COMMANDO Soldier E3000 Series Managed Routing Switch Command Line Interface Guide (CLI Guide)

SoldierOS Version 3K.v1.10 Onwards

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

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Trademarks and Permissions

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

Notice

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

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

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

TABLE OF CONTENTS

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Intended Audience:

This document is intended for:
Network Device configuration and Troubleshooting Engineers

Internetworking Professionals and Experts

System maintenance engineers

Command Symbols

The command symbols that may be found in this document are defined as follows.

Table 1. General command symbols

Symbols	Description
Boldface	The keywords of a command line are in **boldface**. These Keywords are command syntax.
Italic	Command arguments are in *italics.*
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
< >	Compulsory input.
{ }	Optional items.
|	Separated by vertical bars. One item is selected.
#	# sign is comments.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Intended Audience:

This document is intended for:
Network Device configuration and Troubleshooting Engineers

Internetworking Professionals and Experts

System maintenance engineers

Command Symbols

The command symbols that may be found in this document are defined as follows.

Table 1. General command symbols

Symbols	Description
Boldface	The keywords of a command line are in **boldface**. These Keywords are command syntax.
Italic	Command arguments are in *italics.*
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
< >	Compulsory input.
{ }	Optional items.
|	Separated by vertical bars. One item is selected.
#	# sign is comments.

Shortcut Keys
Back Space Delete a character before the cursor, and the cursor moves back.
Up "↑" Show previous command entered. Up to ten recently entered commands can be shown.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Down “↓” Show next command entered. When use the Up key to get previously entered commands, you can use the Down key to return to the next command
Left “←” The cursor moves one character to the left.
Right “→” The cursor moves one character to entered command.
Ctrl +p The same as Up key “↑”.
Ctrl +n The same as Down key “↓”.
Ctrl +b The same as Left key “←”.
Ctrl +f The same as Right key “→”.
Ctrl +z Return to the Admin Mode directly from the other configuration modes
Ctrl +c Break the ongoing command process, such as ping or other command execution.
Tab When a string for a command or keyword is entered, the Tab can be used to complete the command or keyword if there is no conflict.

Help to configure Switch

Under any command line prompt, type in “?” and press Enter will geta brief description of the associated command.

1. Under any command line prompt, enter “?” to get a command list of the current mode and related brief description.

2. Enter “?” after the command keyword with an embedded space. If the position should be a parameter, a description of that parameter type, scope, etc., will be returned. if the position should be a keyword, then a set of keywords with brief description will be returned. if the output is “<cr>“, then the command is complete, press Enter to run the command.

3. “?” immediately following a string. This will display all the commands that begin with that string.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Introduction

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

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

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

cost of ownership, they enable scalable, secure, and energy-efficient business operations with intelligent and automated services.

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

These switches have advanced Security features, and advanced Quality of Service (QoS), ideal for all organizations considering reliable, affordable hardware with well-known CLI and simple Web managed real time interface. Automated PoE/PoE+ scheduling, Scripting capabilities, Layer 3 routing, Automatic MDIX and Auto-negotiation on all ports select the right transmission modes (half or full duplex) as well as data transmission for crossover or straight-through cables dynamically. Moreover, with its innovative energy-efficient technology, can save up to 58% of power consumption, making it an eco-friendly perfect solution for your business network.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

These switches come with lifetime free software upgrades and patching to enhance features and supports patching, which provides fixes for critical bugs and security vulnerabilities between regular maintenance upgrades. This support allows customers to add new features and upgrades without having to pay a single dollar.

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

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

segmentation requirements. This series switches also have provisioning of QOS, Static and dynamic routing for IPV6 clients.

Simplified Configuration and Management

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

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

Remote Manageability

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

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

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

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

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Management Access Modes

Accessing the Switch via console port

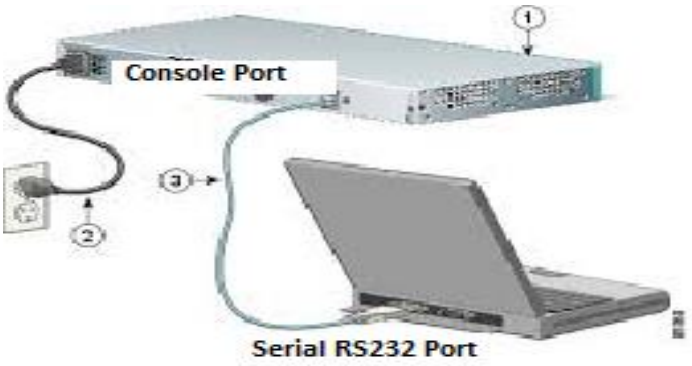
How to Login COMMANDO Series E3000 via console port?

