast Clear	 MAC Address Table 		Q	
Discovery Discovery Discovery Oresuits found. Clear Clear	 Spanning Tree 	Host Total Elapsed Type IPv4/IPv6 Address		
DHCP Multicast Clear Clear	✓ Discovery	0 results found.		
V Multicast Clear	✓ DHCP			
✓ Routing	✓ Multicast	Clear		
	✓ Routing			

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**

COMMANDO												Save	Logout	Reboot	Debug
	Po	rt »	Port Settin	ıg											
✓ Status			Entry	Port	Туре	Description	State	Link Status	Speed	Duplex	Flow Control				^
✓ Network			1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
▼ Port			2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
Port Setting			3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
Error Disabled			4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
 Link Aggregation 			5	GE5	1000M Copper		Enabled	Up	Auto (1000M)	Auto (Full)	Disabled (Off)				
Jumbo Frame			6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
Port Security			7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
Protected Port			8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
Storm Control			9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
			10	GE10	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
V VLAN			11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
 MAC Address Table Spanning Tree 			12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
			13	GE13	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
			14	GE14	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
✓ Multicast			15	GE15	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
✓ Routing			16	GE16	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
✓ Security			17	GE17	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
V ACL			18	GE18	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
✓ QoS			19	GE19	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
✓ Diagnostics			20	GE20	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
✓ Management			21	GE21	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
			22	GE22	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
			23	GE23	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
			24	GE24	1000M Copper		Enabled	Down	Auto	Auto	Disabled				
			25	GE25	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled				
			26	GE26	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled				
			27	GE27	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled				
			28	GE28	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled				

Fig 4.1.1 Port setting table page

COMMANDO	Port »	Port	Setting	3								Save	Logout	Reboot	Debuş
✓ Status															^
* Ret	Port	Setting	g Table												
Port Setting													0		
Error Disabled	_	_	_										Q.		-1
 Link Aggregation 		Entry	Port	Туре	Description	State	Link Status	Speed	Duplex	Flow Control					
EEE Jumbo Framo		1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
Port Security		2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
Protected Port		3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
Storm Control		4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
Mirroring		5	GE5	1000M Copper		Enabled	Up	Auto (1000M)	Auto (Full)	Disabled (Off)					
VLAN		6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
✓ MAC Address Table		7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
V Spanning Tree		8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
V Discovery		9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
		10	GE10	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
Y Routing		11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
 Kouting ✓ Sequrity 		12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
× ACI		13	GE13	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
✓ QoS		14	GE14	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
✓ Diagnostics		15	GE15	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
✓ Management		16	GE16	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
		17	GE17	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
		18	GE18	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
		19	GE19	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
		20	GE20	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
		21	GE21	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
		22	GE22	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
		23	GE23	1000M Copper		Enabled	Down	Auto	Auto	Disabled					
		24	GE24	1000M Copper		Enabled	Down	Auto	Auto	Disabled					v
															_

Fig 4.1.2 Port setting multiple ports selection page.

COMMANDO Por	t » Port Settin	g	Save Logout Reboot Debug
✓ Status ^	dit Dant Catting		^
✓ Network	ait Port Setting		^
▼ Port	,		
Port Setting	Port	GE1-GE28	
Error Disabled	Description	COMMANDO LAN	
✓ Link Aggregation	·		
EEE	Ctoto		
Jumbo Frame	State		
Port Security Distanted Dat		Auto O 10M	
Storm Control	Speed	O Auto - 10M O 100M	
Mirroring	speed	O Auto - 100M O 10G	
✓ VLAN		O Auto - 10M/100M	
✓ MAC Address Table		Auto	
✓ Spanning Tree	Duplex	O Full	
✓ Discovery		O Half	
✓ DHCP		() Auto	
✓ Multicast	Flow Control	O Enable	
✓ Routing		O Disable	
✓ Security			
✓ ACL	Арріу	1056	
✓ Q0S			×
V			V

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

	Port » Error Disabled	Save Logout	Reboot Debug
✓ Status			^
✓ Network		1	
▼ Port	Recovery Interval 300 Sec (30 - 86400)		
Port Setting Error Disabled	BPDU Guard Enable		
 Link Aggregation EEE 	UDLD Enable Self Loop Enable		
Jumbo Frame Port Security Protected Port	Broadcast Flood Enable		
Storm Control Mirroring	Unicast Flood Enable		
VLAN	ACL 🗌 Enable		
 MAC Address Table 	Port Security 🔲 Enable		
✓ Spanning Tree	DHCP Rate Limit Enable		
✓ Discovery✓ DHCP	ARP Rate Limit Enable		
✓ Multicast	Apply		
✓ Routing			¥

Fig 4.2.1 Error disabled selection page.

COMMANDO						
			Save	Logout	Reboot	Debug
F	Port » Error Disabled					
✓ Status						^
✓ Network	[······					
✓ Port	Recovery Interval	300 Sec (30 - 86400)				
Port Setting	,					
Error Disabled	BPDU Guard	Enable				
 Link Aggregation 	UDLD	Enable				
EEE	Self Loop	✓ Enable				
Jumbo Frame Port Security	Broadcast Flood	Enable				
Protected Port	Linknown Multicast Flood					
Storm Control						
Mirroring	Unicast Flood					
VLAN	ACL	Enable				
✓ MAC Address Table	Port Security	Enable				
 Spanning Tree 	DHCP Rate Limit	Enable				
V Discovery	ARP Rate Limit	Enable				
V DHCP	L					
✓ Multicast	Apply					
✓ Routing						
v Conucitu						×

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.

COMMANDO									Save Lo	gout Reboot	t Debug
	Port >	» Link	Aggreg	ation >	» Group						
											^
		Load Bal	ance Alac	rithm	MAC Addres	s					
Port Setting Error Disabled A Link Aggregation Group Port Setting LACP	Link	Apply K Aggreg	gation T	able							
FFF									0		
Jumbo Frame								 	4		
Port Security		LAG	Name	Туре	Link Status	Active Member	Inactive Member				
Protected Port	0	LAG 1									
Storm Control	0	LAG 2									
Mirroring	0	LAG 3									
VLAN	0	LAG 4									
✓ MAC Address Table	Ő	LAG 5									
 Spanning Tree 		LAGE									
 Discovery 		LAGI									
✓ DHCP	0	LAG 7									
✓ Multicast	0	LAG 8						 			
✓ Routing		Edit									
× Security Y											~

Fig 4.3.1 Link Aggregation group selection page.

COMMANDO											
	_								Save	Logout Reboo	t Debug
	Port	» Link	Aggrega	ation >	» Group						
✓ Status	^										^
✓ Network				·····							
✓ Port		Load Ba	ance Algo	rithm	 IP-MAC Addi 	a ress					
Port Setting Error Disabled A Link Aggregation Group Port Setting		Apply	gation Ta	able				 J			
LACP											
EEE Jumbo Eromo									C	2	
Port Security		LAG	Name	Туре	Link Status	Active Member	Inactive Member				
Protected Port	0) LAG 1									
Storm Control	C) LAG 2									
Mirroring	C) LAG 3									- 11
VLAN) IAG4									- 11
 MAC Address Table) LAG 5									- 11
 Spanning Tree 											- 11
 Discovery 											- 11
✓ DHCP		LAG									- 11
✓ Multicast		LAG 8						 			
✓ Routing		Edit									
v Security											v

Fig 4.3.2 Link Aggregation LAG selection for editing page.

COMMANDO		
1	rt » Link Aggregation » Group	
✓ Status		
V Network		
✓ Port	Edit Link Aggregation Group	
Port Setting Error Disabled Link Aggregation Group Port Setting LACP EEE Jumbo Frame Port Security Protected Port Storm Control Mirroring	LAG I Name COMMANDO LAG Type Image: Static mark O LACP Available Port Selected Port GE5 GE1 GE7 GE3 GE8 GE4	
VLAN MAC Address Table Spanning Tree Discovery	GE9 GE10 GE11 GE12	
✓ DHCP		
✓ Multicast	Apply Close	
✓ Routing		
V Socurity		

Fig 4.3.3 Link Aggregation Edit LAG page.

COMMANDO	Port >	> Link	Aggregation >	> Gro	ир				Save Logout	Reboot Debug
✓ Status ^	-									^
✓ Network	[[····		······	MAC	Address					
✓ Port		Load Ba	lance Algorithm	○ IP-M	AC Address					
Port Setting	L									
Error Disabled	A	Apply								
 Link Aggregation 										
Group										
Port Setting	Link	Aggre	gation Table							
EEE	-								Q	
Port Security		LAG	Name	Туре	Link Status	Active Member	Inactive Member			
Protected Port		LAG 1	COMMANDO LAG	Static	Down		GE1-GE4			
Storm Control	0	LAG 2								
Mirroring		LAGR								
VLAN										
✓ MAC Address Table	0	LAG 4								
✓ Spanning Tree	0	LAG 5								
✓ Discovery	0	LAG 6								
✓ DHCP	0	LAG 7								
✓ Multicast	0	LAG 8						 		
✓ Routing		Edit]							
javascript:void(0)			,							Y

Fig 4.3.4 Link Aggregation Table page.

COMMANDO	» Link Aggregation » Group	Save Logout Reboot Debug
✓ Status ✓ Network ✓ Port Edd	it Link Aggregation Group	^
Port Setting Error Disabled A Link Aggregation Group Port Setting LACP EEE Jumbo Frame Port Security Protected Port Storm Control Mirroring V UAN	LAG 2 Name COMMANDO LACP Type O Static ● LACP Available Port Selected Port GE5 GE6 GE9 GE1 GE1 GE1 GE1 GE1 GE1 GE1 GE1	
MAC Address Table Spanning Tree	GE12 GE13 GE14 V	
✓ Discovery		
✓ DHCP	Apply Close	
✓ Multicast		
V Routing		
V Socurity		×

Fig 4.3.5 LACP Edit LAG page.

COMMANDO		× T - 1		C					Save Logou	it Reboot	Deb
	Port	" Lini	Aggregation »	Grou	ıp						
Status	î 🗔										
Network		Lood P	alanaa Algorithm	MAC	Address						
Port		LOAD D) IP-MA	C Address						
Port Setting			dt								
Error Disabled		Apply									
Link Aggregation											
Group											
Port Setting	Lin	k Aggr	egation Table								
									Q,		
Jumbo Frame Dort Scourity		LAG	Name	Туре	Link Status	Active Member	Inactive Member				
Protected Port		LAG 1		Static	Down		GE1-GE4				_
Storm Control			COMMANDO LACE		Down		CE7 CE9				
Mirroring	0	LAG 2	CONIVIANDO LACP	LACP	Down		GE1-GE0				
VLAN	0	LAG 3									
MAC Address Table	0	LAG 4									
Propring Tree	0	LAG 5									
	0	LAG 6									
Jiscovery	0	LAG 7									
HCP	Ő	LAG 8									
Aulticast		2100						 			
Routing		Edit									
Socurity			_								

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**.

COMMANDO	ort >	> Link	Aggrega	tion » Port Set	ting			5	Save Logoi	ıt Reboot	Debug
✓ Status ^											^
✓ Network	Port	Settin	a Table								
- Port			3								
Port Setting									Q		
Error Disabled			-							1	
		LAG	Туре	Description	State	Link Status	Speed	Duplex	Flow Control		
Bort Setting		LAG 1	eth1000M	COMMANDO LAG	Enabled	Down	Auto	Auto	Disabled		
LACP		LAG 2	eth1000M	COMMANDO LACP	Enabled	Down	Auto	Auto	Disabled		
EEE		LAG 3			Enabled	Down	Auto	Auto	Disabled		
Jumbo Frame		LAG 4			Enabled	Down	Auto	Auto	Disabled		
Port Security		LAG 5			Enabled	Down	Auto	Auto	Disabled		
Protected Port		LAG 6			Enabled	Down	Auto	Auto	Disabled		
Storm Control					Enabled	Down	Auto	Auto	Disabled		
Mirroring						Down	Auto	Auto	Disabled		
VLAN	1	LAG 8			CHADled	Down	Auto	Auto	Disabled		
V MAC Address Table		Edit)								~

Fig 4.3.7 Link Aggregation port setting table page

									:	Save Logou	t Reboot	Debi
	Р	ort >	> Link	Aggrega	tion » Port Set	ting						
	^											
		Port	Sottin	a Tablo								
		FUI	Settin	y lable								
										Q		_
			LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control		
			LAG 1	eth1000M	COMMANDO LAG	Enabled	Down	Auto	Auto	Disabled		
			LAG 2	eth1000M		Enabled	Down	Auto	Auto	Disabled		
			LAG 3	ourrooom		Enabled	Down	Auto	Auto	Disabled		
			LAG 4			Enabled	Down	Auto	Auto	Disabled		- 1
			LAG 5			Enabled	Down	Auto	Auto	Disabled		
			LAG6			Enabled	Down	Auto	Auto	Disabled		
			LAG 7			Enabled	Down	Auto	Auto	Disabled		
			LAG 8			Enabled	Down	Auto	Auto	Disabled		
ľ		1										_
	~		Edit	J								

Fig 4.3.8 Link Aggregation selecting port page

COMMANDO			Save	Logout	Reboot	Debug
Port » Li	nk Aggre	gation » Port Setting				
✓ Status ^						^
V Network						^
✓ Port Edit Port Se	tting					
Port Setting Error Disabled A Link Aggregation Group Port Setting LACP EEE Jumbo Frame Port Security Protected Port Storm Control	Port scription State Speed	LAG1-LAG2 COMMANDO LAG ☑ Enable ○ Auto - 10M ○ Auto - 10M ○ Auto - 100M ○ Auto - 100M				
Mirroring VLAN MAC Address Table Spanning Tree Discovery Apply	w Control	Auto Auto Auto Enable Disable				,

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

COMMANDO	ort ») Link	Aggrega	tion » Port S	etting					Save Logou	t Reboot	Debug
✓ Status												
V Network	Port	Settin	a Table									
✓ Port	i on	ocum	g lubic									
Port Setting Error Disabled	_									(2	
 Link Aggregation 		LAG	Туре	Description	State	Link Status	Speed	Duplex	Flow Control			
Group		LAG 1	eth1000M	COMMANDO LAG	Enabled	Down	100M	Auto	Enabled			
Port Setting		LAG 2	eth1000M	COMMANDO LAG	Enabled	Down	100M	Auto	Enabled			
LACP FEE		LAG 3			Enabled	Down	Auto	Auto	Disabled			
Jumbo Frame		LAG 4			Enabled	Down	Auto	Auto	Disabled			
Port Security		LAG 5			Enabled	Down	Auto	Auto	Disabled			
Protected Port		LAG 6			Enabled	Down	Auto	Auto	Disabled			
Storm Control		LAG 7			Enabled	Down	Auto	Auto	Disabled			
		LAG 8			Enabled	Down	Auto	Auto	Disabled			
V MAC Address Table)									
 Spanning Tree 		Edit										
✓ Discovery												
✓ DHCP ✓												

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 nonactive 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.

COMMANDO		Port >	Link A	lggrega	ation » LACP		
✓ Status	\sim						
✓ Network		E	Sustam Dri	ority	0760	(4 65525	default 20760)
✓ Port		E	System Ph			(1 - 05555),	, delault 52706)
Port Setting Error Disabled ~ Link Aggregation Group Port Setting LACP EEE	l		P Port Se	etting 1	lable		
Jumbo Frame			Entry	Port	Port Priority	Timeout	
Port Security			1	GE1	1	Long	
Protected Port Storm Control			2	GE2	1	Long	
Mirroring			3	GE3	1	Long	
			4	GE4	1	Long	
 MAC Address Table 			5	GE5	1	Long	
 Spanning Tree 			6	GE6	1	Long	
 Discovery 			7	GE7	1	Long	
✓ DHCP			8	GE8	1	Long	
 Multicast 			9	GE9	1	Long	
✓ Routing			10	GE10	1	Long	
✓ Security			11	GE11	1	Long	
✓ ACL			12	GE12	1	Long	
V QoS	~		13	GE13	1	Long	

Fig 4.3.6 Link Aggregation LACP Port Setting Table page

COMMANDO						
	P	ort »	Link A	ggrega	tion » LACP	
✓ Status	^					
V Network		LACP	Port Se	etting Ta	able	
▼ Port	i I.,			-		
Port Setting	н.					
Error Disabled			Entry	Port	Port Priority	Timeout
 Link Aggregation 		M	1	GE1	1	Long
Port Setting			2	GE2	1	Long
LACP			3	GE3	1	Long
EEE			4	GE4	1	Long
Jumbo Frame			5	GE5	1	Long
Port Security Protected Port			6	GE6	1	Long
Storm Control			7	GE7	1	Long
Mirroring			8	GE8	1	Long
VLAN			9	GE9	1	Long
 MAC Address Table 			10	GE10	1	Long
 Spanning Tree 			11	GE11	1	Long
 Discovery 			12	GE12	1	Long
V DHCP			13	GE13	1	Long
✓ Multicast			14	GE14	1	Long
✓ Routing			15	GE15	1	Long
✓ Security			16	GE16	1	Long
V ACL			17	GE17	1	Long
✓ QoS	\sim		40	0540		1

Fig 4.3.7 Link Aggregation LACP Port Setting port selection page

COMMANDO	Port » Link Aggregation » LACP
✓ Status	
✓ Network	
✓ Port	Edit LACP Port Setting
Port Setting Error Disabled Link Aggregation Group Port Setting LACP EEE Jumbo Frame Port Security Protected Port Storm Control Mirroring	Port GE1-GE28 Port Priority 1 (1 - 65535, default 1) Timeout O Image: Short
VLAN	
V MAC Address Table	
V Spanning Tree	
✓ Multicast	
✓ Routing	
✓ Security	
✓ ACL	
✓ QoS	

Fig 4.3.8 Edit LACP Port Setting page

COMMANDO						Save Logout Reboot Debu
	Port » Li	ink Agg	regation »	LACP		
✓ Status ^						
 V Network 	Suct	om Drioriti	22760		(1.65525.dofault22768)	
▼ Port	Jayar		1 02700		(1-0555, deladit 52700)	
Port Setting Error Disabled Link Aggregation Group Port Setting	Apply	ort Setti	ng Table			
LACP						
EEE	_					4
Jumbo Frame	Entr	ry Port	Port Priority	Timeout		
Port Security Protocted Port		1 GE1	1	Short		
Storm Control		2 GE2	1	Short		
Mirroring		3 GE3	1	Short		
VLAN		4 GE4	1	Short		
 MAC Address Table 		5 GE5	1	Short		
✓ Spanning Tree		6 GE6	1	Short		
 Discovery 	l n	7 GE7	1	Short		
✓ DHCP		8 GE8	1	Short		
✓ Multicast		9 GE9	1	Short		
✓ Routing		0 GE10	1	Short		
✓ Security		1 GE11	1	Short		
✓ ACL		2 0512	4	Short		
✓ Q0S ✓		3 GE12	1	Short		

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 linkup 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 а 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.

	Port » EE	E.		
Status Network Port Port Port Setting Error Disabled	EEE Sett	ing Table		
 Link Aggregation 		Entry	Port	State
Group		, 1	GE1	Disabled
Port Setting			GE2	Disabled
LACP			GE3	Disabled
Jumbo Frame		4	GE4	Disabled
Port Security		5	GES	Disabled
Protected Port		6	GE6	Disabled
Storm Control		7	GE7	Disabled
VLAN		8	GE8	Disabled
V MAC Address Table		9	GE9	Disabled
Spanning Tree		10	GE10	Disabled
 Discovery 		11	GE11	Disabled
V DHCP		12	GE12	Disabled
 Multicast 		13	GE13	Disabled
 Routing 		14	GE14	Disabled
 Security 		15	GE15	Disabled
V ACL		16	GE16	Disabled
~ QoS		17	GE17	Disabled
 Diagnostics 		18	GE18	Disabled
Management		19	GE19	Disabled
		20	GE20	Disabled
		21	GE21	Disabled
		22	GE22	Disabled
	H	23	GE23	Disabled
		24	GE24	Disabled
		25	GE25	Disabled
		26	GE26	Disabled
		27	GE27	Disabled
		28	GE28	Disabled
	Edit			

Fig 4.4.1 Port EEE Setting Table port selection page

S C2000-24GP+8CF	× Ø	RTL8382	2M		X G best ntp server - Google Search X + - 0	×
← → C ▲ Not secu	ire 192.168	.0.2/hon	me.html?ve	er	¢	•
COMMANDO					Save Logout Reboot	Debug
	Port	» EEF	6			
Status	^ 	Entry	Port	State		1
System Information		1	GE1 C	Disabled		
Logging Message		2	GE2 C	Disabled		
Link Aggregation		3	GE3 C	Disabled		
MAC Address Table		4	GE4 D	Disabled		
Network		5	GE5 C	Disabled		
IP Address		6	GE6 C	Disabled		
DNS		7	GE7 C	Disabled		
Hosts System Time		8	GE8 C	Disabled		
System Time		9	GE9 D	Disabled		
Port Setting		10	GE10 C	Disabled		
Error Disabled		11	GE11 C	Disabled		
 Link Aggregation 		12	GE12 D	Disabled		
Group		13	GE13 D	Disabled		
Port Setting		14	GE14 D	Disabled		
EFE		15	GE15 D	Disabled		
Jumbo Frame		16	GE16 E	Disabled		
Port Security		17	GE17 D	Disabled		
Protected Port		18	GE18 E	Disabled		
Storm Control Mirroring		19	GE19 D	Disabled		
POF Setting		20	GE20 D	Disabled		
VLAN		21	GE21 D	Disabled		
MAC Address Table		22	GE22 E	Disabled		

Fig 4.4.2 Port EEE Setting Table all ports selection page

COMMANDO		Save Logout Reboot Debug
Po	rt » EEE	
✓ Status		^
✓ Network		
▼ Port	Edit EEE Setting	
Port Setting Error Disabled Link Aggregation Group	Port GE1-GE28 State Z Enable	
Port Setting LACP EEE Jumbo Frame Bot Security	Apply Close	
Protected Port Storm Control Mirroring		>

Fig 4.4.3 Port EEE Setting port application page

COMMANDO	Port » EEF	2		
System Time	EEE Settin	ig Table		
Logging Message				
✓ Port				
Link Aggregation		Entry	Port	State
MAC Address Table			CEI	Enabled
	H		CE2	Enabled
- Port		-	CER	Enabled
Port Setting Error Disabled			GES	Enabled
 Link Addregation 		2	OE4	Enabled
EEE			GES	Enabled
Jumbo Frame		°,	GE0 CE7	Enabled
Port Security		,	GE7	Enabled
Protected Port Storm Control		°.	GEO	Enabled
Mirroring		9	GES	Enabled
VLAN		10	GE10	Enabled
MAC Address Table		"	GEII	Enabled
Spanning Tree		12	GE12	Enabled
 Discovery 		13	GE13	Enabled
V DHCP		14	GE14	Enabled
 Multicast 		15	GE15	Enabled
 Routing 		16	GE16	Enabled
 Security 		17	GE17	Enabled
V ACL		18	GE18	Enabled
✓ Q0S		19	GE19	Enabled
 Diagnostics 		20	GE20	Enabled
Management		21	GE21	Enabled
		22	GE22	Enabled
		23	GE23	Enabled
		24	GE24	Enabled
		25	GE25	Enabled
		26	GE26	Enabled
		27	GE27	Enabled
		28	GE28	Enabled
	Edit			

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**.

COMMANDO			Sav	ve Logout Reboot D
P ✓ Status ✓ Network ✓ Port	ort » Jumbo Fr Jumbo Frame	ame ☑ Enable		
Port Setting Error Disabled V Link Aggregation EEE Jumbo Frame Port Security	Apply	9216	Byte (1518 - 10000, default 1:	522)
Protected Port Storm Control Mirroring VLAN MAC Address Table				

Fig 4.5.1 Jumbo frame enable page

COMMANDO		Save	Logout	Reboot	Debug
					0
Po	rt » Jumbo Frame				
✓ Status					
✓ Network					
▼ Port	☑ Enable				
Port Setting	9216	Byte (1518 - 10000, default 1522))		
Error Disabled	L				1
 Link Aggregation 	Apply				
EEE					
Jumbo Frame					
Port Security					
Protected Port					
Storm Control					
Mirroring					
VLAN					

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**

COMMANDO										Sav	re Logout Reboot	t Debug
	Port »	Port Secu	rity									
✓ Status	Dort	Socurity Tak	alo									^
✓ Network	Port	Security rat	ле									
✓ Port											Q	
Port Setting		- Ent	TV I	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky	
Error Disabled			1	GE1	Disabled	1	10101	oomgarcu	tiolate Hamber	Protect	Disabled	
 EEE 			2	052	Disabled				•	Protect	Disabled	- L.
Jumbo Frame			2	GE2	Disabled	1			0	Protect	Disabled	
Port Security				000	Disabled				0	Protect	Disabled	
Protected Port			1	GE4	Disabled	1		U	U	Protect	Disabled	
Storm Control			5	GE5	Disabled	1	C	0	0	Protect	Disabled	
Mirroring			8	GEB	Disabled	1	C C	0	U	Protect	Disabled	
VLAN			7	GE7	Disabled	1	C	0	0	Protect	Disabled	
MAC Address Table			8	GE8	Disabled	1	C	0	0	Protect	Disabled	
V Discovery			9	GE9	Disabled	1	c	0	0	Protect	Disabled	
			10	GE10	Disabled	1	C	0	0	Protect	Disabled	
 Multicast 			11	GE11	Disabled	1	C	0	0	Protect	Disabled	
 Monteast Manufactoria 			12	GE12	Disabled	1	C	0	0	Protect	Disabled	
 Routing Security 			13	GE13	Disabled	1	C	0	0	Protect	Disabled	
			14	GE14	Disabled	1	c	0	0	Protect	Disabled	
V 045			15	GE15	Disabled	1	C	0	0	Protect	Disabled	
V Diagnostics			16	GE16	Disabled	1	C	0	0	Protect	Disabled	
 Magazement 			17	GE17	Disabled	1	c	0	0	Protect	Disabled	
· Management			18	GE18	Disabled	1	c	0	0	Protect	Disabled	
			19	GE19	Disabled	1	c	0	0	Protect	Disabled	
			20	GE20	Disabled	1	c	0	0	Protect	Disabled	
			21	GE21	Disabled	1	c	. 0	0	Protect	Disabled	
			22	GE22	Disabled	1	c	0	0	Protect	Disabled	
			23	GE23	Disabled	1	c	0	0	Protect	Disabled	
	I I I		24	GE24	Disabled	1	c	0	0	Protect	Disabled	
			25	GE25	Disabled	1	c	0	0	Protect	Disabled	
				0500							-	×

Fig 4.6.1 Default Port Security Table page

								Save Logout Reboo
1	Port » Port	Security						
		2 022	Disabled			0	0 Protect	DISBOIRD
		3 GE3	Disabled	1	0	0	0 Protect	Disabled
		4 GE4	Disabled	1	0	0	0 Protect	Disabled
tting		5 GE5	Disabled	1	0	0	0 Protect	Disabled
sabled		6 GE6	Disabled	1	0	0	0 Protect	Disabled
gregation		7 GE7	Disabled	1	0	0	0 Protect	Disabled
_		8 GE8	Disabled	1	0	0	0 Protect	Disabled
Frame		9 GE9	Disabled	1	0	0	0 Protect	Disabled
ed Port		10 GE10	Disabled	1	0	0	0 Protect	Disabled
Control		11 GE11	Disabled	1	0	0	0 Protect	Disabled
9		12 GE12	Disabled	1	0	0	0 Protect	Disabled
		13 GE13	Disabled	1	0	0	0 Protect	Disabled
ress Table		14 GE14	Disabled	1	0	0	0 Protect	Disabled
Tree	In	15 GE15	Disabled	1	0	0	0 Protect	Disabled
		16 GE16	Disabled	1	0	0	0 Protect	Disabled
		17 GE17	Disabled	1	0	0	0 Protect	Disabled
	H	18 GE18	Disabled	1	0	0	0 Protect	Disabled
		19 GE19	Disabled	1	0	0	0 Protect	Disabled
		20 GE20	Disabled	1	0	0	0 Protect	Disabled
		24 0524	Disabled		ő	0	0 Protect	Disabled
		21 GE21	Disabled			0	0 Protect	Disabled
3		22 00222	Disabled			0	0 Protect	Disabled
ent		23 GE23	Disabled			0	0 Protect	Disabled
		24 0624	Disabled			0	0 Protect	Disabled
		25 GE25	Disabled			0	0 Protect	Disabled
		28 GE28	Disabled	1	0	0	0 Protect	Disabled
		27 GE27	Disabled	1	0	U	0 Protect	Disabled
		28 GE28	Disabled	1	0	0	0 Protect	Disabled

Fig 4.6.2 Selecting Port Security GE4 page

Port Security Configuration:

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

COMMANDO Port » Port Se	curit	y	Save Logout Reboot Debug
✓ Status ^			^
✓ Network			
✓ Port Edit Port Security			
Port Setting			
Error Disabled	Port	GE4	
✓ Link Aggregation			
EEE .	late		
Port Security Address	imit	1 (1 - 256, default 1)	
Protected Port	•••••	Protect	
Storm Control Violate A	tion	O Restrict	
Mirroring	1	O Shutdown	
VLAN S	icky	Enable	
V MAC Address Table			
✓ Spanning Tree Apply	Clo	Se	
✓ Discovery			
✓ DHCP			
✓ Multicast			
✓ Routing			
✓ Security			
✓ ACL			
V QoS			v

Fig 4.6.3 Edit Port security for GE4 interface page

COMMANDO	Port >	> Port	t Secu	rity						
✓ Status										
V Network	1	St	ate	Enable						
✓ Port										
Port Setting	l	Rate Li	mit 1	00	P	acket / \$	Sec (1 - 600, d	efault 100)		
Error Disabled	_									
✓ Link Aggregation EEE	A	pply	J							
Jumbo Frame	_									
Port Security	Port	Secu	rity Ta	ble						
Protected Port										
Storm Control Mirroring										
VI AN		Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
✓ MAC Address Table		1	GE1	Disabled	1	0	0	0	Protect	Disabled
✓ Spanning Tree		2	GE2	Disabled	1	0	0	0	Protect	Disabled
✓ Discovery		3	GE3	Disabled	1	0	0	0	Protect	Disabled
		4	GE4	Enabled	1	0	0	0	Protect	Enabled
✓ Multicast		5	GE5	Disabled	1	0	0	0	Protect	Disabled
✓ Routing		6	GE6	Disabled	1	0	0	0	Protect	Disabled
✓ Security		7	GE7	Disabled	1	0	0	0	Protect	Disabled
✓ ACL		8	GE8	Disabled	1	0	0	0	Protect	Disabled
✓ QoS		9	GE9	Disabled	1	0	0	0	Protect	Disabled

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.

COMMANDO	Port »	Prote	ected P	ort
 ✓ Network 				
▼ Port	Prot	ected F	ort Tal	ble
Port Setting Error Disabled		Entry:	Dort	Stata
EEE		Entry	ροπ 051	State
Jumbo Frame		1	GET	Unprotected
Port Security		2	GE2	Unprotected
Protected Port		3	GE3	Unprotected
Storm Control Mirroring		4	GE4	Unprotected
		5	GE5	Unprotected
MAC Address Table		6	GE6	Unprotected
		7	GE7	Unprotected
		8	GE8	Unprotected
× DHCP		9	GE9	Unprotected
✓ Multicast		10	GE10	Unprotected
× Routing		11	GE11	Unprotected
✓ Security		12	GE12	Unprotected
× ACL		13	GE13	Unprotected
× QoS		14	GE14	Unprotected
✓ Diagnostics		15	GE15	Unprotected
✓ Management		16	GE16	Unprotected
		17	GE17	Unprotected

Fig 4.7.1 Protected Port Table page

	COMMANDO	Рог	rt »	> Prot	tected	Port	Save Logout Reboot Debu	g
\sim	Status							^
~	Network					- L L -		
-	Port		rot	ected	Port	able		
	Port Setting						0	1
	Error Disabled	1.1	_				4	
	 Link Aggregation 			Entry	Port	State		
	EEE			1	GE1	Unprotected		
	Jumbo Frame	LГ		2	GE2	Unprotected		
	Port Security Protected Port			3	GE3	Unprotected		
	Storm Control			4	GE4	Unprotected		
	Mirroring			5	GE5	Unprotected		
~	VLAN			6	GE6	Unprotected		
~	MAC Address Table			7	GE7	Unprotected		
								. *

Fig 4.7.2 Selection of GE1 port for Protected page

COMMANDO	- 4 % D- 4 - 4 - 1 D- 4	Save Logout	Reboot Debug
P	ort » Protected Port		
✓ Status ^			^
✓ Network			
▼ Port	Edit Protected Port		
Port Setting			
Error Disabled	Port GE1		
✓ Link Aggregation	State 🔽 Protected		
EEE Jumbo France			i
Jumpo Frame Port Security	Apply Close		
Protected Port			
Storm Control			
Mirroring			
VLAN			
✓ MAC Address Table	c		>

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**.

COMMANDO	Po	rt »	> Stor	m Co	ntrol								
✓ Status ^		_											
✓ Network		[r	0 P2	sket / Sec								
▼ Port			Mode	 Kbi 	ts / Sec								
Port Setting		+ = = = =	+	Even	sludo								
Error Disabled			IFG		ude								
✓ Link Aggregation		L	ů										
EEE		Δ	pply	1									
Jumbo Frame													
Port Security													
Storm Control	F	Port	Settin	ng Tab	le								
Mirroring													
VLAN													_
✓ MAC Address Table			E-t-	Deat	Ct-t-	Bro	adcast	Unknow	vn Multicast	Unkno	wn Unicast	A	П
✓ Spanning Tree			Enuy	Pon	State	State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	Action	
✓ Discovery			1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
✓ DHCP			2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
✓ Multicast			3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
✓ Routing			4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
✓ Security			5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
✓ ACL			6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
✓ QoS			7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	

Fig 4.8.1 Default Storm control port setting table page



Port » Storm Control

	4 (0) 447	T								
Network	rt Setting	lable								
Port										
Port Setting	_									
Link Aggregation	Entry	Port	State	Br	oadcast	Unknov	n Multicast	Unkno	wn Unicast	Action
EEE	,			State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
Jumbo Frame	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Port Security	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Protected Port	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Storm Control	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Mirroring	1 5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
VLAN	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
MAC Address Table	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Dron
Spanning Tree		GES	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Discovery		000	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Dree
		GES	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Diop
Multicast	10	GE10	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Routing	4 II	GE11	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Security	12	GE12	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
ACL	13	GE13	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
QoS	14	GE14	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Diagnostics	15	GE15	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Management 🗸	/ 16	GE16	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	17	GE17	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	18	GE18	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	19	GE19	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	20	GE20	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	21	GE21	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	2 22	GE22	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
Ě	2 23	GE23	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	2 24	CE24	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
- I I I I I I I I I I I I I I I I I I I		OFOR	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Dree
	25	GE25	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	20	GE26	Disabled	Disabled	10000	Crisabled	10000	Disabled	10000	Drop
	27	GE27	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
	28	GE28	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Fig 4.8.2 Storm control Selecting port setting page

COMMANDO	ort » Storm Control			
✓ Status ✓ ✓ Network ✓	Edit Port Setting			
	Luit Port Setting			
Fror Disabled	· · · · · · · · · · · · · · · · · · ·			
✓ Link Aggregation	Port	GE1-GE28		
EEE	State	Enable		
Jumbo Frame		Enable		= =
Port Security	Broadcast			= =
Protected Port		100	Kbps (16 - 1000000, default 10000)	
Storm Control Mirroring		Enable		
	Unknown Multicast	1000	Khop (16 100000 default 10000)	= 1
 VLAN MAC Address Table 		1000	Kbps (10 - 1000000, deladit 10000)	
		Enable		
V Diagovani	Unknown Unicast	1000	Kbps (16 - 1000000, default 10000)	
V DHCD				
V Multisast	Action	Drop Shutdown		
	L			
 Routing 	Apply Close			
✓ Security	Close			

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**.

COMMANDO	Dout	Minnoni	W.7				Save Logout Reboot Debug
⊥ Status ^	rort /	// MIFFOFI	ng				
 Network 							
✓ Port	Mirr	roring Tabl	e				
Port Setting Error Disabled							Q
✓ Link Aggregation		Session ID	State	Monitor Port	Ingress Port	Egress Port	
EEE	0	1	Disabled				·
Jumbo Frame Port Security	0	2	Disabled				
Protected Port	0	3	Disabled				
Storm Control	0	4	Disabled				
Mirroring	_	E .49					
VLAN		Edit					
 MAC Address Table 							
 Spanning Tree 		"*" Allow the m	onitor port t	o send or receive	e normal packets	S	
✓ Discovery	L						
✓ DHCP ✓							

Fig 4.9.1 Mirroring Table page

COMMANDO							
	Port » Mirroring						
✓ Status	Edit Mirroring						
✓ Network							
▼ Port	r						
Port Setting	Session ID	1					
Error Disabled	State	Enable					
✓ Link Aggregation EEE Jumbo Frame Port Security	Monitor Port	GE1 🔽 Send or Receive Normal Packet					
Protected Port Storm Control Mirroring		Available Port GE1	Selected Port				
V MAC Address Table	Ingress Port	GE4	-				
✓ Spanning Tree		GE5	-				
✓ Discovery		GE8	<u><</u>				
✓ DHCP		GE9 Y	<u> </u>		!		
✓ Multicast		Available Port	Selected Port				
✓ Routing		Available Fort	Selected Fort				
✓ Security		GE1	GE7				
✓ ACL	Egress Port	GE3	>				
√ QoS		GE4 GE5					
✓ Diagnostics		GE6	<				
∨ Management		GE8 GE9 V					
	Apply Cl	ose]		

Fig 4.9.2 Edit Port Mirroring page

Por	t » Mirro	ring						
М	irroring Ta	ble					Success.	<u>ی</u>
E	Session I	D State	Monitor Port	Ingress Port	Egress Port			
	C	1 Enabled	GE1	GE7	GE7			
	C	2 Disabled						
	0 0	3 Disabled 4 Disabled						
	Edit				1			
		Mirroring Tal	Mirroring Table Session ID State 1 Enabled 2 Disabled 3 Disabled 4 Disabled Edit	Mirroring Table Session ID State Monitor Port 1 Enabled GE1 2 Disabled 3 Disabled 4 Disabled Edit	Mirroring Table Session ID State Monitor Port Ingress Port 1 Enabled GE1 GE7 2 Disabled 3 Disabled 4 Disabled Edit	Mirroring Table Session ID State Monitor Port Ingress Port Egress Port 1 Enabled GE1 GE7 GE7 2 Disabled 3 Disabled 4 Disabled Edit	Mirroring Table Session ID State Monitor Port Ingress Port Egress Port 1 Enabled GE1 GE7 GE7 2 Disabled 3 Disabled 4 Disabled Edit	Mirroring Table Success Session ID State Monitor Port Ingress Port Egress Port 1 Enabled GE1 GE7 GE7 2 Disabled 3 Disabled Edit "" Allow the monitor port to send or receive normal packets

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 standardsbased 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 VI AN, click VI AN, >> VI AN, >> Create VI AN,

COMMANDO	VLAN » V	LAN » (Create V	LAN			
✓ Status							
✓ Network		Available VI		Created VI A			
✓ Port		Available vi					
▼ VLAN		VLAN 2	<u>^</u>	VLAN 1	^		
 ✓ VLAN Create VLAN ✓ VLAN Configuration Membership Port Setting ✓ Voice VLAN ✓ Protocol VLAN 	VLAN	VLAN 4 VLAN 5 VLAN 6 VLAN 7 VLAN 8 VLAN 9			<u>×</u>		
✓ MAC VLAN							
✓ Surveillance VLAN							
✓ GVRP ✓ MAC Addross Table	VLAN lab	le					
 ✓ Spanning Tree 	Showing All	entries			Sho	wing 1 to 1 of 1 entries	i
✓ Discovery			-			1	
✓ DHCP		Name	lype	VLAN Inter	face State		
✓ Multicast	1	default	Default	Ena	bled		
✓ Routing	(-		_				
✓ Security	Edit	Delete	9				
V ACL							

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".

COMMANDO	VL	AN » V	LAN » C	'reate V	/LAN		
✓ Status	^	1	VLAN 3	<u>^</u>	VIAN 1		
✓ Network			VLAN 4		VLAN 2		
✓ Port		VLAN	VLAN 5		VLAN 30		
- VLAN			VLAN 7				
A VLAN			VLAN 8	<			
Create VLAN		1	VLAN 9	~			
VLAN Configuration	E.	i	1.10				
Membership		Apply	1				
Port Setting		Срру	J				
VOICE VLAIN							
	V	AN Tabl	e				
 Surveillance VLAN 			_				
✓ GVRP	Sh	owing All	entries			Showing 1 to 3 of 3 entries	
 MAC Address Table 		VLAN	Name	Туре	VLAN Interface State		
 Spanning Tree 		1	default	Default	Enabled	•	
✓ Discovery		2	VLAN0002	Static	Disabled		
✓ DHCP		30	VLAN0030	Static	Disabled		
✓ Multicast							_
✓ Routing		Edit	Delete				
✓ Security		Luit	Delete				
✓ ACL							

Fig 5.1.2 VLAN Page after VLAN creation

COMMANDO	77 ANI NI N77			T AN	
	VLAN ~ VI		reate v		
✓ Status		VLAN 3	^	VLAN 1	
V Network		VLAN 4		VLAN 2	
V Port	VLAN	VLAN 5 VLAN 6		VLAN 30	
✓ VLAN		VLAN 7			
∧ VLAN Create VLAN VLAN Configuration		VLAN 8 VLAN 9 VLAN 10	× <	<u> </u>	
Membership Port Setting Voice VLAN Protocol VLAN MAC VLAN	Apply VLAN Table	•			
✓ Surveillance VLAN✓ GVRP	Showing All 🗸	entries			Showing 1 to 3 of 3 entries
✓ MAC Address Table		Name	Туре	VLAN Interface State	
✓ Spanning Tree	1	default	Default	Enabled	·
✓ Discovery	2	VLAN0002	Static	Disabled	
✓ DHCP	30	VLAN0030	Static	Disabled	
✓ Multicast					
✓ Routing	Edit	Delete			
✓ Security		20.000			
✓ ACL					

Fig 5.1.3 VLAN Default name after VLAN creation

COMMANDO	
	VLAN » VLAN » Create VLAN
Status Network Port	Edit VLAN Name
✓ VLAN	
∧ VLAN Create VLAN	Name COMMANDO LAN
VLAN Configuration Membership Port Setting	Apply Close
✓ Voice VLAN	
✓ Protocol VLAN	
 ✓ Minoc VLAN ✓ Surveillance VLAN 	
✓ GVRP	
✓ MAC Address Table	
✓ Spanning Tree	
✓ Discovery	
Multicast	
✓ Security	
V ACL	

Fig 5.1.4 Edit VLAN name after VLAN creation

COMMANDO	VLAN » VI	LAN » Create	VLAN		
✓ Status	[Available VI AN	Create		
V Network			Create		
✓ Port				1 ^	
✓ VLAN		VLAN 5	VLAN	30	
 VLAN Create VLAN VLAN Configuration Membership Port Setting Voice VLAN Protocol VLAN MAC VLAN Surveillance VLAN 		VLAN 6 VLAN 7 VLAN 8 VLAN 9 VLAN 10		<u> </u>	
✓ GVRP		C			
✓ MAC Address Table	Showing All 🗸	entries		Showing 1	to 3 of 3 entries
✓ Spanning Tree		Name	Type	VI AN Interface State	
✓ Discovery		default	Default	Enabled	
✓ DHCP			Static	Disabled	
✓ Multicast			Static	Disabled	
✓ Routing		VLAN0030	Static	Disabled	
✓ Security ✓ ACL	Edit	Delete			

Fig 5.1.5 Vlan Table after VLAN name change page

5.1.2 VLAN Configuration

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

For VLAN Configuration, click VLAN >> VLAN Configuration.

Click on "Create VLAN" from menu, Select "VLAN" name from Drop down & Select "Untagged" option on the Ports which required to add to the VLAN, then Click on "Apply".