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

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

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

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



© 2024 COMMANDO Networks Inc., USA. All rights reserved.

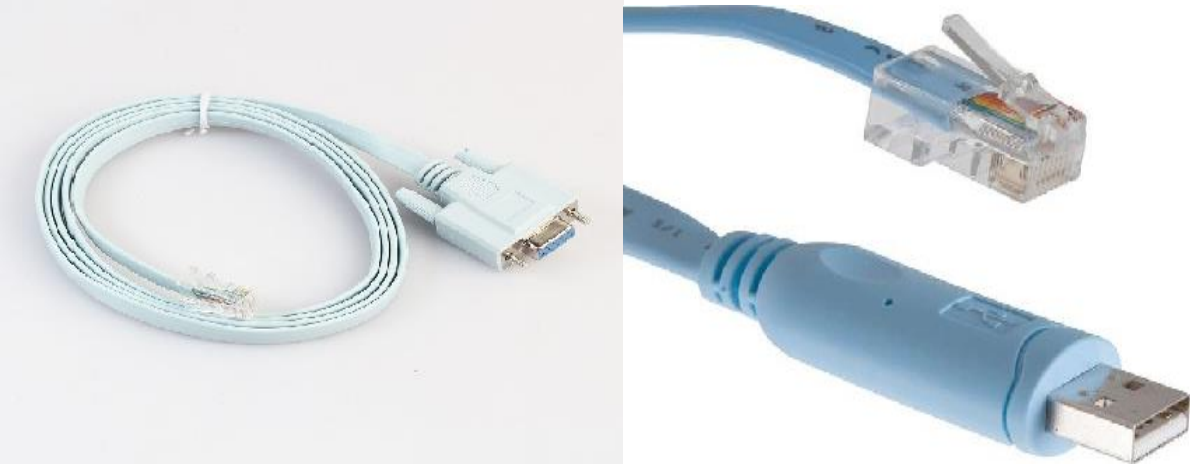


Fig-1. Connection of console port with PC/Laptop via console cable.

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

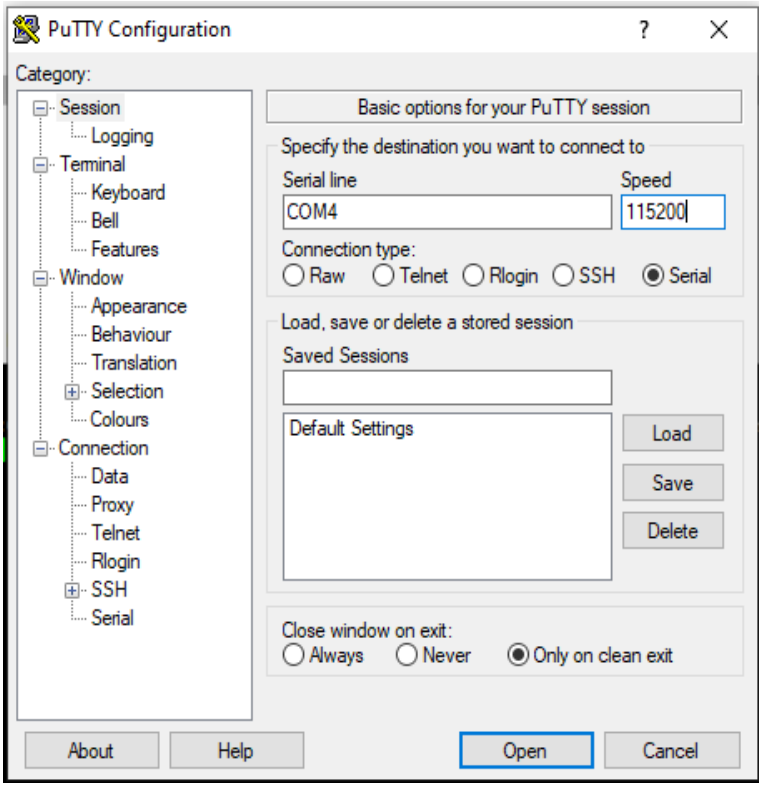


Fig-2. PuTTY configuration in PC for console port access

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

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

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

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

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

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

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

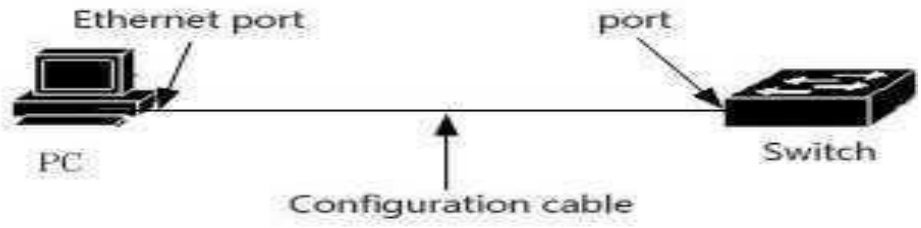


Fig-4. COMMANDO Series E3000 Switch port connected with PC via RJ45 LAN cable.