COMMANDO	VLAN >	» VL₄	AN » I	/LAN Conf	ĩguration			Sa	ve Logout	Reboot	Debug
✓ Status											^
✓ Network		Confi		Table							
✓ Port	VLAN	Config	guration								
✓ VLAN	VLAN	VLAN00	30	~							
∧ VLAN									0		_
Create VLAN	_								~		_
VLAN Configuration	Entry	Port	Mode		Membership)	PVID	Forbidden			
Membership Dort Setting	1	GE1	Trunk	Excluded	○ Tagged	O Untagged					
Voice VLAN	2	GE2	Trunk	Excluded	○ Tagged	O Untagged					
 Protocol VLAN 	3	GE3	Trunk	Excluded	○ Tagged	O Untagged					
V MAC VLAN	4	GE4	Trunk	Excluded	○ Tagged	O Untagged					
✓ Surveillance VLAN	5	GE5	Trunk	Excluded	○ Tagged	O Untagged					
✓ GVRP	6	GE6	Trunk	Excluded	O Tagged	O Untagged					
✓ MAC Address Table	7	GE7	Trunk	Excluded	O Tagged	O Untagged					
✓ Spanning Tree	8	GE8	Trunk	Excluded	O Tagged						
✓ Discovery	9	GF9	Trunk	Excluded	O Tagged	O Untagged					~

Fig 5.1.6 VLAN configuration table page

COMMANDO	LAN	» vl	an » v	LAN Conf	īguration			Sav	'e Logout	Reboot	Debu
✓ Status ^											
✓ Network		06		Tabla							
✓ Port	VLAN	Conti	guration	lable							
▼ VLAN	VLAN	VLAN00	30	×							
∧ VLAN		default							0		
Create VLAN	_	COMMA	NDO LAN					, ,	~		_
VLAN Configuration	Entry	VLAN00	30		Membershi	0	PVID	Forbidden			
Membership	1	GE1	Irunk	Excluded	\odot Tagged	O Untagged					
Port Setung	2	GE2	Trunk	Excluded	\bigcirc Tagged	O Untagged					
Voice VLAN Protocol VI AN	3	GE3	Trunk	Excluded	\bigcirc Tagged	O Untagged					
✓ MAC VLAN	4	GE4	Trunk	Excluded	○ Tagged	O Untagged					
✓ Surveillance VLAN	5	GE5	Trunk	Excluded	○ Tagged	O Untagged					
✓ GVRP	6	GF6	Trunk	Excluded	O Taqqed	O Untagged					

Fig 5.1.8 VLAN Selection tap on VLAN configuration table page

		X/T A N N		N N X/T						
	^	VLAN "	VLA	N // VL	AN Configu	iration				
			Configu	ration T	able					
			soninge		, abic					
		VLAN V	LAN0030	\sim]					
1										
onfiguration		Entry	Port	Mode		Members	hip	PVID	Forbidden	Г
nip		1	GE1	Trunk	Excluded	OTagged	OUntagged			
ting		2	GE2	Trunk	Excluded	OTagged	OUntagged			
NIN VLANI		3	GE3	Trunk	Excluded	◯ Tagged	OUntagged			
		4	GE4	Trunk	Excluded	◯ Tagged	O Untagged			
VLAN		5	GE5	Trunk	Excluded	O Tagged	OUntagged			
		6	GE6	Trunk	Excluded	○ Tagged	OUntagged			
		7	GE7	Trunk	Excluded	O Tagged	OUntagged			
		8	GE8	Trunk	Excluded	O Tagged	OUntagged			
		9	GE9	Trunk	Excluded	OTagged	OUntagged			
		10	GE10	Trunk	Excluded					
		11	GE11	Trunk	Excluded					
		12	GE12	Trunk	Excluded					
		12	GE13	Trunk	Excluded					
		14	CE14	Trunk	Excluded					
		15	CE15	Trunk	Excluded					
		15	CE16	Trunk	Excluded					
	~	10	GETO	TUTK	C Excluded	Tagged	Ontagged			

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

COMMANDO	VLA	N » V	LAN	» Mei	nhershin	
✓ Status	V LA				noersnip	
✓ Network						
✓ Port	Me	mbersh	nip Tab	le		
▼ VLAN						
∧ VLAN	-					
Create VLAN		Entry	Port	Mode	Administrative VLAN	Operational VLAN
VLAN Configuration	0	1	GE1	Trunk	1UP	1UP
Membership	0	2	GE2	Trunk	1UP	1UP
Port Setting	0	3	GE3	Trunk	1UP	1UP
Voice VLAN Protocol VLAN	0	4	GE4	Trunk	1UP	1UP
✓ MAC VLAN	Ō	5	GE5	Trunk	1UP	1UP
✓ Surveillance VLAN	Ŏ	6	GE6	Trunk	1UP	1UP
✓ GVRP		7	GE7	Trunk	1UP	111P
 MAC Address Table 			CEO	Truck	1110	1110
✓ Spanning Tree			GE0	Truck	100	
✓ Discovery		9	GE9	TTUNK	IUP	IUP
✓ DHCP	0	10	GE10	Trunk	10P	10P
✓ Multicast	0	11	GE11	Trunk	1UP	1UP
✓ Routing	0	12	GE12	Trunk	1UP	1UP
✓ Security	0	13	GE13	Trunk	1UP	1UP
V ACL	0	14	GE14	Trunk	1UP	1UP
✓ QoS	0	15	GE15	Trunk	1UP	1UP
✓ Diagnostics	0	16	GE16	Trunk	1UP	1UP
✓ Management ✓	0	17	GE17	Trunk	1UP	1UP

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



 Status Network

Port VLAN VLAN Cre VLA Mei Por Voice Proto MAC Surve GVRF MAC Ad Spannir Discove DHCP Multicas Routing Security ACL QoS Diagnos

VLAN	≫	VLAN	»	Membershi	ľ
------	---	------	---	-----------	---

Membership Table

∧ VLAN		_	_		
Create VLAN	Entry	Port	Mode	Administrative VLAN	Operational VLAN
VLAN Configuration) 1	GE1	Trunk	1UP	1UP
Membership) 2	GE2	Trunk	1UP	1UP
Port Setting) 3	GE3	Trunk	1UP	1UP
Voice VLAN	4	GE4	Trunk	1UP	1UP
V MAC VLAN	, . , 5	CE5	Trunk	111P	11.1P
 Surveillance VI AN 		OFE	Trunk	100	100
✓ GVRP		GEO	TTUNK	IOF	IUP
MAC Address Table) (GE7	Trunk	10P	10P
✓ Spanning Tree) 8	GE8	Trunk	1UP	1UP
✓ Discovery) 9	GE9	Trunk	1UP	1UP
) 10	GE10	Trunk	1UP	1UP
✓ Multicast) 11	GE11	Trunk	1UP	1UP
× Routing) 12	GE12	Trunk	1UP	1UP
× Security) 13	GE13	Trunk	1UP	1UP
) 14	GE14	Trunk	1UP	1UP
) 15	GE15	Trunk	1UP	1UP
 Diagnostics) 16	GE16	Trunk	1UP	1UP
V Management	17	GE17	Trunk	111P	11.IP
	, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	0217	manik	101	101

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

COMMANDO	VLAN » VLAN » Membership	2
✓ Status		
✓ Network		
✓ Port	Edit Port Setting	
▼ VLAN		
^ VLAN	Port GE1	
Create VLAN	*	
VLAN Configuration	Mode I Irunk	
Membership	2 ^	4091T A
Port Setting	10	1UP
VOICE VLAN		
 Surveillance VLAN 		
✓ GVRP	Membership v	
MAC Address Table		
 Spanning Tree 		
Discovery	O Tagged	
V DHCP	Untagged	
✓ Multicast	VID	
✓ Routing	L	
✓ Security	Apply Close	
V ACL		
V QoS		
✓ Diagnostics		
✓ Management		

Fig 5.1.12 Edit VLAN membership for slected port GE1 page



Status ۸ Network ✓ Port VLAN VLAN Create VLAN VLAN Configuration Membership Port Setting ✓ Voice VLAN Protocol VLAN ✓ MAC VLAN ✓ Surveillance VLAN ✓ GVRP MAC Address Table Spanning Tree Discovery ✓ DHCP Multicast ✓ Routing Security V ACL ✓ QoS Diagnostics Management

VLAN » VLAN » Membership

Membership Table

		Entry	Port	Mode	Administrative VLAN	Operational VLAN		
	0	1	GE1	Trunk	1UP, 4091T	1UP, 4091T		
	0	2	GE2	Trunk	1UP	1UP		
	0	3	GE3	Trunk	1UP	1UP		
	0	4	GE4	Trunk	1UP	1UP		
	0	5	GE5	Trunk	1UP	1UP		
	0	6	GE6	Trunk	1UP	1UP		
	0	7	GE7	Trunk	1UP	1UP		
- 1	0	8	GE8	Trunk	1UP	1UP		
- 1	0	9	GE9	Trunk	1UP	1UP		
- 1	0	10	GE10	Trunk	1UP	1UP		
-	0	11	GE11	Trunk	1UP	1UP		
- 1	0	12	GE12	Trunk	1UP	1UP		
	0	13	GE13	Trunk	1UP	1UP		
	0	14	GE14	Trunk	1UP	1UP		
	0	15	GE15	Trunk	1UP	1UP		
	0	16	GE16	Trunk	1UP	1UP		
\sim	0	17	GE17	Trunk	1UP	1UP		

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

COMMANDO	VLAN	[» V]	LAN 3	» Por	t Setti	ng			
✓ Status									
✓ Network									
✓ Port	Port	Settin	ig lab	le					
- VLAN									
~ VLAN									
Create VLAN		Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
VLAN Configuration		1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
Membership Dort Sotting		2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
✓ Voice VLAN		3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
✓ Protocol VLAN		4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
✓ MAC VLAN		5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
✓ Surveillance VLAN		6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
✓ GVRP		7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
V MAC Address Table		8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
 Spanning Tree 		9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
Discovery		10	CE10	Trunk	1	A11	Enabled	Disabled	0x8100
V DHCP		11	0010	Truck		AU	Enabled	Disabled	0x0100
✓ Multicast		10	OF40	Taurala			Enabled	Disabled	0.0100
✓ Routing		12	GETZ	Trunk		All	Enabled	Disabled	008100
✓ Security		13	GE13	Trunk	1	All	Enabled	Disabled	0x8100
V ACL		14	GE14	Trunk	1	All	Enabled	Disabled	0x8100
V QoS		15	GE15	Trunk	1	All	Enabled	Disabled	0x8100
 Diagnostics 		16	GE16	Trunk	1	All	Enabled	Disabled	0x8100
✓ Management ✓		17	GE17	Trunk	1	All	Enabled	Disabled	0x8100

Fig 5.1.14 VLAN port setting table page

MANDO	^ VI	LAN	「≫ v :	LAN	» Por	t Setti	ng			
·k		Port	Settir	ng Tab	le					
/I AN	1.1		Entry	Port	Mode	DVID	Accept Frame Type	Ingress Filtering	Unlink	TPID
Configuration			1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
			2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
			3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
			4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
			5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
N			6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
			7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
			8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
			9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
			10	GE10	Trunk	1	All	Enabled	Disabled	0x8100
			11	GE11	Trunk	1	All	Enabled	Disabled	0x8100
			12	GE12	Trunk	1	All	Enabled	Disabled	0x8100
			13	GE13	Trunk	1	All	Enabled	Disabled	0x8100
			14	GE14	Trunk	1	All	Enabled	Disabled	0x8100
			15	GE15	Trunk	1	All	Enabled	Disabled	0x8100
			16	GE16	Trunk	1	All	Enabled	Disabled	0x8100
	~		17	GE17	Trunk	1	All	Enabled	Disabled	0x8100

Fig 5.1.15 VLAN port setting for selected port page



Fig 5.1.16 Edit port setting for selected ports page

COMM	ANDO

VLAN » VLAN » Port Setting

✓ Status										
✓ Network		Dort	Cottin							
✓ Port		FOIL	Setti	ig lab	le					
✓ VLAN										
∧ VLAN		_								
Create VLAN			Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
VLAN Configuration			1	GE1	Access	4091	Untag Only	Enabled	Disabled	0x8100
Membership			2	GE2	Access	4091	Untag Only	Enabled	Disabled	0x8100
Port Setting			3	GE3	Access	4091	Untag Only	Enabled	Disabled	0x8100
✓ Protocol VLAN			4	GE4	Access	4091	Untag Only	Enabled	Disabled	0x8100
✓ MAC VLAN			5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
✓ Surveillance VLAN			6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
✓ GVRP			7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
 MAC Address Table 			8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
 Spanning Tree 			9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
 Discovery 			10	000	Truck		AII	Enabled	Disabled	0v0100
✓ DHCP			10	GEIU	Tourk		All	Enabled	Disabled	0.0100
 Multicast 			11	GETT	Trunk	1	All	Enabled	Disabled	0X8100
✓ Routing			12	GE12	Trunk	1	All	Enabled	Disabled	0x8100
✓ Security			13	GE13	Trunk	1	All	Enabled	Disabled	0x8100
✓ ACL			14	GE14	Trunk	1	All	Enabled	Disabled	0x8100
✓ QoS			15	GE15	Trunk	1	All	Enabled	Disabled	0x8100
✓ Diagnostics			16	GE16	Trunk	1	All	Enabled	Disabled	0x8100
✓ Management	~		17	GE17	Trunk	1	All	Enabled	Disabled	0x8100

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.

COMMANDO	VI AN N Voice VI AN N Dueneuty
✓ Status	VLAN ~ VOICE VLAN ~ Hoperty
✓ Network	State Enable
✓ Port	
✓ VLAN	VLAN None 🗠
 ✓ VLAN ∧ Voice VLAN Property Voice OUI 	CoS / 802.1p
Protocol VLAN MAC VLAN Surveillance VLAN GVRP	Apply
 MAC Address Table 	Port Setting Table
✓ Spanning Tree	
✓ Discovery	
✓ DHCP	Entry Port State Mode QoS Policy
✓ Multicast	1 GE1 Disabled Auto Voice Packet
✓ Routing	2 GF2 Disabled Auto Voice Packet
✓ Security	□ 3 GE3 Disabled Auto Voice Packet

Fig 5.2.1 Default Voice VLAN state setting table page

COMMANDO							Save	Logout	Reboot	Debug
	VLAN » Vo	oice V	LAN »	Prope	rty					<u>^</u>
V Network	[
✓ Port	S	tate [Enable							
▼ VLAN	v	LAN	VLAN0010	\sim						
✓ VLAN ∧ Voice VLAN Property	CoS / 80 Remar	2.1p king	Enable							
Voice OUI Victory VLAN MAC VLAN Surveillance VLAN VGVRP	Aging T	Fime	10000	Min (3	30 - 65536, defa	ult 1440)				
 MAC Address Table 	Port Settin	a Tabl	e							
✓ Spanning Tree		5								
✓ Discovery								Q		_
V DHCP	Entry	Port	State	Mode	OoS Policy		 			
✓ Multicast		GE1	Disabled	Auto	Voice Packet					_
✓ Routing		GE2	Disabled	Auto	Voice Packet					
✓ Security		CE2	Disabled	Auto	Voice Packet					
*	3	GE3	Disabled	AULO	voice Packet					

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



							Sav	e Logoui	Rebool	Debug
V	'LAN	v» vo	oice V	LAN »	Prope	rty				
✓ Status										^
 Network 	Por	t Settin	a Tab	le						
✓ Port			J							
VLAN								Q		_
		Entry	Port	State	Mode	QoS Policy		,		
Property		1	GE1	Disabled	Auto	Voice Packet				- 11
Voice OUI		2	GE2	Disabled	Auto	Voice Packet				
✓ Protocol VLAN		3	GE3	Disabled	Auto	Voice Packet				
✓ MAC VLAN		4	GE4	Disabled	Auto	Voice Packet				
 Surveillance VLAN GVRP 		5	GE5	Disabled	Auto	Voice Packet				
 MAC Address Table 		6	GE6	Disabled	Auto	Voice Packet				_
 Spanning Tree 		7	GE7	Disabled	Auto	Voice Packet				_
 Discovery 		8	GE8	Disabled	Auto	Voice Packet				_
V DHCP		9	GE9	Disabled	Auto	Voice Packet				_
✓ Multicast		10	GE10	Disabled	Auto	Voice Packet				
 Routing 		11	GE11	Disabled	Auto	Voice Packet				
✓ Security		12	GE12	Disabled	Auto	Voice Packet				

Fig 5.2.3 Voice VLAN setting CoS/802.1p Remarking page

Save Logon VLAN » Voice VLAN » Property	at Reboot Debug
✓ Status ^	^
✓ Network	
V Port Edit Port Setting	
▼ VLAN	
VLAN Port GE2-GE4	
∧ Voice VLAN State ⊡ Enable	
Property	
Volce Con Mode O Manual	
Vice Packet	
Surveillance VLAN	
→ GVRP	
VIAC Address Table Apply Close	
✓ Spanning Tree	
∨ DHCP	
✓ Multicast	
✓ Routing	
✓ Security	V

Fig 5.2.4 Voice VLAN Edit port setting page

COMMANDO	VL	an ×	» Voie	ce VI	.AN »	Prope	rty				Save	e 1	Logout	Re	boot	Debug	3
Status System Information System Time Logging Message Port Link Aggregation MAC Address Table		R Ar App	Remarkin ging Tin Iy	ng 2 ne 1	4 🔽	Min (3	0 - 65536, defa	ult 1440)								,	
✓ Network	Р	ort S	etting	Table	e												1
✓ Port													-				
VLAN													Q				
VLAN Voice VLAN Property Voice OUI VProtocol VLAN MAC VLAN GVRP MAC Address Table			ntry 	Port 521 522 523 524 525 525 526 526 527	State Disabled Enabled Enabled Disabled Disabled Disabled	Mode Auto Auto Auto Auto Auto Auto Auto	QoS Policy Voice Packet Voice Packet Voice Packet Voice Packet Voice Packet Voice Packet Voice Packet										~

Fig 5.2.5 Voice VLAN Port setting table page

5.2.2 Voice OUI

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

COMMANDO	LAN » Voice V	'LAN » Property	Save Logout	Reboot	Debug
✓ Status ^					^
V Network					
✓ Port	Edit Port Setting				
▼ VLAN					
VLAN	Port	GE2-GE4			
A Voice VLAN	State	🗇 Enghle			
Property	Sidle	V LIADIC			
	Mode	Auto Manual			
✓ MAC VLAN ✓ Surveillance VLAN	QoS Policy	Voice Packet			
✓ GVRP	L				
V MAC Address Table	Apply	Close			
✓ Spanning Tree					
✓ Discovery					
✓ DHCP					
✓ Multicast					
✓ Routing					
✓ Security					
V					Ŷ

Fig 5.2.6 Voice VLAN Voice OUI Table page

COMMANDO	VLAN » Voice VLAN »	Voice OUI	Save Logout Reboot Debug
✓ Status			
V Network	Voice OUI Table		
✓ Port			
VLAN	Showing All 🗠 entries	Showing 1 to 8 of 8 entries	Q
Property	00:E0:BB 3COM		
Voice OUI	00:03:6B Cisco		
✓ Protocol VLAN	00:E0:75 Veritel		
	00:D0:1E Pingtel		
 Surveillance VLAN GVRP 	00:01:E3 Siemens		
 MAC Address Table 	00:60:B9 NEC/Philips		
✓ Spanning Tree	00:0E:E2 H3C		
✓ Discovery	✓ 00:09:6E Avava		
✓ DHCP			First Previous 1 Next Last
✓ Multicast	Add Edit	Delete	
✓ Routing			
✓ Security			

Fig 5.2.7 Selecting Voice VLAN Voice OUI page

COMMANDO Save Logout Reboot Deb
VLAIV // Voice VLAIV // Voice OUT
✓ Status ^
V Network
Port Aad voice UUI
▼ VLAN
V VLAN OUI 1a iad i1d
A Voice VLAN
Property Description IP phones
Voice OUI
V Protocol VLAN Apply Close
 GURP
✓ MAC Address Table
✓ Spanning Tree
✓ Discovery
V DHCP
✓ Multicast
✓ Routing
✓ Security ✓

Fig 5.2.8 Voice VLAN Add Voice OUI page

COMMANDD	VI AN X Vo	ico VI AN »	Voice OIII	Save Logout Reboot	: Debug
Status System Information					^
System Time	Voice OUI 1	able			
Logging Message	Showing All 🗸	entries	Showing 1 to 9 of 9 entries	Q	
Link Aggregation		Description			
	00:E0:BE	3 3COM			
✓ Port	00:03:6E	Cisco			- 11
VLAN	00:E0:75	Veritel			- 11
VI AN	00:D0:18	Pingtel			- 11
∧ Voice VLAN	00:01:E3	Siemens			- 11
Property	00:60:B9	NEC/Philips			- 11
Voice OUI	00:0F:E2	H3C			- 11
Protocol VLAN	00:09:6E	Avaya			
Surveillance VLAN	1A:AD:1	P Phones			- 11
✓ GVRP				(First) (Previous) (1) (Ne:	xt) (Last)
V MAC Address Table	Add	Edit	Delete		~

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 protocolbased 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.

 ✓ Status ✓ Network ✓ Port ✓ VLAN ✓ VLAN ✓ VLAN ✓ Voice VLAN ✓ Protocol Group ID Frame Type Protocol Value O results found. ✓ Frest Previous 1 Next Last ✓ Surveillance VLAN ✓ Symming Tree ✓ Discovery ✓ DHCP ✓ Noultcast ✓ Routing ✓ Security 	COMMANDO	VLAN » Protocol VLAN	» Protocol Gi	roup	Save Logout Reboot Debug
 NetWork Port Port VLAN VLAN VlAN Voice VLAN Protocol Toup Group ID Frame Type Protocol Value O results found. First Previous 1 Next Last Add Edit Delete 	✓ Status	^			
VLAN VLAN VLAN VLAN VLAN VLAN VLAN Vlan Protocol Group Group Binding Group Binding MAC VLAN Surveiliance VLAN VLAN VLAN VLAN VACVLAN VACVLAN Sequrity VACVLAN VACVLAN Sequrity Value VACVLAN Value	✓ Network	Brotogol Crown Table			
 VLAN VLAN VLAN VlaN Voice VLAN Protocol VLAN Protocol Croup Group ID Frame Type Protocol Value O results found. First Prevous 1 Next Last Add Edit Delete First Prevous 1 Next Last Showing Tree Discovery DHCP Multicast Routing Routing Security 	✓ Port	Protocol Group Table			
 VAN Voice VLAN Protocol VLAN Protocol VLAN Protocol VLAN O results found. Add Edit Delete Add Edit Delete Add Edit Delete Add Edit Delete 	✓ VLAN	Showing All v entries		Showing 0 to 0 of 0 entries	0
Voice VLAN Protocol VLAN Group Binding Group Binding MAC VLAN WAC VLAN Surveiliance VLAN Oresults found. First Previous 1 Next Last Delete Oresults found. First Previous 1 Next Last Set of the first Previous 1 Next Last Oresults found. First Previous 1 Next Last Oresults found. First Previous 1 Next Last Oresults found. First Previous 1 Next Last Set of the first Previous 1 Next Last Set of the first Previous 1 Next Last Oresults found. First Previous 1 Next Last First Previous 1 Next Last Oresults found. First Previous 1 Next Last Set of the f	VLAN				8
Protocol VCAN Protocol Croup Group Binding MAC VLAN Surveinare VLAN GVRP MAC Address Table Spanning Tree DHCP Multicast V Routing Security	✓ Voice VLAN	Group ID Frame Type	Protocol Value		
Protocol Group Group Binding V MAC VLAN Surveillance VLAN V Surveillance VLAN V SAC Address Table Spanning Tree Discovery OHCP V Routings V Routing V Scuting	A Protocol VLAN			0 results found.	
 MAC VEAN Surveilance VLAN GSVRP MAC Address Table Spanning Tree Discovery DHCP Multicast Multicast Seruntly Seruntly 	Protocol Group Group Binding	Add Edit	Delete		(First) (Previous) 1 (Next) (Last)
 GVRP GVRP Spanning Tree Spanning Tree Discovery OHCP Mulicast Routing Security 					
 MAC Address Table Spanning Tree Discovery OHOP Multcast Routing Security 	✓ GVRP				
 Spanning Tree Discovery DHCP Multicast Routing Security 	 MAC Address Table 				
 Discovery DHCP Multicast Routing Security 	 Spanning Tree 				
 DHCP Multicast Routing Security 	✓ Discovery				
 Multicast Routing Security Y 	✓ DHCP				
V Routing	✓ Multicast				
× Security ×	✓ Routing				
	✓ Security	~			

Fig 5.3.1 Default Protocol VLAN Protocol Group Table page

COMMANDO	ve Logout	Reboot	Debu
VLAN » Protocol VLAN » Protocol Group			
✓ Status			
V Network			
Y Port Add Protocol Group			
VIAN			
 VLAN Voice VLAN Protocol VLAN Protocol Group Group Binding MAC VLAN Sturveillance VLAN Sturveillance VLAN Apply Close 			
V MAC Address Table			
✓ Spanning Tree			
✓ Discovery			
✓ DHCP			
✓ Multicast			
✓ Routing ✓ Security			

Fig 5.3.2 Add Protocol group page

COMMANDO	Save Logout R	eboot Debug
Status Network Port	Add Protocol Group	^
VLAN VLAN Voice VLAN Voice VLAN Protocol VLAN Group Binding MAC VLAN Surveillance VLAN GVRP	Group ID 4 Frame Type IEEE802.3_LLC_Other Protocol Value 0x 8001 0x 8001 (0x600 - 0xFFFE)	
MAC Address Table Spanning Tree Discovery DHCP Multicast Routing Security		v

Fig 5.3.3 Protocol Group Table page

COMMANDO VLAN » Protocol VLAN » Protocol Group	Save Logout Reboot Debug
✓ Status	
v Network	
v Port	
▼ VLAN Showing All ✓ entries Showing 1 to 1 of 1 entries	0
▼ VLAN	~
Voice VLAN Group ID Frame Type Protocol Value	
Protocol VLAN 4 IEEE802.3_LLC_Other 0x8001	
Protocol Group Craus Rinding Add Edit Delete	First Previous 1 Next Last
✓ Surveillance VLAN	
✓ GVRP	
V MAC Address Table	
✓ Spanning Tree	
V Discovery	
V DHCP	
✓ Multicast	
✓ Routing	
✓ Sequifity	

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.

COMMANDO		N.G. D. P.	Save Logout Reboot Debug
	VLAN # Protocol VLAN	W Group Binding	
✓ Status			
✓ Network	Group Binding Table		
✓ Port	Group Binding Table		
▼ VLAN	Showing All 🗸 entries	Showing 0 to 0 of 0 entries	0
VLAN			8
✓ Voice VLAN	Port Group ID VLAN		
▲ Protocol VLAN		0 results found.	
Protocol Group		Delete	First Previous 1 Next Last
	Add Edit	Delete	
✓ MAC VLAN ✓ Supveillance VLAN			
 ✓ GVRP 			
 MAC Address Table 			
✓ Spanning Tree			
✓ Discovery			
V DHCP			
✓ Multicast			
✓ Routing			
✓ Security			

Fig 5.3.5 Default Group Binding Table page

	AN & Proto	Save Logout Reboot I	Debug
✓ Status	Add Come Dindice	Corversity of the billing	^
V Network	Add Group Binding		^
✓ Port			
▼ VLAN		Available Port Selected Port	
VLAN Voice VLAN Protocol VLAN Protocol VLAN Group Binding MAC VLAN VSurveilance VLAN VGVRP	Port	Note: Only VLAN Hybrid port can be set Protocol VLAN	h
 MAC Address Table 	Group ID	4 -	
✓ Spanning Tree			
✓ Discovery	VLAN	(1 - 4094)	
✓ DHCP	L		
✓ Multicast	Apply	Close	
✓ Routing			~
✓ Security			~

Fig 5.3.5 Add Group Binding page

COMMANDO			
		Save Logout Reboot	Debug
V	LAN » Protocol	VLAN » Group Binding	
✓ Status ^	Add Group Binding		· ^
✓ Network			
✓ Port	·		
▼ VLAN	Ava	lable Port Selected Port	
VLAN Voice VLAN Protocol VLAN Protocol VLAN Group Binding MAC VLAN Surveillance VLAN GVRP	Port	Concept of the set Protocol VLAM	h
 MAC Address Table 	Group ID 4		
 Spanning Tree 			
✓ Discovery	VLAN	(1 - 4094)	
✓ DHCP			
✓ Multicast	Apply Cl	bse	
✓ Routing			
✓ Security			×

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.

COMMANDO	VLAN » MAC VLAN » I	ИАС Group	Save Logout Reboot Debug
✓ Status ^			
✓ Network			
✓ Port	MAC Group Table		
▼ VLAN	Showing All v entries	Showing 0 to 0 of 0 entries	0
VLAN		-	Q.
✓ Voice VLAN	Group ID MAC Address	Mask	
 Protocol VLAN 		0 results found	d.
A MAC VLAN			First Previous 1 Next Last
MAC Group	Add Edit	Delete	
Group Binding			
 ✓ GVRP 			
V MAC Address Table			
✓ Spanning Tree			
✓ Discovery			
✓ DHCP			
✓ Multicast			
✓ Routing			
✓ Security			

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".



CUMIMANUU			Save	Logout	Reboot	Debug
_	VLAN » MAC VLAN » MAC Group					
✓ Status			-			
✓ Network						
✓ Port	Add MAC Group					
▼ VLAN						
✓ VLAN ✓ Voice VLAN	Group ID 2	(1 - 2147483647)				
 Protocol VLAN 	MAC Address 1C:2D:FD:A3:AD:A3					
 MAC VLAN MAC Group Group Binding 	Mask 24	9 - 48)				
 Surveillance VLAN GVRP 	Apply Close					
 MAC Address Table 						
 Spanning Tree 						
 Discovery 						
✓ DHCP						
✓ Multicast						
✓ Routing						
✓ Security	, .					

Fig 5.4.2 Add MAC Group ID page

COMMANDO	/LAN » MAC VLAN » MAC Group	Save Logout Reboot Debug
✓ Status ^		
V Network	MAC Group Table	
✓ Port	MAC Group Table	
▼ VLAN	Showing All v entries Showing 1 to 2 of 2 entries	0
VLAN		~
Voice VLAN	Group ID MAC Address Mask	
 Protocol VLAN 	1 1A:D3:4A:3A:35:95 24	
	2 1C:2D:FD:A3:AD:A3 24	
Group Binding		(First) (Previous) (1) (Next) (Last)
Surveillance VI AN	Add Edit Delete	
 ✓ GVRP 		
 MAC Address Table 		
 Spanning Tree 		
✓ Discovery		
✓ DHCP		
✓ Multicast		
✓ Routing		
✓ Security		

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).

COMMANDO			Save Logout Reboot Debug
V	/LAN » MAC VLAN » (Group Binding	
✓ Status			
✓ Network			
✓ Port	Group Binding Table		
▼ VLAN	Showing All v entries	Showing 0 to 0 of 0 entries	0
V VLAN		-	4
✓ Voice VLAN	Port Group ID VLAN		
 Protocol VLAN 		0 results found.	
MAC VLAN MAC Group Group Binding Surveillance VLAN GVRP	Add Edit	Delete	First Previous 1 Next Last
 MAC Address Table 			
✓ Spanning Tree			
✓ Discovery			
✓ DHCP			
✓ Multicast			
✓ Routing			
✓ Security			

Fig 5.4.5 Blank Group binding table page

COMMANDO			Save	Logout	Reboot	Debu	ıg
VLA	N » MAC	VLAN » Group Binding					
✓ Status ^ Add	l Group Binding					^	^
✓ Network							
✓ Port			1			1.1	
VLAN		Available Port Selected Port					
	Port						
✓ GVRP		Note: Only VLAN Hybrid port can be set MAC VLAN					
✓ MAC Address Table	Group ID	1 -					
✓ Spanning Tree	•••••••						
✓ Discovery	VLAN	(1 - 4094)					
✓ DHCP							
✓ Multicast	Apply	Close					
✓ Routing							
✓ Security						*	×

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.

COMMANDD Save Lorent Rebect Del	
Save Logout Reboot Det	Jug
VLAN » Surveillance VLAN » Property	
✓ Status ^	^
V Network	
V Port	
VLAN VLAN None V	
VLAN Voice VLAN Protocol VLAN Protocol VLAN	ł
V MAC VLAN Aging Time 1440 Min (30 - 65536, default 1440)	
A Surveillance VLAN	
Property Apply Apply	
✓ MAC Address Table Port Setting Table	
✓ Spanning Tree	
V Discovery	
V DHCP	1
V Multicast	
Routing CE: Disabled Auto Video Packet	
✓ Security 3 GE3 Disabled Auto Video Packet	~

Fig 5.5.1 Surveillance VLAN Property page

Surveillance VLAN Configuration:

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

Configuration object and description:

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

COMMANDO VLAN » Survei	lance VLAN » Property	Save Logout	: Reboot Debug
✓ Status ^			,
V Network State	Enable		
V Port	V// AN(0000		
VLAN VLAN			
✓ VLAN CoS / 802.1p	Enable		
Voice VLAN Remarking	7 🗸		
Aging Time	Min (30 - 65536, delauli 1440)		
Property			
Surveillance OUI			
✓ GVRP			
MAC Address Table Port Setting Table	le		
✓ Spanning Tree			
✓ Discovery		Q	
✓ DHCP Entry Port	State Mode QoS Policy		
✓ Multicast I GE1	Disabled Auto Video Packet		
✓ Routing ✓ 2 ✓ 2	Disabled Auto Video Packet		
✓ Security	Disabled Auto Video Packet		

Fig 5.5.2 Surveillance VLAN port setting page for selected GE2 port

COMMANDO	N » Surveillance VLAN » Property	Save	Logout	Reboot	Debug
Status Network Port Edi	Port Setting				^
VLAN VLAN Voice VLAN Voice VLAN Protocol VLAN MAC VLAN MAC VLAN Surveillance VLAN Property Surveillance OUI VGVRP	Port GE2 State □ Enable Mode ● Auto Manual ● QoS Policy ● Video Packet				
V MAC Address Table V Spanning Tree V Discovery V DHCP Multicast V Routing V Constitution	Apply Close				1
					¥

Fig 5.5.3 Surveillance VLAN Edit port setting for GE2 port page

COMMANDO								Save Logout Reboot	Debug
× Status	VLAN » S	urveill	ance VLAN	N » Pro	operty				^
V Network		· · · · · · · · · · · · · · · · · · ·					1		
✓ Port		State	Enable Enable						
- VLAN		VLAN	VLAN0002 🗸						
VLAN Voice VLAN Vrotocol VLAN MAC VLAN Surveillance VLAN Property Surveillance OI II	CoS / 802.1p ☑ Enable Remarking 7 ☑ Aging Time 1000 Min (30 - 65536, default 1440)								
✓ GVRP		_							
 MAC Address Table 	Port Setti	ng Tabl	P						
 Spanning Tree 		ing inibi	•						
 Discovery 								0	
✓ DHCP			C (1)		0.00.			-	_
✓ Multicast		y Port	State	Mode	QoS Policy				
✓ Routing		1 GE1	Disabled	Auto	Video Packet				
✓ Security		Z GE2	Enabled	Auto	Video Packet				
✓ ACL		3 GE3	Disabled	Auto	Video Packet				
✓ Q0S		4 GE4	Disabled	Auto	Video Packet				
 Diagnostics 		5 GE5	Disabled	Auto	Video Packet				×

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.

COMMANDO			Save L	.ogout Reboot	Debug
	VLAN » Surveillance VLAN	N » Surveillance OUI			
✓ Status ^					
V Network					
✓ Port	Surveillance OUI Table				
▼ VLAN	Showing All v entries	Showing 0 to 0 of 0 entries		0	
VLAN				G I	_
Voice VLAN	OUI Description				
V Protocol VLAN		0 results found.			
 Nuxe VLAN Property Surveillance OUI GVRP 	Add Edit [Delete		First Previous 1	Next Last
 MAC Address Table 					
✓ Spanning Tree					
✓ Discovery					
✓ DHCP					
✓ Multicast					
✓ Routing					
✓ Security					
✓ ACL					
∨ QoS					
✓ Diagnostics					

Fig 5.5.5 Surveillance OUI Table page

COMMANDO		Save Legent P	shoot Dahur
		Save Logout Ro	eboot Debug
	VLAN » Surveillance VLAN » Surveillance OUI		
✓ Status ^			^
V Network			
✓ Port	Add Surveillance OUI		
- VLAN			
 ✓ VLAN ✓ Voice VLAN ✓ Protocol VLAN ✓ MAC M AN 	OUI AA : BB : CC Description COMMANDO OUI		
Surveillance VLAN Property Surveillance OUI GVRP	Apply Close		
 MAC Address Table 			
 Spanning Tree 			
 Discovery 			
✓ DHCP			
✓ Multicast			
✓ Routing			
✓ Security			
V ACL			
∨ QoS			
✓ Diagnostics			×

Fig 5.5.6 Add Surveillance OUI page

COMMANDO	VI AN W Supplitunes VI AN V		Save Logout Reboot Debug
✓ Status ✓ Network	Surveillance OUI Table		
✓ Port ✓ VLAN ✓ VLAN ✓ VLAN ✓ Voice VLAN	Showing All ventries	Showing 1 to 1 of 1 entries	٩
Protocol VLAN MAC VLAN Surveillance VLAN Property	AA:BB:CC COMMANDO OUI	ete	(First) (Previous) 1 (Next) (Last)
Surveillance OUI			
 ✓ Spanning Tree 			
Discovery DHCP			
✓ Multicast			
✓ Routing			
✓ Security			
V ACL			
 ✓ Q05 ✓ Diagnostics 			

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.

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.

COMMANDO		Save Logout Reboot Debug
	VLAN » GVRP » Property	
✓ Status	A	~
✓ Network ✓ Port	State Enable	
VLAN	Operational Timeout	
✓ VLAN✓ Voice VLAN	Join 20 cs (2 - 16375, default 20)	
 Protocol VLAN 	Leave 60 cs (45 - 32760, default 60)	
 ✓ MAC VLAN ✓ Surveillance VLAN ▲ GVRP 	Leave All 1000 cs (65 - 32765, default 1000)	
Property Membership Statistics	Αρρίγ	
✓ MAC Address Table	Port Setting Table	
✓ Spanning Tree		
✓ Discovery		Q
✓ DHCP	Entry Port State VI AN Creation Registration	
✓ Multicast		
✓ Routing	2 GE2 Disabled Enabled Normal	
✓ Security	2 GE2 Disabled Enabled Normal	
✓ ACL	4 GE4 Disabled Enabled Normal	v

Fig 5.6.1 Default GVRP Property page

COMMANDO		Save Logout Reboot Debu	ıg
	VLAN » GVRP » Property		
✓ Status	^		^
V Network	State 🗹 Enable		
✓ Port			
✓ VLAN	Operational Timeout		
	Join 20 cs (2 - 16375, default 20)		
 Protocol VLAN 	Long 50 oc (45, 22750, default 50)		
V MAC VLAN			
✓ Surveillance VLAN	Leave All 1000 cs (65 - 32765, default 1000)		
A GVRP Property Membership Statistics	Apply		
✓ MAC Address Table	Port Setting Table		
✓ Spanning Tree			
✓ Discovery		Q	
✓ DHCP	Entry Port State VI AN Creation Registration		
✓ Multicast	1 GE1 Disabled Enabled Normal		
✓ Routing	2 GE2 Disabled Enabled Normal		
✓ Security	3 GE3 Disabled Enabled Normal		
✓ ACL	↓ 4 GE4 Disabled Enabled Normal		~

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

COMMANDO	VLAN » GVRP »	Property	Save Logout	Reboot Debi	ıg
✓ Status ^					^
✓ Network					
✓ Port	Edit Port Setting				
▼ VLAN					
VLAN	Port	GE2-GE3			
✓ Voice VLAN	State				
✓ Protocol VLAN	Jule				
✓ MAC VLAN	VLAN Creation	Enable			
✓ Surveillance VLAN		Normal			
A GVRP	Registration	⊖ Fixed			
Nomborchin		O Forbidden			
Statistics					
 MAC Address Table 	Apply Clo	ose			
✓ Spanning Tree					
 Discovery 					
V DHCP					
✓ Multicast					
✓ Routing					
× .					Y

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

COMMANDO VLAN » G	VRP »	Property	,			Save Logout R	eboot Debug
✓ Status ∧							^
V Network	to 🛛 F	nable					
∨ Port					i		
✓ VLAN Operation	al Timeo	ut					
VLAN	in 20		or (2 16	375. dofault 20)			
✓ Voice VLAN			05 (2 - 10	575, delault 20)			
V Protocol VLAN Lea	/e 60		cs (45 - 3	2760, default 60)			
 ✓ Nince VLAN ✓ Surveillance VLAN 	1000		cs (65 - 3	2765 default 1000)			
∧ GVRP			00 (00 0		i		
Property Membership Statistics)						
V MAC Address Table Port Settin	g Table						
✓ Spanning Tree	-						
✓ Discovery						Q	
✓ DHCP	Port	State	VI AN Creation	Registration			
✓ Multicast	GE1	Disabled	Enabled	Normal			
✓ Routing	GE2	Enabled	Enabled	Normal			
✓ Security	CE3	Enabled	Enabled	Normal			
✓ ACL	CE4	Disabled	Enabled	Normal			
✓ QoS	0024	Disabled	Endbled	N			×

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.

COMMANDO	VLAN » GVRP » Members	hip	Save Logout Reboot Debug
✓ Status	<u>`</u>		
✓ Network	Membership Table		
✓ Port			
✓ VLAN	Showing All 🗸 entries	Showing 0 to 0 of 0 entries	Q
∧ VLAN	VIAN Nomber Dynamic Nomber	Tuna	
VI AN Configuration	VLAN Member Dynamic Member	0 statute found	
Membership		o results lound.	
Port Setting			First Previous 1 Next Last
Voice VLAN			
 Protocol VLAN 			
V MAC VLAN			
 Surveillance VLAN GVRP 			
Property			
Membership			
Statistics			
 MAC Address Table 			
 Spanning Tree 			
 Discovery 			
V DHCP			
✓ Multicast			
✓ Routing			
✓ Security			
V ACL	/		

Fig 5.6.5 GVRP Membership Default page

	VLAN » GVRP » Membership							
 Status 								
 Network 	Membe	ership Table						
 Port 								
VLAN	Showing A	II 🗸 entries		8	nowing 1 to 1 of 1 entries	Q		
V VLAN	VLAN	Member	Dynamic Member	Type				
Voice VLAN	1	GE1-GE25.GE28.LAG1-LAG8		Static				
Protocol VLAN MAC MARK	-					First Previous 1 Next Last		
 Surveillance VLAN 								
∧ GVRP								
Property								
Membership								
Statistics								

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.

COMMANDO	AN W CVDD W Statistics	
Y	CALV " GVKF " Statistics	
✓ Status ^		
✓ Network	Dert CE1	
✓ Port		
▼ VLAN	All	
∧ VLAN	Statistics O Receive	
Create VLAN	O Transmit	
VLAN Configuration		
Membership	○ None	
Port Setting	Refresh Rate	
Voice VLAN	• 10 sec	
✓ Protocol VLAN		
✓ MAC VLAN		
✓ Surveillance VLAN	Clear	
∧ GVRP		
Property	Receive	
Membership	Join empty 0	
Statistics		
✓ MAC Address Table	Empty 0	
✓ Spanning Tree	Leave Empty 0	
✓ Discovery	loin In 🖞 0	
✓ DHCP		
✓ Multicast	Leave In 0	
✓ Routing	Leave All 0	

Fig 5.6.7 Default GVRP statistics page

	TAN N CUDD Y	N 64-42	41
×	LAN # GVRP #	State	tics
 Status 			
 Network 	Dest 1	054	
v Port	Port	GE1 V	
VLAN		GE1	
VLAN	Statistics	GE2	
Voice VLAN		014	n.
Protocol VLAN	2	GE3	
MAC VLAN		CE4	
 Surveillance VLAN 	Refresh Rate	GE4	
A GVRP	L	GE5	
Membershin)
Statistics	Clear	GE6	
MAC Address Table		GE7	
Spanning Tree	Receive		
Discovery	Join empty	GE8	
v Multicast	Empty	GE9	
v Routing	Lenus Empty		
Security	Leave Empty	GE10	
ACL	Join In	OE 11	
009	Leave In	GEII	
Diagonatics	Leave All	GE12	
- Mananamani		0540	
 Management 	Transmit	GE13	
	Join empty	GE14	***************************************
	Emoty		
	Empty :	GE15 +	1

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.

COMMANDO		
		Save Logout Reboot Debug
	MAC Address Table » Dynamic Address	
✓ Status		
✓ Network	[
✓ Port	Aging Time 300 Sec (10 - 630, default 300)	
VLAN		
 MAC Address Table 	Apply	
Dynamic Address		
Static Address	Dynamic Address Table	
Filtering Address		
Port Security Address	Showing All ventries Showing 1 to 1 of 1 entries	Q
✓ Spanning Tree	VIAN MAC Address Port	
 Discovery 		
✓ DHCP		
 Multicast 		First Previous 1 Next Last
 Routing 	Refresh Add Static Address	
✓ Security		
✓ ACL		
✓ Q₀S		
 Diagnostics 		
✓ Management		

Fig 6.1.1 Dynamic MAC address table page

COMMANDO	MAC Address Table » Dyna:	mic Address	Save Logout Reboot Debug
✓ Status			
V Network			1
✓ Port	Aging lime 300	Sec (10 - 630, default 300)	
VLAN			1
 MAC Address Table 	Apply		
Dynamic Address Static Address Filtering Address Port Security Address	Dynamic Address Table	Showing 1 to 1 of 1 entries	0
✓ Spanning Tree			8
✓ Discovery	VLAN MAC Address P	Port	
✓ DHCP	□ 1 28:D2:44:0A:7E:9C G)E1	
✓ Multicast			First Previous 1 Next Last
✓ Routing	Refresh Add Static Address		
✓ Security			
✓ ACL			
✓ Q₀S			
✓ Diagnostics			
✓ Management			

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. To configure and view the Static Address, click **MAC Address Table >> Static Address**.

COMMANDO			Save Logout Reboot Debug
	MAC Address Table » Static	Address	
✓ Status			
V Network			
✓ Port	Static Address Table		
VLAN	Showing All v entries	Showing 0 to 0 of 0 entries	0
 MAC Address Table 			4
Dynamic Address Static Address Filtering Address Port Security Address	VLAN MAC Address Port	0 results found. elete	(Fint) (Previous) 1 (Next) (Lext)
✓ Spanning Tree			
✓ Discovery			
✓ DHCP			
✓ Multicast			
✓ Routing			
✓ Security			
✓ ACL			
✓ Q₀S			
✓ Diagnostics			
✓ Management			

Fig 6.2.1 Default Static MAC address table default page

COMMANDO		Save	Logout	Reboot	Debug
	MAC Address Table » Static Address				
✓ Status					/
✓ Network					
✓ Port	Add Static Address				
V VLAN					
 MAC Address Table 	MAC Address 29:02:44:0A-7E-9C				
Dynamic Address Static Address Filtering Address Port Security Address	VLAN 1 (1 - 4094) Port GE1 V				
✓ Spanning Tree					
✓ Discovery	Apply Close				
✓ DHCP					
✓ Multicast					
✓ Routing					
✓ Security					
✓ ACL					
∨ QoS					
✓ Diagnostics					
∨ Management					

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

COMMANDO	MAC Address Table » Static	Address	Save Logout Reboot Debug
✓ Status			
✓ Network	Statia Address Table		
✓ Port	Static Address Table		
VLAN	Showing All 🗸 entries	Showing 1 to 1 of 1 entries	0
 MAC Address Table 			4
Dynamic Address	ULAN MAC Address P	Port	
Static Address	1 28:D2:44:0A:7E:9C G	GE1	
Filtering Address		2-1-4-	First Previous 1 Next Last
Port Security Address	Add Edit D	Jelete	
✓ Spanning Tree			
✓ Discovery			
✓ DHCP			
✓ Multicast			
✓ Routing			
✓ Security			
✓ ACL			
Y QoS			
✓ Diagnostics			
✓ Management			

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.

COMMANDO	MAC Address Table » Filter	ing Address	Save Logou	ıt Reboot Debug
✓ Status				
V Network	Filtering Address Table			
✓ Port	Filtering Address Table			
VLAN	Showing All v entries	Showing 0 to 0 of 0 entries	0	
 MAC Address Table 			G	
Dynamic Address Static Address Eiltering Address	VLAN MAC Address	0 results found	d.	
Port Security Address	Add Edit E	Delete	First	Previous 1 Next Last
 Spanning Tree 				
✓ Discovery				
✓ DHCP				
✓ Multicast				
✓ Routing				
✓ Security				
✓ ACL				
✓ Q₀S				
✓ Diagnostics				
✓ Management				

Fig 6.3.1 Filtering address table default page

COMMANDO	MAC Address Table » Filtering Address	Save Logout Reboot Debug
✓ Status		^
✓ Network		
✓ Port	Add Filtering Address	
VLAN		
✓ MAC Address Table	MAC Address 14-2B-CA-C5-D3-2A	
Dynamic Address Static Address Filtering Address Bett Seguritu Address	VLAN 1 (1 - 4094)	
 Spanning Tree 	Apply Close	
✓ Discovery		
✓ DHCP		
✓ Multicast		
✓ Routing		
✓ Security		
✓ ACL		
∨ QoS		
✓ Diagnostics		
✓ Management		

Fig 6.3.2 Add Filtering mac address to Specified VLAN page

	MAC Address Table W File		Save Logout Reboot Debug
	MAC Address Table " Fille	ring Address	
✓ Status			
V Network	Filtering Address Table		
✓ Port			
VLAN	Showing All 🗸 entries	Showing 1 to 1 of 1 entries	0
✓ MAC Address Table			~
Dynamic Address	VLAN MAC Address		
Static Address	1 1A:2B:C4:C5:D3:2A		
Filtering Address		Delete	First Previous 1 Next Last
Port Security Address		Delete	
V Spanning Tree			
V Discovery	4		
→ DHCP	4		
✓ Multicast	4		
✓ Routing	4		
✓ Security	4		
✓ ACL	4		
∨ QoS			
✓ Diagnostics			
✓ Management			

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.

COMMANDO	MAC Address Table » Port 5	Security Address	Save Logout Reboot Debug
✓ Status			
✓ Network	Dort Coourity Address Table		
✓ Port	Port Security Address Table		
VLAN	Showing All 🗸 entries	Showing 0 to 0 of 0 entries	0
 MAC Address Table 			4
Dynamic Address	ULAN MAC Address Type	Port	
Static Address		0 results found.	
Filtering Address Port Security Address	Add Edit [elete	First Previous 1 Next Last
✓ Spanning Tree			
✓ Discovery			
✓ DHCP			
✓ Multicast			
✓ Routing			
✓ Security			
∽ ACL			
✓ Q0S			
✓ Diagnostics			
✓ Management			

Fig 6.4.1 Port Security address table default page

COMMANDO MAC Address Table » Por	Security Address	Save	Logout	Reboot	Debug
✓ Status					^
V Network					
Port Add Port Security Address					
VLAN					
▼ MAC Address Table	η.εε.δα				
Dynamic Address Static Address VLAN 10 Filtering Address Port Security Address Port GE10 ✓	(1 - 4094)				1
✓ Spanning Tree					
Discovery Apply Close					
V DHCP					
✓ Multicast					
✓ Routing					
✓ Security					
✓ ACL					
✓ QoS					
✓ Diagnostics					
✓ Management					

Fig 6.4.2 Add Port Security MAC address page

COMMANDO	MAC Address Table » Port S	Security Addre	ss		Save Logout Reboot Deb
✓ Status					
∨ Network	Port Security Address Table				
✓ Port	For Security Address Table				
VLAN	Showing All 🗸 entries		Showing 1 to 1	1 of 1 entries	0
 MAC Address Table 					4
Dynamic Address	VLAN MAC Address	Туре	Port		
Static Address	10 AA:BB:CC:DD:EE:AA	SecureConfigured	GE10		
Filtering Address Port Security Address	Add Edit D	lelete			First Previous 1 (Next) Last
✓ Spanning Tree					
✓ Discovery					
✓ DHCP					
✓ Multicast					
✓ Routing					
✓ Security					
✓ ACL					
Y QoS					
✓ Diagnostics					
∨ Management					

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 .



Status

Spanning Tree » Property

v Network	State "		
✓ Port			
VLAN		STP	
 MAC Address Table 	Operation Mode	RSTP	
✓ Spanning Tree		MSTP	
Property			
Port Setting	Path Cost		
MST Instance MST Port Setting		Snort	i
Statistics		Filtering	
 Discovery 	BPDU Handling	Flooding	
V DHCP	L		
 Multicast 	Priority "	37768	(0 - 61440 default 32768)
✓ Routing			(0-01440, 00100, 02100)
✓ Security	Helio Time	2	Sec (1 - 10, default 2)
V ACL	Max Age	20	Sec (6 - 40. default 20)
~ Q0S			
Diagnostica	Forward Delay	15	Sec (4 - 30, default 15)
 Management 	Tx Hold Count	6	(1 - 10, default 6)
	iii		······
	Region Name	005040-00000	
	Revision	0	(0 - 65535, default 0)
	Max Hop	20	(1 - 40. default 20)
	Operational Status		
	Bridge identifiter	32768-00:E0:4C:00:00	:00
	Designated Root Bridge	32768-00:E0:4C:00:00	:00
	Root Port	N/A	
	Root Path Cost	0	
	Topology Change Count	4	
	Topology change Count		
	Last Topology Change	0D/0H/48M/2S	i
	And		
	Apply		

Fig 7.1.2 Default Spanning Tree property page

COMMANDO		Save Logout	Reboot Debug
✓ Status			<u> </u>
✓ Network			
✓ Port			
VLAN	Changing STP mode might cau	se the	
✓ MAC Address Table	connection interrupted.		
✓ Spanning Tree	Do you want to continue?		
Property			
Port Setting	OK Cancel		
MST Instance			
MST Port Setting			
Statistics		40, default 32768)	
✓ DHCP	Hello Time 2		
✓ Multicast			······

Fig 7.1.2 Change Spanning Tree mode property page

Spann	ning Tree » Propert	у	
✓ Status ✓ Network			
v Port	State :	Enable	
VIAN		(a) em	
MAC Address Table			
	Operation Mode		
 spanning free 		○ MSTP	
Property			
Port Setting	Path Cost		
MST Port Setting			
Statistics		Filtering	
 Discovery 	BPDU Handling	Elonding	
V DHCP	ä		
Multicast			
- Reutica	Priority	32768	(0 - 61440, default 32768)
V Routing			Cana (d. 10. destruction)
 Security 	Hello Time ;	P2	sec (1 - 10, default 2)
ACL	Max Arte "	20	Sec (5 - 40 default 20)
v QoS			
 Diagnostics 	Forward Delay	15	Sec (4 - 30, default 15)
 Management h== 			
	Tx Hold Count	6	(1 - 10, default 6)
	Pagion Name "	005040-00000	
i in	Region Name	002040.00000	
	Revision !!	0	(0 - 65535, default 0)
	Max Hop	20	(1 - 40, default 20)
L			
50	perational Status		
line line	Bridge identifiter	32768-00:E0:4C:00:0	0:00
	Designated Root Bridge	32768-00:E0:4C:00:00	0:00
i	Root Port	NA	
	Root Path Cost	0	
	Tonology Change Count in	2	
	reporting change count		
	Last Topology Change	0D/0H/1M/35S	
L			

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**.

COMMANDO															Save L	.ogout Reboot	Debug
	S	panni	ing Tr	ree »]	Port Setti	ng											
✓ Status	ľ																٨
✓ Network		D	o - 44	- T -14-													
∨ Port		РОП	Settin	g ladie													
Y VLAN															0		- 1
✓ MAC Address Table		_	_	,	,										4		_
 Spanning Tree 			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	Ц
Property			1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-00:E0:4C:00:00:00	128-1	20000	
Port Setting	L		2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000	
MST Instance	L		3	GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000	
Statistics	L		4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000	
✓ Discovery	L		5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000	
V DHCP	1		6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000	
✓ Multicast	1		7	GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000	
✓ Routing	1		8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000	
✓ Security	1		9	GE9	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000	
✓ ACL			10	GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000	
∨ QoS			11	GE11	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000	
✓ Diagnostiα			12	GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000	
✓ Management			13	GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000	
	I		14	GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000	11
	Ш		15	GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000	
	H		18	GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000	
	H		17	GE17	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000	
	H		18	GE18	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000	
	Ш		19	GE19	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000	
	H		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	
		Ī	24	GE24	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-24	20000	ч
																	Y

Fig 7.2.1 Spanning tree port setting page

COMMANDO	_														Save Log	out Reboot	Debu
	Sp	anni	ng Tr	ee » I	Port Setti	ıg											
Status Network		Dort (Cotting	Tabla													ľ
Port		PUIL	setung	Table													
/LAN															0		-
MAC Address Table	1.1														~		mil I
Spanning Tree		Щ	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	Ц.
Property		Ц	1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-00:E0:4C:00:00:00	128-1	20000	-11
MST Instance			2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000	
MST Port Setting			3	GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000	
Statistics			4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000	
iscovery			5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000	-
ICP		님	-	GEO	Enabled	20000	120	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-0	20000	- 11
ulticast	- 11			GE/	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000	- 11
uting	- 11	님	8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000	
curity		H	9	GES	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000	
<u>.</u>	- 11	님	10	GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000	
8	- 11	H	11	GETT	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00	128-11	20000	
agnostics	- 11	H	12	GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000	
anagement	11	Ц	13	GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000	
	11	Ц	14	GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000	- 1
	11	Ц	15	GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000	
	11	Ц	16	GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000	
	11	Ц	17	GE17	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000	
	11		18	GE18	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000	
		Ц.	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	
	Ш		24	GE24	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-24	20000	

Fig 7.2.2 Selecting port for Setting all Spanning Tree Parameters page



Fig 7.2.3 Setting ports for Spanning Tree Parameters page

COMMANDO

Save	Logout	Reboot	Debug
------	--------	--------	-------

	sh	ашшш	g m	ee // F	ort setu	шg											
✓ Status																	^
✓ Network	Ι,			T-1-1-													
∨ Port		ort S	etting	Table													
✓ VLAN															0		- 1
✓ MAC Address Table			_												ч		41
 Spanning Tree 			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	
Property			1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Designated	Forwarding	32768-00:E0:4C:00:00:00	128-1	20000	11
Port Setting			2	GE2	Enabled	1000	128	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	1000	11
MST Instance			3	GE3	Enabled	1000	128	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	1000	11
MST Port Setting Statistics			4	GE4	Enabled	1000	128	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	1000	11
			8	GE5	Enabled	1000	128	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	1000	11
V DHCP			6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000	11
✓ Multicast			7	GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000	11
✓ Routing			8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000	11
✓ Security			9	GE9	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000	11
Y ACL			10	GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000	11
√ QoS			11	GE11	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000	11
✓ Diagnostics			12	GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000	11
∨ Management			13	GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000	11
		Ē	14	GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000	15
		ō	15	GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000	
		Π	18	GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000	
		Π	17	GE17	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000	
		Ē	18	GE18	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000	
		Π	19	GE19	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000	
		ī	20	GE20	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000	
		Ē	21	GE21	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-21	20000	
		п	22	GE22	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-22	20000	
		Π	23	GE23	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-23	20000	
		п	24	GE24	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-24	20000	
		_															- Y

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).





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



	_										Save Logout Reboot L
	Sp	anni	ng Tre	e » M	ST Instance						
tus											
vork											
		NST	Instan	ice Tabl	e						
N											0
Address Table	1.1										ч
nning Tree			MSTI	Priority	Bridge Identifiter	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN	
operty		0	0	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	1-4094	
rt Setting		0	1	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
ST Instance		0	2	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
I Port Setting		0	3	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
		0	4	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
p		0	5	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
cast	11	0	6	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
ina	11	0	7	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
irity	11	Ō	8	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
	11	0	9	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
		0	10	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
nostics	11	õ	11	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
agement		0	12	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
	11	õ	13	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
		õ	14	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
	Ш	õ	15	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20		
		E	dit							-	

Fig 7.3.1 Fig 7.3.1 Spanning tree MST instance Table page

	Spann	ing Tr	ee » M	ST Instance					
✓ Status									
∨ Network									
✓ Port	MST	Insta	nce Tabl	e					
VLAN									
MAC Address Table	_								
 Spanning Tree 		MSTI	Priority	Bridge Identifiter	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
Property	0	0	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	1-4094
Port Setting	0	1	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
MST Instance	0	2	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
MST Port Setting Statistics	0	3	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
	0	4	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
	0	5	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
✓ Multicast	0	6	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
✓ Routing	0	7	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
✓ Security	0	8	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
V ACL	0	9	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
Y QoS	0	10	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
✓ Diagnostics	0	11	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
✓ Management	0	12	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
	0	13	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
	0	14	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
	0	15	32768	32768-00:E0:4C:00:00:00	32768-00:E0:4C:00:00:00	N/A	0	20	
		Edit]						

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**.

COMMANDO												Save	Logout Ret	ooot Debug
	Span	ning T	ree »	MST Por	t Settin	g								
✓ Status														^
✓ Network														
✓ Port	MS	ST Port	Setting	g Table										
VLAN	MST	ri 🛛 🗸												
 MAC Address Table 														
 Spanning Tree 	-												4	_
Property] Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Туре	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop	
Port Setting] 1	GE1	20000	128	Designated	Forwarding	STP	Boundary	32768-00:E0:4C:00:00:00	128-1	0	20	
MST Instance] 2	GE2	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-2	0	20	
MST Port Setting Statistics] 3	GE3	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-3	0	20	
] 4	GE4	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-4	0	20	
] 5	GE5	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-5	0	20	
✓ Multicast] 6	GE6	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-6	0	20	
× Routing] 7	GE7	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-7	0	20	
✓ Security] 8	GE8	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-8	0	20	
✓ ACL] 9	GE9	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-9	0	20	
✓ QoS] 10	GE10	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-10	0	20	
✓ Diagnostics] 11	GE11	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-11	0	20	
∨ Management] 12	GE12	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-12	0	20	
] 13	GE13	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-13	0	20	
] 14	GE14	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-14	0	20	
] 15	GE15	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-15	0	20	
] 16	GE16	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-16	0	20	· ·

Fig 7.4.1 Spanning tree MST port setting table page

MMANDO	õpanni	ing Ti	ree »	MST Por	t Setting	1						Save 1	Logout Reboo
		-											
	MSI	Port	Setting	j lable									
	MSTI	0 🗸	Ī										
		0	1										0
	_	1											4
		2	Port	Path Cost	Priority	Port Role	Port State	Mode	Туре	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
		2	GE1	20000	128	Designated	Forwarding	STP	Boundary	32768-00:E0:4C:00:00:00	128-1	0	20
		5	GE2	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-2	0	20
		4	GE3	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-3	0	20
		5	GE4	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-4	0	20
		6	GE5	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-5	0	20
		7	GE6	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-6	0	20
		8	CE7	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-7	0	20
		9	CER	20000	120	Disabled	Disabled	отр	Boundary	0.00:00:00:00:00:00	120-7	0	20
		10	GE8	20000	128	Disabled	Disabled	51P	Boundary	0-00.00.00.00.00.00	128-8	0	20
	12	11	GE9	20000	128	Disabled	Disabled	SIP	Boundary	0-00:00:00:00:00:00	128-9	0	20
		12	GE10	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-10	0	20
		13	GE11	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00	128-11	0	20
		14	GE12	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-12	0	20

Fig 7.4.2 Spanning tree MST Instant selection page

												Save	Logout Rel	boot
	Spann	ning T	ree »	MST Por	t Settin	g								
														_
			• ···											
	MS	ΓΡΟΠ	Setting	g lable										
	MSTI	4 ~	Ĩ											
dress Table			1											_
ng Tree	_			,									G I	_
rty		Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Туре	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop	
etting		1	GE1	20000	128	Designated	Forwarding	STP	Boundary	32768-00:E0:4C:00:00:00	128-1	0	20	
stance		2	GE2	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-2	0	20	
ice		3	GE3	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-3	0	20	
N.		4	GE4	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-4	0	20	
·)		5	GE5	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-5	0	20	
		6	GE6	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-6	0	20	
		7	GE7	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-7	0	20	
		8	GE8	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-8	0	20	
		9	GE9	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-9	0	20	
		10	GE10	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-10	0	20	
ics		11	GE11	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-11	0	20	
ment		12	GE12	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-12	0	20	
		13	GE13	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-13	0	20	
		14	GE14	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-14	0	20	
		15	GE15	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-15	0	20	
		16	GE16	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-16	0	20	

Fig 7.4.3 Spanning tree MST port selection page

COMMANDO	Spanning Tree » MST	Γ Port Setting	
✓ Status			
✓ Network			
✓ Port	Edit MST Port Setting		
VLAN			
 MAC Address Table 	MSTI	4	
 Spanning Tree 	Dort	CE6-CE7	
Property Port Setting MST Instance MST Port Setting Statistics	Path Cost Priority	100 96 🗸	(0 - 20000000) (0 = Auto)
✓ Discovery		r	
✓ DHCP	Port Role	Disabled	
✓ Multicast	Port State	Disabled	
✓ Routing	Mode	STP	
✓ Security	Tuno	Poundon	
✓ ACL	туре	Boundary	
∨ QoS	Designated Bridge	0-00:00:00:00:00:00	
 Diagnostics 	Designated Port ID	128-6	
✓ Management	Designated Cost	20000	
	Remaining Hop Apply Close	20	

Fig 7.4.4 Edit MST port setting for selected port page



Status
 Network
 Port
 VLAN
 MAC Address
 Spanning Tree

Property Port Setting MST Instant MST Port S Statistics

												Save	Logout Rebo	ot Debug
	Span	ning T	ree »	MST Por	t Settin	g								
														^
	MS	T Port	Settin	g Table										
	MST	4 ~	Ī											
able													Q	
		Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Туре	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop	
		1	GE1	20000	128	Designated	Forwarding	STP	Boundary	32768-00:E0:4C:00:00:00	128-1	0	20	
		2	GE2	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-2	0	20	- 11
tting		3	GE3	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-3	0	20	- 11
		4	GE4	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00	128-4	0	20	- 11
		5	GE5	1000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-5	0	20	
		6	GE6	20000	96	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-6	٥	20	
		7	GE7	20000	96	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-7	0	20	
		8	GE8	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-8	0	20	
		9	GE9	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00	128-9	0	20	
		10	GE10	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00	128-10	0	20	
		11	GE11	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-11	0	20	
		12	GE12	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00	128-12	0	20	
		13	GE13	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-13	0	20	
		14	GE14	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-14	0	20	
		15	GE15	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00	128-15	0	20	
		16	GE16	20000	128	Disabled	Disabled	STP	Boundary	0-00:00:00:00:00:00	128-16	0	20	v