In PC following LAN setting required.

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

IP Address: 192.168.0.(2-254)
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.0.1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

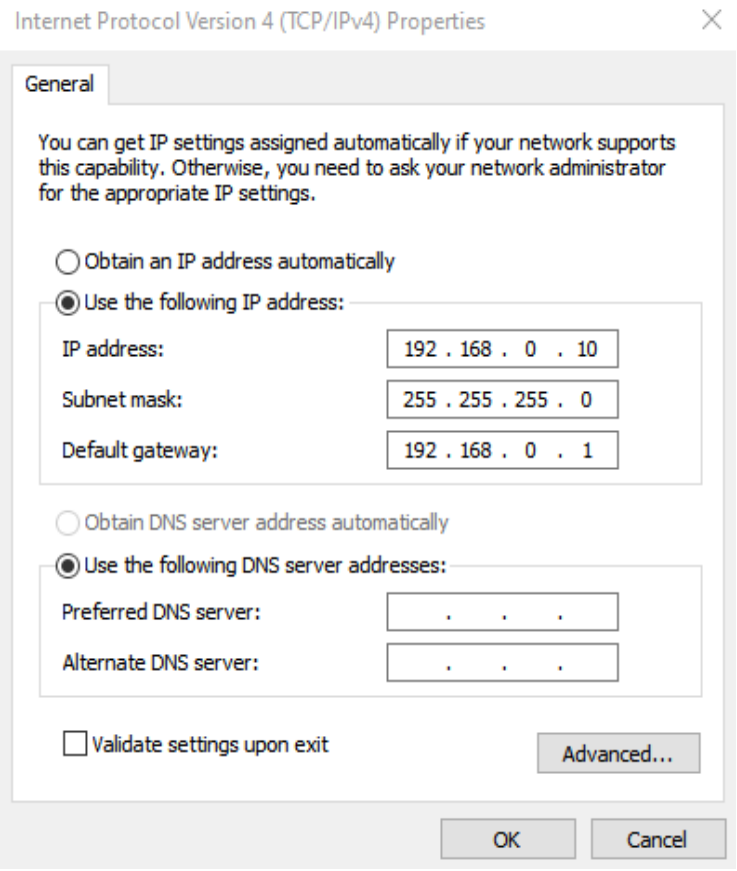


Fig-5. Local Area Connection properties for Web Interface

Now Open any web browser type http://192.168.0.1 and hit **"Enter"** following window will appear.

Use following login details to enter in WEB GUI mode,

Username: **admin**
Password: ********
(Note: Password is mentioned on backside of device)