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
```

COMMANDO	
	Spanning Tree » Statistics
✓ Status	
✓ Network	
✓ Port	STP Port Statistic
VLAN	
 MAC Address Table 	Port GE1
✓ Spanning Tree	
Property Port Setting MST Instance MST Port Setting	Refresh Rate 5 sec 0 10 sec 0 30 sec
Statistics	Receive BPDU
	Config 0
	Transmit PDDU
V ACL	Traising by Do
• wanagement	MSTP 1724
	Refresh Clear Close

Fig 7.5.2 Spanning tree Port Statistic page

Chapter 8 Discovery

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

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

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

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

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

Packet View : LLDP packet view information displayed.

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

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

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

8.1 LLDP

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

8.1.1 LLDP Property

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

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

COMMANDO					
				Save Logout Reb	oot Debug
Di	scovery » LLDP » Pro	perty			
✓ Status					^
✓ Network	LLDP				
∨ Port	State	🗸 Enable			
∨ VLAN	State				
 MAC Address Table 	LLDP Handling	Filtering Bridaina			
✓ Spanning Tree		 Flooding 			
▼ Discovery	TLV Advertise Interval	30	Sec (5 - 32767. default 30)		
∧ LLDP	L				
Property Dort Softing	Hold Multiplier	4	(2 - 10, default 4)		
MED Network Policy	Reinitializing Delay	2	Sec (1 - 10, default 2)		
MED Port Setting	Transmit Delay	2	Sec (1 - 8191, default 2)		
Packet View		F			
Neighbor	LLDP-MED				
Statistics	Ouisk Start Dansat Count	0	(4 40 dofault 0)		
V DHCP	QUICK START Repeat Count	P			
✓ Multicast	Apply				
✓ Routing	Арріў				v

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**

COMMANDO	Dis	SCOV	егу »	• LLD	op » p	ort Setting	Save Logout Reboot Deb
✓ Status	^						
✓ Network		Port	Cottin	a Tab	10		
✓ Port		FUIL	Setti	iy iab	IC		
VLAN							0
 MAC Address Table 		_					Q
 Spanning Tree 			Entry	Port	Mode	Selected TLV	
			1	GE1	Normal	802.1 PVID	
∧ LLDP			2	GE2	Normal	802.1 PVID	
Property			3	GE3	Normal	802.1 PVID	
Port Setting			4	GE4	Normal	802.1 PVID	
MED Network Policy			5	GE5	Normal	802.1 PVID	
MED Port Setting			6	GE6	Normal	802.1 PVID	
Local Information			7	GE7	Normal	802 1 PVID	
Neighbor			8	GE8	Normal	802 1 PV/D	
Statistics			0	GEO	Normal	802.1 PV/D	
V DHCP			10	GE9	Normal	002.1 PVID	
✓ Multicast			10	GE10	Normal	802.1 PVID	
✓ Routing			11	GE11	Normal	802.1 PVID	
	V I		12	GE12	Normal	802.1 PVID	

Fig 8.2.1 Default LLDP port setting table page

COMMANDO	Di	scov	ery »	LLI	op » p	ort Setting	Save Logout Reboot Debuş
✓ Status ^							
V Network		Port	Settir	ng Tab	le		
✓ Port			ocun	ig iub			
VLAN							0
 MAC Address Table 		_	_				~
 Spanning Tree 			Entry	Port	Mode	Selected TLV	
✓ Discovery			1	GE1	Normal	802.1 PVID	
∧ LLDP			2	GE2	Normal	802.1 PVID	
Property			3	GE3	Normal	802.1 PVID	
Port Setting			4	GE4	Normal	802.1 PVID	
MED Network Policy			5	GE5	Normal	802.1 PVID	
MED Port Setting Packet View			6	GE6	Normal	802.1 PVID	
Local Information			7	GE7	Normal	802.1 PVID	
Neighbor			8	GE8	Normal	802.1 PVID	
Statistics			9	GE9	Normal	802.1 PVID	
✓ DHCP			10	GE10	Normal	802 1 PV/D	
✓ Multicast			11	CE11	Normal	902.1 FVID	
✓ Routing			12	GE12	Normal	802.1 PVID	

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

COMMANDO		
		Save Logout Keboot Debug
	Discovery // LLDP // Port Setting	
✓ Status		^
✓ Network		
✓ Port	Erlit Port Setting	^
✓ VLAN		
✓ MAC Address Table		
✓ Spanning Tree	Port GE2-GE4	
 Discovery 	C Transmit	
∧ LLDP	Note Receive	
Property	O Normal	
Port Setting	Disable	
MED Network Policy		
MED Port Setting	Available TLV Selected TLV	
Packet View	Port Description	
Local Information	Optional TLV System Name System Capabilities	
Neighbor	802.3 MAC-PHY 802.1 PVID	
Statistics	802.3 Maximum Frame Size V	
✓ DHCP		
∨ Multicast	Available VLAN Selected VLAN	
✓ Routing		
✓ Security	802.1 VLAN Name	
✓ ACL	VLAN 10	
∨ QoS		
✓ Diagnostics		
∽ Management		
	Apply Close	¥

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

COMMANDO	D	isco	very »	LLD	P » Po	rt Setting	 Save	Logout	Reboot	Debu
✓ Status										
✓ Network		_								
∨ Port		Por	t Settii	ng Tab	le					
✓ VLAN										
✓ MAC Address Table		_					 	Q.		_
✓ Spanning Tree			Entry	Port	Mode	Selected TLV				
 Discovery 			1	GE1	Normal	802.1 PVID				
∧ LLDP			2	GE2	Receive	System Description , System Capabilities , 802.1 PVID , 802.1 VLAN Name				
Property			3	GE3	Receive	System Description , System Capabilities , 802.1 PVID , 802.1 VLAN Name				
Port Setting			4	GE4	Receive	System Description , System Capabilities , 802.1 PVID , 802.1 VLAN Name				
MED Network Policy			5	GE5	Normal	802.1 PVID				
Packet View			6	GE6	Normal	802.1 PVID				
Local Information			7	GE7	Normal	802.1 PVID				
Neighbor			8	GE8	Normal	802.1 PVID				- P
Statistics			9	GE9	Normal	802.1 PVID				
✓ DHCP			10	GE10	Normal	802.1 PVID				
✓ Multicast			11	GE11	Normal	802.1 PVID				
✓ Routing			12	GE12	Normal	802.1 PVID				
✓ Security			13	GE13	Normal	802 1 PVID				
∽ ACL			14	GE14	Normal	802.1 PVID				
∨ QoS		H	15	CE15	Normal	802.1 PVID				
✓ Diagnostics			16	GE15	Normal	802.1 PVID				
✓ Management			17	GE10	Normal	802.1 PVID				

Fig 8.2.4 LLDP port setting table after Editing page

8.3 MED Network Policy

Enables the advertisement and discovery of network 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**.

COMMANDO	Discovery » LLDP » MED	Network Policy	Save Logout Reboot Debug
✓ Status ✓ Network	MED Network Policy Table		
VLAN MAC Address Table	Showing All 🗸 entries	Showing 0 to 0 of 0 entries	Q
 ✓ Spanning Tree ✓ Discovery 	Policy ID Application VLA	N VLAN Tag Priority DSCP 0 results found.	
∧ LLDP Property Port Setting	Add Edit	Delete	(First) (Previous) (1) (Next) (Last)
MED Network Policy MED Port Setting			
Packet view Local Information Neighbor			
Statistics			
 ✓ Britci ✓ Multicast 			
✓ Routing			
✓ Security			
✓ ACL			
~ QoS			
 ✓ Diagnostics ✓ Management 			

Fig 8.3.1 LLDP MED Network Policy page

COMMANDO	Discovery » LLD	P »	M	ED Network Policy
✓ Status				
✓ Network				
✓ Port	Add MED Network Poli	су		
VLAN				
 MAC Address Table 				
 Spanning Tree 	Policy ID	1	<u> </u>	
	Application	1		
 LLDP Property Port Setting MED Network Policy MED Port Setting Packet View Local Information Neighbor Statistics DHCP Multicast Routing 	VLAN VLAN Tag Priority DSCP	2 3 4 5 6 7 8 9 10 11 12		Range (0 - 4095) ed jged
✓ Security		13		
× ACI		44		

Fig 8.3.2 LLDP MED Network Policy ID page

COMMANDO	Discovery » LLDI	Save Logout Reboot] P » MED Network Policy	Debug
✓ Status ^			^
✓ Network			Ĩ.
✓ Port	Add MED Network Policy	1	
VLAN			
 MAC Address Table 	Policy ID	4	
✓ Spanning Tree			
✓ Discovery	Application	Video Conferencing v	1
∧ LLDP	VLAN	1 Range (0 - 4095)	
Port Setting MED Network Policy	VLAN Tag	○ Tagged ● Untagged	
MED Port Setting	Priority	7 -	
Packet View	DAOD	20	
Local Information	DSCP		
Neighbor			
Statistics	Apply C	lose	
✓ DHCP			¥

Fig 8.3.3 LLDP Add MED Network Policy page

COMMANDO				Save Logout Reboot Debug
	Discovery » LLDP » MED	Network Policy		
✓ Status ^				^
✓ Network				
✓ Port	MED Network Policy Table			
VLAN	Showing All 🗸 entries	Showing 1 to 1 of 1	entries	0
 MAC Address Table 				4
✓ Spanning Tree	Policy ID Application	VLAN VLAN Tag	Priority DSCP	
	4 Video Conferencin	g 1 Untagged	7 13	
∧ LLDP Property Dot Setting	Add Edit	First Previous 1 Next Last		
MED Network Policy				*

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**.

COMMANDO	D	iscov	very ») LLD	op » Mi	ED Poi	rt Setting			Save	Logo	ut	Reboot	Debu
✓ Status	^													
✓ Network	ι.													
✓ Port	ι.	ME) Port	Setting	g Table									
VLAN	ι.										0	_		
✓ MAC Address Table	н.	_								 	ч			_
✓ Spanning Tree			Entry	Port	State	Netw	ork Policy	Location	Inventory					
✓ Discovery					outo	Active	Application	Looudon	lintentory					
∧ LLDP			1	GE1	Enabled	Yes		No	No					
Property			2	GE2	Enabled	Yes		No	No					
Port Setting			3	GE3	Enabled	Yes		No	No					
MED Network Policy	11		4	GE4	Enabled	Yes		No	No					
Packet View			5	GE5	Enabled	Yes		No	No					
Local Information			6	GE6	Enabled	Yes		No	No					
Neighbor			7	GE7	Enabled	Yes		No	No					_
Statistics			8	GE8	Enabled	Yes		No	No					_
✓ DHCP	~		0	GE0	Enabled	Voc		No	No					

Fig 8.4.1 LLDP MED port setting table page

COMMANDO	Disco	very »		Р≫ МІ	ED Poi	•t Setting			Save Logout Reboot Del	ug
✓ Status										^
✓ Network										
✓ Port	ME	D Port	Setting	g Table						
VLAN										
✓ MAC Address Table	_								ų į	
✓ Spanning Tree		Entry	Port	State	Netw	ork Policy	Location	Inventory		
- Discovery		Lindy	1 on	otate	Active	Application	Location	inventory		
∧ LLDP		1	GE1	Enabled	Yes		No	No		
Property		2	GE2	Enabled	Yes		No	No		
Port Setting		3	GE3	Enabled	Yes		No	No		
MED Network Policy		4	GE4	Enabled	Yes		No	No		
Packet View		5	GE5	Enabled	Yes		No	No		
Local Information		6	GE6	Enabled	Yes		No	No		
Neighbor		7	GE7	Enabled	Yes		No	No		
Statistics		8	GE8	Enabled	Yes		No	No		
✓ DHCP ✓		0	GE0	Enabled	Voc		No	No		~

Fig 8.4.2 LLDP MED port setting for ports page

	Discovery » LLDP >	» MED Port Sett	ing				
✓ Status							
✓ Network	Edit MED Port Setting						
✓ Port							
VLAN	Port	GF2-GF6				7	
 MAC Address Table 							
 Spanning Tree 	State :	Enable					
- Discovery		Available TI V		Selected TLV			
 LLDP Property Port Setting MED Network Policy MED Port Setting 	Optional TLV	Location	~ > ~ <	Network Policy Inventory	^		
Packet View Local Information		Available Policy		Selected Policy			
Neighbor Statistics	Network policy		^ >	4 (Video Conferencin	g) ^		
→ DHCP							
✓ Multicast			<u> </u>		Y		
✓ Routing	,					,	
✓ Security	Location						
✓ ACL	Coordinate			(16 p	airs of hexaded	imal characters)	
✓ Q05	+						
	Civic			(6 - 1	too pairs of hex	adecimal characters)	
✓ Management	ECS ELIN			(10 -	25 pairs of hex	adecimal characters)	
	Apply Close	e					

Fig 8.4.3 Edit LLDP MED port setting for selected ports page

Status	Disco	overy ») LLD	P » MI	ED Port	Setting			Save Logout Reboot Di	eb
Network	ME		Setting	n Table						
Port		PUL	ocuni	Jane						
VLAN										
MAC Address Table			_							
Spanning Tree		Entry	Port	State	N	etwork Policy	Location	Inventory		
Discovery		Linuy		State	Active	Application	Location	inventory		
∧ LLDP		1	GE1	Enabled	Yes		No	No		
Property		2	GE2	Enabled	Yes	Video Conferencing	No	Yes		
Port Setting		3	GE3	Enabled	Yes	Video Conferencing	No	Yes		
MED Network Policy		4	GE4	Enabled	Yes	Video Conferencing	No	Yes		
Packet View		5	GE5	Enabled	Yes	Video Conferencing	No	Yes		
Local Information		6	GE6	Enabled	Yes	Video Conferencing	No	Yes		
Neighbor		7	GE7	Enabled	Yes		No	No		
Statistics		8	GE8	Enabled	Yes		No	No		
DHCP		0	GEO	Enabled	Vec		No	No		
Multicast		9	OE40	Enabled	Vee		No	No		
Routing		10	GE10	Enabled	res		NO	NO		
	V K									

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.**

COMMANDO	Disco	wery X	> LLI	DP » Packet	View		Save	Logout	Reboot	Debug
✓ Status ^										^
✓ Network		direct Mar								
✓ Port	Pac	CKET VIE	ew Tat	bie						
VLAN								0		_
 MAC Address Table 	-							ų		_
✓ Spanning Tree		Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status				_
✓ Discovery	0	1	GE1	38	1450	Not Overloading				- 11
∧ LLDP	0	2	GE2	162	1326	Not Overloading				- 11
Property	0	3	GE3	162	1326	Not Overloading				
Port Setting	0	4	GE4	162	1326	Not Overloading				
MED Network Policy	0	5	GE5	130	1358	Not Overloading				
Packet View	0	6	GE6	130	1358	Not Overloading				
Local Information	0	7	GE7	38	1450	Not Overloading				
Neighbor	0	8	GE8	38	1450	Not Overloading				
Statistics	0	9	GE9	38	1450	Not Overloading				
✓ DHCP	0	10	GE10	39	1449	Not Overloading				
✓ Multicast		11	GE11	30	1449	Not Overloading				
✓ Routing		10	00011	39	1449	Not Overloading				
×		12	GETZ	39	1449	Not Overloading				×



COMMANDO	Disco	overy »	> LLI	DP » Packet	View		Save Logout Reboot Debuş	g
✓ Network								
✓ Port	Pa	cket Vie	ew Tab	ole				
VLAN							0	
 MAC Address Table 	-			,			4	
 Spanning Tree 		Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status		
- Discovery	۲	1	GE1	38	1450	Not Overloading		
∧ LLDP	0	2	GE2	162	1326	Not Overloading		
Property	0	3	GE3	162	1326	Not Overloading		
Port Setting	0	4	GE4	162	1326	Not Overloading		
MED Network Policy	0	5	GE5	130	1358	Not Overloading		
Packet View	0	6	GE6	130	1358	Not Overloading		
Local Information	0	7	GE7	38	1450	Not Overloading		
Neighbor	0	8	GE8	38	1450	Not Overloading		
Statistics	0	9	GE9	38	1450	Not Overloading		
✓ DHCP	0	10	GE10	39	1449	Not Overloading		
✓ Multicast		11	GE11	30	1449	Not Overloading		
✓ Routing	0	12	GE12	39	1449	Not Overloading		~

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.

COMMANDO	Discov	ery »	LLDP	» Local In	formation				
✓ Status									
✓ Network	Devi								
✓ Port	Devi	ce sun	nmary						
VLAN									
 MAC Address Table 		Chas	sis ID Sut	NAC ad	MAC address				
 Spanning Tree 			Chass	is ID 00:E0:40	00:E0:4C:00:00:00				
 Discovery 			System N	ame Switch					
 LLDP Property Port Setting MED Network Policy 		Syste Supporte Enable	m Descri ed Capabi ed Capabi	ption RTL838 lities Bridge, I lities Bridge, I	RTL8382M Bridge, Router Bridge, Router				
MED Port Setting Packet View Local Information Neighbor Statistics	Port	P	ort ID Sut	otype Local					
✓ DHCP									
 Multicast 									
✓ Routing		Entry	Port	LLDP State	LLDP-MED State				
✓ Security	0	1	GE1	Normal	Enabled				
✓ ACL		2	GE2	Receive	Enabled				
✓ QoS	0	3	GE3	Receive	Enabled				
 Diagnostics 	Ö	4	GE4	Receive	Enabled				
✓ Management	Ŏ	5	GE5	Normal	Enabled				

Fig 8.6.1 LLDP Local Information device summary page

COMMANDO	Discov	ery »	LLDP	» Local In	formation					
✓ Status										
✓ Network	Davis	0								
✓ Port	Devi	ce sun	nmary							
VLAN	[
MAC Address Table	Chassis ID Subtype : MAC address									
✓ Spanning Tree	Chassis ID 00:E0:4C:00:000									
✓ Discovery			System N	lame Switch						
 LLDP Property Port Setting MED Network Policy MED Port Setting Packet View Local Information Neighbor 		Syste Supporte Enable P	m Descri ed Capabi ed Capabi ort ID Sub	ption RTL8382 lities Bridge, F lities Bridge, F btype Local	2M Router Router					
Statistics	Port	Status	Table							
✓ DHCP										
 Multicast 	_									
✓ Routing		Entry	Port	LLDP State	LLDP-MED State					
✓ Security		1	GE1	Normal	Enabled					
✓ ACL	0	2	GE2	Receive	Enabled					
✓ Q0S	0	3	GE3	Receive	Enabled					
 Diagnostics 	Õ	4	GE4	Receive	Enabled					
✓ Management	0	5	GE5	Normal	Enabled					

Fig 8.6.2 LLDP Local Information Selecting port GE1 page

COMMANDO	
	Discovery » LLDP » Local Information
✓ Status	
✓ Network	
✓ Port	Local Information Detail
VLAN	
 MAC Address Table 	Chassis ID Subtype MAC address
 Spanning Tree 	
 Discovery 	Chassis ID 00.E0.4C.00.00.00
∧ LLDP	System Name Switch
Property	System Description RTL8382M
Port Setting	Sunnorfed Canabilities Bridge Router
MED Network Policy	
MED Port Setting	Enabled Capabilities Bridge, Router
Packet View	Port ID GE1
Local Information	Dort ID Subtyne Local
Neignbor Statiation	
	Port Description
V Multicast	
	Management Address Table
Routing	Address Subtype Address Interface Subtype Interface Number
✓ Security	0 results found.
✓ ACL	
✓ QoS	MAC/PHY Detail
 Diagnostics 	Auto Negatiation Supported N/A
✓ Management	

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**.

COMMANDO	Discovery » LLDP » Neighbo	or				Save Logo	out Reboot	Debuş
✓ Status								
✓ Network	Naishbas Tabla							
✓ Port	Neighbor lable							
VLAN	Showing All v entries	Showi	ing 0 to 0 of 0 entries				0	
 MAC Address Table 							4	
✓ Spanning Tree	Local Port Chassis ID Subtype	Chassis ID Port ID Subtype	Port ID System Name	Port Description	System Capabilities	Management IP Address	Time to Live	
 Discovery 			0 results	found.				
LLDP Property Port Setting MED Network Policy MED Port Setting Packet View Local Information Neighbor Statistics	Clear Refresh Det	ail				Frat	Previous 1 Ne	ext) (Last)
V DHCP								
✓ Multicast								
✓ Routing								
✓ Security								
✓ ACL								
√ QoS								
 Diagnostics 								
- Monogomont								

Fig 8.7.1 LLDP Neighbors table default page

	Discovery » LLDP » Neighbor	
✓ Port ▲ Link Aggregation MAC Address Table	Neighbor Table	
 Network 	Showing All 🕶 entries Showing 1 to 2 of 2 entries	Q
v Port	C Lord Bert Charala D Subhura Charala D Bart D Subhura Bart D Surfam Nama Tima ta Liur	
 POE Setting 	Cocal Port Chassis ID Subtype Chassis ID Port ID Subtype Port ID System Name Time to Live	
V VLAN	GE1 MAC address 00:E0:4C:00:00:0 Local gi1 102	
MAC Address Table	OE2 MAC address 00:E0:4C:00:00 Local g/2 102	
 Spanning Tree 		(Pint) (Previous) [1] (Next) (Last)
 Discovery 	Clear Refresh Detail	
LLDP Property Port Setting MED Network Policy MED Port Setting Packet View Local Information Neighbor Statistics		

Fig 8.7.2 LLDP Neighbors table after enabling LLDP page

	Discovery » LLDP » Neighbor							
Port Link Aggregation MAC Address Table	Neighbor Information Detail							
Network								
Port	Lacal Part - CE1							
POE Setting	Lucarport							
VLAN	Basic Detail							
MAC Address Table	Chassis ID Publics 100 address							
Spanning Tree	Chassis ID Subtype MAC abdress							
Discovery	Chassis ID 00:E0:4C:00:00							
LLDP	Port ID Subtype Local							
Property	Port ID gi1							
Port Setting	Dart Description							
MED Network Policy								
MED Port Setting	System Name							
Packet View Local Information	System Description							
Neighbor	Supported Capabilities N/A							
Statistics	Enabled Capabilities N/A							
Multicast								
Routing	Management Address Table							
Security	Address Subtype Address Interface Subtype Interface Number							
ACL	0 results found.							
QoS								
Diagnostics	MAC/PHY Detail							
Management	Auto Monotistian Cunnorted M/A							

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**.

✓ Status	Discov	very »	> LLD	P≫ Statistics	5						
✓ Network											
∨ Port	Global Statistics										
VLAN	[:										
✓ MAC Address Table		Insertio	ons 0								
✓ Spanning Tree		Deletio	ons 0								
 Discovery 		Dro	ps 0								
 LLDP Property Port Setting MED Network Policy MED Port Setting Packet View Local Information Neighbor Statistics 	Stat	AgeO Clear istics	uts 0 Ref	iresh							
✓ DHCP		Entry	Port	Transmit Frame	R	eceive Fran	ne	Re	ceive TLV	Neighbor	
V Multicast				Total	Total	Discard	Error	Discard	Unrecognized	Timeout	
v Roduny		1	GE1	309	0	0	0	0	0	0	
		2	GE2	0	0	0	0	0	0	0	
		3	GE3	0	0	0	0	0	0	0	
		4	GE4	0	0	0	0	0	0	0	
		5	GE5	0	0	0	0	0	0	0	

FIG 8.8.1 LLDP GIODAI STATISTICS PAGE	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**.

COMMANDO	DH	ICF	P≫ Pi	ropert	y		Save	Logout	Reboot	Debug
✓ Status ^		_	_							^
✓ Network		[itate 🗌 🛛 F	Enable				
✓ Port			04-4 ¹ - 5	• • • • • • • • • • • •						
VLAN		¦	Static E	inding	First 📋 L	Enable				
 MAC Address Table 				1						
✓ Spanning Tree	l	A	арріу	J						
✓ Discovery										
▼ DHCP		DHC	P Por	t Setti	ng Table					
Property IP Pool Setting								Q		
VLAN IF Address Group Setting			Entry	Port	State					
Client List Client Static Binding Table			1	GE1	Disabled					
			2	GE2	Disabled					
× Pouting			3	GE3	Disabled					
			4	GE4	Disabled					
			5	GE5	Disabled					
V ACL			6	GEG	Disabled					
Y Q05			0	GLU	Disabieu					

Fig 9.1.1 Default DHCP Property page

COMMANDO	DHC	P » P	ropert	y		Save	Logout	Reboot	Debug
✓ Status ^									^
✓ Network	1			tate 🛛	Enable				
✓ Port		04-4i- F							
VLAN	L.	Static E	sinaing i	·irst	Enable				
 MAC Address Table 		Ample							
 Spanning Tree 		Арріу	J						
✓ Discovery									
▼ DHCP	DH	CP Por	t Setti	ng Table					
Property IP Pool Setting							Q		
VLAN IF Address Group Setting		Entry	Port	State					
Client List Client Static Binding Table		1	GE1	Disabled					
		2	GE2	Disabled					
		3	GE3	Disabled					
× Security		4	GE4	Disabled					
		5	GE5	Disabled					
		6	GEG	Disabled					
▼ Q05		0	GLO	Disableu					

Fig 9.1.2 Enable DHCP Property page

COMMANDO	DHCF	>» Pro	operty			Save Logout Reboot D	ebug
✓ Status	-						1
✓ Network			Sta	te 🔽 Enal	hle.		
✓ Port		0					
✓ VLAN	l	Static Bil	nding Fir	st 📋 Enal	Die		
 MAC Address Table 		and a	_				
✓ Spanning Tree		крріу					
✓ Discovery							
▼ DHCP	DHC	P Port	Setting	g Table			
Property IP Pool Setting	_					Q	
Client List		Entry	Port	State			
Client Static Binding Table		1	GE1	Disabled			
✓ Multicast		2	GE2	Disabled			
✓ Routing		3	GE3	Disabled			
✓ Security		4	GE4	Disabled			
✓ ACL		5	GE5	Disabled			
∨ QoS		6	GE6	Disabled			
✓ Diagnostics		7	GE7	Disabled			
✓ Management		8	GE8	Disabled			
		9	GE9	Disabled			

Fig 9.1.3 Selecting ports on DHCP Property page

COMMANDO	ICP » Pro	operty	Save Logout Reboot Deb	ug
✓ Status ^				^
✓ Network				
✓ Port	Edit Port Settin]		
VLAN				
V MAC Address Table	Port	GE1-GE28,LAG1-LAG8		
✓ Spanning Tree	State	☑ Fnable		
✓ Discovery	L		i	
▼ DHCP	Apply	Close		
Property				
IP Pool Setting				
VLAN IF Address Group Setting				
Client List				
Client Static Binding Table				4
✓ Multicast				
✓ Routing				
× Security ×				

Fig 9.1.4 Edit ports setting DHCP Property page

COMMANDO	DH	łCP	» Pro	perty			Save	Logout	i Reboot	t Deb	ug
✓ Status ^		_									^
V Network				State	Enab	a					
✓ Port		·····	Statia Dia	alina Firm							
VLAN		·	statić Bin	aing Firs		le					
✓ MAC Address Table		٨	anlı								
✓ Spanning Tree		Αp	phiy								
V Discovery											
▼ DHCP		DHC	P Port	Setting	Table						
Property IP Pool Setting								Q			
VLAN IF Address Group Setting Client List			Entry	Port	State						
Client Static Binding Table			1	GE1	Enabled						
✓ Multicast			2	GE2	Enabled						
✓ Routing			3	GE3	Enabled						
✓ Security			4	GE4	Enabled						
V ACL			5	GE5	Enabled						
✓ QoS			6	GE6	Enabled						
< >			7	GE7	Enabled						v

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.

COMMANDO	онср	• » I	P Pool Settin	ıg					Save 1	Logout F	Reboot	Debug
✓ Status ^												
✓ Network			ablo									
✓ Port		001 10	able									
VLAN	Showin		✓ entries		Sh	owing 0 to 0 of (entries			0		
✓ MAC Address Table		-1 1								4		_
✓ Spanning Tree		Pool		Section		Gateway	Mask	DNS Primary Server	DNS Second Server	Lease time		
✓ Discovery			Section Star	t Address	End Address	cutenay	Mask	biter mility eerver		Leuse ame		
▼ DHCP							0 resu	Its found.				
Property IP Pool Setting VLAN IF Address Group Setting Client List Client Static Binding Table		Add	Edit	Dele	te					(First) (Previous	i 1 Ne	t Last
✓ Multicast												
✓ Routing												
✓ Security												
✓ ACL												
✓ Q0S												

Fig 9.2.1 Default DHCP IP Pool setting page

COMMANDO	CP » IP Pool Settin	g	
✓ Status			
✓ Network			
✓ Port	IP Pool Table		
VLAN			
✓ MAC Address Table		400.400.0.0	
✓ Spanning Tree	P001	192.166.0.0	(1 to 52 alphanumenc characters)
✓ Discovery	Gateway	192.168.0.1	
▼ DHCP		055 055 055 0	
Property	Маѕк	255.255.255.0	
IP Pool Setting		Section 1	
VLAN IF Address Group Setting			
Client List	IP Address Section	Start Address 192.168.	0.50
Client Static Binding Table		End Address 192.168.	0.100
✓ Multicast			
✓ Routing	DNS Primary Server	Enable 8.8.8.8	
✓ Security			
→ ACL	DNS Second Server		
✓ Q0S	Lease time	1 Day 00 - Hou	ur 00 🗸 Minute
✓ Diagnostics	L		
✓ Management	Apply Close		

Fig 9.2.2 Edit DHCP IP Pool setting page

COMMANDO	DHC	ср » IP Ро	ol Settin	ıg					Save	Logout	Reboot Debug
✓ Status											
✓ Network	IP	Pool Table									
✓ Port											
VLAN	Show	wing All 🗸 entr	ries		s	howing 1 to 1 of 1	entries			Q	
V MAC Address Table	-	1	Casting				1	- ,			
✓ Spanning Tree] Pool	Castlen	Section	Ford Address	Gateway	Mask	DNS Primary Server	DNS Second Server	Lease time	
✓ Discovery			Section	Start Address	End Address		055 055 055 0				L
▼ DHCP] 192.168.0.0	1	192.168.0.50	192.168.0.100	192.168.0.1	255.255.255.0	8.8.8.8	8.8.4.4	1: 0: 0	
Property IP Pool Setting VLAN IF Address Group Setting Client List Client Static Binding Table		Add	Edit	Delete						(First) (Prev	ious 1 Next Last
✓ Multicast											
✓ Routing											
✓ Security											
✓ ACL											
∨ QoS											
✓ Diagnostics											
✓ Management											

Fig 9.2.3 DHCP IP Pool Table after setting page

9.3 VLAN IF Address Group Setting

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

COMMANDO	
	DHCP // VLAN IF Address Group Setting
✓ Status	
V Network	
✓ Port	DHCP Server Group Table
VLAN	
✓ MAC Address Table	DHCP Server Group
✓ Spanning Tree	
✓ Discovery	Group IP Address 192.168.0.1
- DHCP	
Property IP Pool Setting VLAN IF Address Group Setting Client List Client Static Binding Table	Apply Close
✓ Multicast	
✓ Routing	
✓ Security	
V ACL	
V QoS	
✓ Diagnostics	
✓ Management	

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

COMMANDO	Save Logout Reboot Deb	ıg
✓ Status		
✓ Network	VI AN Interface Address Pool Table	
✓ Port		
VLAN		3
✓ MAC Address Table		4
✓ Spanning Tree	DHCP Server Group	
✓ Discovery		
▼ DHCP	Арру	
Property IP Pool Setting VLAN IF Address Group Setting Client List Client Static Binding Table	DHCP Server Group Table	
✓ Multicast	Group ID Group IP Address Bind VLAN Interface	1
✓ Routing	O 1 192.168.0.1 vlan 1	
✓ Security		
V ACL	Add Edit Delete	
✓ QoS		
✓ Diagnostics		
✓ Management		

Fig 9.3.2 DHCP Binding VIan 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.

Network Connection Details						
Network Connection Details:						
Property	Value	^				
Connection-specific DN						
Description	Intel(R) 82579LM Gigabit Network Cor					
Physical Address	28-D2-44-0A-7E-9C					
DHCP Enabled	Yes					
IPv4 Address	192.168.0.50					
IPv4 Subnet Mask	255.255.255.0					
Lease Obtained	Thursday, October 8, 2020 18:32:04					
Lease Expires	Friday, October 9, 2020 18:32:04					
IPv4 Default Gateway	192.168.0.1					
IPv4 DHCP Server	192.168.0.1					
IPv4 DNS Servers	8.8.8.8					
	8.8.4.4					
IPv4 WINS Server						
NetBIOS over Tcpip En	Yes					
Link-local IPv6 Address	fe80::8003:dca9:2897:9e22%4					
IPv6 Default Gateway		~				
<	>					
		_				
	Close					

Fig 9.4.1 DHCP Client list page.

COMMANDO	DHCP » Client Liet		Save Logout Reboot Debug
	Differ - Chent List		
✓ Status			
✓ Network	DHCP Client List		
✓ Port			
✓ VLAN	Showing All V entries	Showing 1 to 1 of 1 entries	0
✓ MAC Address Table			8
✓ Spanning Tree	MAC Address Table IPv4 Add	dress VLAN Hostname	
✓ Discovery	28:D2:44:0A:7E:9C 192.168.	.0.50 1 DESKTOP-CQ78BP7	
▼ DHCP			First Previous 1 Next Last
Property	Refresh		
IP Pool Setting			
VLAN IF Address Group Setting			
Client List Client Static Binding Table			
✓ Multicast			
✓ Routing			
✓ Security			
✓ ACL			
V QoS			
✓ Diagnostics			
✓ Management			

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.

COMMANDO	DHCP » Client Static Bind	ing Table		Save Lo	gout Reboot Debug
✓ Status					
V Network					
✓ Port	Static Binding Table				
VLAN	Showing All v entries	Showi	ng 0 to 0 of 0 entries	0	
V MAC Address Table					4
✓ Spanning Tree	MAC Address Table IPv4 A	ddress VLAN User Name			
 Discovery 			0 results found.		
▼ DHCP	Add Delete			Fin	at Previous 1 Next Last
Property	Add Delete				
IP Pool Setting					
VLAN IF Address Group Setting					
Client Static Binding Table					
✓ Multicast					
✓ Routing					
✓ Security					
V ACL					
✓ QoS					
✓ Diagnostics					
✓ Management					

Fig 9.5.1 Default DHCP Client Binding Table page.

COMMANDO	HCP » Client Si	atic Binding Table		Save Logout Reboot Debug
✓ Status				^
✓ Network				
✓ Port	Static Binding Table Add	1		
VLAN				
V MAC Address Table	MAC Address	AD-2E-AC-7E-0A-9C		
✓ Spanning Tree	MAC Address	AD.2E.A0.7E.3A.00		
V Discovery	VLAN	1	(1 - 4094)	
▼ DHCP	IPv4 Address	192 168 0 59		
Property	in the Address	102.100.0.00		
IP Pool Setting	User Name	COMMANDO PC	(1 - 32)	
VLAN IF Address Group Setting Client List				
Client Static Binding Table	Apply C	lose		
✓ Multicast				
✓ Routing				
✓ Security				
V ACL				
✓ QoS				
✓ Diagnostics				
✓ Management				
				Y

Fig 9.5.2 DHCP Client add static binding page.

COMMANDO	DHCP » Client Static Bindin	g Table		Save Logout Reboot Debug
✓ Status				
✓ Network	Static Binding Table			
✓ Port	otatic binang labie			
VLAN	Showing All v entries	Showing 1 to	1 of 1 entries	0
 MAC Address Table 				<u>ح</u>
✓ Spanning Tree	MAC Address Table IPv4 Ad	dress VLAN User Name		
✓ Discovery	AD:2E:A6:7E:9A:8C 192.168	0.59 1 COMMANDO PC		
▼ DHCP	Add Delete			First Previous 1 Next Last
Property	Add Delete			
IP Pool Setting				
VLAN IF Address Group Setting				
Client List				
Client Static binding Table				
Multicast				
 Routing Security 				
✓ Security				
✓ ACL				
✓ Q6S				
✓ Diagnóstics				
✓ Management				

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 239.0.00 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 oneto-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**



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.

COMMANDO	Multicast » General » Group A	ddress	Save Logout Reboot Debug
✓ Status ^			
✓ Network	Course Addresse Table		
✓ Port	Group Address Table		
VLAN	IP Version IPv4 V		
 MAC Address Table 			
✓ Spanning Tree	Showing All 🗸 entries	Showing 0 to 0 of 0 entries	0
 Discovery 		Time 116 (0-c)	
V DHCP	U VLAN Group Address Member	Type Life (Sec)	
 Multicast 		U results found.	
Ceneral Property Group Address Router Port Forward All Throtiling Filtering Profile Filtering Binding VIGMP Snooping MVR Routing Security ACL QoS Diagnostics V	Add Edit Delete	Refresh	First Previous 1 Next Last

Fig 10.1.2 Multicast default group address table page

COMMANDO	Multicaset » Canaral » Crown Addrass	Save Logout Reboot Debug
	Multures of Octorial of Oroup Address	
✓ Status		^
✓ Network		
∨ Port	Add Group Address	
VLAN		
 MAC Address Table 	VLAN 2 V	
 Spanning Tree 		
 Discovery 	IP Version	
✓ DHCP	Group Address 239.0.0.4	
 Multicast 		
General Property Group Address Router Port Forward All Throttling Filtering Profile Filtering Pinding V IIGMP Snooping WI D Receipting	Available Port Selected Port GE1 GE2 GE4 GE5 GE6 GE7 GE8 C GE10 C	
✓ MLD Snooping	Apply Close	
× Routing		
v Security		
× ACI		
× 008		
✓ Diagnostics		v

Fig 10.1.3 Multicast add group address page

COMMANDO			Save Logout Reboot Debug
	Multicast » General » Group	Address	
✓ Status ∧			
✓ Network	Group Address Table		
∨ Port			
✓ VLAN	IP Version IPv4 🗸		
✓ MAC Address Table			
✓ Spanning Tree	Showing All 🗸 entries	Showing 1 to 1 of 1 entries	Q
✓ Discovery	VLAN Group Address Memb	er Type Life (Sec)	
✓ DHCP	2 239.0.0.4 GE2.GI	E5 Static	
▼ Multicast			First Previous 1 Next Last
∧ General	Add Edit Dele	te Refresh	
Group Address			
Router Port			
Forward All			
Throttling			
Filtering Profile			
Filtening Binding			
 MLD Snooping 			
∽ MVR			
✓ Routing			
✓ Security			
∨ ACL			
∨ QoS			
✓ Diagnostics ✓			

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.

COMMANDO		Sava Lagant Rabart Dabug
		Save Logout Keboot Debug
	Multicast » General » Router Port	
✓ Status	^ ·	
✓ Network	Benter Bert Table	
∨ Port	Router Port lable	
VLAN	IP Version IPv4 🗸	
 MAC Address Table 		
 Spanning Tree 	Showing All ventries Showing 0 to 0 of 0 entries	Q
 Discovery 	VIAN Nomber Static Part Farbidden Part Life (See)	
V DHCP		te found
✓ Multicast	U Tesui	IS IOUID.
∧ General	Add Edit Defeet	Pirst Previous 1 (Next) Last
Property	Add Edit Reliesi	
Bouter Port		
Forward All		
Throttling		
Filtering Profile		
Filtering Binding		
✓ IGMP Snooping		
V MLD Snooping		
× Routing		
× Security		
V ACL		
✓ QoS		
v Diagnostics	v	

Fig 10.1.5 Multicast default router port table page

COMMANDO			Save Logout Reboot Debug
	Multicast » Gen	eral » Router Port	
✓ Status ✓ Network ✓ Port	Add Router Port		^
VLAN			
 MAC Address Table 	5		
 Spanning Tree 		Available VLAN Selected VLAN	
✓ Discovery			
✓ DHCP	10.01		
▼ Multicast	VLAN		
∧ General Property Group Address			
Forward All	IP Version	IPv4 🗸	
Throttling Fitering Profile	Туре	Static Forbidden	
KMP Snooping MLD Snooping MLD Snooping MVR Routing Security AcL GoS Diagnostics Management	Port	Available Port Selected Port	

Fig 10.1.6 Multicast router port selection page

COMMANDO	Multicast » General » Router Port	Save Logout Reboot Debug
✓ Status		
✓ Network	Pouter Port Table	
✓ Port		
VLAN	IP Version IPv4 V	
 MAC Address Table 		
 Spanning Tree 	Showing All ventries Showing 1 to 1 of 1 entries	Q
✓ Discovery	VI AN Member Static Port Forbidden Port Life (Sec)	
V DHCP		
✓ Multicast		(Find) (Fundame) (1) (Hand) (Find)
 > General Property Group Address Router Port Forward All Throttling Filtering Profile Filtering Binding > IGMP Snooping > MLD Snooping 	Add Edit Refresh	(FRE) (FREVOUS] (NEXE) LASE

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.**

COMMANDO	Iulticast » General » Forward All	Save Logout Reboot Debug
✓ Status ^		
V Network	Forward All Table	
✓ Port	Forward All Table	
VLAN	IP Version IPv4 V	
V MAC Address Table		
✓ Spanning Tree	Showing All ventries Showing 0 to 0 of 0 entries	Q
✓ Discovery	VII AN Statis Bort Forbidden Bort	
✓ DHCP		
✓ Multicast	U results tound.	
	Add Edit Delete	Frst Prevous 1 (Next) Last

Fig 10.1.8 Multicast default forward all table page

S RTL8382M	x S C2000-24GP+8CF x +	- ō ×
← → C ▲ Not secure	192.168.0.1/home.html?ver	☆ 💟 🗄
COMMANDO	Multicast » General » Forward All	Save Logout Reboot Debug
	VLAN Selected VLAN	
Discovery LLDP Multicast General Property Group Address Beuter Part	IP Version Type	
router 1 of Forward All Throttling Filtering Profile Filtering Binding VICMP Shooping MULD Shooping MVR Routing Security	Available Port Selected Port GE1 GE2 GE4 GE5 GE6 GE6 GE6 GE9 V	
 ACL QoS Diagnostics Management 	Apply Close	
ा २ 🧕 🗮 🖀	i zi 🔤 📀 🖉 🦛 👩 🚾 🌞	Links * ^ <i>(</i> 723:21 8/21/2020

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**.

MANDO							Sav
	N	Iultic	cast »	Gen	eral » Thi	ottling	
	^						
		Thre	ottling	Table			
		mit	Jung	lable			
		IP Ver	sion IF	v4 ∨			
;							
9							
	11		Entry	Port	Max Group	Exceed Action	
	11	남		051	256	Dopy	
	11			OFR	200	Deny	
	11		2	GE2	256	Deny	
			3	GE3	256	Deny	
s			4	GE4	256	Deny	
			5	GE5	256	Deny	
			6	GE6	256	Deny	
			7	GE7	256	Deny	
ding			8	GE8	256	Deny	
ng 1			9	GE9	256	Denv	
			10	GE10	256	Deny	
	~		10	0210	200	Deny	

Fig 10.1.10 Multicast Default throttling table page

COMMAND							Save Logout Reboot Del
	Ν	/Iulti	icast »	Gen	eral » Thr	ottling	
✓ Status	<u>^</u>						
✓ Network		Thr	ottling	Table			
✓ Port			orung	Tuble			
VLAN		IP Ve	ersion IF	Pv4 ∨			
 MAC Address Table 							
 Spanning Tree 							Q
 Discovery 			Entry	Port	Max Group	Exceed Action	
✓ DHCP		븝	Linuy	051	050	Dony	
✓ Multicast			1	GET	206	Deny	
∧ General			2	GE2	256	Deny	
Property			3	GE3	256	Deny	
Group Address			4	GE4	256	Deny	
Router Port			5	GE5	256	Deny	
Forward All			6	GE6	256	Deny	
Eitoring			7	GE7	256	Deny	
Filtering Profile			8	GE8	256	Deny	
V IGMP Snooping			9	GE9	256	Denv	
✓ MLD Snooping			10	GE10	256	Denv	
× MV/P	~		10	0210	200	Deny	

Fig 10.1.11 Multicast Selecting port for throttling page

COMMANDO		Save	Logout	Reboot	Debug
✓ Status ^	Multicast » General » Throttling				^
✓ Network					
✓ Port	Edit Throttling				
✓ VLAN		_			
 MAC Address Table 	Port GE4-GE5				
✓ Spanning Tree					
✓ Discovery	IP version IPv4				
✓ DHCP	Max Group 2 (0 - 256)				
✓ Multicast	O Deny				
General Property Group Address Router Port Forward All Throttling Filtering Profile Filtering Binding	Apply Close				
IGMP Snooping MLD Snooping					

Fig 10.1.11 Edit Multicast throttling page

oot Debuş

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**.

COMMANDO	Multicast » General » Filtering Profile	Save Logout Reboot Debug
✓ Status	~	
V Network	Elleview Beefle Table	
✓ Port	Filtering Profile Table	
V VLAN	IP Version IPv4 V	
 MAC Address Table 		
 Spanning Tree 	Showing All ventries Showing 0 to 0 of 0 entries	Q
 Discovery 	Profile ID Start Address End Address Action	
✓ DHCP		
✓ Multicast		Cint Device (Mart) (est
 ∧ General Property Group Address Router Port Forward Ali Throttling Filtering Profile Filtering Binding ✓ IGMP Snooping ✓ MLD Snooping 	Add Edit Delete	Frst Prevous in Next Last

Fig 10.1.13 Multicast default filtering profile table page

COMMANDO		Save	Logout	Reboot	Debug
✓ Status	nuncast » General » Futering Prome				^
V Network					
✓ Port	Add Profile				
VLAN		-			
✓ MAC Address Table	Profile ID 2 (1 - 128)				
✓ Spanning Tree					
✓ Discovery	IP Version				
✓ DHCP	Start Address 224.0.0.1				
✓ Multicast					
∧ General	End Address 225.0.0.10				
Property Group Address	Action O Allow				
Router Port	l Deny				
Forward All					
Throttling	Арріу Сіозе				
Filtering Profile					
Filtering Binding					
V IGMP Shooping					
✓ MVR ✓					~

Fig 10.1.14 Multicast Add filtering profile page

COMMANDO	Multicast » General » Filtering Profile	Save Logout Reboot Debug
✓ Status	A	
✓ Network	Filtering Drofile Toble	
✓ Port	Filtering Profile Table	
VLAN	IP Version IPv4 V	
V MAC Address Table		
✓ Spanning Tree	Showing All ventries Showing 1 to 1 of 1 entries	Q
✓ Discovery	Brofile ID Start Address End Address Action	
✓ DHCP		
✓ Multicast	2 224.0.0.1 225.0.0.10 Deny	
	Add Edit Delete	(TTSL) (PEYDUS) ((NEAL (LASL)

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.

COMMANDO	M	Iultic	cast »	• Gen	eral » Fi	lterinș	g Binding				Sav	e 1	Logout	: R	eboot	Deb	ug
✓ Status	^								 								^
✓ Network		Filto	ring E	indin	Table												
✓ Port		Fille	anng E	sinding	y lable												
VLAN		IP Ver	rsion IF	Pv4 ∨													
 MAC Address Table 																	
 Spanning Tree 													Q			_	
 Discovery 			Entry	Port	Profile ID	1			 	 		_					1
✓ DHCP		님		051	i i one ib												
 Multicast 			1	GET													
∧ General			2	GE2													
Property			3	GE3													
Group Address			4	GE4													
Router Port			5	GE5													
Forward All			6	GE6													
Throttling			7	GE7													
Filtering Profile			8	GE8													
Filtering Binding				050													
V IGMP Shooping			9	GE9													
	~		10	GE10													

Fig 10.1.16 Multicast default filtering binding table page

COMMANDO						Save	Logout	Reboot	Debu
	Mul	ticast ×	Gen	eral » Fi	Filt	ring Binding			
✓ Status									
V Network									
✓ Port	Fi	Itering E	Binding	g Table					
VLAN	IP 1	Version	Pv4 🗸						
 MAC Address Table 									
✓ Spanning Tree							Q		_
V Discovery	100	D. Enter	Dent	Drafile ID					
V DHCP			Pont	Prome ib					_
✓ Multicast		⊴ 1 ⊐ 0	GE1						
∧ General		2 2	GE2						
Property		⊴ 3	GE3						
Group Address		2 4	GE4						
Router Port		5	GE5						
Forward All		6	GE6						
I nrottling		7	GE7						
Filtering Profile		8	GE8						
✓ IGMP Snooping		7 9	GE9						
✓ MLD Snooping		10	GE10						
			OLIO						

Fig 10.1.17 Multicast filtering Binding Port selection page

COMMANDO					
		Save	Logout	Reboot	Debug
Ν	Iulticast » General » Filtering Binding				
✓ Status					^
V Network					
✓ Port	Edit Filtering Binding				
VLAN					
 MAC Address Table 	Port GE1-GE4				
✓ Spanning Tree	IP Version DV/				
✓ Discovery					
✓ DHCP	Profile ID	1			
✓ Multicast	2 ~				
∧ General		1			
Property	Apply Close				
Group Address					
Router Port					
Forward All					
Throttling					
Filtering Profile					
Filtering Binding					
 IGMP Snooping 					
✓ MLD Snooping					
✓ MVR ✓					~

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.

										Save Log	gout Reboot De
		Multic	ast »]	GMP Snooping	» Property						
✓ Status	^										
✓ Network	. I.			· · · · · · · · · · · · · · · · · · ·							
✓ Port				State Enabl	e						
VLAN				Version IGMP	12						
 MAC Address Table 					/3						
 Spanning Tree 		F	Report Su	ippression 🖂 Enabl	e						
 Discovery 											
V DHCP		A	pply								
✓ Multicast											
✓ General		VLAN	N Settin	ng Table							
∧ IGMP Snooping											
Property										Q	
Querier					Poutor Port	Quant	Querr	Ouony Max	Last Mombor	Last Mombor	
Statistics MLD Speeping			VLAN	Operational Status	Auto Loarn	Pohuetnose	Intorval	Response Interval	Query Counter	Quory Interval	Immediate Leave
✓ MVR			- 1	Disabled	Enabled	2	126	10	guery counter	4	Disabled
✓ Routing				Disabled	Enabled	2	125	10	2		Disabled
✓ Security			2	Disabled	Enabled	2	125	10	2	1	Disabled
× ACL			3	Disabled	Enabled	2	125	10	2	1	Disabled
× QoS			10	Disabled	Enabled	2	125	10	2	1	Disabled
 Diagnostics 		E	dit								
✓ Management											

Fig 10.2.1 Default IGMP snooping property page

COMMANDO	Multi	cast »	IGMP Snoopin	g » Prope	rty					Save Logout	Reboot	Debug
✓ Status ,	^											
✓ Network												
✓ Port			State 🛛 🗠 En	able								
VLAN			Version IGN	IPv2								
 MAC Address Table 			; O IGN	Enable IGMIP/2 GMIP/3 Enable								
✓ Spanning Tree		Report S	Suppression 🛛 🖂 En	able								
✓ Discovery		_		able								
✓ DHCP	4	Apply VLAN Setting Table										
 Multicast 												
 ✓ General ∧ IGMP Snooping Property Querier 	VLA	N Setti	ng Table							Q		
Statistics		VIAN	Operational Status	Router Port	Query	Query	Query Max	Last Member	Last Member	Immodiate Leave		
✓ MLD Snooping		VLAN	Operational Status	Auto Learn	Robustness	Interval	Response Interval	Query Counter	Query Interval	Infineurate Leave		- 11
✓ MVR		1	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ Routing		2	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ Security		3	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ ACL		10	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ Q₀S			2	_	_	_					_	
✓ Diagnostics		Edit	J									
✓ Management	×											

Fig 10.2.2 IGMP snooping property VLAN setting page

COMMANDO				
	Multicast » IGMP Snooping »	P	roperty	
V Status				
✓ Network				
✓ Port	Edit VLAN Setting			
VLAN				
 MAC Address Table 		315 - 5		
 Spanning Tree 	VLAN		1-3,10	
✓ Discovery	! State	1F = !!		
V DHCP		# =		
✓ Multicast	Router Port Auto Learn		Enable	
✓ General	Immediate leave	11 -	C Enable	
∧ IGMP Snooping	L	ji -		······
Property		15 -		
Querier	Query Robustness		5	(1 - 7, default 2)
Statistics	Query Interval	1	1250	Sec (30 - 18000, default 125)
 MLD Snooping 		# =		3ee(30 - 10000, deladit 123)
✓ MVR	Query Max Response Interval		10	Sec (5 - 20, default 10)
✓ Routing	L	JL -		·
✓ Security	Last Mambas Overs Country	15 -	0	(4 7 defeude 2)
V ACL		#=	 2	(1 - 7, delault 2)
✓ QoS	Last Member Query Interval	1	10	Sec (1 - 25, default 1)
✓ Diagnostics	· · · · · · · · · · · · · · · · · · ·	ji -		
✓ Management	Operational Status			
		77 -		
	Status	# =	Disabled	
	Query Robustness	1	2	
		# = !!	125 (Sec)	
		# =	120 (000)	
	Query Max Response Interval		10 (Sec)	
	Last Member Query Counter		2	
	Last Momber Query Internal	#=	1 (See)	
	Last member Query Interval	JL _	(() e c)	
	Apply Close			

Fig 10.2.3 IGMP snooping Edit VLAN setting page

COMMANDO										s	Save Logout	Reboot	Debug
	M	ultic	ast »	IGMP Snoopin	g » Prope	rty							
 Status 	^												^
✓ Network	Í	·											
✓ Port				State : M En	adie								
VLAN				Version IGN	/Pv2								
 MAC Address Table 					/IPV3								
 Spanning Tree 		l	Report S	uppression 🛛 🖂 En	able								
 Discovery 		_											
V DHCP		A	pply										
- Multicast													
✓ General		VLA	N Setti	ng Table									
∧ IGMP Snooping													
Property											Q		
Querier					Router Port	Query	Query	Query Max	Last Member	Last Member			
Statistics			VLAN	Operational Status	Auto Learn	Robustness	Interval	Response Interval	Query Counter	Query Interval	Immediate Leave		- 11
✓ MCD Shooping ✓ MVR			1	Enabled	Enabled	2	125	. 10	2	1	Enabled		
Routing			2	Enabled	Enabled	2	125	10	2	1	Enabled		- 11
 Security 			3	Enabled	Enabled	2	125	10	2	1	Enabled		- 11
ACL			10	Enabled	Enabled	2	125	10	2	1	Enabled		- 11
V QoS			10	Linabled	Lindbled	2	125	10	2		Linableu		
 Diagnostics 		E	Edit										
 Management 	~												v

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.

COMMANDO									;	Save 1	Logout	Reboot	Debug
		Multi	cast »	IGMP	Snooping » Qu	erier							
✓ Status	^												
✓ Network		•	·										
✓ Port		Que	rier la	ble									
✓ VLAN											0		
 MAC Address Table 		_						 			4		_
 Spanning Tree 			VLAN	State	Operational Status	Version	Querier Address						
 Discovery 			1	Disabled	Disabled								
✓ DHCP			2	Disabled	Disabled								
 Multicast 			3	Disabled	Disabled								
✓ General			10	Disabled	Disabled								
 IGMP Snooping 													
Property			Edit										
Querier				-									
 MLD Snooping 													
✓ MVR													
✓ Routing													
✓ Security													
✓ ACL													
∨ QoS													
✓ Diagnostics													
✓ Management	\sim												

Fig 10.2.5 Default IGMP snooping Querier table page

COMIMANDO	Multi	cast »	IGMP	Snooping » Qu	erier	Save
 ✓ Multicast ^ General A IGMP Snooping Property 	Que	erier Ta	ble			
Querier		VLAN	State	Operational Status	Version	Querier Address
✓ MLD Snooping		1	Disabled	Disabled		
V MVR		2	Disabled	Disabled		
✓ Routing		3	Disabled	Disabled		
✓ Security		10	Disabled	Disabled		
✓ ACL	_					
✓ QoS		Edit				

Fig 10.2.6 IGMP snooping Selecting Vlan Querier page

COMMANDO	Save Logout Reboot De	ebug
_	ulticast » IGMP Snooping » Querier	
 ✓ Multicast ^ General ∧ IGMP Snooping Property 	Edit Querier	
Querier Statistics	VLAN 1-3,10	1
 ✓ MLD Snooping 	State 🗵 Enable	
✓ MVR	Version IGMPv2	Ε.
✓ Routing	O IGMPv3	
V QoS	Appiy Close	
✓ Diagnostics		
✓ Management		>

Fig 10.2.7 IGMP snooping Edit Querier page

COMMANDO				a . N a		Sav	ve Logout	Reboot	Debug
Ν	Iulti	cast »	IGMP	Snooping » Qu	erier				
 ✓ Multicast ^ General ^ IGMP Snooping Property Querier 	Que	erier Ta	ble				Q [
Statistics		VLAN	State	Operational Status	Version	Querier Address			
 ✓ MUD Shooping ✓ MVR 		1	Enabled	Enabled	IGMPv2	0.0.0.0			
✓ Routing		2	Enabled	Enabled	IGMPv2	0.0.0.0			- 11
✓ Security		3	Enabled	Enabled	IGMPv2	0.0.0.0			- 11
V ACL		10	Enabled	Enabled	IGMPv2	0.0.0.0			
✓ QoS									
✓ Diagnostics		Edit	J						
✓ Management									

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.

COMMANDO	Multicont N ICMD Secondary N Statistics
∨ Status	Municast # IGMF Snooping # Statistics
 Network 	
∨ Port	Receive Packet
VI AN	Total 1
V MAC Address Table	Valid 1
	InValid " 0
v Dilor ▼ Multicast	Leave # 0
• multicast	Report # 1
✓ General	General Query
Property	
Querier	Special Group Query " 0
Statistics	Source-specific Group Query 0
✓ MLD Snooping	
∨ MVR	Transmit Packet
✓ Routing	Leave # 0
✓ Security	Report 0
✓ ACL	
∨ QoS	General Query 1
✓ Diagnostics	Special Group Query 0
∨ Management	Source-specific Group Query 0
	Clear Refresh

Fig 10.2.9 IGMP snooping statistics page

10.3 MLD Snooping

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

The COMMANDO 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.**

COMMANDO			MDC	N. D	6 -7					Save Logout	Reboot De	bug
⊥ y Status	viunuo	cast "	MLD Shooping	" Proper	ty							^
V Network	· · · · ·											
✓ Port			State 📋 En	able								
VLAN			Version ML	Dv1								
V MAC Address Table			, O ML	Dv2								
✓ Spanning Tree	l	Report S	Suppression 🛛 🖂 En	able								
✓ Discovery												
V DHCP	A	Apply	ļ									
✓ Multicast												
✓ General	VLA	N Setti	ing Table									
✓ IGMP Snooping												
∧ MLD Snooping										Q		18
Statistics			On another all Status	Router Port	Query	Query	Query Max	Last Member	Last Member	In the second second		1
✓ MVR		VLAN	Operational Status	Auto Learn	Robustness	Interval	Response Interval	Query Counter	Query Interval	Immediate Leave		
✓ Routing		1	Disabled	Enabled	2	125	10	2	1	Disabled		1
✓ Security		2	Disabled	Enabled	2	125	10	2	1	Disabled		
V ACL		3	Disabled	Enabled	2	125	10	2	1	Disabled		
V QoS		10	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ Diagnostics	_											
✓ Management	E	Edit)									

Fig 10.3.1 Multicast MLD Snooping default property page

										Save Logout	Reboot Debu	ug
Ν	Aultic	ast »	MLD Snooping	» Proper	ty							
✓ Status	_											^
✓ Network			State 🛛 🖂 En	ahla								
✓ Port												
✓ VLAN			Version O ML	DV1 Dv2								
✓ MAC Address Table												
✓ Spanning Tree	l	Report S	Suppression 🔛 En	able								
✓ Discovery												
✓ DHCP	Α	крріу	ļ									
▼ Multicast												
✓ General	VLA	N Setti	ing Table									
✓ IGMP Snooping												
∧ MLD Snooping										Q,		
Property				Router Port	Query	Query	Query Max	Last Member	Last Member			
V MVR		VLAN	Operational Status	Auto Learn	Robustness	Interval	Response Interval	Query Counter	Query Interval	Immediate Leave		
✓ Routing		1	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ Security		2	Disabled	Enabled	2	125	10	2	1	Disabled		
V ACL		3	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ Q0S		10	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ Diagnostics	_	_										
✓ Management	E	Edit										
			,									¥

Fig 10.3.2 Enabling MLD Snooping property page

COMMANDO	Multi	cast »	MLD Snooping	» Propert	y					Save Logout	Reboot Deb
Status											
V Network											
Port			State ¦ ⊠ Ena	able							
VLAN			Version O ML	.Dv1							
MAC Address Table			¦ ● MLI	.Dv2							
 Spanning Tree 		Report	Suppression 🛛 🗹 Ena	able							
Discovery)								
Discovery DHCP		Apply)								
Discovery DHCP Multicast		Apply)								
 Discovery DHCP Multicast General 		Apply	ing Table								
 ✓ Discovery ✓ DHCP ✓ Multicast ✓ General ✓ IGMP Snooping 	VLA	Apply	ing Table								
Discovery DHCP Multicast General IGMP Snooping MLD Snooping	VLA	Apply AN Setti	ing Table							٩	
Discovery DHCP Multicast General IGMP Snooping MLD Snooping Property Otherity		Apply	ing Table	Router Port	Query	Query	Query Max	Last Member	Last Member	Q	
Discovery Discovery Discovery Multicast General GMP Snooping Property Statistics MUD		Apply AN Setti VLAN	ing Table Operational Status	Router Port Auto Learn	Query Robustness	Query	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Q Immediate Leave	
Discovery Discovery Multicast General IGMP Snooping AMLD Snooping Property Statistics MVR Brutinn		Apply AN Setti VLAN 1	Operational Status	Router Port Auto Learn Enabled	Query Robustness 2	Query Interval 125	Query Max Response Interval 10	Last Member Query Counter 2	Last Member Query Interval	Q Immediate Leave Disabled	
Discovery Discovery Discovery Multicast General IGMP Snooping MLD Snooping Property Statistics WVR Routing Security		Apply AN Setti VLAN 1 2	ing Table Operational Status Disabled Disabled	Router Port Auto Learn Enabled Enabled	Query Robustness 2 2	Query Interval 125 125	Query Max Response Interval 10 -10	Last Member Query Counter 2 2	Last Member Query Interval 1	Q Immediate Leave Disabled Disabled	
Discovery Discovery Discovery Multicast General IGMP Snooping Property Statistics MUD Snooping Property Statistics MVR Routing Security ACL		Apply AN Setti VLAN 1 2 3	ing Table Operational Status Disabled Disabled	Router Port Auto Learn Enabled Enabled	Query Robustness 2 2 2 2	Query Interval 125 125 125	Query Max Response Interval 10 10 10	Last Member Query Counter 2 2 2 2	Last Member Query Interval 1 1	Q Immediate Leave Disabled Disabled	
Discovery Discovery DHCP Multicast General IGMP Snooping MLD Snooping Property Statistics MVR Routing Security ACL OoS		Apply AN Setti VLAN 1 2 3 10	ing Table Operational Status Disabled Disabled Disabled	Router Port Auto Learn Enabled Enabled Enabled	Query Robustness 2 2 2 2 2 2	Query Interval 125 125 125 125	Query Max Response Interval 10 10 10 10	Last Member Query Counter 2 2 2 2	Last Member Query Interval 1 1 1	Q Immediate Leave Disabled Disabled Disabled	
Discovery DicP Multicast General IGMP Snooping MLD Snooping Property Statistics WVR Routing Security ACL QoS Diagnostics		Apply AN Setti VLAN 1 2 3 10	ing Table Operational Status Disabled Disabled Disabled Disabled	Router Port Auto Learn Enabled Enabled Enabled Enabled	Query Robustness 2 2 2 2 2 2 2	Query Interval 125 125 125 125 125	Query Max Response Interval 10 10 10 10	Last Member Query Counter 2 2 2 2 2 2 2	Last Member Query Interval 1 1 1 1	Q Immediate Leave Disabled Disabled Disabled	

Fig 10.3.3 Selecting Vlan for MLD Snooping property page



Multicast » MLD Snooping » Property

Network		
Port		
VLAN	Edit VLAN setting	
MAC Address Table		
Spanning Tree	VLAN 2-3	
Discovery		
	State 🗹 Enal	ble
	Router Port Auto Learn "	ble
lticast		
neral	Immediate leave 🛛 🔽 Enal	ble
MP Snooping	L	
D Snooping		
operty	Query Robustness	(1 - 7, default 2)
tistics		0
	Query Interval 1024	Sec (30 - 18000, default 125)
	Query Max Response Interval 8	Sec (5 - 20, default 10)
	L	
	_	
	Last Member Query Counter 5	(1 - 7, default 2)
	Last Member Query Interval	Coold 25 default 1)
tics		Sec(1-25, delault 1)
jement		
	Operational Status	
	Status " Disabled	
	Query Robustness 2	
	0	
	Query Interval # 125 (Sec	2)
	Query Max Response Interval 10 (Sec)	
	Last Member Query Counter ii 2	
	Last Member Query Interval # 1 (Sec)	

Fig 10.3.4 Edit Vlan Setting for MLD Snooping page

COMMANDO	/Iultic	cast »	MLD Snooping	» Proper	ty				9	Save Logout	Reboot	Debug
✓ Status	_											^
V Network	[·····		State 🖂 En	blo								
✓ Port												
VLAN			Version O MLI	Dv1								
V MAC Address Table	ļ			JVZ								
✓ Spanning Tree	l	Report 9	Suppression 🛛 🖂 Ena	ible								
✓ Discovery	_		1									
V DHCP	A	pply	ļ									
 Multicast 												
✓ General	VLA	N Setti	ing Table									
✓ IGMP Snooping										_		
∧ MLD Snooping										Q		_
Statistics			0 1 1011	Router Port	Query	Query	Query Max	Last Member	Last Member			
✓ MVR		VLAN	Operational Status	Auto Learn	Robustness	Interval	Response Interval	Query Counter	Query Interval	Immediate Leave		- 11
✓ Routing		1	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ Security		2	Enabled	Enabled	6	1024	8	5	3	Enabled		- 11
V ACL		3	Enabled	Enabled	6	1024	8	5	3	Enabled		- 11
✓ QoS		10	Disabled	Enabled	2	125	10	2	1	Disabled		
✓ Diagnostics		-				_						_
✓ Management	E	dit)									

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.**

COMMANDO				Save Logou	it Reboot Debug
N∧	lulticast » MVI	R » Property	у		
Veteork Veteork Veteork VLAN	State	Enable		 	
 MAC Address Table Spanning Tree 	Mode	 Compatible Dynamic 			
Discovery DHCP	Group Start	0.0.0.0		 	
▼ Multicast	Group Count	1	(1 - 128)	 	
 ✓ General ✓ IGMP Snooping 	Query Time	1	Sec (1 - 10)	 	
 MLD Snooping MVR 	Operational Grou	ıp		 	
Property Port Setting Group Address	Maximum Current	128 0		 	
✓ Routing	Apply				
✓ Security					
✓ ACL					

Fig 10.4.1 Default MVR Property page

COMMANDO	ulticast » MVI	R » Property		Save	Logout	Reboot	Debug
✓ Status							
✓ Network	State	Enable					
✓ Port							
VLAN	VLAN	3 🗠					
V MAC Address Table	Mode	O Compatible					
✓ Spanning Tree		Dynamic					
✓ Discovery	Group Start	239.0.0.5					
✓ DHCP	Group Count	1	(1 - 128)				
✓ Multicast	Group Count		(1-120)				
✓ General	Query Time	1	Sec (1 - 10)				
IGMP Snooping MLD Snooping MVR	Operational Grou	h					
Property	Maximum	128					
Port Setting Group Address	Current	0					
✓ Routing	Apply						
✓ Security							
✓ ACL							

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.

COMMANDO								Save	Logout	1
	M	Iulti	cast »	MV	s » P	ort Setting				
tatus	^									
etwork		_								
Port		Pon	t Settii	ng lab	le					
VLAN										
MAC Address Table		_			, <u> </u>				G	_
Spanning Tree			Entry	Port	Role	Immediate Leave	e			
iscovery			1	GE1	None	Disabled				
DHCP			2	GE2	None	Disabled				
Multicast			3	GE3	None	Disabled				
✓ General			4	GE4	None	Disabled				
 IGMP Snooping 			5	GE5	None	Disabled				
MLD Shooping			6	GE6	None	Disabled				
Property			7	GE7	None	Disabled				
Port Setting			8	GE8	None	Disabled				
Group Address			9	GE9	None	Disabled				
Routing			10	GE10	None	Disabled				
Security			11	GE11	None	Disabled				
ACL	~		12	GE12	None	Disabled				

Fig 10.4.3 Multicast MVR Port Setting page



Save | Logout | Reboot | Debug

	Multi	icast »	MVI	s » b	ort Setting							
✓ Status							^					
V Network	D.			1.								
✓ Port	Port Port Setting Table											
V VLAN						0						
 MAC Address Table 	_					4						
✓ Spanning Tree		Entry	Port	Role	Immediate Leave							
V Discovery		1	GE1	None	Disabled		11					
V DHCP		2	GE2	None	Disabled							
▼ Multicast		3	GE3	None	Disabled							
✓ General		4	GE4	None	Disabled							
✓ IGMP Snooping		5	GE5	None	Disabled							
 MLD Snooping 		6	GE6	None	Disabled							
∧ MVR Property		7	GE7	None	Disabled							
Port Setting		8	GE8	None	Disabled							
Group Address		9	GE9	None	Disabled							
✓ Routing		10	GE10	None	Disabled							
✓ Security		11	GE11	None	Disabled							
✓ ACL		12	GE12	None	Disabled		v					

Fig 10.4.4 Multicast MVR Port Selection page

	Aulticast » MVR »	Save Logou Port Setting	t Reboot Debug
✓ Status ^			^
✓ Network			
✓ Port	Edit Port Setting		
VLAN			-
 MAC Address Table 	Port	GE1-GE28,LAG1-LAG8	
 Spanning Tree 		None	
✓ Discovery	Role	O Receiver	
✓ DHCP		O Source	
✓ Multicast	Immediate Leave	☑ Enable	
 General IGMP Snooping MLD Snooping MVR Property Port Setting Group Address 	Apply Close	2	

Fig 10.4.5 Multicast MVR Edit port setting page

COMMANDO	Multi	cast »	MVR	× » P	ort Setting	Save Logout Reboot	Debug
✓ Status ^							^
✓ Network	Des	4.0 - 441		-			
✓ Port	Pol	t Settir	ig labi	е			
VLAN						0	- 1
 MAC Address Table 						8	_
✓ Spanning Tree		Entry	Port	Role	Immediate Leave		
✓ Discovery		1	GE1	None	Enabled		
✓ DHCP		2	GE2	None	Enabled		
✓ Multicast		3	GE3	None	Enabled		
✓ General		4	GE4	None	Enabled		
✓ IGMP Snooping		5	GE5	None	Enabled		
✓ MLD Snooping		6	GE6	None	Enabled		
		7	GE7	None	Enabled		
Port Setting		8	GE8	None	Enabled		
Group Address		9	GE9	None	Enabled		

Fig 10.4.6 Multicast MVR Port setting Table page

9.4.3 Group Address

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

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

COMMANDO	Mult	icast »	MVR » Gr	oup Add	ress			Save Logout Reboot Debug
✓ Status	^							
✓ Network								
✓ Port	Gr	oup Ado	dress Table					
VLAN	Shov	ving All 🗸	entries		Showi	ng 0 to 0 of 0 ent	tries	
 MAC Address Table 			7			-		4
 Spanning Tree 		VLAN	Group Address	Member	Туре	Life (Sec)		
✓ Discovery						0 re	sults found.	
✓ DHCP								First Previous 1 Next Last
✓ Multicast		Add	Edit	Delete	R	efresh		
∽ General								
✓ IGMP Snooping								
 MLD Snooping 								
∧ MVR								
Property								
Port Setting								
Group Address								

Fig 10.4.7 Multicast MVR default group address Table page

COMMANDO	lticast » MVR »	Crown Address	Save Logout Reboot	Debug
✓ Status		Group Additions		^
✓ Network				
✓ Port	Add Group Address			
VLAN				
✓ MAC Address Table	VLAN	3		
✓ Spanning Tree	Croup Addross	220.0.0.5		
✓ Discovery	Group Address	239.0.0.5 (239.0.0.5 - 239.0.0.5)		
✓ DHCP		Available Port Selected Port		
✓ Multicast				
 ✓ General ✓ IGMP Snooping ✓ MLD Snooping ▲ MVR Property Port Setting Group Address ✓ Routing 	Member Apply Clos			
✓ Security				
✓ ACL				~

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.

COMMANDO	Routing » IP	v4 Managemen	it and Inte	erfaces	» IPv	4 Interface	Save Logout Reboot Debug
✓ Status							
V Network	IPv4 Interfac	e Table					
✓ Port	ii v+interiue	C TUDIC					
VLAN							0
 MAC Address Table 		,					~
 Spanning Tree 	Interface	IP Address Type	IP Address	Mask	Status		
✓ Discovery						0 results found.	
✓ DHCP	Add	Doloto					
✓ Multicast	Add	Delete					
 IPv4 Management and Interface 							
IPv4 Interface							
IPv4 Routes							
ARP							
 IPv6 Management and Interface 							
✓ Security							
V ACL							
✓ QoS							
< >	1						

Fig 11.1.1 Default IPv4 interface table page

			Save Logou	t Reboot	Debug
R	Routing » IPv4 M	anagement and Interfaces » IPv4 Interface			
✓ Status					^
✓ Network					
✓ Port	Add IPv4 Interface				
VLAN					
V MAC Address Table					
✓ Spanning Tree	Interface				
✓ Discovery		() Loopback			
V DHCP	Address Type				
✓ Multicast					
✓ Routing	IP Address	192.168.20.1			
 IPv4 Management and Interface 		Network Mask 255 255 255 0			
IPv4 Interface	Mask	C Herrork maan 200.200.00			
IPv4 Routes		O Prefix Length (8 - 30)			
ARP	L	·			
 IPv6 Management and Interface 	Apply	lose			
✓ Security					
✓ ACL					
✓ QoS					
< >					~

Fig 11.1.2 IPv4 interface configuration page

COMMANDO		Save Legent Debug
		Save Logout Keboot Debug
Routi	ng » IPv4 M	anagement and Interfaces » IPv4 Interface
✓ Status		A
✓ Network		
✓ Port Add	IPv4 Interface	
VLAN		
✓ MAC Address Table		
✓ Spanning Tree	Interface	
V Discovery		Loopback
✓ DHCP	Address Type	O Dynamic
✓ Multicast	,,	Static
✓ Routing	IP Address	1.1.1.1
 IPv4 Management and Interface 		Network Mask
IPv4 Interface	Mask	
IPv4 Routes		● Prefix Length 24 (8 - 30)
✓ IPv6 Management and Interface		
✓ Security	Apply C	lose
✓ ACL		
✓ Q0S		
Ý		

Fig 11.1.3 Creating IPv4 loopback interface configuration page

COMMANDO	Routin	ng » IPv	4 Management	t and Interf	aces » IPv4	Interf	ace	Save Logout	Reboot I	Debi
∽ Status										
✓ Network	IPv4	Interface	Table							
✓ Port		monuoo	TUDIO							
✓ VLAN								0		
MAC Address Table								~		_
 Spanning Tree 		Interface	IP Address Type	IP Address	Mask	Status				
/ Discovery		Loopback1	Static	1.1.1.1	255.255.255.0	Valid				
/ DHCP		VLAN 2	Static	192.168.20.1	255.255.255.0	Valid				
 Multicast 		Add	Delete							
- Routing		Add	Delete							
▲ IPv4 Management and Interface										
IPv4 Interface										
IPv4 Routes										
ARP										
 IPv6 Management and Interface 										
 Security 										
/ ACL										
V QoS										
< >>										

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.

COMMANDO	Routin	ng » IPv4	Manag	gement and I	nterfaces » IP	v4 Routes		Save Logout	Reboot Debug
✓ Status ^									
✓ Network	IDv4	Douting T	abla						
✓ Port	IPV4	Routing	able						
✓ VLAN									0
 MAC Address Table 	_								G I
 Spanning Tree 		Destination	IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
 Discovery 		1.1.1.0		24	Directly Connected				Loopback1*
✓ DHCP		192.168.0.0		24	Directly Connected				MGMT VLAN*
✓ Multicast					1		_		
	/	Add	Edit	Delete	J				
 IPv4 Management and Interface 									
IPv4 Interface									
IPv4 Routes									
ARP									
 IPv6 Management and Interface 									
 Security 									
✓ ACL									
✓ QoS									
*									

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.

COMMANDO	outing » IPv4 Managemen	t and Interfaces	» IPv4 Rout	es	Save Logout	: Reboot Debug
✓ Status						^
V Network						
✓ Port	Add IPv4 Static Route					
VLAN						
 MAC Address Table 	IP Address	192 168 100 0				
✓ Spanning Tree	IF Address	1.52.100.100.0				
✓ Discovery		 Network Mask 				
V DHCP	Mask	Drefix Length	24	(0 - 32)		
✓ Multicast				(0 - 02)		
- Routing	Next Hop Router IP Address	192.168.1.1				
 IPv4 Management and Interface IPv4 Interface 	Metric	10	(1 - 255, default	1)		
IPv4 Routes						
ARP	Apply Close					
 IPv6 Management and Interface 						
✓ Security						
✓ ACL						
✓ QoS						

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.

COMMANDO	ting » IPv4 Management	and Interfaces	» IPv4 Routes	Save Logout	: Reboot Debug
✓ Status					^
✓ Network					
✓ Port A	dd IPv4 Static Route				
VLAN					
V MAC Address Table	IP Address	0000			
✓ Spanning Tree					
✓ Discovery		 Network Mask 			
✓ DHCP	Mask	Prefix Length)	(0 - 32)	
✓ Multicast		© Frenk Eengar	, 	(0 - 02)	
✓ Routing	Next Hop Router IP Address	192.168.0.254			
▲ IPv4 Management and Interface IPv4 Interface	Metric	1	(1 - 255, default 1)		
IPv4 Routes ARP ✓ IPv6 Management and Interface	Apply Close				

Fig 11.2.3 Add IPv4 Default route page

1	Routin	ng≫ IPv4 Manag	gement and l	Interfaces » IP	v4 Routes				
 Status System Information Logging Message 	IPv4	Routing Table							
 Port Link Aggregation 	-								۹
MAC Address Table		Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface	
v Network		0.0.0.0	0	Default	192.168.0.254	1	1	MGNT VLAN*	
v Part		10.10.10.0	24	Directly Connected				Loopbeck1*	
POE Setting		192.168.0.0	24	Directly Connected				MGNT VLAN*	
~ VLAN		144 E-49	Dalata						
 MAC Address Table 		ADD EDI	Delete						
 Spanning Tree 									
 Discovery 									
 Multicast 									
 Routing 									
 IPv4 Management and Interfaces 									
IPv4 Interface									
IPv4 Routes									
ARP									
 IPvo Management and Interfaces 									
v Security									
V AUL									
~ Qes									
v Diagnostics									
 Management 									

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.

COMMANDD		Save Logout Reboot Debug
	Routing » IPv4 Management and Interfaces » ARP	
✓ Status ^		
V Network		
✓ Port	ARP Entry Age Out 1200 Sec (15 - 21600, default 1200)	
VLAN	O All	
 MAC Address Table 	Clear ARP Table Entries	
✓ Spanning Tree	Statuc Normal Age Out	
V Discovery		
V DHCP	Apply Cancel	
✓ Multicast		
Routing	APP Table	
 IPv4 Management and Interface 	ARP TODIC	
IPv4 Interface		0
IPv4 Routes		4
ARP	Interface IP Address MAC Address Status	
 IPv6 Management and Interface 	VLAN 1 192.168.0.21 28:d2:44:0a:7e:9c Dynamic	
✓ Security		
✓ ACL	Add Edit Delete	
✓ QoS		

Fig 11.1.4 Default ARP table page

COMMANDO			Sava	Logout	Pehoot	Debug
			Save	Logout	Reboot	Debug
Routing »	IPv4 M	anagement and Interfaces » ARP				
✓ Status						^
V Network						
✓ Port Add ARP						
VLAN						
✓ MAC Address Table		VIAN 2 V				
✓ Spanning Tree	nterface					
✓ Discovery		Note: Only interfaces with an valid IPv4 address are available for selection				
V DHCP IP	Address	192.168.1.10				
V Multicast	Address	AA-BB-CC-77-75-11				
✓ Routing	Address	PR05.00.11.10.11				
IPv4 Management and Interface IPv4 Interface IPv4 Interface IPv4 Routes ARP IPv6 Management and Interface Security		se				
V ACL						
✓ QoS v						

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.

COMMANDO	Douti	ng » IPy	v6 Manag	oment and I	ntarfacas » Dr.6	Intarfaca		Save	Logout	Reboot	Debug
	Kouth	<u>ц</u> п п									
	[
		IPv6 Unica	st Routing	Enable							
	4	Apply	Cancel								
✓ MAC Address Table											
✓ Spanning Tree	IPvf) Interfac	e Table								
		mionuo	0 10010								
✓ DHCP									0		
✓ Multicast	_								4]	_
✓ Routing				DHCPv6 (Client						
 IPv4 Management and Interface 		Interface		Information	Minimum Information	Auto Configuration	DAD Attempts				
 IPv6 Management and Interface 			Stateless	Refresh Time	Refresh Time						
IPv6 Interface					(0 results found.					
IPv6 Addresses	_							_	_	_	_
IPv6 Routes		Add	Edit	Delete							
IPv6 Neighbors											

Fig 11.2.1 Default IPv6 interface Table page

								Save Logout Re	eboot Debug
	Routi	ng » IPv	6 Manag	ement and I	nterfaces » IPv6	Interface			
✓ Status ^									
✓ Network	- E	IRve Union	t Douting						
✓ Port	i	IF V6 Offica:	scrouling				i		
VLAN		Apply	Cancel						
V MAC Address Table		- the test	Gancer						
✓ Spanning Tree									
✓ Discovery	IPve	6 Interface	e Table						
✓ DHCP									
∽ Multicast	-							q	
✓ Routing				DHCPv6 (Client				
 IPv4 Management and Interface 		Interface	Statelocc	Information	Minimum Information	Auto Configuration	DAD Attempts		
 IPv6 Management and Interface 			Stateless	Refresh Time	Refresh Time				
IPv6 Interface					() results found.			
IPv6 Addresses									
IPv6 Routes		Add	Edit	Delete	J				
IPV6 Neighbors									

Fig 11.2.2 Enableing IPv6 Unicast Routing page

COMMANDO	uting » IPv6 Management and I	Interfaces » IPv6 Interface	Save Logout Reboot Deb	ug
✓ Status				^
V Network				
✓ Port	Add IPv6 Interface			
V VLAN				
V MAC Address Table				
✓ Spanning Tree	Interface			
V Discovery		🔿 Loopback		
V DHCP	Auto Configuration	☑ Enable		
✓ Multicast	DAD Attempts	1 (0 - 600 default 1)		
Routing		(0 000, delaut 1)		
✓ IPv4 Management and Interfaces	DHCPv6 Client			
 IPv6 Management and Interfaces 	Stateless	Enable		
IPv6 Interface	Information Refresh Time	86400 (86400 - 4294967294, default 86400)		
IPv6 Addresses				
IPv6 Routes	Minimum Information Refresh Time	600 (600 - 4294967294, default 600)		
× Security				
× ACI	Apply Close			
× 00\$				
V Diagnostics				
✓ Management				~

Fig 11.2.3 Add IPv6 interface page

COMMANDO	outi	ng » IPv	76 Manag	gement and I	Interfaces » IPv6	Interface		Save Logout Reboot Debug					
✓ Status													
V Network	[IDv6 Unica	t Pouting	Enable									
✓ Port	i	ii vo onica:											
✓ VLAN	Apply Cancel												
✓ MAC Address Table	Apply Cancel Apply Cancel												
✓ Spanning Tree													
✓ Discovery	IPve	6 Interface	e Table										
✓ DHCP								0					
✓ Multicast	_							ų					
✓ Routing				DHCPv6	Client								
 IPv4 Management and Interfaces IPv6 Management and Interfaces 		Interface	Stateless	Information Refresh Time	Minimum Information Refresh Time	Auto Configuration	DAD Attempts						
IPv6 Interface		VLAN 2	Enabled	86400	600	Enabled	1						
IPv6 Addresses IPv6 Routes IPv6 Neighbors		Add	Edit	Delete									
✓ Security													
V ACL													
✓ Q₀S													
✓ Diagnostics													
✓ Management													

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.

HOMINAVIA					Save Logout	Reboot Debug
_	Routing » IPv6 Ma	nagement and In	terfaces » IPv6	Addresses		
✓ Status						
V Network						
✓ Port	IPv6 Address Tabl	e				
VLAN	Interface VLAN 2 V					
V MAC Address Table						
 Spanning Tree 					Q	
✓ Discovery	D IDef Address Top	a IDuC Address	Dut Deefer Lemeth	DAD Status	-4	
V DHCP	IPV6 Address Typ	e IPV6 Address	IPV6 Prelix Lengui	DAD Status		
✓ Multicast	Link Local	1eou2eu.4cii.ieuu.u	04	rentative		
- Routing	Multicast	mu2::1				
✓ IPv4 Management and Interfaces	Multicast	#01::1				
 IPv6 Management and Interfaces 	Add Del	ete				
IPv6 Interface						
IPv6 Addresses						
IPv6 Neighbors						
✓ Security						
✓ ACL						
V QoS						
✓ Diagnostics						
✓ Management						

Fig 11.2.5 IPv6 address table page

COMMANDO	uting » IPv6 Mana	Save Logout Reboot Debug gement and Interfaces » IPv6 Addresses
✓ Status		
✓ Network		
✓ Port	Add IPv6 Interface	
VLAN		
✓ MAC Address Table	Interface	VLAN 2
✓ Spanning Tree		O Global
✓ Discovery	IPv6 Address Type	Link Local
✓ DHCP	IPv6 Address	20011f
✓ Multicast	II VO Address	
✓ Routing	Prefix Length	(3 - 128)
 IPv4 Management and Interface 	EUI-64	Enable
IPv6 Management and Interface	L	
IPv6 Interface	Apply Close	
IPv6 Addresses		
IPv6 Routes		
IPv6 Neighbors		

Fig 11.2.6 Add IPv6 interface page

COMMANDO	outir	ng » IPv6 Mana	agement and Int	erfaces » IPv6	Addresses	Save Logout Reboot	Debug
✓ Status							^
✓ Network	10.0	A.I.I					
✓ Port	IPv6	Address Table					
VLAN	Interf	ace VLAN 2 V					
✓ MAC Address Table							
✓ Spanning Tree						Q	
✓ Discovery		IPv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status		
✓ DHCP		Link Local	fe80::2e0:4cff:fe00:0	64	Tentative		- 12
✓ Multicast		Global	2001::1f	64	Tentative		
		Multicast	ff02-1		Tornauvo		
 IPv4 Management and Interface 		Multicast	ff011				
 IPv6 Management and Interface 	Ľ.	wuucast	11011				_
IPv6 Interface	-	Add Delete					
IPV6 Addresses							
IP vo Roules							

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.

COMMANDO	Routing » IPv6 Manager	nent and Inter	faces » IPv6	ý Routes		Save Log	sout Reboot De	bug
✓ Status								
V Network								
✓ Port	IPv6 Routing Table							
VLAN						0		
✓ MAC Address Table						Q		-
✓ Spanning Tree	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface	
V Discovery				0 results found.				
V DHCP								_
✓ Multicast	Add Edit	Delete						
✓ Routing								
✓ IPv4 Management and Interfaces								
 IPv6 Management and Interfaces 								
IPv6 Interface								
IPv6 Addresses								
IPv6 Routes								
IPv6 Neighbors								
✓ Security								
V ACL								
✓ QoS								
✓ Diagnostics								
✓ Management								

Fig 11.2.8 Default IPv6 routing table page

COMMANDO	outing » IPv6 N	Ianagement	and Interfaces »	IPv6 Routes	Save	Logout	Reboot	Debug
✓ Status								^
V Network								
v Port	Add IPv6 Static Route							
VLAN								
✓ MAC Address Table	[2001.					
✓ Spanning Tree		ir vo Fleitx	μων ι					
✓ Discovery	IPv6	Prefix Length	48	(0 - 128)				
✓ DHCP	Next Hop Pou	tor ID Addrose	2002					1.1
✓ Multicast	Hext hop Rou	ter in Address	2002aa					
✓ Routing		Metric	1	(1 - 255, default 1)				
 IPv6 Management and Interfaces IPv6 Management and Interfaces IPv6 Interface IPv6 Addresses IPv6 Routes IPv6 Neighbors 	Apply (Close						
✓ Security								
✓ ACL								
✓ Q₀S								
✓ Diagnostics								
✓ Management								

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.

COMMANDO		Save Logout Reboot Debug
Logging Message	Routing » IPv6 Management and Interfaces » IPv6 Neighbors	
 ✓ Port Link Aggregation MAC Address Table 	Clear Neighbor Table	
✓ Network	NA	
✓ Port	[
VLAN	Apply Cancel	
 MAC Address Table 		
 Spanning Tree 	ID-0 Malakhan Tahla	
 Discovery 	IPV6 Neighbor ladie	
✓ DHCP		
✓ Multicast		4
- Routing	Interface IPv6 Address MAC Address Status Router	
✓ IPv4 Management and Interface	0 results found.	
∧ IPv6 Management and Interface IPv6 Interface IPv6 Addresses	Add Edit Delete	
IPv6 Routes		
IPv6 Neighbors		

Fig 11.2.11 Default IPv6 neighbor page

Status Network VLAN VLAN Management and Interfaces ≫ IPv6 Neighbors Add Heighbor Add Heighbor ULAN Interface VLAN Interface VLAN Interface VLAN Interface IP Address 2002::1c Interface
V Status Network Port VLAN VLAN VLAN Spanning Tree Interface VLAN 1 VLAN Interface VLAN 1 VLAN Interface VLAN 1 VLAN Interface Interface VLAN Interface Interface VLAN Interface Interface VLAN Interface Inter
V Network Vort VLAN VLAN VLAN VLAN Discovery Discovery Discovery
Y Port VLAN VLAN VLAN VAC Address Table Interface VLAN In
 VLAN MAC Address Table Spanning Tree Discovery IP Address
 MAC Address Table Spanning Tree Discovery DHCP
Spanning Tree IP Address 2002::1c
V Discovery 2002::1c 2002::1c
MAC Address AA:BB:CC:11:22:33
V Multicast
Routing Apply Clase
V IPv4 Management and Interface
→ IPv6 Management and Interface
IP-6 Interface
IP-0 Audresses
IPv6 Neighbors

Fig 11.2.12 Add IPv6 neighbor page

Chapter 12 Security

Group Header:- Security

After clicking **Security** 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**

COMMANDO	Security » RADIUS			Save	Logout	Reboot	Debug
✓ Status ^							^
✓ Network	Use Default Parameter						
✓ Port	Detroi D	(4 40 4-5-010)					
VLAN	Retry 3	Retry 3 (1 - 10, default 3)					
 MAC Address Table 	Timeout 3	Timeout 3 Sec (1 - 30, default 3)					
 Spanning Tree 							
✓ Discovery	Key String						
✓ DHCP							
✓ Multicast	Apply						
✓ Routing							
✓ Security	RADIUS Table						
RADIUS TACACS+	Showing All ventries	Showing 0 to 0 of 0 entries			Q		
AAA Authentication Manager	Server Address Server	Port Priority Retry Timeout	Usage				
 ✓ Authentication Manager ✓ DoS 			0 results found.				
Dynamic ARP Inspection DHCP Snooping IR Source Guard	Add Edit	Delete			First Previous	s 1 Next	Last

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.



Security » RADIUS

* otatuo			
✓ Network			
✓ Port	Add RADIUS Server		
VLAN			
 MAC Address Table 	[]	O !!!!	
 Spanning Tree 	Address Type	Hostname Pv4	
 Discovery 		O IPv6	
✓ DHCP			
∽ Multicast	Server Address	192.168.0.50	
✓ Routing	Server Port	1812	(0 - 65535, default 1812)
 Security 		-	
RADIUS	Priority	2	(0 - 65535)
TACACS+ V AAA V Authentication Manager V DoS	Key String	 ✓ Use Default ✓ Use Default 	
Dynamic ARP inspection DHCP Snooping IP Source Guard	Retry	3	(1 - 10, default 3)
V ACL		🗸 Use Default	
✓ QoS	Timeout	3	Sec (1 - 30. default 3)
 Diagnostics 			
✓ Management	Usage	 ○ Login ○ 802.1X ● All 	
	Apply Close		

Fig 11.1.2 Add RADIUS server page

COMMANDO				Save Logout	Reboot Debug
✓ Status	Security » RADIUS				^
✓ Network	Lise Default Parameter				
✓ Port					
VLAN	Retry 3	(1 - 10, default 3))		
 MAC Address Table 	Timeout 3	Sec (1 - 30, defa	ult 3)		
 Spanning Tree 					
 Discovery 	Key String				
✓ DHCP					
✓ Multicast	Apply				
✓ Routing					
✓ Security	RADIUS Table				
RADIUS TACACS+	Showing All ventries	Showin	g 1 to 1 of 1 entries	Q	
	Server Address Server	Port Priority Retry	Timeout Usage		
 Authentication Manager > DoS 	192.168.0.50	1812 2 3	3 All		
Dynamic ARP Inspection DHCP Snooping	Add Edit	Delete		First Previou	is 1 Next Last

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.

		•	
COMMANDO	security » TACACS+		Save Logout Reboot Debug
✓ Status ^			
V Network	Use Default Parameter		
✓ Port			
VLAN	Timeout	Sec (1 - 30, default 5)	
V MAC Address Table	Key String		
✓ Spanning Tree	L		i
✓ Discovery	Apply		
V DHCP			
✓ Multicast	TACACS+ Table		
✓ Routing	IACACST Table		
✓ Security	Showing All ventries	Showing 0 to 0 of 0 entries	0
RADIUS			8
TACACS+	Server Address Server P	ort Priority Timeout	
✓ AAA		0 results found.	
 Authentication Manager Dec 	Add Edit	Delete	First Previous 1 Next Last
✓ DOS ✓ Dynamic ARP Inspection		Delete	
 DHCP Snooping 			
✓ IP Source Guard			

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.

COMMANDO	curity » TACAC	S+	
✓ Status			
V Network			
✓ Port	Add TACACS+ Server		
VLAN			
✓ MAC Address Table		 Hostname 	
✓ Spanning Tree	Address Type	IPv4	
✓ Discovery		⊖ IPv6	
✓ DHCP	Server Address	192.168.1.100	
✓ Multicast		4.0	
✓ Routing	Server Port	49	(0 - 65535, detault 49)
✓ Security	Priority	1	(0 - 65535)
RADIUS			
TACACS+	Key String		
✓ AAA Authortication Manager	, ,		
		Use Default	
 Dynamic ARP Inspection 	Timeout		
✓ DHCP Snooping		5	Sec (1 - 30, default 5)
✓ IP Source Guard			
✓ ACL	Apply Clos	se	
✓ QoS			

Fig 12.2.2 Add TACACS+ server page

COMMANDO	Security » TACACS+	Save Logout Reboot Debug
✓ Status ^		
✓ Network	Use Default Parameter	
✓ Port		
VLAN	sec (1 - 30, default 5)	
✓ MAC Address Table	Key String	
✓ Spanning Tree	L	i
✓ Discovery	Apply	
V DHCP		
✓ Multicast	TACACS+ Table	
✓ Routing		
✓ Security	Showing All ventries Showing 1 to 1 of 1 entries	0
RADIUS		~
TACACS+	Server Address Server Port Priority Timeout	
	192.168.1.100 49 1 5	
Authentication Manager Dos	Add Fdit Delete	First Previous 1 Next Last
Dos D		
✓ DHCP Snooping		
✓ IP Source Guard		

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.



12.3.1 AAA Method List

AAA stands for authentication, authorization, and accounting. AAA is a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. AAA provides authentication, authorization, and accounting functions for users, preventing unauthorized users from logging in to a switch and improving system security. AAA Method Lists can be used to assign a list of methods for Authentication, Authorization, Accounting. Methods Lists can be used to specify the order. If authentication service is not available or was not successful from the first method, second method can be used and so on.

To view and configure AAA Method List , click Security >> AAA >> Method List.

COMMANDO	Security »	AAA » M	lethod List	Save Logout Reboot Debug
✓ Multicast ^				
✓ Routing	Mathad	et Teble		
✓ Security	method L	St Table		
RADIUS TACACS+	Showing All	 entries 	Showing 1 to 1 of 1 entries	Q
AAA	Name	Sequence		
Method List	defaul	(1) Local		
Login Authentication Authentication Manager DoS Dynamic ARP Inspection DHCP Snooping IP Source Guard	Add	Edit	Delete	First Previous 1 Next Last

Fig 12.3.2 Default AAA Method List table page



Security » AAA » Method List

✓ Status	
✓ Network	
✓ Port	Add Method List
VLAN	
✓ MAC Address Table	
✓ Spanning Tree	Name COMMANDO
✓ Discovery	
	○ None
✓ Multicast	Method 1 O Local
	Q Enable
	RADIUS
• security	
RADIUS TACACS+ AAA Method List Login Authentication Authentication Manager DoS Dynamic ARP Inspection DHCP Snooping IP Source Guard ACL	Method 2 Empty None Local RADIUS TACACS+ Method 3 Empty None Local Enable RADIUS RADIUS
V dos	O TACACS+
 ✓ Diagnostics ✓ Management 	Method 4 Empty None Local Enable RADIUS TACACS+

Fig 12.3.3 Edit AAA Method List page

COMMANDO	Security » AAA » Method List	Save Logout Reboot Debug
✓ Multicast ^		
✓ Routing		
✓ Security	Method List lable	
RADIUS	Showing All ventries Showing 1 to 2 of 2 entries	0
TACACS+		4
~ AAA	Name Sequence	
Method List	default (1) Local	
Login Authentication	(1) RADIUS	
 Authentication Manager DoS 	(2) TACACS+	
 Dynamic ARP Inspection 	COMMANDO (3) Enable	
✓ DHCP Snooping	(4) Local	
✓ IP Source Guard		First Previous 1 Next Last
✓ ACL	Add Edit Delete	
✓ QoS		
✓ Diagnostics		
✓ Management		

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.

COMMANDO		Save Logout Reboot Debug
S	ecurity » 🗛	AA » Login Authentication
✓ Multicast ^		
✓ Routing	Console	default v (1) Local
RADIUS	Telnet	default v (1) Local
TACACS+	SSH	default v (1) Local
Method List	нттр	default (1) Local
Login Authentication ✓ Authentication Manager	HTTPS	default 🖂 (1) Local
 DoS Dynamic ARP Inspection DHCP Snooping IP Source Guard ACL QoS Diagnostics Management 	Apply	

Fig 12.3.5 AAA Login Authentication page

		Save	Logout Reboot Debug
Sec	urity » A	AA » Login Authentication	
✓ Multicast ^			
✓ Routing	Console	default (1) Local	
✓ Security	Console		
RADIUS	Telnet	default v (1) Local	
TACACS+ AAA Method List Login Authentication	SSH	(1) RADIUS (2) TACACS+ (3) Enable (4) Local	
 Authentication Manager 	HTTP	default (1) Local	
DoS Dynamic ARP Inspection DHCP Snooping IP Source Guard	HTTPS	(1) RADIUS (2) TACACS+ (3) Enable (4) Local	
✓ ACL			
✓ QoS	Apply		
✓ Diagnostics			
V Management			

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.

COMMANDO	Se	curi	ty »	Authe	ntication	Manager	» Propert	y					Save Logout Reboot	Debug
VLAN	^	_												^
 MAC Address Table 		[·····				802 1x								
 Spanning Tree 														
 Discovery 	11			Authent	ication Type	мас-ва	sed							
✓ DHCP		I				WEB-Ba	ased							
✓ Multicast						Enable								
✓ Routing					Guest VLAN									
 Security 														
RADIUS			MAC-Ba	ased Use	er ID Format	XXXXXXXXXX	XXXX 🗸							
TACACS+		L									<u>.</u>			
✓ AAA		A	pply											
 Authentication Manager 														
Property		Dent	Mada	Table										
Port Setting		Pon	wode	able										
MAC-Based Local Account														_
Sessions		_	_										4	_
✓ DoS			Entry	Dort	A	uthentication	Туре	Heat Made	Order	Mathod	Guest VII AN	VI AN Assign Mode		
 Dynamic ARP Inspection 			cituy	Port	802.1x	MAC-Based	WEB-Based	HOSE MODE	Order	Methou	GUEST VLAN	VLAN ASSIGN MODE		
 DHCP Snooping 			1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static		
✓ IP Source Guard			2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static		
✓ ACL			3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static		
✓ Q0S			4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static		
 Diagnostics 			5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802 1x	RADIUS	Disabled	Static		
✓ Management	~			050	Dischied	Disabled	Disabled	Manapie / autentication	000.4.	DADINO	Disabled	Otatic Otatic		~

Fig 12.4.1 Default Authentication Manager Port Mode Table page

COMMANDO																	
													Save	Logout	Reboot	Debu	g
	Se	curi	ty »	Authe	ntication	Manager	» Propert	y									
VLAN ^	1.1										-						^
 MAC Address Table 		1				802 1x					1						
✓ Spanning Tree																	
✓ Discovery				Aument	ication Type	мас-ва	sea										
V DHCP		1				🗧 WEB-Ba	ased										
✓ Multicast						Enable											
✓ Routing					Guest VLAN	1											
✓ Security						*											
RADIUS		1	MAC-Ba	ased Use	er ID Format	30000.30000.300	ox 🗸										
TACACS+	1.1					JL					·]						
✓ AAA		A	pply														
 Authentication Manager 																	
Property		Port	Mode	Table													
Port Setting		FUIL	woue	able													
WEB-Based Local Account																	
Sessions	1.1													4		_	
✓ DoS			Entry	Port	4	uthentication	Туре	Host Mode	Order	Method	Guest VI AN	VI AN Assign Mode					
 Dynamic ARP Inspection 			ency.		802.1x	MAC-Based	WEB-Based	nostmout	Graci	u	Sacat VLAN	Com Assign Mode					
✓ DHCP Snooping			1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static					
 IP Source Guard 			2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static					
✓ ACL			3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static					
V QoS			4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static					
✓ Diagnostics			5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802 1x	RADIUS	Disabled	Static					
✓ Management			5	020	0.000160	0.000160	Disabled.	indiapro / adrenitedatori	002.14		Disabled	otatio					~

Fig 12.4.2 Authentication Manager Selecting Ports page

COMMANDO		
	Security » Authenticati	on Manager » Property
✓ Status		
V Network	Edit Port Mode	
V Port		
V VLAN	P	
V MAC Address Table	Port	GE2-GE4
✓ Spanning Tree		✓ 802.1x
✓ Discovery	Authentication Type	MAC-Based
✓ Multicast		U WEB-Based
✓ Routing		Multiple Authentication
▼ Security	Host Mode	O Multiple Hosts
RADIUS		Single Host
TACACS+		
~ AAA		Available Type Select Type
 Authentication Manager 		WEB-Baser A S 802.1x A
Property	Order	MAC-Baser
Port Setting		
WEB-Based Local Account		
Sessions		
✓ DoS		Available Method Select Method
 Dynamic ARP Inspection 		Local 🔨 💦 RADIUS 🔨
✓ DHCP Snooping	Method	
✓ IP Source Guard		
✓ ACL		
	Guest VLAN	Enable
✓ Diagnostics		
Management	VI AN Assign Mode	
	VLAN Assign Mode	
	L	
	Apply Close	
	Cide Cide	

Fig 12.4.3 Authentication Manager Property edit page

COMMANDO												Save Logou	ıt Reboot Debug		
-	s	ecurit	y≫ ∦	Authen	tication I	Manager »	Property								
			·										<u>^</u>		
V VEAN		·····			1r										
MAC Address Table					1	☑ 802.1x									
✓ Spanning Tree			Authentication Type AC-Based												
✓ Discovery					t i										
✓ DHCP		ļ													
✓ Multicast			Guest V AN												
✓ Routing				G	UEST VLAN	1 ~									
✓ Security															
RADIUS		<u> </u> •	MAC-Ba	sed User	ID Format	X000X.X000X.X000X	\sim								
TACACS+															
✓ AAA		Ap	oply												
 Authentication Manager 															
Property		Dent	Mada	Table											
Port Setting		Port	wode	lable											
MAC-Based Local Account															
WED-Based Local Account															
			-			Authentication	Туре								
 Dynamic ARP Inspection 			Entry	Port	802.1x	MAC-Based	WEB-Based	Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode			
✓ DHCP Snooping			1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802 1x	RADIUS	Disabled	Static			
✓ IP Source Guard				CES	Enabled	Enabled	Disabled	Multiple Authentication	802 1x MAC-Based	PADILIS	Disabled	Static			
V ACL			2	OE2	Enabled	Enabled	Disabled	Multiple Authentication	002.1x, MAC-Based	DADILIO	Disabled	Ctatic			
✓ QoS			8	623	Enabled	Enabled	Disabled	multiple Addrentication	auz. IX, MAC-Based	RADIUS	Disabled	Static			
✓ Diagnostics			4	GE4	Enabled	Enabled	Disabled	Multiple Authentication	802.1X, MAC-Based	RADIUS	Disabled	static			
✓ Management			5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static	, v		

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.

COMMANDO													Save	Logout Reboot	Debug
	Secur	ity »	Authe	ntication M	anager » Port S	Setting									
✓ Status															^
V Network															
✓ Port	Por	t Setti	ng Tab	ble											
VLAN														~	_
MAC Address Table	-		_											u l	-
 Spanning Tree 		Entry	Port	Port Control	Reauthentication	Max Hosts	Commo	n Timer			802.1x Par	ameters		Web-Based Parameters	5
 Discovery 		Linuy	Fort	FortControl	Readmentication	Max nosts	Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login	
V DHCP		1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
✓ Multicast		2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
✓ Routing		3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
 Security 		4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
RADIUS		5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
TACACS+		6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
		7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
Authentication Manager		8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
Port Setting		9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
MAC-Based Local Account		10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
WEB-Based Local Account	l H	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
Sessions	H	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
V Duosmic APP Inspection		13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
DHCP Snooping		14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30			3
V IP Source Guard		15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2		3
V ACL		16	OE16	Disabled	Disabled	256	3600	60	60	30	30	30	2		-
✓ Q₀S		10	0010	Disabled	Disabled	200	3600	60	60	30	30	30	2		2
 Diagnostics 		10	0517	Disabled	Disabled	200	3600	60	60	30	30	30	2		2
✓ Management		10	0010	Disabled	Disabled	200	3600	60	60	30	30	30	2		2

Fig 12.4.5 Authentication Manager Property Port Mode Table page

COMMANDO	Secur	ity »	Authe	entication M	anager » Port S	Setting							Save	Logout Reboo	t
atus etwork	Por	t Setti	ng Tak	ble											
ort	_		-												
AC Address Table														Q	
panning Tree			<u> </u>				Commo	n Timer			802.1x Pa	rameters		Web-Based Parame	ete
scovery		Entry	Port	Port Control	Reauthentication	Max Hosts	Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login	1
HCP		1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2		1
ulticast		2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2		
outing		3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2		
ecurity		4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2		
RADIUS		5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2		
TACACS+		6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2		
AAA Authentication Manager		7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2		
Property		8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2		
Port Setting		9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2		
MAC-Based Local Account		10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2		
Sessions		11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2		
DoS		12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2		
Dynamic ARP Inspection		13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2		
DHCP Snooping		14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30	2		
P Source Guard		15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2		
nS		16	GE16	Disabled	Disabled	256	3600	60	60	30	30	30	2		
agnostics		17	GE17	Disabled	Disabled	256	3600	60	60	30	30	30	2		
anagement		18	GE18	Disabled	Disabled	256	3600	60	60	30	30	30	2		
		19	GE19	Disabled	Disabled	256	3600	60	60	30	30	30	2		

Fig 12.4.6 Authentication Manager Property Selecting Port page



✓ Status V Network Edit Port Setting ✓ Port VLAN Port GE1-GE28 MAC Address Table ----- Disabled Spanning Tree Port Control Discovery V DHCP Auto Multicast := # Reauthentication Routing _____ Security Max Hosts 256 (1 - 256, default 256) RADIUS _____ Common Timer TACACS+ ~ AAA Reauthentication 3800 Sec (300 - 2147483647, default 3600) ····· Authentication Manager Inactive 600 Sec (60 - 65535, default 60) Property ----------Port Setting Quiet 600 Sec (0 - 65535, default 60) MAC-Based Local Account 802.1x Parameters WEB-Based Local Account Sessions TX Period 30 Sec (1 - 65535, default 30) ✓ DoS ✓ Dynamic ARP Inspection Supplicant Timeout 30 Sec (1 - 65535, default 30) ✓ DHCP Snooping ----- IP Source Guard Server Timeout 30 Sec (1 - 65535, default 30) ACL Max Request 2 (1 - 10, default 2) ∽ QoS Diagnostics Web-Based Parameters Max Login 3 (3 - 10, default 3) Management _____ Apply Close

Security » Authentication Manager » Port Setting

Fig 12.4.7 Authentication Manager Property edit port setting page

COMMANDO	Secu	rity »	Auth	ontication M	anager » Port	Sotting							Save	Logout Reboot	Det	bug
✓ Status ✓ Network ✓ Port	Port	t Settin	g Tabl	e	anager # 1011	setting										Ŷ
VLAN															~	
V MAC Address Table	_														9	2
✓ Spanning Tree		Entry	Port	Port Control	Reauthentication	Max Hosts	Commo	n Timer			802.1x Par	ameters		Web-Based Parame	ters	
✓ Discovery		Linuy	FUIL	Fort control	Readmentication	max nosts	Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login		
✓ DHCP		1	GE1	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
✓ Multicast		2	GE2	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
✓ Routing		3	GE3	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
 Security 		4	GE4	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
RADIUS		5	GE5	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
TACACS+		6	GE6	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
 AAA Authentication Manager 		7	GE7	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
Property		8	GE8	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
Port Setting		9	GE9	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
MAC-Based Local Account		10	GE10	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
WEB-Based Local Account	In.	11	GE11	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
Sessions V DoS	I ā	12	GE12	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
 Dynamic ARP Inspection 	II.	13	GE13	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
✓ DHCP Snooping	II Ā.	14	GE14	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
✓ IP Source Guard	I n	15	GE15	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
✓ ACL	I n	16	GE16	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
~ QoS		17	GE17	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
✓ Diagnostics	H H	18	GE18	Auto	Enabled	256	3600	600	600	30	30	30	2		3	
✓ Management						050									-	~

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".

COMMANDO	a		Save Logout Reboot Debug
	Security » Authentication Manag	er » MAC-Based Local Account	
✓ Status			
✓ Network	MAG Deced Local Account Table		
∨ Port	MAC-Based Local Account lable		
VLAN	Showing All v entries	Showing 0 to 0 of 0 entries	0
 MAC Address Table 			8
✓ Spanning Tree	MAC Address Control VIAN	Timeout (Sec)	
✓ Discovery		Reauthentication Inactive	
✓ DHCP		0 results found.	
✓ Multicast	A 44 543 Delete	1	First Previous 1 Next Last
✓ Routing	Add Edit Delete		
 Security 			
RADIUS			
TACACS+			
✓ AAA			
Authentication Manager			
Port Setting			
MAC-Based Local Account			
WEB-Based Local Account			
Sessions			
✓ DoS			
 Dynamic ARP Inspection 			
V DRCP Shooping			
✓ QoS			
✓ Diagnostics			
✓ Management			

COMMANDO	ecurity » Authentic	ration Manager »	MAC-Based Local Account	Save Logout Reboot Deb	ug
✓ MAC Address Table					^
✓ Spanning Tree	Add MAC Based Level Asso				
✓ Discovery	Add MAC-Based Local Acco	unt			
✓ DHCP	[l		
✓ Multicast	MAC Address	11:22:33:AA:BB:cc			
✓ Routing		Eoroo Authorized			
▼ Security	Port Control	 Force Unauthorized 			
RADIUS		Ilser Defined			
TACACS+	VLAN	C Oser Denneu			
✓ AAA		2	(1 - 4094)		
 Authentication Manager Property 	Assigned Timer				
Port Setting		User Defined			
MAC-Based Local Account	Reauthentication	0000			
WEB-Based Local Account		3600	Sec (300 - 214/48364/)		
Sessions		User Defined			
✓ DoS	Inactive	60	Sec (60 - 65535)		
Dynamic ARP Inspection			000 (00 00000)		
V DHCP Snooping	Annhu				
	Appiy Close	9			

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

COMMANDO	Security » Authenti	cation Manage	r » M	[AC-Based Local Acco	unt	Save]	Logout Reboot	Debug
✓ Spanning Tree ^								
✓ Discovery	MAC Based Local /	accust Table						
V DHCP	WAG-Dased Local A	iccount lable						
✓ Multicast	Showing All v entries			Showing 1 to 1 of 1 entries			0	
✓ Routing							4	_
✓ Security	MAC Address	Control	VIAN	Timeout (Sec)				- 1
RADIUS		0011101		Reauthentication Inactive				
TACACS+	11:22:33:AA:BB:CC	Force Authorized	2	3600 60				
✓ AAA							First Previous 1 N	ext) (Last)
∧ Authentication Manager	Add Edit	Delete						
Property								
Port Setting								
MAC-Based Local Account								
Sessions								
 Dvnamic ARP Inspection 								
✓ DHCP Snooping								
✓ IP Source Guard								
✓ ACL								
✓ QoS								
✓ Diagnostics								

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.

COMMANDO	Security » Authentication M	anager » WEB-Based Local Account	Save Logout Reboot Debug
✓ Spanning Tree ^			
 Discovery 	WER Record Local Account 1	Fable	
✓ DHCP	WEB-Based Local Account	lable	
 Multicast 	Showing All v entries	Showing 0 to 0 of 0 entries	0
✓ Routing			~
- Security	Username VLAN	imeout (Sec)	
RADIUS	Reauthe	ntication Inactive	
TACACS+		0 results found.	
	Add Edit D	Delete	First Previous 1 Next Last
Authentication Manager			
Port Setting			
MAC-Based Local Account			
WEB-Based Local Account			
Sessions			
✓ DoS			
 Dynamic ARP Inspection 			
DHCP Snooping			
 ACI 			
V ACL			
 Diagnostics 			
 Diagnostics 			

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".

COMMANDO				Save Logout	Reboot Debu
Securi	ty » Authentics	ntion Manager » Y	WEB-Based Local Account		
✓ Spanning Tree ^					
✓ Discovery	WEB-Based Local Accour	11			7
✓ DHCP					
✓ Multicast	Username	COMMANDO			
✓ Routing	. .				
- Security	Password	•••••			
RADIUS	Confirm Password	•••••			
TACACS+		🔽 Ilser Defined			
✓ AAA	VLAN				
Authentication Manager		2	(1 - 4094)		
Property Port Setting	ssigned Timer				
MAC-Based Local Account		🗹 User Defined			
WEB-Based Local Account Sessions	Reauthentication	3600	Sec (300 - 2147483647)		
✓ DoS		User Defined			
 Dynamic ARP Inspection 	Inactive		0, (00, 05505)		
✓ DHCP Snooping		pu	Sec (00 - 00000)		
✓ IP Source Guard					
▼ ACL	Apply Close				
✓ Q0S					~
✓ Diagnostics					

Fig 12.4.13 Add WEB-Based Local Account page

COMMANDO	Security » Authentication N	fanager » WEB-Based Local Account	Save Logout Reboot Debug
✓ Spanning Tree			
V Discovery	WEB-Based Local Account	Table	
V Multicast	Showing All 🗸 entries	Showing 1 to 1 of 1 entries	Q
✓ Routing		Timeout (Sec)	
▼ Security	Username VLAN	thentication Inactive	
RADIUS			
IACACS+		3000 00	
 AAA Authentication Manager 	Add Edit	Delete	First Previous 1 Next Last
Pronerty			
Port Setting			
MAC-Based Local Account			
WEB-Based Local Account			
Sessions			
∨ DoS			
 Dynamic ARP Inspection 			
✓ DHCP Snooping			
✓ IP Source Guard			
✓ ACL			
∨ QoS			
✓ Diagnostics			

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.

												Sav	re Logo	out Reboot Debug
	Secur	ity » Autl	henti	cation Mana	iger » Sessi	ons								
✓ Spanning Tree ^														
✓ Discovery	S	aiana Tabl	_											
✓ DHCP	Ses	sions labi	e											
 Multicast 	Showin	ng All 🗸 entr	ies			Showin	g 0 to 0 of 0	entries					0	
✓ Routing							1				1		~~	
✓ Security						Operational Information			n		Authorized Information	ion		
RADIUS		Session ID	Port	MAC Address	Current Type	Status	VLAN	Session	Time	Quiet	VLAN	Reauthentication	Timoout	
								0 result	s found	Time		renou	Timeout	
Authentication Manager			_					0 Tesui	is lound.				First	Provinue 1 Next Let
Property Port Setting		Clear	Refres	1									Filst	Previous I (Next) Last
WEB-Based Local Account														
Sessions														
✓ DoS														
✓ Dynamic ARP Inspection														
✓ DHCP Snooping														
V IP Source Guard														
✓ ACL														
 Diagnostics 														

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.

COMMANDO		
s	ecurity » DoS » Proj	perty
✓ Status	POD	Enable
 Network 	+	
V Port	Land	Enable
VLAN	LIDD Blat "	
MAC Address Table		
Spanning Tree	TCP Blat	Enable
 Discovery 	L	L
V DHCP	DMAC = SMAC "	Enable
 Multicast 	binac - amac	
Routing	Null Scan Attack	Enable
- Security		
BADILIS	X-Mas scan Attack	
TACACS+	TCP SYN-FIN Attack	Enable
× AAA	L	
 Authentication Manager 	[
∧ DoS	TCP SYN-RST Attack	Enable
Property	CMP Fragment "	
Port Setting		
 Dynamic ARP inspection 		Enable
 DHCP Snooping 	TCP-SYN	Nieke Server Dark - 1001
 IP Source Guard 		
~ ACL		Enable
~ QoS	TCP Fragment	Alaber Officet - d
 Diagnostics 	L	Note. Oriset = 1
 Management 	r	r - <u></u>
		Enable IPv4
	Ding May Size	
	Fing max alzo	
		512 Byte (0 - 65535, default 512)
	+ + + + + + + + +	
		Enable
	TCP Min Hdr size -	20 Byte (0 - 31 default 20)
		Dive (0 - 01, delauk 20)
		Enable
	IPv6 Min Fragment	;
		1240 Byte (0 - 65535, default 1240)
	p==============	
	Smurf Attack	
		Netmask Length (0 – 32, default 0)
	L	L
	Apply	

Fig 12.5.1 DoS property page

COMMANDO	Secu	rity »	DoS X	> Port S	Save Logout Reboot Debr
VLAN	^				
✓ MAC Address Table	De				
✓ Spanning Tree	10	n setti	ig iab	le	
✓ Discovery					0
✓ DHCP	L e				ч
✓ Multicast		Entry	Port	State	
✓ Routing		1	GE1	Disabled	
- Security		2	GE2	Disabled	
RADIUS		3	GE3	Disabled	
TACACS+		4	GE4	Disabled	
✓ AAA		5	GE5	Disabled	
 Authentication Manager 		6	GE6	Disabled	
A DOS Proportiu		7	GE7	Disabled	
Property Port Setting		8	GE8	Disabled	
 Dynamic ARP Inspection 		9	GE9	Disabled	
✓ DHCP Snooping		10	GE10	Disabled	
✓ IP Source Guard		11	GE11	Disabled	
✓ ACL		12	GE12	Disabled	
∨ QoS		12	GE12	Disabled	
 Diagnostics 		13	GE 13	Disabled	
✓ Management		14	GE14	Disabled	

Fig 12.5.2 Default DoS Port Setting page

COMMANDO	Secur	rity » 🛙	DoS »	Port S	Save Logout Reboot Debug
✓ VLAN	^				۸
✓ MAC Address Table	Po	rt Sattir	ng Tabl	•	
✓ Spanning Tree		ri ocili	ig lab	C	
✓ Discovery					0
∽ DHCP	l e				۳. ۲.
✓ Multicast		Entry	Port	State	
✓ Routing		1	GE1	Disabled	
✓ Security		2	GE2	Disabled	
RADIUS		3	GE3	Disabled	
TACACS+		4	GE4	Disabled	
✓ AAA		5	GE5	Disabled	
 Authentication Manager 		6	GE6	Disabled	
∧ U03 Property		7	GE7	Disabled	
Port Setting		8	GE8	Disabled	
✓ Dynamic ARP Inspection		9	GE9	Disabled	
✓ DHCP Snooping		10	GE10	Disabled	
✓ IP Source Guard		11	GE11	Disabled	
✓ ACL		12	GE12	Disabled	
∨ QoS		13	GE13	Disabled	
✓ Diagnostics		14	GE14	Disabled	
✓ Management					v

Fig 12.5.3 Selecting Port DoS Setting page

COMMANDO	Save Logout 1rity » DoS » Port Setting	Reboot Debug
✓ Multicast ^		^
✓ Routing		
▼ Security	dit Port Setting	
RADIUS TACACS+ V AAA V Authentication Manager	Port GE1-GE28,LAG1-LAG8 State ☑ Enable	
Property Port Setting Dynamic ARP Inspection DHCP Snooping	Appiy Close	
✓ IP Source Guard		
✓ ACL		
✓ QoS		
✓ Diagnostics		
✓ Management		¥

Fig 12.5.4 DoS Port Setting Table after enableing all ports page



Save	Logout	Reboot	Debu

	Seci	ırity »	Do	s » Por	t Setting	
VLAN	^					
 MAC Address Table 	D,	ort Sotti	na 1	able		
 Spanning Tree 		Jit Jetu	ng i	able		
 Discovery 	1 - I					0
/ DHCP	1.0		_			~
 Multicast 	ШH	En En	try	Port	State	
 Routing 			1	GE1	Enabled	
 Security 			2	GE2	Enabled	
RADIUS			3	GE3	Enabled	
TACACS+			4	GE4	Enabled	
✓ AAA			5	GE5	Enabled	
 Authentication Manager 			6	GE6	Enabled	
∧ DoS Property			7	GE7	Enabled	
Port Setting			8	GE8	Enabled	
 Dynamic ARP Inspection 			9	GE9	Enabled	
 DHCP Snooping 			10	GE10	Enabled	
✓ IP Source Guard		1	11	GE11	Enabled	
ACL		-	12	GE12	Enabled	
∕ Q₀S		-	13	GE13	Enabled	
 Diagnostics 		-	14	GE14	Enabled	
Management			14	GL 14	Linabled	

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.

COMMANIO V Status	Sec	curity	×»I	Dynami	ic ARP Ins	spection » Propert	y			Save	Logout	Reboot	Debug	
✓ Network	L F	·	···· y ·											ĺ
✓ Port		S	tate	Enab	le									
VLAN			1	Available	VLAN	Selected VLAN								
 MAC Address Table 			1	VLAN 1	~									
 Spanning Tree 				VLAN 2										
✓ Discovery		V	LAN	VLAN 3										
V DHCP														
✓ Multicast														
✓ Routing			1		~	v								ľ
▼ Security	Į L	·	å.					i						
RADIUS	ſ	Ap	ply											
TACACS+														
✓ AAA		1 + 0		a Tabla										
 Authentication Manager Dec 		-οπ 8	eπn	g lable										
 Dus Dynamic ARP Inspection 											0		_	
Property		_	_							 	G I		_	
Statistics			Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit					
✓ DHCP Snooping			1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited					
✓ IP Source Guard			2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited					
✓ ACL			3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited					
∨ QoS			4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited					
 Diagnostics 			5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited					
✓ Management		_	6	QE6	Disphad	Displad	Disabled	Disphlad	Unlimited					ł.

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

COMMANDO	Sec	urity	y »	Dynar	nic ARP	Inspection » Pro	perty			Save Logout Reboot De	ebug
✓ Status											^
✓ Network	LE										
∨ Port		5	tate		adie						
VLAN			1	Availab	le VLAN	Selected VLAN					
 MAC Address Table 			1	VLAN	1 ^	VLAN 2 A					
✓ Spanning Tree			1	VLAN	3						
 Discovery 		V	LAN	VLAN	10						
✓ DHCP			1								
 Multicast 											
✓ Routing			1		~	v					
 Security 	L L								i		
RADIUS	ſ	Ap	ply								
TACACS+											
✓ AAA											
 Authentication Manager 		ort s	settir	ng lab	e						
✓ D0S A Dynamic APP Inspection										0	-
Property		_		_						ų į	
Statistics	LE	2 E	Intry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit		
✓ DHCP Snooping			1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited		
✓ IP Source Guard			2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited		
✓ ACL			3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited		
✓ QoS		_ _	4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited		1
 Diagnostics 			5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited		
✓ Management ✓			6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited		v

Fig 12.6.3 Dynamic ARP Inspection (DAI) port selection page

COMMANDO			6 I I	- Debert - Deber
			Save Logout	Reboot Debug
Se	curity » Dynamic ARP I	nspection » Property		
✓ Spanning Tree ∧				^
 Discovery 				
✓ DHCP	Edit Port Setting			
✓ Multicast				
✓ Routing	Port	GE1-GE28 AG1- AG8		
✓ Security	Truet			
RADIUS	IIUSL			
TACACS+	Source MAC Address	Enable		
✓ AAA	Destination MAC Address	Enable		
Authentication Manager		Enable		
 Dvnamic ARP Inspection 	IP Address	Allow Zero (0.0.0.0)		
Property Statistics	Rate Limit	20 pps (1 - 50, default 0), 0 is Unlimited		
DHCP Snooping	Apply Close			
	(hpp) 003c			
V ACL				

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

COMMANDO								Save Logou	t Reboot Debug
•	Soonnity M	Dynamia	ADD Incno	ation » Property					
∨ Status	Security "	Dynamic	AKF IIIspe	cuon " Property					
						-			^
v Port	State	🗌 Enable							
		Available VI /	AN Sel	ected VI AN		1			
		VLAN 1 VLAN 3		AN 2 A					
	10.41	VLAN 10							
	VLAN								
v Multicast									
V Routing									
✓ Noturity		1 1 1	×	V					
PADILIS									
TACACS+	Apply								
V AAA									
✓ Authentication Manager	Port Set	ting Table							
∨ DoS									
 Dynamic ARP Inspection 								Q	
Property	E F	ntry Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit		
STATISTICS		1 GE1	Enabled	Enabled	Enabled	Disabled	20		
 IP Source Guard 		2 052	Enabled	Enabled	Enabled	Disabled	20		
✓ ACL		2 GE2	Enabled	Enabled	Enabled	Disabled	20		
✓ QoS		3 GE3	Enabled	Enabled	Enabled	Disabled	20		
 Diagnostics 		4 GE4	Enabled	Enabled	Enabled	Disabled	20		
✓ Management		5 GE5	Enabled	Enabled	Enabled	Disabled	20		
V		6 GE6	Enabled	Enabled	Enabled	Disabled	20		v

Fig 12.6.5 DAI Port Setting Table page after enabling ports page

12.6.2 Dynamic ARP Inspection (DAI) Statistics

This page allow user to browse all statistics that recorded by Dynamic ARP Inspection function. Displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with DAI enabled (active).

To view Dynamic ARP Inspection Statistics , click Security >> Dynamic ARP Inspection >> Statistics.

COMMANDO	Securi	ty »	Dynai	nic ARP	Inspection	» Statistics			Save Logout	Reboot Debuş
Spanning Tree										
Discovery										
DHCP	Stat	istics	Table							
Multicast									0	
Routing	_								Q	
Security		Friday	Dent	Ferryard	Source MAC	Destination MAC	Source IP	Destination IP	IP-MAC	
RADIUS		Entry	For	Forwaru	Failure	Failure	Validation Failure	Validation Failure	Mismatch Failure	
TACACS+		1	GE1	0	0	0	0	0	0	
✓ AAA		2	GE2	0	0	0	0	0	0	
 Authentication Manager 		3	GE3	0	0	0	0	0	0	
✓ DoS		4	GE4	0	0	0	0	0	0	
Dynamic ARP inspection		5	CES	0	0	ů	ů	0	0	
Statistics		5	GEG	0	0	0	0	0	0	
 DHCP Snooping 		6	GEb	U	0	U	0	U	U	
/ IP Source Guard		7	GE7	0	0	0	0	0	0	
ACL		8	GE8	0	0	0	0	0	0	
QoS		9	GE9	0	0	0	0	0	0	
Diagnostics		10	GE10	0	0	0	0	0	0	

Fig 12.6.7 Dynamic ARP Inspection (DAI) Statistics Table page

12.7 DHCP Snooping

DHCP Snooping is a layer 2 security technology incorporated into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. DHCP Snooping prevents unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. This page allow user to configure global and per interface settings of DHCP Snooping.



Fig 12.7.1 DHCP Snooping Concept

12.8.1 DHCP Snooping Property

DHCP snooping provides a security mechanism to prevent receiving false DHCP response packets and to log DHCP addresses. It does this by treating ports on the device as either trusted or untrusted. A trusted port is a port that is connected to a DHCP server and is allowed to assign DHCP addresses. DHCP messages received on trusted ports are allowed to pass through the device.

An untrusted port is a port that is not allowed to assign DHCP addresses. By default, all ports are considered untrusted until you declare them trusted.

To view and configure DHCP Snooping, click Security >> DHCP Snooping >> Property.



Fig 12.8.1 Default DHCP Snooping Port setting Table page

COMMANDO	urity » DHCP Suganing » Property	Save Logout Reboot Debuş
Vision dates faile Sagning Tree Discovery Dircovery Dircovery Multicast Multicast Rouling Security RADIUS TACACS+ AAA Authentication Manager ObS Oynamic ARP Inspection DirCP Snopping Property Statistics	State Enable Available VLAN VLAN VLAN VLAN Apply ort Setting Table	
Option82 Property Option82 Circuit ID		Q
✓ ACL	Image: Construct of the state of t	
 ✓ QoS ✓ Diagnostics ✓ Management 	2 2 GE2 Disabled Disabled Unlimited 3 GE3 Disabled Disabled Unlimited	

Fig 12.8.2 DHCP Snooping for selected Port setting page

COMMANDO	Save Logout Reboot Debug Security » DHCP Snooping » Property	ŗ
RADIUS TACACS+ V AAA V Authentication Manager	Edit Port Setting	^
 Dynamic ARP Inspection 	Port GE1-GE28,LAG1-LAG8	
∧ DHCP Snooping	Trust 🛛 Enable	
Property Statistics	Verify Chaddr 🛛 Enable	
Option82 Property Option82 Circuit ID	Rate Limit 20 pps (1 - 300, default 0), 0 is Unlimited	
 ✓ IP Source Guard ✓ ACL ✓ QoS ✓ Diagnostics 	Apply Close	*

Fig 12.8.3 Created VLAN DHCP Snooping State page

COMMANDO	Security »	DHCP Snooping	» Property			Save Logout Reboot Debug
✓ Port ^						^
✓ VLAN	State	- Enable				
 MAC Address Table 	State					
 Spanning Tree 		Available VLAN	Selected VLAN			
✓ Discovery		VLAN 2 A	VLAN 1 🔥			
✓ DHCP			VLAN 3			
✓ Multicast	VLAN		VENU IO			
✓ Routing						
Security RADIUS TACACS+ AAA Authentication Manager DoS Vnamic ARP Inspection	Apply Port Setti	ng Table	v			
∧ DHCP Snooping						
Property						Q
Statistics		Entry Port	Trust	Verify Chaddr	Rate Limit	
Option82 Property Option82 Circuit ID		1 GE1	Enabled	Enabled	20	
V IP Source Guard		2 GE2	Enabled	Enabled	20	
V ACL		2 052	Enabled	Enabled	20	
√ QoS		3 GE3	Enabled	Enabled	20	
✓ Diagnostics		4 GE4	Enabled	Enabled	20	
✓ Management		5 GE5	Enabled	Enabled	20	
		n GH6	Enabled	Enabled	20	

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**.

COMMANDO										Save	Logout	Reboot	Debug
	Se	curi	ty »	DHCI	° Snoopi	ng » Statisti	cs						
 Spanning Tree 	^												^
 Discovery 		Stati	istics	Table									
V DHCP													
∽ Multicast											Q		
✓ Routing	1.1							Untrust Port]			
- Security			Entry	Port	Forward	Chaddr Check	Untrust Port	with Option82	Invalid				- 11
RADIUS						Drop	Drop	Drop	Drop				- 11
TACACS+			1	GE1	0	0	0	. 0	0				
 AAA Authentication Manager 			2	GE2	0	0	0	0	0				
 Authentication manager > DoS 			3	GE3	0	0	0	0	0				
 Dynamic ARP Inspection 			4	GE4	0	0	0	0	0				
∧ DHCP Snooping			5	GE5	0	0	0	0	0				
Property			6	GE6	0	0	0	0	0				
Statistics			7	GE7	0	0	0	0	0				
Option82 Circuit ID			8	GE8	0	0	0	0	0				
✓ IP Source Guard			q	GE9	0	0	0	0	0				
✓ ACL			10	GE10	0	0	0	0	0				
✓ Q0S			11	GE11	0	0	0	0	0				
✓ Diagnostics			12	GE12	0	0	0	0	0				
✓ Management	~		12	CE12	0	0	0	0	0				~

Fig 12.8.5 DHCP Snooping statistics Table page

12.8.3 Option82 Property

Option 82 (DHCP Relay Agent Information Option) passes port and agent information to a central DHCP server, indicating where an assigned IP address physically connects to the network.

The main goal of option 82 is to help to the DHCP server select the best IP subnet (network pool) from which to obtain an IP address. This DHCP Snooping Option82 allow user to set string of DHCP option82 remote ID filed. The string will attach in option82.

To view and configure DHCP Snooping Option82 Property, click Security >> DHCP Snooping >> Option82 Property.

COMMANDO	cur	ity »	DHCI	2 Snoodi	ng » Optior	182 Property	Save	Logout	: Reboot	Debug
		5		-	<u> </u>	I J				^
✓ Spanning Tree	· · · · ·		· · · · · · · · · · ·							
✓ Discovery				User Defin	ed					
V DHCP		Remote								
✓ Multicast	i		i							
✓ Routing	0	peration	al Stati	19						
- Security		Description				- Dute Order)				
RADIUS	l	Remote		J:e0:4c:00:0	J:00 (Switch Mac I	n Byte Order)				
TACACS+	_									
× AAA	-	Apply	J							
 Authentication Manager 										
✓ DoS	Por	Settir	g Tab	le						
 Dynamic ARP Inspection 			.g .u							
∧ DHCP Snooping								0		
Property								4		_
Statistics		Entry	Port	State	Allow Untrust					
Option82 Property		1	GE1	Disabled	Drop					
Option82 Circuit ID		2	GE2	Disabled	Drop					
✓ IP Source Guard		3	GE3	Disabled	Drop					
V ACL		4	GE4	Disabled	Drop					v

Fig 12.8.6 Default DHCP Snooping Option82 Port setting table page

COMMANDO	Securi	ty »]	DHCI	? Snoopi	ng » Option	182 Property	Save	Logout	Reboot	Debug		
Spanning Tree		Remote		User Defir	ned					^		
	ł											
 Multicast 	Operational Status											
✓ Routing		Remote	ID 00);e0:4c:00:0								
✓ Security	i					i]						
RADIUS TACACS+ V AAA V Authentication Manager V DoS	A Port	pply Settin	g Tab	le								
 Dynamic ARP Inspection 								Q				
∧ DHCP Snooping		Entry	Port	State	Allow Untrust							
Property		1	GE1	Disabled	Drop							
Statistics		2	GE2	Disabled	Drop							
Option82 Circuit ID		2	OE2	Disabled	Drop							
✓ IP Source Guard		3	GE3	Disabled	Drop							
	\leq	4	GE4	Disabled	Drop							
COMMANDO	Save Logout Reboot Debug											
---	--------------------------------											
Security » DHCP Snooping » Option82 Property												
Security RADIUS TACACS+ AA Edit Port Setting												
Authentication Manager Port GE1-GE28,LAG1-LAG8												
✓ DoS ✓ Dynamic ARP Inspection State ☑ Enable												
∧ DHCP Snooping ○ Keep Property Allow Untrust ○ Drop Statistics ◎ Replace												
Option82 Property Option82 Circuit ID ✓ IP Source Guard												
 ✓ ACL ✓ QoS ✓ Diagnostics 												
✓ Management ✓	~											

Fig 12.8.7 DHCP Snooping Option82 Port Selecting Ports page

Fig 12.8.8 DHCP Snooping Option82 Edit Port Setting page

COMMANDO							Save Logout Reboot Debug
	Securi	ity » DI	HCP Sn	ooping » (Option82 Prope	rty	
	`		_				· · · · · · · · · · · · · · · · · · ·
 Spanning free 				vr Dofinad			
✓ Discovery		Remote ID	036	a Denneu			
			00:e0:4	c:00:00:00			
✓ Multicast							
✓ Routing	Op	perational	Status				
 Security 		Remote ID	00:e0:4	c:00:00:00			
RADIUS	i					······	
TACACS+	A	Apply					
✓ AAA		46.7					
 Authentication Manager 							
✓ U0S X Duramia ADD Inspection	Port	Setting	Table				
Dynamic ARP inspection DHCP Snooping							
Property							Q
Statistics		Entry	Port	State	Allow Untrust		
Option82 Property		1	GE1	Enabled	Replace		
Option82 Circuit ID		2	GE2	Enabled	Poplace		
✓ IP Source Guard		2	002	Enabled	Deplace		
✓ ACL		3	GES	Enabled	Replace		
∨ QoS		4	GE4	Enabled	Replace		
✓ Diagnostics		5	GE5	Enabled	Replace		
✓ Management		6	GE6	Enabled	Replace		

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

12.8.4 Option82 Circuit ID

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

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

COMMANDO	Security » DHCP Snoopi	ng » Option82 Circuit ID	Save Logout Reboot Debug
✓ Security			
RADIUS	Option82 Circuit ID Table	•	
 ✓ AAA ✓ Authentication Manager 	Showing All v entries	Showing 0 to 0 of 0 entries	Q
✓ DoS	Dert VLAN Circuit ID		
 Dynamic ARP Inspection DHCP Specification 		0 results found.	
Property Statistics Option82 Property Option82 Circuit ID ✓ IP Source Guard	Add Edit	Delete	(First) (Previous) 1 (Next) (Last)
✓ ACL			
✓ QoS			
Management			

Fig 12.8.10 DHCP Snooping Option82 Circuit ID Table page

COMMANDO	curity » DHCP Snoopin	ng » Option82 Circuit ID	Save Logout	Reboot Debug
✓ Security RADIUS				
TACACS+	Add Option82 Circuit ID			
 ✓ AAA ✓ Authentication Manager 	P. d DEA			
✓ DoS	Ροπ GE6 <u></u>			
Dynamic ARP Inspection	VLAN 2	(1 - 4094) (Keep empty to set without VLAN)		
Property	Circuit ID 123456			
Statistics Option82 Property Option82 Circuit ID V IP Source Guard V ACL V QoS V Diagnostics	Apply Close			
✓ Management				

Fig 12.8.11 DHCP Snooping Add Option82 Circuit ID page

COMMANDO	Security » DHCP Snooping	g » Option82 Circuit ID	Save Logout Reboot Debug
✓ Security RADIUS TACACS+	Option82 Circuit ID Table		
✓ AAA ✓ Authentication Manager	Showing All ventries	Showing 1 to 1 of 1 entries	Q
 DoS Dynamic ARP Inspection 	□ Port VLAN Circuit ID □ GE6 2 123456		
 DHCP Snooping Property Statistics 	Add Edit	Delete	First Previous 1 (Next) (Last)
Option82 Property Option82 Circuit ID VIP Source Guard			
✓ ACL			
✓ QoS			
 ✓ Diagnostics ✓ Management 			

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.

COMMANDO	ecur	ity »	IP Sou	irce Gua	rd » Port S	Setting		Save Logout Reboot Del	ug
✓ Security ^	Por	t Settir	ng Tabl	е					^
RADIUS TACACS+								Q	
 Authentication Manager 		Entry	Port	State	Verify Source	Current Entry	Max Entry		
✓ DoS		1	GE1	Disabled	IP	0	Unlimited		
 Dynamic ARP Inspection 		2	GE2	Disabled	IP	0	Unlimited		
DHCP Snooping		3	GE3	Disabled	IP	0	Unlimited		
Property		4	GE4	Disabled	IP	0	Unlimited		
Option82 Property		5	GE5	Disabled	IP	0	Unlimited		
Option82 Circuit ID		6	GE6	Disabled	IP	0	Unlimited		
▲ IP Source Guard		7	GE7	Disabled	IP	0	Unlimited		
Port Setting		8	GF8	Disabled	IP	0	Unlimited		
IMPV Binding		0	GEQ	Disabled	IP.	0	Unlimited		
Save Database		10	GE10	Disabled	IP	0	Unlimited		
		11	GE11	Disabled	IP	0	Unlimited		

Fig 12.9.2 IP source guard default Port Setting table page

COMMANDO	ecur	ity » :	IP Sou	irce Gua	rd » Port S	Setting		Save Logout R	eboot Debug
✓ Security ^	Por	t Settir	ng Tabl	е					^
RADIUS TACACS+								Q	
 Authentication Manager 		Entry	Port	State	Verify Source	Current Entry	Max Entry		
✓ DoS		1	GE1	Disabled	IP	0	Unlimited		
 Dynamic ARP Inspection 		2	GE2	Disabled	IP	0	Unlimited		
∧ DHCP Snooping		3	GE3	Disabled	IP	0	Unlimited		
Statistics		4	GE4	Disabled	IP	0	Unlimited		
Option82 Property		5	GE5	Disabled	IP	0	Unlimited		
Option82 Circuit ID		6	GE6	Disabled	IP	0	Unlimited		
▲ IP Source Guard		7	GE7	Disabled	IP	0	Unlimited		
Port Setting		8	GE8	Disabled	IP	0	Unlimited		
Save Database		9	GE9	Disabled	IP	0	Unlimited		
✓ ACL		10	GE10	Disabled	IP	0	Unlimited		
✓ QoS		11	GE11	Disabled	IP	0	Unlimited		~

Fig 11.9.2 IP source guard Selecting Ports for Setting page

COMMANDO	Save Logout Reboot	Debug
S	ecurity » IP Source Guard » Port Setting	
 ✓ Security ADIUS TACACS+ ✓ AAA 	Edit Port Setting	^
 Authentication Manager DoS 	Port GE1-GE28,LAG1-LAG8	
 Dynamic ARP Inspection 	State 🗹 Enable	
► DHCP Snooping Property Statistics	Verify Source	
Option82 Property Option82 Circuit ID	Max Entry 1 (1 - 50, default 0), 0 is Unlimited	
IP Source Guard Port Setting	Apply Close	
IMPV Binding Save Database		
✓ ACL		
✓ QoS		¥

Fig 12.9.3 Edit IP source guard Ports Setting page

COMMANDO	Secur	ity » 🛙	IP Sou	rce Gu	urd » Port !	Setting		Save Logout Reboot I	Debug
✓ Security ^	Por	t Settir	ng Tabl	е					^
RADIUS TACACS+								0	-
V AAA	-	- (~	-11
 Authentication Manager 		Entry	Port	State	Verify Source	Current Entry	Max Entry		-11
✓ DoS		1	GE1	Enabled	IP-MAC	0	1		
Dynamic ARP Inspection		2	GE2	Enabled	IP-MAC	0	1		
∧ DHCP Shooping		3	GE3	Enabled	IP-MAC	0	1		
Statistics		4	GE4	Enabled	IP-MAC	0	1		
Option82 Property		5	GE5	Enabled	IP-MAC	0	1		
Option82 Circuit ID		6	GE6	Enabled	IP-MAC	0	1		
▲ IP Source Guard		7	GE7	Enabled	IP-MAC	0	1		
Port Setting		, Q	CE9	Enabled		0	1		
IMPV Binding		0	OL0			0	1		
Save Database		9	GE9	Enabled	IP-MAC	0	1		
✓ ACL		10	GE10	Enabled	IP-MAC	0	1		
✓ QoS ✓		11	GE11	Enabled	IP-MAC	0	1		¥

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.

COMMANDO	Security » IP	Source Guard	» IMPV I	Binding			Save Logout Reboot Debug
✓ Security A RADIUS TACACS+ AAA v Authentication Manager	IP-MAC-Port-	VLAN Binding	Table Show	ring 0 to 0 of 0 e	ntries		9
DoS DoS Dynamic ARP Inspection DHCP Snooping	Port VLA	AN MAC Address	IP Address	Binding 0 r	Type results for	Lease Time	
Property Statistics Option82 Property Option82 Circuit ID IP Source Guard Port Setting IMPV Binding Save Database	Add	Edit)elete				First) (Previous) 1 (Next) (Last)
V ACL							

Fig 12.9.5 IP Source Guard Default IMPV Binding Table page

COMMANDO				Save Logout	Reboot	Debug
Sec	curity » IP Sourc	e Guard » I	MPV Binding			
 ✓ Security ADIUS TACACS+ ✓ AAA 	Add IP-MAC-Port-VLAN Bin	ding		 		^
Authentication Manager DoS Dynamic ARP Inspection DHCP Snooping	Port	GE10 🗸 3	(1 - 4094)			
Property Statistics Option82 Property Option82 Circuit ID	Binding MAC Address	 ○ IP-MAC-Port-VL ● IP-Port-VLAN 	AN			
∧ IP Source Guard Port Setting IMPV Binding Save Database	IP Address Apply Clo	192.168.20.1 se	/ 255.255.255.0			
✓ ACL ✓ QoS				 		v

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.

COMMANDO				Save Logout	Reboot Debug
Security ^	ity » IP Soul	rce Guard » Sa	ive Database		
RADIUS TACACS+ V AAA	Туре	○ None○ Flash● TFTP			
 Authentication Manager DoS 	Filename	192.168.0.10			
Dynamic ARP Inspection DHCP Snooping	Address Type	⊖ Hostname● IPv4			
Property Statistics	Server Address	192.168.0.1			
Option82 Property	Write Delay	300	Sec (15 - 86400, default 300)		
 ✓ IP Source Guard Port Setting IMPV Binding Save Database 	Timeout	300	Sec (0 - 86400, default 300)		
✓ ACL ✓ QoS ✓					

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.

COMMANDO			
			Save Logout Reboot Debug
-	ACL » MAC ACL		
 Spanning Tree 	^		
 Discovery 			
✓ DHCP	ACL Name		
✓ Multicast			
✓ Routing	Apply		
✓ Security			
▼ ACL	ACL Table		
MAC ACL			
MAC ACE	Showing All 🖌 entries	Showing 0 to 0 of 0 entries	Q
IPv4 ACL			
IPv4 ACE	ACL Name Rule Port		
IPv6 ACL		0 results found.	
IPv6 ACE			First Previous 1 Next Last
ACL Binding	Delete		
V QoS			
✓ Diagnostics			

Fig 13.1.1 Default MAC ACL Table page

COMMANDO			Save Logout Reboot Debug
	ACL » MAC ACL		
 Spanning Tree 			
 Discovery 	r		
✓ DHCP	ACL Name		
✓ Multicast			
✓ Routing	Apply		
✓ Security			
▼ ACL	ACL Table		
MAC ACL			
MAC ACE	Showing All v entries	Showing 1 to 1 of 1 entries	Q
IPv4 ACL	ACI Namo Rulo Port		
IPv4 ACE			
IPv6 ACL	COMMANDO 0		
IPv6 ACE			First Previous 1 Next Last
ACL Binding	Delete		
✓ QoS			
 Diagnostics 			
✓ Management	× .		

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

COMMANDO										Sav	e Lo	ogout R	eboot	Debug
	ACL	» MAC A	ACE											
✓ Spanning Tree														
✓ Discovery														
✓ DHCP	ACE	Table												
✓ Multicast														
✓ Routing	ACLI	vame COM	MANDO	~										
✓ Security	Showin	ig All 🗸 entr	ies			Showing 0 to 0	of 0 entries					0		
✓ ACL	_											~		_
MAC ACL		Sequence	Action	Source	MAC	Destinatio	on MAC	Ethertype	VLAN	802.1p				
MAC ACE				Address	Mask	Address	Mask			Value	Mask			
IPv4 ACL							0 result	ts found.						
IPv4 ACE	_										F	First Previous	1 Nex	xt Last
IPv6 ACL		Add	Edit	De	elete									
IPv6 ACE														
ACL Binding														
✓ QoS														
✓ Diagnostics														
✓ Management														

Fig 13.2.1 Default MAC ACE page

COMMANDO				
	ACL » MAC ACE			
tatue				
etwork	Add ACE			
ort				
1 AN	ACL Name			
AC Address Table			<u></u>	
	Sequence	10	(1 - 2147483647)	
iscovery		Allow		
HCP	Action	O Deny		
uttionet		🔘 Shutdown		
outing		Any Any		
ecurity	Source MAC		,	(4 ddaeee (10 e-1))
Cl		;; 	/	(Address / Mask)
		🗹 Any		
	Destination MAC	***************************************	/	(Address / Mask)
IPv4 ACL	÷	i 	····	(Address / Index)
IPv4 ACE		🗹 Any		
IPv6 ACL	Ethertype	0x	(0x600 ~ 0xFFFF)	
IPv6 ACE			(
ACL Binding	VIAN	Any		
0S	VLAN	2 (1 - 4094)		
iagnostics				
anagement	802.1p			
		6	17	(Value / Mask) (0 -
	L			

Fig 13.2.2 Add MAC ACE page

COMMANDO	ACL » MAC ACE	Save Logout Reboot Debug
✓ Status		
✓ Network		
✓ Port	ACE lable	
V VLAN	ACL Name COMMANDO	
MAC Address Table		
✓ Spanning Tree	Showing All we entries Showing to 1 of 1 entries	Q
✓ Discovery	Source MAC Destination MAC 9034p	
✓ DHCP	Sequence Action Source which bestimation what Ethertype VLAN 002.19	
✓ Multicast	Address Mask Address Mask Value Mask	
✓ Routing	L 10 Allow Any Any Any Any Any 2 6 /	
✓ Security	Add Edit Delete	First Previous 1 Next Last
▼ ACL		
MAC ACL		
MAC ACE		
IPv4 ACL		
IPv4 ACE		
IPv6 ACL		
ACL Binding		
✓ QoS		
✓ Diagnostics		
✓ Management		

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 $\,$

COMMANDO	ACL » IPv4 ACL		Save Logout Reboot Deb	ug
VLAN ^				
✓ MAC Address Table	ACL Name			
✓ Spanning Tree				
✓ Discovery	Apply			
✓ DHCP	Арру			
✓ Multicast				
✓ Routing	ACL Table			
✓ Security		Showing 0 to 0 of 0 entries	a	
▼ ACL	Showing All v entries		Q	
MAC ACL	ACL Name Rule Port			٦.
MAC ACE		0 results found.		1
IPv4 ACL			First Previous 1 Next Las	5
IPv4 ACE	Delete			
IPv6 ACL	Delete			
IPv6 ACE				
ACL Binding				
✓ QoS				
✓ Diagnostics				
✓ Management				

Fig 13.3.1 Default ACL Table page

COMMANDO	ACL » IPv4 ACL		Save Logout Reboot Debug
✓ VLAN			
 MAC Address Table 		4	
 Spanning Tree 		ч 	
✓ Discovery	Annh		
✓ DHCP	Арріу		
✓ Multicast			
✓ Routing	ACL Table		
✓ Security	A	Chausian 0 to 0 of 0 antrian	
▼ ACL	Showing All Y entries	Showing to to the entries	Q
MAC ACL	ACL Name Rule Port		
MAC ACE		0 results found.	
IPv4 ACL			First Previous 1 Next Last
IPv4 ACE	Delete		
IPV6 ACL			
V Q05			
✓ Diagnostics			
✓ Management			

Fig 13.3.2 Edit IPv4 ACL Name page

COMMANDO				Save	Logout Reboo	t Debug
4	ACL " II VI ACL					
VLAN ^						
 MAC Address Table 						
✓ Spanning Tree						
✓ Discovery						
✓ DHCP	Apply					
✓ Multicast						
✓ Routing	ACL Table					
✓ Security						
▼ ACL	Showing All v entries		Showing 1 to 1 of 1 entries		Q	_
MAC ACL	ACL Name Rule	Port				
MAC ACE	COMMANDO1 0					
IPv4 ACL					Eirst Dravious 1	Next Last
IPv4 ACE	Delete				Previous I	HEAT Last
IPv6 ACL	Delete					
IPv6 ACE						
ACL Binding						
✓ QoS						
 Diagnostics 						
✓ Management						

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

COMMANDO														Save	Logout	Reboot	Debug
	ACL	» IPv4 A	CE														
✓ Status																	
✓ Network		T Table															
✓ Port	AC	E lable															
VLAN	ACL	Name COM	MANDO1	~													
 MAC Address Table 																	
 Spanning Tree 	Show	ing All 🗸 ent	ries				SI	lowing 0 to I	0 of 0 entries						Q		_
 Discovery 		1			Source	ID.	Doctina	ion ID	1	1	1	Tu	no of Somico	ICI			
V DHCP		Sequence	Action	Protocol	Sourc	e IP	Desulta		Source Port	Destination Port	TCP Flags	DECD	D Deservice	Turne	Code		
✓ Multicast					Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code		
✓ Routing									o results found.								
✓ Security		Add	Edit	De	elete										First	vious 1 Ne	oxt Last
▼ ACL																	
MAC ACL																	
MAC ACE																	
IPv4 ACL																	
IPV4 ACE																	
IPv6 ACE																	
ACL Binding																	
~ QoS																	
 Diagnostics 																	
✓ Management																	

Fig 13.4.1 Default IPv4 ACE Table page

COMIMANDO					
	ACL » IPv4 ACE				
	Add ACE				
V Network	_				
V Port					
VLAN	ACL Name	COMMANDO1			
 MAC Address Table 	Sequence	20	(1	- 2147483647)	
 Spanning Tree 					
✓ Discovery	Action	Denv			
✓ DHCP		Shutdown			
✓ Multicast		<u> </u>			
✓ Routing					
✓ Security	Protocol	Select T	CP 🗸		
✓ ACL				(0 255)	
MAC ACL				(0 - 255)	
MAC ACE		Any			
IPv4 ACL	Source IP	102 168 0 100	1	055 055 055 0	(Address (Mask)
IPv4 ACE		132.100.0.100	۹۲. ۱۳		(Address / mask)
IPv6 ACL		🗹 Any			
IPV6 ACE	Destination IP		1		(Address / Mask)
		Any			
	Type of Service	O DSCP		(0 - 63)	
 Management 	Type of service				
		IP Precede	ence	(0	- 7)
	Source Port	Single		(0 - 65535)
		O Range		_	(0, 65535)
		- Mange		-	(0.00000)

Fig 13.4.2 Add IPv4 ACE page

COMMANDO	ACL	» IPv4	AC.	E											Save	Logout	Reboot	Debug
✓ Status																		
∨ Network	100	Table																
∨ Port	AG																	
VLAN	ACL	Name C	DMMA	ND01 🗸														
 MAC Address Table 																		
✓ Spanning Tree	Showin	g All 🗸	entries					Showing 1 to	1 of 1 entries							Q		
✓ Discovery						Sour	rce IP	Destination IP]	Tvn	e of Service	ICMP			_		
✓ DHCP		Seque	nce	Action	Protocol	Address	Address Mask		Maak	Source Port	Destination Port	TCP Flags	DECD	ID Drocodonce	Tune Code			
✓ Multicast			20	Dony	тер	402.469.0.400	200 200 200 0	Anv	Any	A. 94	Anv		Any	IF Frecedence	Type Code			_
✓ Routing		_	20	Deny	TUP	192.100.0.100	200.200.200.0	Any	Any	Any	Any		Any	Any		(7) (200
✓ Security		Add		Edit	Delet	e										First	Previous 1 Ne	ent Last
▼ ACL																		
MAC ACL																		
MAC ACE																		
IPv4 ACL																		
IPv4 ACE																		
IPV6 AUL																		
INVO ACE																		
ACL Binding																		
ACL Binding ✓ QoS																		
ACL Binding V QoS V Diagnostics																		

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

COMMANDO		Save Logout Reboot Debi
	ACL » IPv6 ACL	
✓ Status		
✓ Network		
∨ Port	ACL Name	
VLAN		
✓ MAC Address Table	Apply	
✓ Spanning Tree		
✓ Discovery	ACL Table	
✓ DHCP		
✓ Multicast	Showing All vertries Showing 0 to 0 of 0 entries	Q
✓ Routing		
✓ Security		
✓ ACL	o readita found.	(Test) (Tester) (T. Met) (Test
MAC ACL	Delete	(Final (Fieldulla) (Nett) Last
MAC ACE	Detete	
IPv4 ACL		
IPv4 ACE		
IPV6 ACE		
ACL Binding		
~ QoS		
✓ Diagnostics		
✓ Management		

Fig 13.5.1 Default IPv6 ACL Table page

COMMANDO		Save Logout Reboot Debug
	ACL » IPv6 ACL	
✓ Status		
V Network		
✓ Port	ACL Name COMMANDO2	
VLAN		
 MAC Address Table 	Apply	
 Spanning Tree 		
✓ Discovery	ACL Table	
✓ DHCP		
✓ Multicast	Showing All ventres showing the U or U entries	Q
✓ Routing	ACL Name Rule Port	
✓ Security	0 results found.	
→ ACL		First Previous 1 Next Last
MAC ACL	Delete	
MAC ACE		
IPV4 ACL		
IPv6 ACE		
IPv6 ACE ACL Binding		
IPv6 ACE ACL Binding V QoS		
PV6 ACE ACL Binding V QoS V Diagnostics		

Fig 13.5.2 IPv6 ACL Name page

COMMAND	ACL » IPv6 ACL		Save Logout Reboot Debug
✓ Status			
✓ Network	ACI Nama		
✓ Port	ACL name		
VLAN			
 MAC Address Table 	Арріу		
✓ Spanning Tree			
✓ Discovery	ACL Table		
✓ DHCP			
✓ Multicast	Showing All v entries	showing nu non renues	Q
✓ Routing	ACL Name Rule Port		
✓ Security	COMMANDO2 0		
✓ ACL			First Previous 1 Net Last
MAC ACL	Delete		
MAC ACE			
IPv4 ACL			
IPV6 ACL			
IPv6 ACE			
ACL Binding			
∨ QoS			
✓ Diagnostics			
∨ Management			

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

COMMANDO	ACL	» IPv6 A	CE												Save Log	out R	eboot Debug
v Statue																	
v Network																	
V Port	ACI	E Table															
				1													
V MAC Address Table	ACL	Name COMM															
✓ Spanning Tree	Showin	ng 📶 🗸 entr	les					Showing	0 to 0 of 0 entries						Q		
✓ Discovery		1	1		0	- 10	Destinat	ID						10110		-	
✓ DHCP		Sequence	Action	Protocol	Sourc	ie IP	Destinat	ION IP	Source Port	Destination Port	TCP Flags	Туре	e of service	ICMP			
✓ Multicast					Address	Prefix	Address	Prefix				DSCP	IP Precedence	Type Code			
✓ Routing										0 results found.							
✓ Security		Add	Edit	Delet	e										FI	st Previou	s 1 Next Last
✓ ACL					_												
MAC ACL																	
MAC ACE																	
₽v4 ACL																	
IPv4 ACE																	
Pv6 ACL																	
IPV6 ACE																	
Acc binding																	
V Disgraphics																	
V Management																	
 Management 																	

Fig 13.6.1 Default IPv6 ACE Table page

COMMANDO	ACL » IPv6 ACE				
✓ Status					
✓ Network					
✓ Port	Add ACE				
VLAN					
MAC Address Table	ACL Name	COMMANDO	12		
 Spanning Tree 	ACLINAII	COMMANDO			
 Discovery 	Sequence	200	(1 - 2	147483647)	
✓ DHCP		Allow			
✓ Multicast	Action	O Deny			
✓ Routing		O Shutdow	/n		
✓ Security		Any			
✓ ACL	Dratasal	⊖ Select	TCP V		
MAC ACL	Protocol				
MAC ACE		 Define 		(0 - 255)	
IPv4 ACL					
IPv4 ACE	Source IP				
		2001::1	/ 64		(Address / Prefix (0 - 128))
ACL Binding		🖂 Any			
✓ QoS	Destination IP		/		(Address / Prefix (0 - 128))
 Diagnostics 			·····		(1001000711011(0-120))
Management		Any			
	Type of Service	O DSCP		(0 - 63)	

Fig 13.6.2 Add IPv6 ACE page

COMMANDO	ACL	» IPv6 A	CE											Save	Logoi	ıt Reboot	Debug
✓ Status																	
✓ Network	AC	E Table															
✓ Port	AC																
VLAN	ACL	Name COM	IMANDO2	~													
 MAC Address Table 																	
✓ Spanning Tree	Show	ing All 🗸 er	ntries					s	Showing 1 to 1 of 1 e	ntries							
✓ Discovery		1	1	1	Source	in ID	Doctinat	ion ID	1	1	1	Tv	no of Sonvice		CMD		
V DHCP		Sequence	Action	Protocol	Address	Deafin	Address	Deefin	Source Port	Destination Port	TCP Flags	DECD	ID Decendence	Tuna	Cada		
✓ Multicast					Address	Preiix	Address	Prenx				DSCP	IP Precedence	Type	Code		
✓ Routing		200	Allow	Any (IP)	2001::1	64	Any	Any				Any	Any				
✓ Security		Add	Edit	De	elete												First
▼ ACL																	
MAC ACL																	
MAC ACE																	
IPv4 ACL																	
IPv4 ACE																	
IPV6 ACL																	
A OL Diadian																	
ACL BINGING																	
✓ QoS ✓ Diagnostics																	

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 policymap 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

COMMANDO										
							Save	Logout	Reboot	Debug
	ACL	, » <u>ac</u>	L Bin	ding						
✓ Status										^
 Network 										
✓ Port	AC		ing iai	Jie						
VLAN										_
 MAC Address Table 										_
 Spanning Tree 		Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL				_
 Discovery 		1	GE1							
V DHCP		2	GE2							
 Multicast 		3	GE3							
✓ Routing		4	GE4							
✓ Security		5	GE5							
- ACL		6	GE6							
MAC ACL		7	GE7							
MACACE		8	GE8							
IPv4 ACL		9	GE9							
IPv6 ACL		10	GE10							
IPv6 ACE		11	GE11							
ACL Binding		12	GE12							
~ QoS		13	GE13							
 Diagnostics 		14	GE14							
Management	- 16	1 15	GE15							
		1 16	GE16							
	- E F	17	GE17							~
	_									

Fig 13.7.1 ACL Binding Table page

												Save	Logout	Reboot	D
	ACL	» AC	L Binding												
✓ Status		18	GE18												
 Network 		19	GE19												
✓ Port		20	GE20												
VLAN		21	GE21												
 MAC Address Table 		22	GE22												
 Spanning Tree 		23	GE23												
Discovery		24	GE24												
DHCP		25	GE25												
 Multicast 		26	GE26												
 Routing 		27	GE27												
 Security 		28	GE28												
ACL		29	LAG1												
MAC ACL		30	LAG2												
MAC ACE		31	LAG3												
IPv4 ACL		32	LAG4												
IPV4 ACE IPV6 ACI		33	LAG5												
IPv6 ACE		34	LAG6												
ACL Binding		35	LAG7												
V QoS		36	LAG8												
 Diagnostics 					_	_	_	_	_	 	_	_	_	_	
√ Management		Bind	Unbind	Edit											

Fig 13.7.2 Selecting port for ACL Binding page

	Save Log L » ACL Binding	out Reboot Debug
✓ Discovery ^		^
✓ DHCP		
✓ Multicast	Add ACL Binding	
✓ Routing		
✓ Security	GE1-GE28.LAG1-LAG8	
- ACL	Port	
MAC ACL		
MAC ACE		
IPv4 ACL	IPv4 ACL None	
IPv4 ACE		
IPv6 ACL	IPv6 ACL COMMANDO2	
IPv6 ACE		
ACL Binding	Apply Close	
✓ QoS		
✓ Diagnostics		
V Management		~



COMMANDO	A	ACL >	» AC	L Bino	ling			Save Lo	gout]	Reboot]	Debug	Ş
✓ Discovery ^											^	5
✓ DHCP												
✓ Multicast		ACL	Bindi	ng lan	bie							
✓ Routing									0		- 1	
✓ Security		_							4		- 10	1
- ACL			Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL					
MAC ACL			1	GE1	COMMANDO		COMMANDO2					
MAC ACE			2	GE2	COMMANDO		COMMANDO2					
IPv4 ACL			3	GE3	COMMANDO		COMMANDO2					
			4	GE4	COMMANDO		COMMANDO2					
			5	GE5	COMMANDO		COMMANDO2					
ACL Binding			6	GE6	COMMANDO		COMMANDO2					
✓ QoS			7	GE7	COMMANDO		COMMANDO2					
✓ Diagnostics			8	GE8	COMMANDO		COMMANDO2					
✓ Management			9	GE9	COMMANDO		COMMANDO2					

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 4byte 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.

COMMANDO	QoS >	» Gen	eral »	> Pro	perty						Save	Logout Re	boot D	ebug
✓ Status	_								 					^
V Network			tata 🕺 🗆						 					
✓ Port					ле 				 					
VLAN			9	CoS										
V MAC Address Table		Trust M	lode		DSCP									
✓ Spanning Tree) IP Pr	ecedence									
V Discovery	L		JL						 					
V DHCP		Apply												
✓ Multicast														
✓ Routing	Por	t Setti	ng Tah	le										
✓ Security		. ootai	ig ius											
V ACL												0		-
▼ QoS	-	-							 	 				
∧ General		Entry	Port	CoS	Trust		Remark	ing						
Property		L				Cos	DSCP	IP Precedence		 				-
Queue Scheduling		1	GE1	0	Enabled	Disabled	Disabled	Disabled						
DSCP Mapping		2	GE2	0	Enabled	Disabled	Disabled	Disabled						
IP Precedence Mapping		3	GE3	0	Enabled	Disabled	Disabled	Disabled						
✓ Rate Limit		4	GE4	0	Enabled	Disabled	Disabled	Disabled						
 Diagnostics 		5	GE5	0	Enabled	Disabled	Disabled	Disabled						
✓ Management		6	GE6	0	Enabled	Disabled	Disabled	Disabled						
		7	GE7	0	Enabled	Disabled	Disabled	Disabled						

Fig 14.1.1 Default QoS Port Setting table page

COMMANDO	QoS	» (Gen	eral »	P Pro	perty						Save	Logout	Reboot	Debug
✓ Status	-					· ·									^
✓ Network	100									 					
✓ Port			St	tate 🛛 🗠	Enal	ble				 					
VLAN				C) CoS	_									
✓ MAC Address Table		Tri	ust Me	ode 🗧) DSC	P									
✓ Spanning Tree) IP Pr	ecedence									
✓ Discovery	Ŀ			ä?	· · · · · ·					 i					
V DHCP		Арр	oly												
✓ Multicast															
✓ Routing	Po	ort S	ettin	ng Tabl	le										
✓ Security		11.0	cum	iy iabi											
✓ ACL													0		_
▼ QoS	-	-	_							 	 		~		_
∧ General] E	intry	Port	CoS	Trust		Remark	king line i						
Property							Cos	DSCP	IP Precedence						_
Queue Scheduling			1	GE1	0	Enabled	Disabled	Disabled	Disabled						
Cos Mapping DSCR Mapping			2	GE2	0	Enabled	Disabled	Disabled	Disabled						
IP Precedence Mapping			3	GE3	0	Enabled	Disabled	Disabled	Disabled						
✓ Rate Limit			4	GE4	0	Enabled	Disabled	Disabled	Disabled						
✓ Diagnostics			5	GE5	0	Enabled	Disabled	Disabled	Disabled						
✓ Management			6	GE6	0	Enabled	Disabled	Disabled	Disabled						
	Г	1	7	GE7	0	Enabled	Disabled	Disabled	Disabled						

Fig 14.1.2 Enableing QoS on Switch page

COMMANDO									Save Log	out Reboot	t Debug
	QoS » G	eneral >	» Pro	perty							
✓ Status	-	_		_	_	_					^
✓ Network	[State									
∨ Port		State		oie							
✓ VLAN		(
 MAC Address Table 	Trus	t Mode		-DSCP							
✓ Spanning Tree				recedence							
 Discovery 		JL									
✓ DHCP	Apply										
✓ Multicast											
✓ Routing	Port Set	tting Tab	ble								
✓ Security		ang ian									
✓ ACL									C		_
▼ QoS		_	-		1	Domork	ina			•)	
∧ General	🗌 🗌 Ent	ry Port	CoS	Trust	6.00	Reliark	III Dressdanas				
Property Output Only of the full		4 054		Fashlad	Disabled	Disabled	Dischlad		 		_
Queue Scheduling CoS Manning		I GET	0	Enabled	Disabled	Disabled	Disabled				
DSCP Mapping		2 GE2	0	Enabled	Disabled	Disabled	Disabled				
IP Precedence Mapping		3 GE3	0	Enabled	Disabled	Disabled	Disabled				
✓ Rate Limit		4 GE4	0	Enabled	Disabled	Disabled	Disabled				
✓ Diagnostics		5 GE5	0	Enabled	Disabled	Disabled	Disabled				
✓ Management		6 GE6	0	Enabled	Disabled	Disabled	Disabled				
		7 GE7	0	Enabled	Disabled	Disabled	Disabled				

Fig 14.1.3 Selecting Ports for Qos setting page

COMMANDO	QoS » General » Property	Save Logout Reboot Debug
✓ Status		^
✓ Network		
✓ Port	Edit Port Setting	
VLAN		
 MAC Address Table 	Bort CE2 CE2	
✓ Spanning Tree		
 Discovery 	CoS 4 (0 - 7)	
V DHCP	Trust 🕅 Enable	
✓ Multicast		
✓ Routing	Remarking	
✓ Security	CoS 🕅 Enable	
V ACL		
▼ QoS		
∧ General	IP Precedence Enable	
Property		
Queue Scheduling	Apply Close	
CoS Mapping		
DSCP Mapping		
IP Precedence Mapping		
Rate Limit		
		v
✓ Wanagement		>

Fig 14.1.4 Edit Ports setting for Qos page

COMMANDO	Q ₀ S	» Gen	ieral >	> Pro	perty							5	Save	Logout	Reboo	t De	bug
✓ Status										_							^
✓ Network	1		tato [
✓ Port	h = =								 	-							
VLAN			(
✓ MAC Address Table		Trust N	lode		-DSCP												
✓ Spanning Tree			0) IP Pr	ecedence												
✓ Discovery	·								 	- 1							
✓ DHCP		Apply															
✓ Multicast																	
✓ Routing	Por	rt Setti	ng Tab	le													
✓ Security																	
✓ ACL														0			-
▼ QoS		-	1	-			Demod	-1	 		 						1
∧ General		Entry	Port	CoS	Trust	6-6	Remark	ung									
Property			0.51			Cos	DSCP	IP Precedence	 		 						
Queue Scheduling		1	GE1	0	Enabled	Disabled	Disabled	Disabled									
DSCR Mapping		2	GE2	4	Enabled	Enabled	Enabled	Disabled									
IP Precedence Mapping		3	GE3	4	Enabled	Enabled	Enabled	Disabled									
✓ Rate Limit		4	GE4	0	Enabled	Disabled	Disabled	Disabled									
 Diagnostics 		5	GE5	0	Enabled	Disabled	Disabled	Disabled									
✓ Management		6	GE6	0	Enabled	Disabled	Disabled	Disabled									
		7	GE7	0	Enabled	Disabled	Disabled	Disabled									

Fig 14.1.5 QoS Port Setting table page

14.1.2 Queue Scheduling

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue and queue 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled, Strict Priority (SP) and Weighted Round Robin (WRR).

Strict Priority (SP): Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.

Weighted Round Robin (WRR): In WRR mode the number of packets sent from the queue is proportional to the weight of the queue higher the weight, the with more priority frames are sent.

The queuing modes can be selected on the Queue page. When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with queue-8 (the highest priority queue) and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced. It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in Strict Priority. In this case traffic for the SP queues is always sent before traffic from the WRR queues. After the SP queues have been emptied, traffic from the WRR queues is forwarded.

To view and configure Queue Scheduling ,click QoS >> General >> Queue Scheduling

COMMANDO						Save Logout Reboot Debr	ug
	QoS » G	General » Q	ueue	Schedu	ling		
✓ Status							
✓ Network		Scheduling	Table				
✓ Port	Queue	ocheuunny	lable				
VLAN				Method			1
✓ MAC Address Table	Queue	Strict Priority	WRR	Weight	WRR Bandwidth (%)		I
 Spanning Tree 	1	۲	0	1			1
 Discovery 	2	Õ	õ	2			1
✓ DHCP	3		0	3			1
✓ Multicast			0				1
✓ Routing	1		0	+ -			1
✓ Security	5	•	0	p			1
✓ ACL	6	۲	0	9			1
▼ QoS	7	۲	0	13			1
∧ General	8	۲	0	15			J
Property Queue Scheduling CoS Mapping DSCP Mapping IP Precedence Mapping V Rate Limit Diagnostics V Management	Appl	ly					

Fig 14.1.6 Default QoS Scheduling table page

COMMANDO	2₀s ≫ G	eneral » Q	ueue S	Schedu	ling	Save Logout Reboot
✓ Status						
Port	Queue	Scheduling 1	Table			
		_				1
	Queue			Method		
Spanning Tree		Strict Priority	WRR	Weight	WRR Bandwidth (%)	
iscoverv	1	0	۲	1	6.67%	
HCP	2	0	۲	2	13.33%	
lulticast	3	0	۲	3	20%	
Routing	4	0	۲	4	26.67%	
lecurity	5	0	۲	5	33.33%	
CL	6	۲	0	9		
0.0	7	۲	0	13		
General	8	۲	0	15		
Ververal Property Queue Scheduling CoS Mapping DSCP Mapping IP Precedence Mapping Y Rate Limit Diagnostics	Appl	У				

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**

COMMANDO		Save Logout Reboot Debug
	Qos # General # Cos Mapping	
✓ Status	CoS to Queue Mapping	^
✓ Network		
✓ Port	CoS Queue	
VLAN	0 2 🗸	
 MAC Address Table 		
 Spanning Tree 	2 3 🗸	
✓ Discovery	3 4 -	
V DHCP	4 5 🗸	
✓ Multicast	5 6 4	
✓ Routing	6 7 -	
✓ Security	7 8	
V ACL		
✓ QoS	Apply	
General Property Queue Scheduling	Queue to CoS Mapping	
Cos Mapping	Queue CoS	
IP Precedence Manning		
✓ Rate Limit	2 0 ~	
✓ Diagnostics	3 2 -	
✓ Management	4 3 ~	
	5 4 ~	
	6 5 -	
	Apply	~

Fig 14.1.8 Default CoS to Queue Mapping page

COMMANDO		Save Logout Reboot	Debug
QoS »	General » CoS Mapping		
 ✓ Spanning rise ✓ Discovery ✓ DHCP CoS to the second s	to Queue Mapping		^
✓ Multicast CoS	Queue		
V Routing	4 ~		-11
✓ Security			- 11
	4 ~		- 11
	2 ~		
Property 4	5 -		
Queue Scheduling 5	7 -		
CoS Mapping	7 ~		
DSCP Mapping	8 ×		
IP Precedence Mapping			
A Diagnostics	Apply		
 ✓ Diagnosics ✓ Management 			

Fig 14.1.9 CoS to Queue Mapping Changing Queue values page

COMMANDO)0S » G	enera	Save Logout Reboot Debug I » CoS Mapping
			^
 Discovery 	0		Manning
✓ DHCP	Queue	to Cos	марріпд
✓ Multicast	Queue	Cos	
✓ Routing	Queue	1 1	
✓ Security	1		
V ACL	2	2~	
▼ QoS	3	3 ~	
Conoral	4	3 ~	
Proporty	5	5 ~	
Queue Scheduling	6	5 ~	
CoS Mapping	7	7 -	
DSCP Mapping	· ·		
IP Precedence Mapping	8	/ ⊻	
✓ Rate Limit	Appl	,	
✓ Diagnostics	, thbi		
V Management			

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.

COMMANDO)oS≫ Ge	neral »	DSCP	Mappin	g			
Network	DSCP to	0	Inning					
V Port	DSCF 10	Queuen	napping					
VLAN	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
V MAC Address Table	0[CS0]	1	16 [CS2]	3	32 [CS4]	5	48 [CS6]	7.4.4
✓ Spanning Tree	1	1	17	3	33	5	49	7
 Discovery 	2	1	18 (AF21)	3	34 [AF41]	5	50	7
V DHCP	3	1	19	3	35	5	51	7
V Multicast		1	20 (AE22)	3	35 (AE42)	5	52	7
V Routing	5	1	21	3	37	5	53	7
✓ Security	6	1	22 (AE23)	3	38 (AF43)	5	54	7
✓ ACL	7	1	23	3	39	5	55	7
✓ Q05	8/CS11	2	24 (CS3)	4	40 ICS51	6	56 IC:S71	8
∧ General	0	2	25	4	41	6	57	8
Queue Scheduling	10 (4511)	2	26 (4631)	4	42	6	58	8
CoS Mapping	10 [24 11]	2	20 [21 01]		43	6	50	8
DSCP Mapping	12 (4512)	2	28 (4832)				60	
IP Precedence Mapping	12 [0112]	2	20 [Ar 32]	* ~	45	°	61	°
✓ Rate Limit	10	2 ~	29	* <u>~</u>	40	°	60	° ~~
V Diagnostics	14 [AP 13]		30 (AF 33)	· ~	40[EF]	° ~	62	° ~
Management	15	2	31	4 ~	4/	• ~	63	° ~
	Apply							
	Queue to	DSCP I	Mapping					
	Queue	DSCP	_					
	1	0 [CS0]	~					
	2	8[CS1]	~					
	3	16 [CS2]	~					
	4	24 [CS3]	~					
	5	32 [CS4]	~					
	6	40 [C:S5]	~					
	7	48 [CS6]	~					
	8	56 [C:S7]	~					
	_							
	Apply							

Fig 14.1.11 Default DSCP to Queue Mapping page

COMMANDO

Save | Logout | Reboot | Debug

	QoS » Ge	neral X	DSCP I	Mappin	ıg				
Status									
Network	DOODA	•							
Port	DSCP to	Queue	Mapping						
VLAN	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue	
IAC Address Table	0 (CS0)	5 ~	16 ICS21	3 ~	32 [CS4]	4 🗸	48 [CS6]	7 ×	
panning Tree	1		17	2 ~	33	6 ~	49	7	
iscovery	2		18 (AF21)	3	34 [AF41]	5	50	7	
HCP	2	1	10 [11 21]	2	25	5	50		
ulticast			20 (4522)	2	26 (45 42)	5	50		
outing			20 [AF22]	2 🗸	30 [AF42]	5 V	52		
ecurity	5		21	3 ~	3/	5 ~	53		
CL	6	5 ~	22 [AF23]	3 ~	38 [AF43]	5 ~	54		
oS	7	3 ~	23	3 ~	39	5 ~	55		
General	8 [CS1]	2 ~	24 [CS3]	4 ~	40 [CS5]	6 ~	56 [CS7]	8 🗸	
Property	9	2 ~	25	4 ~	41	6 🗸	57	3 🗸	
Queue Scheduling	10 [AF11]	2 ~	26 [AF31]	8 ~	42	4 ~	58	8 🗸	
CoS Mapping	11	8 ~	27	4 ~	43	6 ~	59	8 🗸	
DSCP Mapping	12 [AF12]	2 ~	28 [AF32]	4 ~	44	6 ~	60	8 🗸	
Precedence Mapping Rate Limit	13	5 ~	29	4 ~	45	6 ~	61	8 ~	
Diagnostics	14 [AF13]	1 ~	30 [AF33]	4 ~	46 [EF]	6 ~	62	8 🗸	
Management	15	2 ~	31	4 ~	47	6 ~	63	8 🗸	

Fig 14.1.12 Changing DSCP to Queue Mapping page

COMMANDO	0.05 >> 0	eneral » D	Save Logout Reboot Debug
v spanning nee	2 00 0	2	a or multing
✓ Discovery	`		^
✓ DHCP	Queue	to DSCP Ma	pping
✓ Multicast	Queue	DSCP	
✓ Routing	1	0.10201	
✓ Security			
V ACL	2	8 [CS1] V	
▼ QoS	3	8 [CS1] 🗸	
A General	4	24 [CS3] 🗸	
Property	5	32 [CS4] 🗸	
Queue Scheduling	6	26 [AF31] ~	
CoS Mapping	7	34 [AF41] ~	
DSCP Mapping	8	17 🗸	
IP Precedence Mapping			
✓ Rate Limit	Appl	y	
 Diagnostics 			
V Management	,		v

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.

COMMANDD			
	OoS » Conoral	Save Logout	: Reboot Debug
	Q05 " General	" I receuence scapping	
✓ Status	IP Precedenc	e to Queue Mapping	<u>^</u>
V Network	IP Precedence	Queue	
✓ Port	0		
VLAN			
MAC Address Table	1		
✓ Spanning Tree	2	3 🗸	
✓ Discovery	3	4 🗸	
✓ DHCP	4	5 🗸	
✓ Multicast	5		
✓ Routing	6	7 🗸	
✓ Security	7	8 🗸	
V ACL	Annh		
	Арру		
∧ General			
Property Output Scheduling	Queue to IP P	Precedence Mapping	
CoS Mapping			
DSCP Mapping	Queue IP Pres	cedence	
IP Precedence Mapping	1 0 🗸		
✓ Rate Limit	2 1 🗸		
 Diagnostics 	3 2 🗸		
✓ Management	4 3 🗸		
	5 4 🗸		
	6 5 🗸		
	7 6 🗸		
	8 7 🗸		
	Apply		~

Fig 14.1.15 IP Precedance to queue Mapping page

COMMANDO	QoS » Genera	1 » IP	Save Logout Reboot Debug Precedence Mapping
✓ Multicast ^	IP Precedenc	e to Qi	eue Mapping
✓ Routing			iono mapping
✓ Security	IP Precedence	Queue	
✓ ACL	0	1 ~	
✓ QoS	1	5 ~	
∧ General	2	5 ~	
Property	3	8 ~	
Queue Scheduling	4	7 ~	
CoS Mapping	5	2 ~	
IP Precedence Manning	6	3 ×	
 ✓ Rate Limit 	7		
✓ Diagnostics		0	
✓ Management	Apply		•

Fig 14.1.16 Changing IP Precedance to queue Mapping values page
COMMANDO	Q0S » (General » IP	Precedence Mappi	ng	Save Logout	Reboot	Debug
✓ Multicast ^	Queue	to IP Precede	ence Mapping				^
✓ Routing	Queue	IB Brogodopoo					
✓ Security	Queue	IF Frecedence					_
✓ ACL	1	0 ~					
▼ QoS	2	3 ~					
∧ General	3	2 ~					
Property	4	6 ~					
Queue Scheduling	5	4 ~					- L.
CoS Mapping	6	2 ~					- 11
DSCP Mapping	7	2					- 11
IP Precedence Mapping		3 🗸					- 11
✓ Rate Limit	8	7 ~					
✓ Diagnostics	Ann	lv.					
✓ Management	Abb	y .					v

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.

COMMANDO									Save	Logout	Reboot	Debug
✓ Status	Q05	" Kau	e Limi	t ~ Ingi	ress / Egres:	s Port						
												^
✓ Port	Ing	ress / I	Egress	Port Tab	ole							
VLAN												
V MAC Address Table	_									Q		
✓ Spanning Tree				In	gress	E	gress		1			
✓ Discovery		Entry	Port	State	Rate (Kbps)	State	Rate (Kbps)					
✓ DHCP		1	GE1	Disabled		Disabled			1			
✓ Multicast		2	GE2	Disabled		Disabled						
✓ Routing		3	GE3	Disabled		Disabled						
✓ Security		4	GE4	Disabled		Disabled						
V ACL		5	GE5	Disabled		Disabled						
▼ QoS		6	GE6	Disabled		Disabled						
✓ General	Πā	7	GE7	Disabled		Disabled						
∧ Rate Limit		8	GE8	Disabled		Disabled						
Egress / Egress Port		9	GE9	Disabled		Disabled						
		10	GE10	Disabled		Disabled						
✓ Management		11	GE11	Disabled		Disabled						~

Fig 14.2.2 Ingress / Egress Port Table page

COMMANDO	QoS	» Rat	e Limi	it » Ing	ress / Egres	s Port			Save	Logout	Reboot	Debuş
✓ Status												
V Network			_									
✓ Port	Ing	ress /	Egress	Port Tal	ble							
VLAN										0		
 MAC Address Table 									_	Q		
 Spanning Tree 		-		Ir	ngress	E	gress					
 Discovery 		Entry	Ροπ	State	Rate (Kbps)	State	Rate (Kbps)					
✓ DHCP		1	GE1	Disabled		Disabled						
 Multicast 		2	GE2	Disabled		Disabled						
✓ Routing		3	GE3	Disabled		Disabled						
✓ Security		4	GE4	Disabled		Disabled						
✓ ACL		5	GE5	Disabled		Disabled						
▼ QoS		6	GE6	Disabled		Disabled						
✓ General		7	GE7	Disabled		Disabled						
∧ Rate Limit			GER	Disabled		Disabled						
Ingress / Egress Port		0	CEO	Disabled		Disabled						
		9	GE9	Disabled		Disabled						
		10	GE10	Disabled		Disabled						
		11	GE11	Disabled		Disabled						

Fig 14.2.4 Selecting Ingress / Egress Port page

imit » Ingress / I	Save Logout Reboot Debug Egress Port
	^
ss Port	
GE1-GE28	
Enable	
4000	(here (46, 4000000)
1000	Kups (10 - 1000000)
Enable	
5000	Kbps (16 - 1000000)
Close	······································
	imit ≫ Ingress / I ss Port GE1-GE28 ☑ Enable [1000 ☑ Enable 5000] Close

Fig 14.2.5 Edit Rate Ingress / Egress Port page

COMMANDO	0S >	> Rate	e Limi	t » Ing	ress / Egres	s Port		Save	Logout	Reboot	Debug
✓ VLAN											ŕ
✓ MAC Address Table	Ingr	ess / F	aress	Port Tak	le						
✓ Spanning Tree	ingi	03376	gross	I OIT IU	//0						
✓ Discovery									0		_
✓ DHCP	-					_		 _	~		
✓ Multicast		Entry	Port	In	gress	E	gress				
✓ Routing				State	Rate (Kbps)	State	Rate (Kbps)				_
✓ Security		1	GE1	Enabled	1008	Enabled	5008				
✓ ACL		2	GE2	Enabled	1008	Enabled	5008				
▼ QoS		3	GE3	Enabled	1008	Enabled	5008				
					4000	Enabled	5008				
✓ General		4	GE4	Enabled	1008	Enabled	5000				
✓ General ∧ Rate Limit		4 5	GE4 GE5	Enabled Enabled	1008	Enabled	5008				
 ✓ General ∧ Rate Limit Ingress / Egress Port 		4 5 6	GE4 GE5 GE6	Enabled Enabled Enabled	1008 1008 1008	Enabled Enabled Enabled	5008 5008				
 General Rate Limit Ingress / Egress Port Egress Queue 		4 5 6 7	GE4 GE5 GE6 GE7	Enabled Enabled Enabled Enabled	1008 1008 1008 1008	Enabled Enabled Enabled	5008 5008 5008 5008				

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.

COMMANDO																			
	0.	Q W D	. 4. T :-													1	Save Log	out Re	boot Debu;
v Status	Ψ	о ″ К	ate Li	шп ″ Ц	gress Queu	le													
✓ Sidius																			· · · · ·
✓ Port	Eg	ress Qi	ueue 1	Table															
VLAN																	-		
✓ MAC Address Table		_	_			_										_	Q		
✓ Spanning Tree		Entry	Dort	Qu	eue 1	Qu	eue 2	Qu	ieue 3	Qı	ieue 4	Qı	Jeue 5	Qu	ieue 6	Qu	ieue 7	Qu	eue 8
✓ Discovery			Port	State	CIR (Kbps)														
✓ DHCP] 1	GE1	Disabled															
✓ Multicast] 2	GE2	Disabled															
✓ Routing] 3	GE3	Disabled															
✓ Security] 4	GE4	Disabled															
✓ ACL] 5	GE5	Disabled															
▼ QoS] 6	GE6	Disabled															
✓ General] 7	GE7	Disabled															
∧ Rate Limit] 8	GE8	Disabled															
Faress Queue] 9	GE9	Disabled															
✓ Diagnostics] 10	GE10	Disabled															
✓ Management] 11	GE11	Disabled															

Fig 14.2.7 Default Egress Queue Table page

COMMAND	QoS	» R:	nte Lin	nit » Eg	iress Queu	e											Save Lo;	gout R	eboot	Debug
✓ Status																				^
✓ Network	Ferre			a h la																
∨ Port	Egre	255 QL	leue	apie																
VLAN																	0			_
 MAC Address Table 	_																			_
✓ Spanning Tree		Entry	Port	Qu	eue 1	Qu	eue 2	Qu	ieue 3	Qu	eue 4	Qu	eue 5	Qu	ieue 6	Q	Jeue 7	Q	ieue 8	
✓ Discovery		chuy	1011	State	CIR (Kbps)	State	CIR (Kk	ips)												
∨ DHCP		1	GE1	Disabled		Disabled														
✓ Multicast		2	GE2	Disabled		Disabled														
✓ Routing		3	GE3	Disabled		Disabled														
✓ Security		4	GE4	Disabled		Disabled														
✓ ACL		5	GE5	Disabled		Disabled														
▼ QoS		6	GE6	Disabled		Disabled														
✓ General		7	GE7	Disabled		Disabled														
∧ Rate Limit		8	GE8	Disabled		Disabled														
Ingress / Egress Port		9	GE9	Disabled		Disabled														
		10	GE10	Disabled		Disabled														
 ✓ Management 		11	GE11	Disabled		Disabled														

Fig 14.2.8 Selecting Egress Queue ports page



QoS » Rate Limit » Egress Queue

✓ Status

✓ Network
 ✓ Port
 ✓ VLAN

MAC Address Table
Spanning Tree
Discovery
DHCP
Multicast
Routing
Security
ACL
QoS
General
Rate Limit

Ingress / Egress Port Egress Queue

✓ Diagnostics
✓ Management

Edit Egress Queue

Queue 1	🗸 Enable		
QUEUE I	20000	Kbps (16 - 1000000)	
0	Enable		
Queue 2	30000	Kbps (16 - 1000000)	
	🗸 Enable		
Queue 3	40000	Kbps (16 - 1000000)	
	Enable		
Queue 4	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 5	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 6	60000	Kbps (16 - 1000000)	
	Enable		
Queue 7	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 8	100000	Khos (18 - 1000000)	

Fig 14.2.9 Edit Egress Queue page



																Save	Logout	Reboot	Debug
-	Qos	s » R	ite Lin	ıit » Eg	ress Queue														
✓ Status																			٨
✓ Network				hla															
∨ Port	Egre	255 QU	eue la	IDIE															
∨ VLAN																			0
✓ MAC Address Table	-																		4
✓ Spanning Tree		Entry	Port	Qu	eue 1	Qu	eue 2	Qu	eue 3	Qu	ieue 4	Qu	eue 5	Qu	eue 6	Qu	eue 7	Qu	eue 8
✓ Discovery			1011	State	CIR (Kbps)	State	CIR (
∨ DHCP		1	GE1	Disabled		Disabled													
✓ Multicast		2	GE2	Enabled	20000	Enabled	30000	Enabled	40000	Disabled		Disabled		Enabled	60000	Disabled		Disabled	
✓ Routing		3	GE3	Enabled	20000	Enabled	30000	Enabled	40000	Disabled		Disabled		Enabled	60000	Disabled		Disabled	
✓ Security		4	GE4	Enabled	20000	Enabled	30000	Enabled	40000	Disabled		Disabled		Enabled	60000	Disabled		Disabled	
✓ ACL		5	GE5	Enabled	20000	Enabled	30000	Enabled	40000	Disabled		Disabled		Enabled	60000	Disabled		Disabled	
▼ QoS		6	GE6	Disabled		Disabled													
✓ General		7	GE7	Disabled		Disabled													
∧ Rate Limit		8	GE8	Disabled		Disabled													
Ingress / Egress Port Egress Queue		9	GE9	Disabled		Disabled													
✓ Diagnostics		10	GE10	Disabled		Disabled													
✓ Management		11	GE11	Disabled		Disabled													

Fig 14.2.10 Egress Queue Table after Editing Queue page

Chapter 15 Diagnostics

Logging:-->Log files of a switch are classified into: user log files and diagnostic log files.

Property: A diagnostic log file records the service processing flow and fault information. These logs sent to the log buffer, console, or terminal monitors.

Remote Server: You can set up a switch to automatically transfer diagnostic information to a remote server. If a fault occurs, you can provide your customer support.

Ping:-->Ping (Packet Internet Groper) tests the connection between two network nodes by sending packets to a host and measure the round-trip time.

Traceroute:-->Traceroute is used to display the route (path) 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



Diagnostics » Logging » Property

Status			
letwork	State "		
Port			
POE Setting	Aggregation "		
/LAN	Aggregation		_
AC Address Table	Aging Time 3	00	Sec (15 - 3600, default 300)
panning Tree			
)iscovery	Console Logging		
НСР	State 🖞 🗸	Enable	
ulticast		formational	
outing	Minimum		
ecurity	Seventy	ote: Emergency, Alert, Criti	cal, Error, Warning, Notice, Informational
\CL			
loS	RAM Logging		
)iagnostics	State 🛛 🗸	Enable	
Logging	Minimum	mergency 🗸	
Property	Severity		
Remote Server	L	ole. Emergency	
Mirroring Dina	Elash Longing		
Traceroute			
Copper Test	State ¦i ⊵	j Enadie	
Fiber Module	Minimum	Alert 🗸	
UDLD	Severity	ote: Emergency, Alert	
		erer miller gerregt / siere	

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.**

COMMANDO								Save Log	out Reboot	Debug
D	Diagnos	stics »	Logging »	Remote Se	rver					
 Spanning Tree 										
✓ Discovery	Remo	ote Serv	er Table							
✓ DHCP										
✓ Multicast									Q	
✓ Routing						Minimum			,	
✓ Security		Entry S	erver Address	Server Port	Facility	Severity				
✓ ACL	E++					0010111	results found	 		
✓ QoS	_	_				0	results found.	 		
✓ Diagnostics	A	dd	Edit	Delete						
Property										
Remote Server										
Mirroring										
Ping										
Traceroute										
Copper Test Eiber Module										
✓ Management										

Fig 15.1.3 Diagnostic Logging Deafult remote server page

COMMANDO	agnostics » Loggi	ng » Remote Se	iver	Save	e Logout	Reboot	Deb
 Spanning Tree 							
 Discovery 							
✓ DHCP	Add Remote Server						
✓ Multicast							
✓ Routing		 Hostname 					
✓ Security	Address Type	IPv4 IPv6					
V ACL			_				
✓ QoS	Server Address	10.10.10.10					
✓ Diagnostics	Server Port	514	(1 - 65535, default 514)				
 Logging Property 	Facility	Local 6 🗸					
Remote Server	Minimum	Debug 🗸					
Mirroring Ping Traceroute	Severity	Note: Emergency, Aler	t, Critical, Error, Warning, Notice, Informational, Debug				
Copper Test	Apply Clos	e					
Fiber Module							
✓ UDLD							
✓ Management							

Fig 15.1.4 Diagnostic Logging Add remote server page

COMMANDO	Diag	nostics	» Logging »	Remote S	erver			Save	Logout	Reboot	Debug
✓ Spanning Tree	^										
 Discovery 	Re	mote S	erver Table								
✓ DHCP		mote o									
✓ Multicast									Q		
✓ Routing	100		1		1					1	
✓ Security		Entry	Server Address	Server Port	Facility	Severity					
✓ ACL		1 1	10 10 10 10	514	Local 6	Debug		 			_
✓ Q0S			10.10.10	014	Locaro	Debug	 	 			_
 Diagnostics 		Add	Edit	Delete							
Logging Property Remote Server Mirroring Ping Traceroute Copper Test Fiber Module UDLD Management	×										

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**.

COMMANDO	Diagnostics » Ping
✓ Status	
V Network	
∨ Port	Address Type O IPv4
✓ POE Setting	O IPv6
V VLAN	
 MAC Address Table 	Server Address
✓ Spanning Tree	Count 4 (1 - 65535)
✓ Discovery	ii
✓ DHCP	Ping Stop
✓ Multicast	
✓ Routing	Ding Deput
✓ Security	Ping Result
∨ ACL	
∨ QoS	Packet Status
 Diagnostics 	Status "N/A
∧ Logging	
Property	
Remote Server	Receive Packet 0
Mirroring	Packet Lost 0%
Traceroute	
Copper Test	Round Trip Time
Fiber Module	Min 0.0 ms
∨ UDLD	Max " 0.0 ms
✓ Management	Average " 0.0 ms

Fig 15.2.1 Diagnostic Default Ping test page



Diagnostics » Ping

✓ Status	
✓ Network	
∨ Port	Address Type
✓ POE Setting	⊖ IPv6
∨ VLAN	Conver Address
 MAC Address Table 	
✓ Spanning Tree	Count 4 (1 - 65535)
✓ Discovery	L
✓ DHCP	Ping Stop
✓ Multicast	
✓ Routing	Ping Docult
✓ Security	
∨ ACL	
∨ QoS	Packet Status
 Diagnostics 	Status Success
 Logging Property Remote Server Mirroring 	Transmit Packet 4 Receive Packet 4 Packet Lost 0 %
Ping Traceroute Copper Test Fiber Module	Round Trip Time Min 0 ms
∨ UDLD ∨ Management	Max 0 ms Average 0 ms

Fig 15.2.2 Diagnostic Ping test result page

15.3 Traceroute

Traceroute discovers the IP routes along which packets were forwarded by sending an IP packet to the target host and back to the device. The Trace route page shows each hop between the device and a target host, and the round-trip time to each such hop. You can Traceroute any IP or Hostname for that click **Diagnostic >> Traceroute**.

	Diagnostics » Traceroute		
 ✓ Spanning Tree 			
✓ Discovery	Addross Tupo S Hostname		1
V DHCP	O IPv4		
✓ Multicast	Server Address		
✓ Routing	User Defined		
✓ Security	Time to Live		
✓ ACL	30	(2 - 255, default 30)	1
✓ QoS			
✓ Diagnostics	Apply Stop		
	Traceroute Result		
Property Remote Server			
Mirroring			
Ping			
Traceroute			
Copper Test			
Fiber Module			
 ✓ Management 			

Fig 15.3.1 Diagnostic Traceroute Default test page

COMMANDO	No			
	Jagnostics » Trac	eroute		
✓ Spanning Tree				
✓ Discovery	Address Type	 Hostname 		
✓ DHCP		● IPv4		
✓ Multicast	Server Address	192.168.0.21		
✓ Routing	4	User Defined		
✓ Security	Time to Live			
V ACL		2	(2 - 255, detault 30)	
V QoS		-		
✓ Diagnostics	Appiy	p		
∧ Logging Property	Traceroute Result			
Remote Server				
Mirroring	traceroute to 192.168.0.2	21 (192.168.0.21), 2 hop	s max, 38 byte packets	
Ping	Trace complete	8.0.21) 0.000 ms 0.000	ms 0.000 ms	
Copper Test				
Fiber Module				
V UDLD				
✓ Management				

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.**

		Save	Logout	Reboot	Debug
Dia	gnostics » Copper Test				
× Spanning Tree					
 Discovery 	Port GE1 V				
V DHCP					
✓ Multicast	Copper Test				
✓ Routing					
✓ Security	Conner Test Result				
V ACL	opper lest Result				
V QoS					
	Cable Status				
 ∧ Logging Property Remote Server Mirroring Ping Traceroute Copper Test Fiber Module ∨ UDLD ✓ Management 	Port N/A Result N/A Length N/A				

15.4.1 Diagnostic Default Copper Test Result page

	Diagnostics & Copper Test
 Spanning Tree 	[r
✓ Discovery	Port GE1 V
✓ DHCP	
✓ Multicast	Copper Test
✓ Routing	
✓ Security	Conner Test Desult
✓ ACL	copper rest result
V QoS	
✓ Diagnostics	Cable Status
	Port GE1
Property	Result: OK
Remote Server	
Mirroring	
Ping	
Copper Test	
Fiber Module	
V UDLD	
✓ Management	

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**.

COMMANDD	Diagnosti	cs » Fiber Mo	odule				Save	Logout 1	Reboot Debug
✓ Spanning Tree									
 Discovery 	Fiber M	odule Table							
✓ DHCP									
✓ Multicast								Q	
✓ Routing	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal	
✓ Security					0 results four	nd.			·
✓ ACL									
✓ QoS	Defres	h Detail							
▼ Diagnostics	riterites	Detail							
Logging Property Remote Server Mirroring Ping Traceroute Copper Test Fiber Module VUDLD Vanagement v									

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 spanningtree) that protects the upper layer protocols from causing loops in the network. Unidirectional link occurs when traffic is transmitted between neighbors in one direction only which can cause spanning-tree topology loops. After enabling UDLD on the connected interface of the other switch, we can see that the local switch has detected its neighbor and updated the link's status to bidirectional.

15.6.1 Property

When a unidirectional link is detected, UDLD shuts down the affected LAN port and alerts the user. Unidirectional links can cause a variety of problems, including spanning tree topology loops. UDLD is a Layer 2 protocol that works with the Layer 1 protocols to determine the physical status of a link. This page allow user to configure global and per interface settings of UDLD.

To view and configure UDLD Property , click **Diagnostics >> UDLD >> Property**.

COMMANDO	iagı	nostics	» UD	old » f	Property				Save	Logout	Reboot	Debug
 Spanning Tree 	····			·····								Â
✓ Discovery		Messa	ge Time	15	Sec (1 -	90, default 15)						
✓ DHCP	L							i				
✓ Multicast		Apply										
✓ Routing												
✓ Security	Der	4 0 . 441.	w Tabl									
✓ ACL	POI	t Settin	ig lab	le								
✓ QoS										0		_
 Diagnostics 	_									4		_
✓ Logging		Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor					
Mirroring		1	GE1	Disabled	Unknown		0					
Ping		2	GE2	Disabled	Unknown		0					
Traceroute		3	GE3	Disabled	Unknown		0					
Copper Test		4	GE4	Disabled	Unknown		0					
		5	GE5	Disabled	Unknown		0					
Property		6	GE6	Disabled	Unknown		0					
Neighbor		7	GE7	Disabled	Unknown		0					
✓ Management		8	GE8	Disabled	Unknown		0					v

Fig 15.6.1 UDLD Default Port Setting Table page



									Save	Logout	Reboot	Debug
	Diag	nostics	, » UI)LD » I	Property							
	^											^
 Spanning Tree 				v				,				
 Discovery 		Messa	ige Time	15	Sec (1 -	90, default 15)						
V DHCP				A				i				
 Multicast 		Apply										
 Routing 												
 Security 												
ACL	PO	n sen	ng lab	le								
v QoS										0		
 Diagnostics 		_								G		_
✓ Logging] Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor					
Mirroring] 1	GE1	Disabled	Unknown		0					
Ping] 2	GE2	Disabled	Unknown		0					
Traceroute] 3	GE3	Disabled	Unknown		0					
Copper Test		4	GE4	Disabled	Unknown		0					
		-	GE5	Disabled	Unknown		0					
Property		1 6	GE6	Disabled	Linknown		0					
Neighbor		, 0 1 7	GE7	Disabled	Unknown		0					
/ Management		, ,	GE/	Disabled	Unknown		0					
	×	8	GE8	Disabled	Unknown		0					v

Fig 15.6.2 UDLD Port selection page

COMMANDO		
Dia	gnostics » UDLD » Property	
 Spanning Tree 		
✓ Discovery	Edit Dart Satting	
V DHCP		
✓ Multicast	r	
✓ Routing	Port GE1-GE4	-
✓ Security	O Disabled	
✓ ACL	Mode Normal	
✓ QoS		1
✓ Diagnostics	Apply Close	
✓ Logging		
Mirroring		
Traceroute		
Copper Test		
Fiber Module		
Neighbor		
✓ Management		

Fig 15.6.3 UDLD Edit Port Setting page

COMMANDO	Diag	gnostics	» UI)LD » I	Property				Save	Logout	Reboot	Debi
panning Tree	^			γ					1			
iscovery		Messa	ige Time	15	Sec (1 -	90, default 15)						
НСР								i				
ulticast		Apply										
uting			_									
curity		ort Soffi	na Tab	lo								
L		ni əcili	ing idu	ic .								
S										0		
agnostics		_					rr			~		_
ogging] Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor					_
lirroring] 1	GE1	Normal	Unknown	Link up	0					
ina] 2	GE2	Normal	Unknown	Link down	0					_
		1 0	GE3	Normal	Unknown	Link down	0					
aceroute] 3	OL5									
aceroute opper Test] 3	GE4	Normal	Unknown	Link down	0					
aceroute opper Test per Module] 3] 4] 5	GE4 GE5	Normal Disabled	Unknown Unknown	Link down	0 0					
eroute opper Test oer Module DLD Property] 3] 4] 5] 6	GE4 GE5 GE6	Normal Disabled Disabled	Unknown Unknown Unknown	Link down	0 0 0					
aceroute opper Test ber Module DLD Property Neighbor] 3] 4] 5] 6] 7	GE4 GE5 GE6 GE7	Normal Disabled Disabled Disabled	Unknown Unknown Unknown Unknown	Link down	0 0 0					

Fig 15.6.4 UDLD Port Setting Table page

15.6.2 UDLD Neighbor

After enabling UDLD on the connected interface of the other switch, we can see that the local switch has detected its neighbor and updated the link's status to bidirectional. UDLD is capable of tracking multiple neighbors per interface.

To view and configure Neighbor page, click **Diagnostics** >> UDLD >> Neighbor

COMMANDO	Diagnos	tics » UD	DLD » Neighbor						Save Logout	Reboot	Debug
✓ Spanning Tree											
✓ Discovery	Neiah	bor Table									
✓ DHCP											
✓ Multicast									Q		
✓ Routing		Expiration					Message	Timeout	- ,		
✓ Security	Entry	Time	Current Neighbor State	Device ID	Device Name	Port ID	Interval	Interval			
✓ ACL					0 results	s found					_
✓ QoS	_										_
✓ Diagnostics	Refr	esh									
Logging Mirroring Ping Traceroute Copper Test Fiber Module UDLD Property Neighbor Management V Management V											

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.

COMMAND	Management » User Account		Save Logout Reboot Debug
✓ Status	^		
✓ Network			
✓ Port	User Account		
VLAN		Charity 4 is 4 of 4 orbits	
 MAC Address Table 	Showing All v entries	Showing I to For Fentiles	Q
 Spanning Tree 	Username Privilege		
 Discovery 	admin Admin		
✓ DHCP			First Previous 1 Next Last
✓ Multicast	Add Edit De	alete	
✓ Routing			
✓ Security			
✓ ACL			
✓ QoS			
 Diagnostics 			
✓ Management			
User Account V Management Access V Firmware Configuration V SNMP Restore Factory Default			

Fig 16.1.1 Default User Account page

COMMANDO		Save	Logout	Reboot	Debug
Ma	nagement » User Account				
✓ VLAN ^					^
 MAC Address Table 					
 Spanning Tree 	Add User Account				
V Discovery		-			
V DHCP	Username				
✓ Multicast		-			
✓ Routing	Password				
✓ Security	Confirm Password				
V ACL					
✓ QoS	Privilege Olser				
 Diagnostics 		<u>.</u>			
✓ Management	Apply Close				
User Account Management Access Firmware Configuration SNMP Restore Factory Default					v

Fig 16.1.2 Add User Account having all privilege page

COMMANDO	anagement » User Account	Save	Logout	Reboot	Debug
✓ VLAN					^
 MAC Address Table 					
✓ Spanning Tree	Add User Account				
 Discovery 					
✓ DHCP	Username COMMANDO1				
✓ Multicast					
✓ Routing	Password				
✓ Security	Confirm Password				
✓ ACL					
✓ QoS	Privilege O Aamin Ilser				
✓ Diagnostics		1			
▼ Management	Apply Close				
User Account V Management Access Firmware Configuration SNMP Restore Factory Default					

Fig 16.1.3 Add User Account having very limited access page

COMMANDO	Management » User Account		Save Logout Reboot Debug
✓ VLAN			
 MAC Address Table 	User Account		
 Spanning Tree 			
✓ Discovery	Showing All ventries	Showing 1 to 3 of 3 entries	0
✓ DHCP			
✓ Multicast	Username Privilege		
✓ Routing	admin Admin		
✓ Security			
✓ ACL	COMMANDO1 User		
✓ QoS	Add Edit Delete		First Previous 1 Next Last
✓ Diagnostics			
✓ Management			
User Account V Management Access V Firmware Configuration V SNMP Restore Factory Default V			

Fig 16.1.4 All User Account page

COMMANDO	Management » User Account	Save Logout Reboot Debug
✓ VLAN ^		
 MAC Address Table 	Liser Account	
✓ Spanning Tree	User Account	
✓ Discovery	Showing All v entries Showing 1 to 3 of 3 entries	0
✓ DHCP		~~~~
✓ Multicast	Username Privilege	
✓ Routing	admin Admin	
✓ Security	COMMANDO Admin	
V ACL	COMMANDO1 User	
✓ QoS		First Previous 1 Next Last
✓ Diagnostics		
✓ Management		
User Account		
 Management Access 		
✓ Firmware		
 Configuration 		
✓ SNMP		
RIVION Restore Eactory Default		
Restore Factory Delault		

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

COMMANDO	Management » User Acco	unt	Save Logout Reboot Debug
✓ VLAN ^			
 MAC Address Table 	Liser Account		
 Spanning Tree 			
 Discovery 	Showing All 🗸 entries	Showing 1 to 2 of 2 entries	0
✓ DHCP			۲
✓ Multicast	Username Privilege		
✓ Routing			
✓ Security	COMMANDO1 User		
✓ ACL	Add Edit	Delete	First Previous 1 Next Last
✓ QoS		Delete	
 Diagnostics 			
✓ Management			
User Account Management Access Firmware Configuration SNMP RMON Restore Factory Default			

Fig 16.1.6 Deleting default admin account for security purpose page



Fig 16.1.7 Login with COMMANDO admin privilege account page



Fig 16.1.8 C2000 Switch access with COMMANDO admin privilege account page

	COMMANDO
L. L	Jsername: COMMANDO1
H	Password: ••••••
	Login

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**.

COMMANDO		Save Logout Reboot Debug
	Management » Management Access » Management VLAN	
✓ MAC Address Table		
✓ Spanning Tree	1. default	
✓ Discovery	Management VLAN	
✓ DHCP	Note: Change Management VLAN may cause connection interrupted.	
✓ Multicast		
✓ Routing	Apply	
✓ Security		
V ACL		
✓ QoS		
✓ Diagnostics		
✓ Management		
User Account		
 Management Access 		
Management VLAN		
Management ACL		
Management ACE		
✓ Firmware		
✓ Configuration		
Restore Factory Default		

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.

COMMANDO			
м	anagement 🤇	» Management Acc	ess » Management Service
✓ Status	Management	Service	:
× Network	Telnet	Enable	
Y Port	++		
VLAN	SSH ;		
V MAC Address Table	HTTP	Enable	
✓ Spanning Tree	HTTPS	Enable	
✓ Discovery	++		
V DHCP	SNMP ;		i
✓ Multicast	Constant Time		
✓ Routing	Session lim	eout	
✓ Security	Console	10	Min (0 - 65535, default 10)
✓ ACL	Telnet	10	Min (0 - 65535. default 10)
∨ QoS	++		
✓ Diagnostics	SSH	10	Min (0 - 65535, default 10)
✓ Management	нттр	10	Min (0 - 65535. default 10)
User Account	+=======+		
∧ Management Access	HTTPS	10	Min (0 - 65535, default 10)
Management VLAN	· · · · · · · · · · · · · · · · · · ·		
Management ACL	Password R	etry Count	
Management ACE	Console	3	(0 - 120, default 3)
 Firmware Configuration 	Telnet	3	(0 - 120, default 3)
✓ SNMP ✓ RMON	SSH	3	(0 - 120, default 3)
Restore Factory Default	Silont Time		
	hard the		
	Console	0	Sec (0 - 65535, default 0)
	Telnet	0	Sec (0 - 65535, default 0)
	SSH	0	Sec (0 - 65535, default 0)
	L		

Fig 16.2.2 Management services page



Management » Management Access » Management Service

✓ Status	Managemen	t Service	
✓ Network	Telnet	Enable	
Port			
VLAN	5 SH ;		
MAC Address Table	HTTP	🗸 Enable	
Spanning Tree	HTTPS	🔽 Enable	
Discovery			
HCP	SNMP	Enable	
lulticast			
outing	Session Tim	eout	
ecurity	Console	1000	Min (0 - 65535, default 10)
CL	Talaat	4000	
loS	ieinet	[1000	_ Min (u - 00030, detaut 10)
liagnostics	SSH	1000	Min (0 - 65535, default 10)
lanagement	υπο	500	Min (0, 85525 dofault 10)
User Account			
Management Access	HTTPS	500	Min (0 - 65535, default 10)
Management VLAN			
Management ACL	Password R	etry Count	
Management ACE	Console	3	(0 - 120, default 3)
Firmware	Telnet	3	(0 - 120 default 3)
NMP		-	-
MON	SSH	3	(0 - 120, default 3)
lestore Factory Default			
	Silent Time		
	Console	100	Sec (0 - 65535, default 0)
L.			
	Telnet	100	Sec (0 - 65535, default 0)
, i i i i i i i i i i i i i i i i i i i	SSH	100	Sec (0 - 65535, default 0)
1			

Fig 16.2.3 Enabling Management services page



Management » Management Access » Management Service

✓ Status	Management	Service	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
✓ Network	Telnet	Enable	
Y Port	но с ч цо с		
VLAN			
✓ MAC Address Table	HTTP	Enable	
✓ Spanning Tree	HTTPS	Enable	
✓ Discovery	+		
V DHCP	SNMP ;;		i
✓ Multicast	· · · · · · · · · · · · · · · · · · ·		
Y Routing ₽	Session Time	eout	
✓ Security	Console	1000	Min (0 - 65535, default 10)
Y ACL	Telnet "	1000	Min (0 - 85535 default 10)
Y QoS			win (o - 00000, delaute to)
✓ Diagnostics	S SH	1000	Min (0 - 65535, default 10)
▼ Management	HTTP	500	Min (0 - 65535, default 10)
User Account	HTTPS	500	Min (0 - 65535, default 10)
Management VLAN Management Service Management ACL	Password Re	etry Count	
Management ACE	Console	3	(0 - 120, default 3)
Firmware Configuration	Telnet	3	(0 - 120, default 3)
V SNMP V RMON	SSH	3	(0 - 120, default 3)
Restore Factory Default	Silent Time		
	Console	100	Sec (0 - 65535, default 0)
	Telnet	100	Sec (0 - 65535, default 0)
	SSH	100	Sec (0 - 65535, default 0)

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.

Management » Management Acc	cess » Management ACL	Save Logout Reboot Debug
ACL Name		
Apply		
, oppy		
Management ACL Table		
Showing All y antries	Showing 0 to 0 of 0 entries	
Showing All v entries		q
ACL Name State Rule		
	0 results found.	
Active Deactive Delete		(First) (Previous) 1) (Next) (Last)
	Management » Management Acc ACL Name Apply Management ACL Table Snowing All entries ACL Name State Rule Active Deactive Delete	Management >> Management Access >> Management ACL Active Active Delete

Fig 16.3.1 Default Management ACL Table page

COMMANDO	Management » Managemen	it Access » Management ACL	Save Logout Reboot Debug
✓ MAC Address Table			
✓ Spanning Tree	ACL Name COMMANDO		
✓ Discovery	i.		
✓ DHCP	Apply		
✓ Multicast	· • • • •		
✓ Routing			
✓ Security	Management ACL Table		
✓ ACL	Showing All v entries	Showing 0 to 0 of 0 entries	
✓ QoS			u j
✓ Diagnostics	ACL Name State Rule		
✓ Management		0 results found.	
User Account ^ Management Access Management VLAN Management ACL Management ACL / Management ACE > Firmware < Configuration > SNMP < RMON Restore Factory Default	Active Deactive D	Delete	Fint Previous 1 (Next) Last

Fig 16.3.2 Adding Management ACL Name page

COMMANIIO	Management » Management Access » Management ACL	Save Logout Reboot Debug
✓ MAC Address Table ^		
✓ Spanning Tree	ACI Name	
✓ Discovery		
V DHCP	Apply	
✓ Multicast	rdby	
✓ Routing		
✓ Security	Management ACL Table	
✓ ACL	Showing All V antrias Showing 1 to 1 of 1 entries	
✓ Q₀S		4
 Diagnostics 	ACL Name State Rule	
✓ Management	COMMANDO Active 0	
User Account		First Previous 1 Next Last
 Management Access 	Active Deactive Delete	
Management VLAN		
Management Service		
Management ACE		
✓ Firmware		
✓ Configuration		
✓ SNMP		
V RMON		
Restore Factory Default		

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.

COMMANDO	Management » Management A	reese » Managemen	t ACF	Si	ave Logout	Reboot Debu	ıg
^	Management - Management A	eeess - managemen					
✓ MAC Address Table							
✓ Spanning Tree	Management ACE Table						
✓ Discovery							
✓ DHCP	ACL Name COMMANDO V (Active)						
✓ Multicast	Chausian All and antice	Showing	to 0 of 0 entries		0		
✓ Routing	anowing Air 🗸 entries	chowing c			Q		
✓ Security	Priority Action Service Port	Address / Mask					1
∽ ACL		· · · · ·	0 results found.				1
∨ QoS					First Prev	ious 1 Next Last	1
✓ Diagnostics	Add Edit Delet	e					
User Account							
∧ Management Access							
Management VLAN							
Management Service							
Management ACL							
✓ Configuration							
✓ SNMP							
✓ RMON							
Restore Factory Default							

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.

COMMANDO	gement >	Save Logout Reboot Debug » Firmware » Upgrade
✓ DHCP ^		
✓ Multicast	Action	
✓ Routing	Acuon	Obligane
✓ Security	Method	O TFTP
✓ ACL	·····	
✓ QoS	Filename	Browse No file selected.
✓ Diagnostics		
✓ Management	Apply	
User Account		
✓ Management Access		
∧ Firmware		
Upgrade		
Active Image		
✓ Configuration		
✓ SNMP		
✓ RMON		
Restore Factory Default		

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, 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

COMMAND		Save Logout Reboot Debug
	Management » Firmware » Active Image	
✓ Status		^
✓ Network		
✓ Port	Imageo Mageo	
V VLAN	Active image	
✓ MAC Address Table	Note: the image was selected for the next boot	
✓ Spanning Tree		
 Discovery 	Active image	
V DHCP	Firmware Image1*	
∽ Multicast	Version SoldierOS.2K.v1.5	
✓ Routing	Name vmlinux.bix	
✓ Security	Sita 015220 Datas	
V ACL		
~ Q0S	Created 2020-10-10 16:45:59	
✓ Diagnostics	· · · · · · · · · · · · · · · · · · ·	
✓ Management	Backup Image	
User Account	Firmware Image0	
 Management Access 	Version SoldierOS.2K.v1.4	
∧ Firmware	Nama	
Upgrade		
Active Image	Size 9125273 Bytes	
 Configuration 	Created 2020-09-30 16:28:18	
✓ SNMP		
V RMON	Apply	
Restore Factory Default		

Fig 16.3.3 Firmware Active Image page

16.4 Configuration

The Configuration Management and Update Firmware features allow you to browse to save and retrieve files directly from your local system. This is the easiest and recommended method.

Alternatively, you can use a TFTP (Trivial File Transfer Protocol) server to centralize the storage of your configuration and firmware files. Free TFTP servers for Windows and Linux are available on the web. They are generally easy to install and setup.

16.4.1 Upgrade

This page allow user to upgrade or backup configuration file through HTTP or TFTP server.

To view and configure firmware upgrade or backup , click

Management >> Configuration >> Upgrade or Configuration >> Backup

COMMANDO						
			Save	Logout	Reboot	Debug
Manager	ment » C	Configuration » Upgrade				
✓ Spanning Tree						
✓ Discovery	Action	Upgrade				
V DHCP	Action	O Backup				
✓ Multicast	Method	O TFTP				
✓ Routing		HTTP				
✓ Security		Running Configuration				
V ACL	nfiguration	Startup Configuration Backup Configuration				
✓ QoS		O RAM Log				
✓ Diagnostics		 Flash Log 				
✓ Management	Filename	Browse No file selected.				
User Account						
 Management Access 	IV					
✓ Firmware						
Upgrade Save Configuration						
✓ SNMP						
✓ RMON						
Restore Factory Default						

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.

COMMANDO			Save Logout Reboot Debug
Man	agement » C	Configuration » Upgrade	Sale Degout Reboot Debug
✓ Spanning Tree		· · · · ·	
✓ Discovery	Antina	O Upgrade	
V DHCP	Action	Backup	
✓ Multicast	Method	O TFTP	
✓ Routing	Method	HTTP	
✓ Security		Running Configuration	
V ACL	Configuration	Startup Configuration Backup Configuration	
✓ QoS		O RAM Log	
✓ Diagnostics		O Flash Log	
Management User Account User Account Management Access Firmware Configuration Upgrade Save Configuration SNMP SNMP Restore Factory Default v	Apply		

Fig 16.4.2 Backup of Configuration from running configuration page

COMMANDO	lanagement » Configuration » Upgrade	Save Logout Reboot Debug
✓ Spanning Tree		
× DHCP	Backup Running Configuration completed successfully	
Multicast	Duckup haining configuration completed successfully	
× Routing	Done	
V Socurity	Opening rupping-config cfg	
V ACL	opening contracty	
	You have chosen to open:	
	running-config.cfg	
	which is: cfg File (1.3 KB)	
✓ Management	from: http://192.168.0.1	
User Account	What should Firefox do with this file?	
 Management Access 		
Configuration		
	₩ <u>i2ave rite</u>	
Save Configuration	Do this <u>a</u> utomatically for files like this from now on.	
✓ SNMP		
V RMON	OK Cancel	
Restore Factory Default		

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.

COMMANDO			Save	Logout	Reboot	Debug
М	anagement » Co	nfiguration » Save Configuration				
					<u> </u>	
✓ Spanning Tree						
✓ Discovery		Running Configuration				
✓ DHCP	Source File	Startup Configuration Reskup Configuration				
✓ Multicast						
✓ Routing	Destination File	Startup Configuration Reskup Configuration				
✓ Security	L					
✓ ACL	Apply					
✓ QoS						
✓ Diagnostics						
✓ Management						
User Account						
 Management Access 						
✓ Firmware						
 Configuration 						
Upgrade						
Save Configuration						
Restore Factory Default						

Fig 16.4.4 Save running Configuration to Startup Configuration page

COMMANDO		Save Logout Reboot Debug
Ν	Management » Configuration » Save Configuration	
 Spanning Tree 		_
	Running Configuration	
V DHCP	Source File O Startup Configuration	
✓ Multicast	Backup Configuration	
✓ Routing	Destination File	
✓ Security	Backup Conniguration	
✓ ACL	Apply	
✓ QoS	(499)	
✓ Diagnostics		
✓ Management		
User Account		
 Management Access 		
✓ Firmware		
 Configuration 		
Opgrade Save Configuration		
SNMP		
✓ RMON		
Restore Factory Default		

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.

COMMANDO	Management » SNMP » View		Save Logout Reboot Debug
Kouting Security ACL QoS	View Table	Showing 1 to 1 of 1 entries	0
V Diagnostics Management User Account Management Access	View OID Subtree Type all .1 Included		(First) (Previous) (1) (Next) (Last)
 Firmware Configuration SNMP View Group Group 			
User Engine ID Trap Event Notification V RMON Restore Factory Default			

Fig 16.5.1 Default SNMP View Table page

COMMANDO	Management » SNMP » View	Save	Logout	Reboot	Debug
✓ Routing ^					^
✓ Security					
✓ ACL	Add View				
✓ QoS		_			
✓ Diagnostics	View 12				
✓ Management					
User Account	OID Subtree 2				
 Management Access 					
✓ Firmware	Type 🔘 Excluded				
✓ Configuration	L				
∧ SNMP	Apply Close				
View					
Group					
Community					
User					
Engine ID					
Trap Event					
Notification					
✓ RMÓN					
Restore Factory Default					v

Fig 16.5.2 SNMP add View page

COMMANDO	Management » SNMP » View		Save Logout Reboot Debug
✓ Routing ^			
✓ Security	View Table		
V ACL	Showing All v entries	Showing 1 to 2 of 2 entries	Q
✓ Diagnostics ✓ Management	Uiew OID Subtree Type		
User Account	12 .2 Excluded all .1 Included		
Firmware Configuration SNMP	Add Delete		(First) (Previous) 1 (Next) (Last)
View Group Community User Engine ID Trap Event Notification			
✓ RMON Restore Factory Default ✓			

Fig 16.5.3 SNMP View Table page

16.5.2 Group

A group defines read/write privileges and a level of security. It becomes operational when it is associated with an SNMP user or community.

To view and configure SNMP group settings, click Management >> SNMP >> Group.

COMMANDO	Мапа	gemen	t » SNI	MP » Group					Save Logout Reboot Debug
✓ Routing ^									
✓ Security	Gro	un Tabl	•						
✓ ACL	GIU	up lab	C						
V QoS	Showin	Showing All ventries Showing 0 to 0 of 0 entries						0	
✓ Diagnostics	-	,		1			_		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
✓ Management		Group	Version	Security Level		View			
User Account					Read	Write	Notify		
✓ Management Access								0 results found.	
✓ Firmware									(First) (Previous) (1) (Next) (Last)
✓ Configuration	Confi	gure SNM	P View to a	ssociate a non-defa	ault view i	with a gro	up.		
∧ SNMP		Add	Edit	Delete					
View									
Group									
Community									
User									
Engine ID									
Trap Event									
Notification									
✓ RMON									
Restore Factory Default									

Fig 16.5.4 SNMP Default Group Table page

COMMANDO	gement » SN	MP » Group	Save Logout Reboot Debug
✓ Discovery			^
V DHCP Add	d Group		^
✓ Multicast			
✓ Routing	C	40	
✓ Security	Group	12	
V ACL		O SNMPv1	
✓ Q0S	Version	SNMPv2 SNMPv2	
✓ Diagnostics		U SINIIPV3	
- Management		No Security	
User Account	Security Level	Authentication Authentication and Privacy	
✓ Management Access			
✓ Firmware		Read	
✓ Configuration		12 🗸	
∧ SNMP	}		
View		✓ Write	
Group	View	12 -	
Community			
User		☑ Notify	
Engine ID	1	12	
Trap Event	ä		
Notification			
✓ RMON	Apply Clo	se	
Restore Factory Default			· ·

Fig 16.5.5 SNMP Add Group page

COMMANDO	Mana	agemen	t » SNI	∕IP ≫ Group)				Save Logout Reboot Debug
 Discovery 	·								
✓ DHCP	C		le.						
✓ Multicast	Gro	oup lab	le						
 Routing 	Shov	ring All 🗸	entries				Showing	1 to 1 of 1 entries	0
✓ Security	-								4
V ACL		Group	Version	Security Level		View			
∨ QoS		Group	Version	Security Level	Read	Write	Notify		
 Diagnostics 		12	SNMPv2	No Security	12	12	12		
✓ Management	_								First Previous 1 Next Last
User Account V Management Access Firmware Configuration SNMP View Group Community User Engine ID Trap Event Notification V RMON Restore Factory Default		Add	IP View to a	Delete	ault view	with a gr	oup.		

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**.

COMMANDO	Management » SNM	• ≫ Community	Save Logout Reboot Debug
✓ Discovery	、 		
✓ DHCP	Community Table		
✓ Multicast			
✓ Routing	Showing All v entries	Showing 1 to 1 of 1 entries	0
✓ Security			3
✓ ACL	Community Group	View Access	
✓ Q₀S	public	all Read-Only	
 Diagnostics 	The second data for some	A first first have seen and a strength set of a state	(First Previous 1 Next Last
 Management 	Configure SNMP Group to as	nity is defined by a group under advanced mode. sociate a group with a community.	
User Account • Management Access • Firmware • Configuration • SIMDP View Group Community User Engine ID Trap Event Notification • RMON Restore Factory Default	Add Edit	Delete	

Fig 16.5.7 SNMP Community Table page

V Discovery V Discovery V Discovery Add Community Add Community Add Community	^
DHCP Multicast Add Community AddIng Sourcety	
✓ Multicast Add Community ✓ Routing	
✓ Routing	
✓ Security	
V ACL Community COMMANDO	
V QoS O Basic	
✓ Diagnostics ④ ¹ YPP ^a ④ Advanced	
✓ Management View all ✓	
User Account V Management Access Firmware Configuration SNMP View Group Community User Engine ID Trap Event Notification V RMON KMON	

Fig 16.5.8 Add SNMP Community page

COMMANDO	Management » SNMP » Community	Save Logout Reboot Debug
✓ Discovery	、 	
✓ DHCP	0	
✓ Multicast	Community lable	
✓ Routing	Showing All v antrins Showing 1 to 2 of 2 entries	
✓ Security	Showing 741 V entres	q
✓ ACL	Community Group View Access	
✓ Q₀S	COMMANDO 12	
✓ Diagnostics	public all Read-Only	
✓ Management		First Previous 1 Next Last
User Account Management Access Firmware Configuration SNMP View Group	Configure SIMP Group to associate a group with a community. Add Edit Delete	
Communify User Engine ID Trap Event Notification V RMON Restore Factory Default		

Fig 16.5.9 SNMP Community Table after adding community page

16.5.4 User

An SNMP user is defined by the login credentials (username, passwords, and authentication method) and by the context and scope in which it operates by association with a group and an Engine ID.

The configured user has the attributes of its group, having the access privileges configured within the associated view.

To view and configure SNMP users, click Management >> SNMP >> User.

COMMANDO	Management » SNMP » User	Save Logout Reboot Debug
✓ Discovery ∧		
✓ DHCP		
✓ Multicast	User lable	
✓ Routing	Showing 0 to 0 of 0 entries	0
✓ Security		q
✓ ACL	User Group Security Level Authentication Method Privacy Method	
✓ Q₀S	0 results found.	
✓ Diagnostics		(First) (Previous) 1 (Next) (Last)
✓ Management	Configure SNMP Group to associate an SNMPv3 group with an SNMPv3 user.	
User Account Vanagement Access Firmware Configuration SNMP View Group Community User Engine ID Trap Event Notification Restore Factory Default V	Add Edit Delete	

Fig 16.5.10 SNMP Default user Table page

	anagement » SN	MP » User
V MAC Address Table		
✓ Spanning Tree	Add User	
✓ Discovery	[
V DHCP	User	COMMANDO
✓ Multicast		
✓ Routing	Group	
✓ Security		No Security
V ACL	Security Level	Authentication
V QoS		Authentication and Privacy
✓ Diagnostics		
✓ Management	Autnentication	
User Account V Management Access V Firmware	Method	None Mon5 SHA
 ✓ Configuration △ SNMP 	Password	
View	Privacy	
Community User Engine ID Trap Event Notification	Method Password	None DES
RMON Restore Factory Default		

Fig 16.5.11 SNMP Add user page

		Save Logout Reboot Debug
	Management » SNMP » User	Saro Legour Meson Leoug
✓ MAC Address Table ^		
✓ Spanning Tree	User Table	
 Discovery 		
V DHCP	Showing All 🗸 entries Showing 1 to 1 of 1 entries	Q
✓ Multicast	User Group Security Level Authentication Method Privacy Method	
✓ Routing		
✓ Security		
✓ ACL	Configure SNMP Group to associate an SNMPv3 group with an SNMPv3 user.	First Previous 1 Next Last
✓ Q0S		
 Diagnostics 		
✓ Management		
User Account		
 Management Access 		
✓ Firmware		
 Configuration CNMD 		
View		
Group		
Community		
User		
Engine ID		
Trap Event		
Notification		
Y RMON		

Fig 16.5.12 SNMP user Table after adding User page

16.5.5 Engine ID

The Engine ID is used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set) and sends trap messages to a manager. The agent's local information is encapsulated in fields in the message. Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is comprised of the enterprise number and the default MAC address.

This engine ID must be unique for the administrative domain, so that no two devices in a network have the same engine ID.

To view and configure and display SNMP local and remote engine ID, click Management >> SNMP >> Engine ID.

COMMANDO			
		Save Logout	Reboot Debug
	Management » SNMP » Engine ID		
✓ MAC Address Table ^			
 Spanning Tree 	Local Engine ID		
 Discovery 	i UserDefined		
V DHCP	Engine ID		
✓ Multicast	80006a920300e04c01 (10 - 64 Hexadecimal Characters)		
✓ Routing			
 Security 	Apply		
V ACL			
~ QoS	Remote Engine ID Table		
 Diagnostics 			
✓ Management	Showing All ventries Showing 0 to 0 of 0 entries	Q	
User Account	Server Address Engine ID		
 Management Access 	0 results found.		
V Firmware		(First) (Pre	vious 1 Next Last
 Conliguration SNMP 	Add Edit Delete		
View			
Group			
Community			
User			
Engine ID			
Notification			
V RMON			
Restore Factory Default 🗸			

Fig 16.5.13 SNMP Default Remote Engine ID Table page

COMMANDO		Save Logout Reboot Debug
	Management » SNMP » Engine ID	
✓ MAC Address Table		^
Spanning Tree		
> Discovery	Add Remote Engine ID	
V DHCP		
 Multicast 	Hostname	
✓ Routing	Address Type 🗍 IPv4	
✓ Security	O IPv6	
✓ ACL	Server Address 192.168.100.100	
~ QoS		
✓ Diagnostics	Engine ID Fa220300e04c000000 (10 - 64 Hexadecimal Characters)	
✓ Management		
User Account	Apply Close	
 Management Access 		
✓ Firmware		
 Configuration 		
∧ SNMP		
View		
Group		
Community		
User Facine ID		
Tran Event		
Notification		
Y RMON		
Restore Factory Default		v

Fig 16.5.14 SNMP Add Remote Engine ID page

COMMANDO				
			Save	Logout Reboot Debug
	Management » SNMP » Engine ID			
✓ MAC Address Table				
 Spanning Tree 	Local Engine ID			
 Discovery 	User Defined			
✓ DHCP	Engine ID			
✓ Multicast	80006892030060400 (10-64	Hexadecimal Characters)		
✓ Routing				
✓ Security	Apply			
✓ ACL				
∨ QoS	Remote Engine ID Table			
 Diagnostics 				
✓ Management	Showing All v entries	Showing 1 to 1 or 1 entries		Q
User Account	Server Address Engine ID			
 Management Access 	192.168.100.100 80006a920300e04c000	000		
 Firmware Configuration 				First Previous 1 Next Last
 SNMP 	Add Edit Delete			
View				
Group				
Community				
User				
Engine ID Tran Event				
Notification				
✓ RMON				
Restore Factory Default 🗸 🗸				

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.

COMMANDO		Save Logout Reboot Debug
	Management » SNMP » Notification	
✓ MAC Address Table	^	
✓ Spanning Tree	Notification Table	
 Discovery 		
✓ DHCP	Showing All 🗸 entries Showing 0 to 0 of 0 entries	Q
✓ Multicast	Somer Address Somer Dart Timoout Betry Marsian Turo Community (Mars Socurity Joyal	
✓ Routing	Server Address Server Port Timeout Reity Version Type Community/Oser Security Lever	
✓ Security		
∽ ACL	For SNMPv1.2 Notification, SNMP Community needs to be defined.	First Previous 1 Next Last
∨ QoS	For SNMPv3 Notification, SNMP User must be created.	
 Diagnostics 	Add Edit Delete	
 Management 		
User Account		
 Management Access 		
✓ Firmware		
 Configuration 		
Group		
Community		
User		
Engine ID		
Trap Event		
Notification		
✓ RMON		
Restore Factory Default	×	

Fig 16.5.17 SNMP Default Notification Table page

COMMANDO				
Status	nagement » SNMP	» Notification		
Network	Add Notification			
ort				
VLAN	1	O Hostname		
MAC Address Table	Address Type	Pv4		
Spanning Tree	l	○ IPv6		
Discovery	Server Address	192.168.10.10		
DHCP	+	· · · · · · · · · · · · · · · · · · ·		
Multicast	Version	SNMPv1		
Routing	Version	SNMPv2		
Security	÷	0 -		
ACL	Туре	Inform		
QoS	+			
Diagnostics	Community / User	COMMANDO 🗸		
 Management 	l í	No Security		
User Account	Security Level	 Authentication 		
✓ Management Access	l	 Authentication and Privac 	y	
Firmware Configuration		Use Default		
SNMP	Server Port	162	(1 - 65535, default 162)	
View	1	🔽 Lise Default		
Group	Timeout	15	Sec (1 - 300, default 15)	
Community		10		
User	Betry	Use Default		
Engine D	Rouy	3	(1 - 255, default 3)	
Notification		_		
V RMON	Apply Close			
Restore Factory Default				

Fig 16.5.18 SNMP Add Notification page

COMMANDD	_									Save	. Logout Rebo	ot Debug
	Mana	gement » SNM	MP » Noti	fication								
✓ Discovery ^												
✓ DHCP	Not	ification Table										
✓ Multicast		incation lable										
V Routing	Showi	ing All 🗸 entries				Showing 1 to	o 1 of 1 en	ries			0	
✓ Security	-	-									G I	_
✓ ACL		Server Address	Server Port	Timeout	Retry	Version	Туре	Community / User	Security Level			
✓ QoS		192.168.10.10	162			SNMPv2	Trap	COMMANDO	No Security			
✓ Diagnostics	_						_				(First) (Previous) (1	(Next) (Last)
 Management 	For S	SNMPv1,2 Notification	, SNMP Commu SNMP User mus	unity needs t at be created	io be defi I	ned.						
User Account												
✓ Management Access		Add Edit	Del	ete								
✓ Firmware												
 Configuration 												
∧ SNMP												
View												
Group												
Community												
User												
Irap Event												
Notification												
Restore Eactory Default												

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, c	click Management >>	RMON >> Statistics.
----------------------------	---------------------	---------------------

COMMANDO																Save Logo				ogout Reboot De			
	Manag	ement >	» RM	DN » Stat	istics																		
Status																							
Network																							
Port	Statis	stics Tab	le																				
VLAN	Refres	h Rate 0																					
MAC Address Table			inell i																	0			
Spanning Tree	_		_																	4			
Discovery		Entry	Port	Bytes	Drop	Packets	Broadcast	Multicast	CRC & Align	Undersize	Oversize	Fragments	Jabbers	Collisions	Frames of	Frames of	Frames of	Frames of	rames of Frames of Frames Greater				
DHCP	님문	1		Received	Events	Received	Packets	Packets	Errors	Packets	Packets	•			64 Bytes	65 to 127 Bytes	128 to 255 Bytes	256 to 511 Bytes	512 to 1023 Bytes	than 1024 Bytes			
Multicast		1	GE1	717488	0	3835	738	701	0	0	0	0	0	0	1865	920	99	694	257	0			
Routing		2	GE2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
Security	111	3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
ACL		4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
QoS		5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
Diagnostics		6	GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
Management		7	GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
User Account		8	GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
Management Access Elemente		9	GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
 Configuration 		10	GE10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
SNMP		11	GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
RMON		12	GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
Statistics	ΠĒ	13	GE13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
History	ΠΠ	14	GE14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
Alarm	ΠΠ	15	GE15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
Restore Factory Default	ΠH	16	GE16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			

Fig 16.6.1 RMON Statistics Table page

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.

COMMANDO									Save Logout Re	eboot Debug
_	Man	agemer	nt » I	RMON	» Hist	ory				
✓ MAC Address Table										
✓ Spanning Tree	His	story Tr	able							
✓ Discovery		itory it								
✓ DHCP	Show	ving All	v entries					Showing 0 to 0 of 0 entries		0
✓ Multicast		-						1		
✓ Routing		Entry	Port	Interval	Owner	Sam	iple	-		
✓ Security						Maximum	Current			
V ACL								0 results found.		
∨ QoS	The	SNMP se	ervice is o	currently dis	sabled.					First Previous
✓ Diagnostics	For	RMON co	onfiguratio	on to be effe	ective, the	SNMP service	ce must be	enabled.		
✓ Management										
User Account		Add	E	Edit	Delete	e V	/iew			
✓ Management Access	L —									
✓ Firmware										
 Configuration 										
✓ SNMP										
A RMON										
Statistics										
History										
Event										
Alarm										
Restore Factory Default	<									>

Fig 16.6.2 RMON Default History Table page

COMMANDO		Save Logout Reboot Debug
	Management » RMON » History	
✓ MAC Address Table ^		^
✓ Spanning Tree		
✓ Discovery	Ada History	
V DHCP	[]	
✓ Multicast	Entry 1	
✓ Routing	Port GF3 v	
✓ Security		
V ACL	Max Sample 50 (1 - 50, default 50)	
✓ QoS	Interval 1800 (1 - 3600. default 1800)	
✓ Diagnostics		
✓ Management	Owner COMMANDO	
User Account		
✓ Management Access	Apply Close	
✓ Firmware		
RMON		
Statistics		
History		
Event		
Alarm		*
Restore Factory Default	<	>

Fig 16.6.3 RMON Add History page

	Mana	igemei	nt »]	RMON	» History				Save Logout	Reboot Debug
V MAC Address Table										
✓ Spanning Tree	His	tory Ta	ble							
✓ Discovery		lory it	bie							
✓ DHCP	Show	ing All	entrie	15			Sh	owing 1 to 1 of 1 entries		0
✓ Multicast		-								
✓ Routing		Entry	Port	Interval	Owner	Samp	le			
✓ Security		-				Maximum	Current			
✓ ACL		1	GE3	1800	COMMANDO	50	50			
∨ Q₀S	The S	SNMP se	rvice is	currently di	sabled					First Previou:
✓ Diagnostics	For F	RMON co	nfigurat	ion to be eff	ective, the SNM	service must	be enabled	f.		
✓ Management	_									
User Account		Add		Edit	Delete	View				
✓ Management Access										
✓ Firmware										
 Configuration 										
✓ SNMP										
A RMON										
Statistics										
History										
Event										
Alarm Destore Faster / Default										
Restore Factory Default	<									>

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.

									Save	Logout Reboot Debug
	Mana	gement	» RMO	N » Even	t					
✓ MAC Address Table ^										
✓ Spanning Tree	Eve	nt Table								
✓ Discovery										
✓ DHCP	Showin	ng All 🗸	entries			Show	wing 0 to 0 c	f 0 entries		0
✓ Multicast		-			L					~
✓ Routing		Entry (Community	Description	Notification	Time	Owner			
✓ Security								0 results found.		
V ACL	The S	SNMP servi	ce is currentl	v disabled						First Previous 1 Next Last
✓ Q₀S	For R	MON config	guration to be	e effective, the	SNMP service m	iust be e	nabled.			
✓ Diagnostics										
✓ Management	/	Add	Edit	Delete	View					
User Account										
✓ Management Access										
✓ Firmware										
 Configuration 										
✓ SNMP										
A RMON										
Statistics										
History										
Event										
Alarm										
Restore Factory Default										

Fig 16.6.5 RMON Default Event Table page

COMMANDO		Save	Logout	Reboot	Debug
Management ×	RMON » Event				
V MAC Address Table					^
✓ Spanning Tree					
✓ Discovery Add Event					
✓ DHCP					
✓ Multicast Ent	y 1				
✓ Routing	None				
✓ Security Notification	Event Log				
V ACL	O Trap				
✓ Q₀S	Livent Log and Irap				
✓ Diagnostics Communi	y Default Community				
✓ Management					
User Account					
✓ Management Access Own	er COMMANDO				
V Firmware					
Configuration Apply	Close				
A RMON					
Statistics					
History					
Event					
Alarm Destars Easters Default					
Restore Factory Delaunt					~

Fig 16.6.6 RMON Add Event page

COMMANDO	Mana	детеп	nt » RMO	N » Event				Save Logout Reboot Debug
✓ MAC Address Table								
✓ Spanning Tree	Eve	nt Tabi	le					
 Discovery 								
V DHCP	Showi	ng All	 entries 		Sh	owing 1 to	1 of 1 entries	0
✓ Multicast		Entry	Committee	Description	Madifiantian	Time	0	
✓ Routing		Entry	Community	Description	Notification	Time	Owner	
✓ Security		1		COMMANDO LAN	Event Log		COMMANDO	,
V ACL	The S	SNMP se	rvice is currentl	v disabled.				First Previous 1 Next Last
∨ QoS	For F	MON cor	nfiguration to be	e effective, the SNMP	service must be	enabled.		
 Diagnostics 								
 Management 		Add	Edit	Delete	View			
User Account Management Access Firmware Configuration SNMP SNMP Statistics Kratistics								
History Event Alarm Restore Factory Default								

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**.

COMMANDO															Sava	Logout	Pahaat	Debug
			_					_					_	_	 Save	Logout	Rebool	Debug
	Μ	lanag	emer	at »	RMO	N » A	larm											
✓ Network	·Γ																	
✓ Port	L	A1																
VLAN	ι.	Alarn	n Iad	Die														
 MAC Address Table 	ι.	Showing	AIL	v entrie					5	Showing 0 to () of 0 entries					0		
 Spanning Tree 	L									-						4	J	_
✓ Discovery	Ш		Entry	Dort	Co	inter	Sampling	Interval	Owner	Trigger	Risin	Ig	Falli	ıg				
✓ DHCP	ш		Linuy	FUIL	Name	Value	Jumping	Interval	Owner	inggei	Threshold	Event	Threshold	Event				
✓ Multicast	Ш										0	results fo	und.					
✓ Routing	Ľ	_														(First) (Pre	vious) 1 (N	ext Last
✓ Security	ι.	The SN For RM	VMP se ION co	ervice is	currently	/ disable	d. the SNMP of	envice mus	at he ench	lad								
✓ ACL	ι.	T OF IXIN		ingura	uon to be	CITCOUVE	, are orvan a	ionico mas	st be endb	iuu.								
∨ QoS	ι.	A	dd		Edit	D	elete											
 Diagnostics 	ι.																	
▼ Management	ι.																	
User Account	ι.																	
✓ Management Access	ι.																	
✓ Firmware	ι.																	
 Configuration 	ι.																	
✓ SNMP	ι.																	
∧ RMUN Statistics	ι.																	
History	ι.																	
Event																		
Alarm																		
Restore Eactory Default																		

Fig 16.6.8 RMON Default Alarm page

Ν	[anagement »]	RMON » Alarm		
✓ Status	Add Alarm			
V Network				
✓ Port	[:			
VLAN	Entry	1		
MAC Address Table	Port	GE1 🗸		
 Spanning Tree 	Counter	Received Packets		
Discovery	h			
· DHCP	Sampling	Absolute Date		
Multicast				
Routing	Interval	100	Sec (1 - 2147483647, default 100)	
Security	0			
ACL	Owner			
QoS		Rising		
Diagnostics	Trigger	Falling		
Management		Rising and Falling		
User Account	Distan			
 Management Access 	Rising			
V Firmware	Threshold	100	(0 - 2147483647, default 100)	
✓ SNMP	Event	1 - COMMANDO LAN		
A RMON	Lucit			
Statistics	Falling			
History				
Event	Threshold	20	(0 - 2147483647, default 20)	
Alarm Destare Factory Default	Event	1 - COMMANDO LAN		
Restore Factory Default	Li			
	Apply	Close		

Fig 16.6.9 RMON Add Alarm Counter page

COMMANDO	Mana	gemen	t » F	RMON » AI	arm						3	Save Logout	Reboot Debug			
✓ MAC Address Table																
 Spanning Tree 		m Tabl	e													
 Discovery 	Ala	in fabi	0													
V DHCP	Showin	Showing All 🗸 entries Showing 1 to 1 of 1 entries														
✓ Multicast																
✓ Routing		Entry Port		Sampling	ampling Interval		Trigger		Rising		Falling					
 Security 				Name Value					Threshold	Event	Threshold	Event				
ACL		1	GE1	Pkts 3060	Absolute	100		Rising	100	COMMANDO LAN	20	COMMANDO LAN				
QoS	The S	NMP ser	vice is c	urrently disabled												
Diagnostics	For R	MON con	figuratio	n to be effective, t	he SNMP servi	ice must be	enabled.									
Management	_															
User Account	/	Add	E	dit De	lete											
✓ Management Access																
✓ Firmware																
 Configuration 																
SNMP																
A RMON																
Statistics																
Event																
Alarm																
Restore Factory Default											_		>			

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.

COMMANDO												Save	Logout	Reboot	Debug
	POI	E Se	etting	z ≫ P	OE Port Se	etting									
✓ Status															^
✓ Network			Sys	tem Pov	ver(mW) 0										
✓ Port			Post		vor(mM) 0										
✓ POE Setting			nese												
POE Port Setting POE Port Timer Setting		S	ystem	lempe	rature(C) 47	None									
VLAN				Refr	esh Rate	5 sec									
 MAC Address Table 						10 sec									
✓ Spanning Tree	E.				i.O	30 Sec					i				
 Discovery 															
V DHCP	P	ort s	Settir	ng Tab	le										
 Multicast 				-											
✓ Routing													Q		
✓ Security			Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)				
✓ ACL		21.	1	CE1	Enabled	Off	AE(1)	0	N/A	N/A	NIA				_
✓ QoS				000	Enchled	01	AF(U)		N/A	N/A	NVA				
 Diagnostics 			2	GEZ	Enabled	01	AF(U)	0	IN/A	IN/A	INA				
✓ Management		<u> </u>	3	GE3	Enabled	Off	AF(U)	0	N/A	N/A	N/A				
			4	GE4	Enabled	Off	AF(U)	0	N/A	N/A	N/A				
			5	GE5	Enabled	Off	AF(U)	0	N/A	N/A	N/A				
			6	GE6	Enabled	Off	AF(U)	0	N/A	N/A	N/A				
			7	GE7	Enabled	Off	AF(U)	0	N/A	N/A	N/A				
			8	GE8	Enabled	Off	AF(U)	0	N/A	N/A	N/A				

Fig 17.1.2 PoE Port Setting System Default Info page

COMMANDO	PO	E Set	ting	» PC	DE Port Se	etting						Save Logout Reboot Debug				
✓ Status												,				
✓ Network																
✓ Port	s	System into														
▼ POE Setting					y											
POE Port Setting POE Port Timer Setting			Syste Reser	em Pow ve Pow	er(mW) 37 er(mW) 24	'10 640										
VLAN		System Temperature(C) 47														
 MAC Address Table 		System temperature() 4/														
 Spanning Tree 		O None O 5 sec														
 Discovery 				Refre	sh Rate	10 sec										
V DHCP					0	30 sec										
 Multicast 		_	-													
✓ Routing				. Tabl	_											
✓ Security		OIL SE	stung		e											
✓ ACL												0				
~ QoS	1.00									1		4				
 Diagnostics 		En En	itry	Port	PortEnable	Status	Туре	Level	Actual Power(mW)	Voltage(V)	Current(mA)					
✓ Management			1	GE1	Enabled	Off	AF(U)	0	N/A	N/A	N/A					
	(2	GE2	Enabled	Off	AF(U)	0	N/A	N/A	N/A					
	[3	GE3	Enabled	On	AF(N)	3	1855	53	35					
	[4	GE4	Enabled	Off	AF(U)	0	N/A	N/A	N/A					
	[5	GE5	Enabled	On	AF(N)	0	1855	53	35					
	[6	GE6	Enabled	Off	AF(U)	0	N/A	N/A	N/A					

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

COMMANDO												Save	Logout	Reboot	Debug
_	РС	DE S	ettin	g » Po	OE Port S	etting									
✓ Status															^
✓ Network															
✓ Port		Syst	em in	ito											
▼ POE Setting	ſ	·													
POE Port Setting POE Port Timer Setting			Sys Res	stem Pov erve Pov	ver(mW) 64 ver(mW) 24	66 640									
✓ VLAN		þ	System	n Temper	ature(C) 48										
✓ MAC Address Table															
✓ Spanning Tree						None 5 sec									
✓ Discovery				Refr											
✓ DHCP					Ō	30 sec									
✓ Multicast															
✓ Routing															
✓ Security		Port	Setti	ng lab	le										
✓ ACL															_
✓ QoS		_	_										Q		-
 Diagnostics 			Entry	Port	PortEnable	Status	Туре	Level	Actual Power(mW)	Voltage(V)	Current(mA)				
✓ Management			1	GE1	Enabled	Off	AF(U)	0	N/A	N/A	N/A				
			2	GE2	Enabled	Off	AF(U)	0	N/A	N/A	N/A				
	11		3	GE3	Enabled	On	AF(N)	3	3604	53	68				
			4	GE4	Enabled	Off	AF(U)	0	N/A	N/A	N/A				
			5	GE5	Enabled	On	AF(N)	0	2862	53	54				
			6	GE6	Enabled	Off	AF(U)	0	N/A	N/A	N/A				U

Fig 17.1.3 Selecting PoE Port for Setting page

COMMANDO	Save Logout Reboot Debug POE Setting » POE Port Setting
✓ Status	^
✓ Network	
✓ Port	Edit Port Setting
▼ POE Setting	
POE Port Setting POE Port Timer Setting	Port GE3,GE5
VLAN	PortEnable O Disable
 MAC Address Table 	ii.
 Spanning Tree 	Apply Close
✓ Discovery	
✓ DHCP	
✓ Multicast	
✓ Routing	
✓ Security	
✓ ACL	
✓ QoS	
 Diagnostics 	
✓ Management	

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.

COMMANDO	POE Set	ting	» p	OE I	Port	Tim	er Se	tting											Save	e 1	Logou	ıt]	Reboo	ot	Debuş
Status																									
V Network	Port GE1 V																								
✓ Port	Q															_									
✓ POE Setting		00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
POE Port Setting	Man		-													_ ·			_ ···						
POE Port Timer Setting	MON																								
VLAN	Tue	\square		\leq	\bowtie	\leq		\square	\leq		\sim	\bowtie		\leq	\bowtie	\leq	\square		\leq		\square	\square	\square	\square	
 MAC Address Table 	Wed	\square	\checkmark	\checkmark	\square	\checkmark	\square	\checkmark	\checkmark	\square	\checkmark	\square	\checkmark	\square	\square	\checkmark	\square		\checkmark			\square	\checkmark		
✓ Spanning Tree	Thu	\square	\checkmark	\checkmark	\square	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\square	\checkmark	\checkmark	\square	\checkmark	\bowtie	\checkmark	\checkmark		\checkmark	\square	\checkmark	\square	
✓ Discovery	Fri	\square	\square	\checkmark	\square	\checkmark	\square	\square	\square	\square	\checkmark	\square	\checkmark	\checkmark	\square	\checkmark	\square	\square	\checkmark			\square	\checkmark	\square	
V DHCP	Sat	\square	\checkmark	\checkmark	\square	\checkmark	\square	\checkmark	\checkmark	\checkmark	\checkmark	\square	\checkmark	\leq	\square	\checkmark	\checkmark	\square	\checkmark		\square	\square	\checkmark		
✓ Multicast	Sun	\square	\square	\checkmark		\checkmark	\square	\checkmark	\square	\square	\checkmark			\checkmark		\checkmark	\square	\checkmark	\checkmark				\checkmark		
✓ Routing																									
✓ Security	App	oly																							
V ACL																									
✓ QoS																									
✓ Diagnostics																									
✓ Management																									

Fig 17.2.1 Default PoE Port Timer Setting for GE1 page

COMMANDO	PO	E Set	ting	» P	OE I	Port	Tim	er So	etting	5										Save	e I	ogou	ıt]	Zebo	ot	Debug
✓ Status																										
✓ Network	P	ort GE	3 ~																							
✓ Port																						(a 🗆			
✓ POE Setting	10		00	01	02	02	04	05	06	07	0.0	09	10	11	12	12	14	15	16	17	10	10	20	21	22	22
POE Port Setting POE Port Timer Setting	E	Mon																								
VLAN		Tue	\square	\leq	\bowtie	\square	\checkmark	\checkmark	\square	\checkmark	\square	\square	\checkmark	\square	\square	\checkmark	\leq	\square	\checkmark	\leq	\square	\checkmark	\checkmark	\square	\checkmark	
V MAC Address Table		Wed	\checkmark	\checkmark	\checkmark	\checkmark		\checkmark	\checkmark	\checkmark	\square	\square		\square	\checkmark	\checkmark	\checkmark	\square	\checkmark	\checkmark	\square	\checkmark	\checkmark	\square	\checkmark	
✓ Spanning Tree		Thu	\square	\checkmark	\bowtie	\square	\checkmark	\checkmark	\square	\checkmark	\square	\square	\checkmark	\square	\square	\checkmark	\checkmark	\square	\checkmark	\checkmark	\square	\checkmark	\square	\square	\checkmark	
✓ Discovery		Fri	\square	\leq	\bowtie	\square	\checkmark	\bowtie	\square	\leq	\square	\square	\checkmark	\square	\square	\checkmark	\checkmark	\square	\checkmark	\leq	\square	\checkmark	\square	\square	\checkmark	
✓ DHCP		Sat																								
✓ Multicast		Sun																								
✓ Routing																										_
✓ Security		Appl	ly																							
✓ ACL																										
✓ QoS																										
✓ Diagnostics																										
✓ Management																										

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