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

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

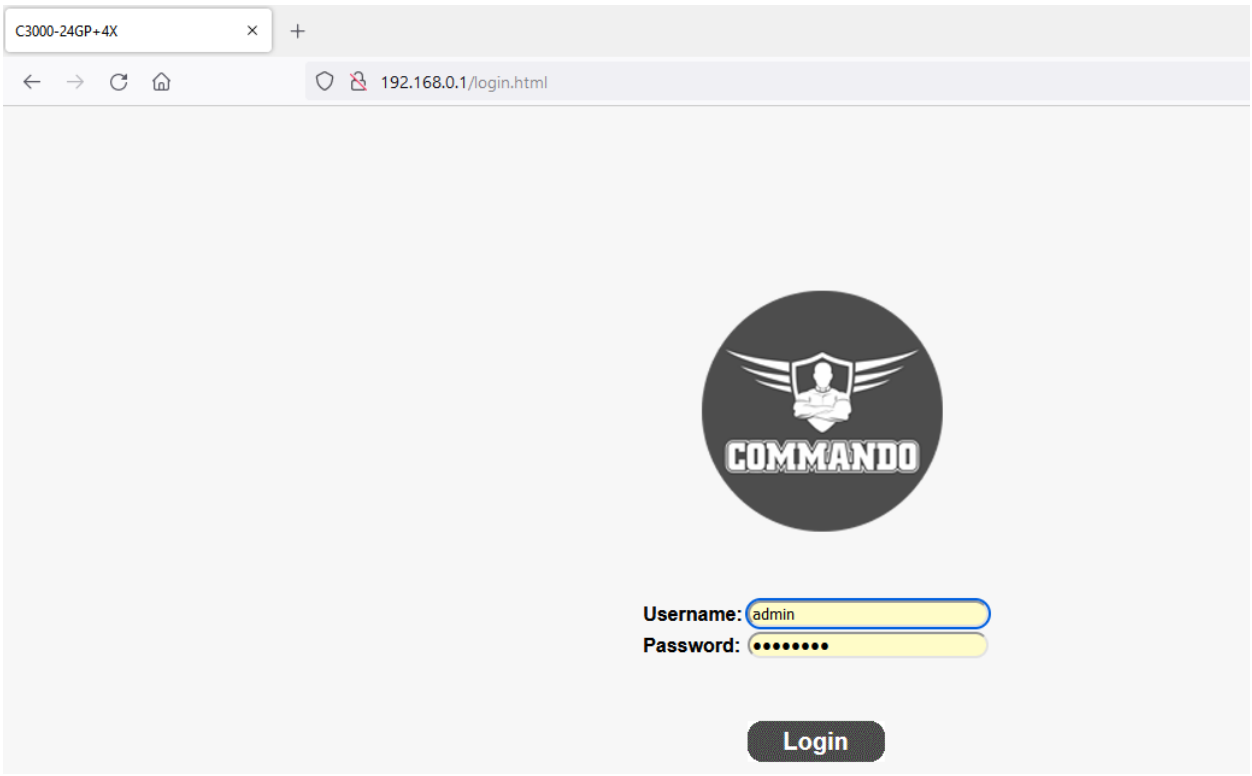


Fig-6. COMMANDO E3000 Switch WEB GUI Administrator Login Page

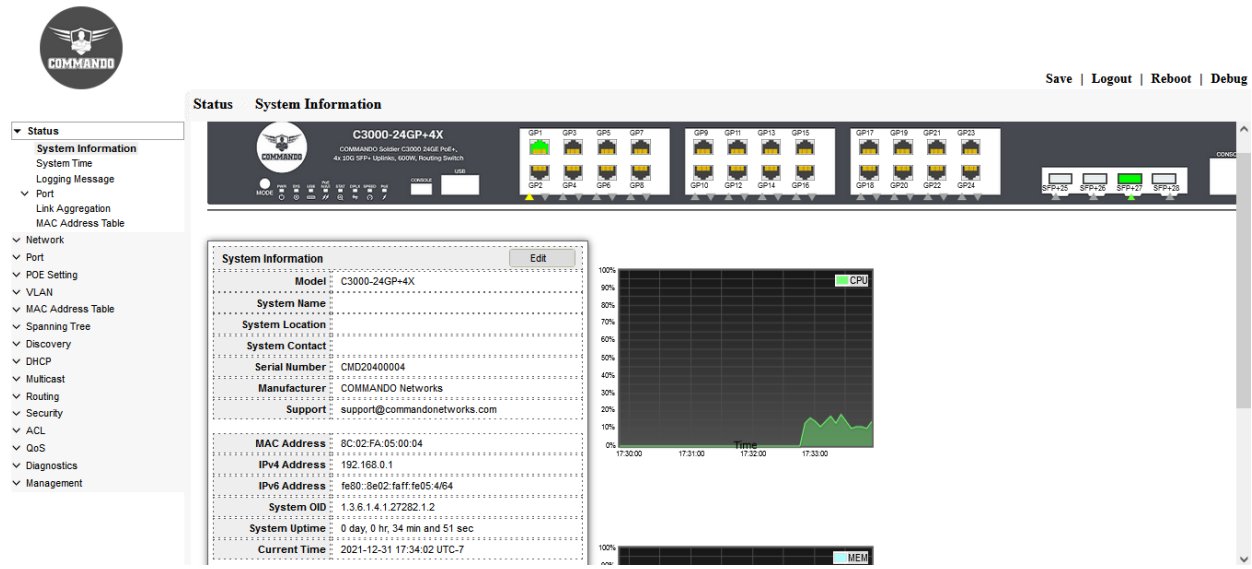


Fig-7. COMMANDO E3000 Switch WEB GUI starting Page

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Following steps are required to access CLI via telnet lines.

Management>>Management Access>>Management Service

Click on **Management**

Click on **Management Access**

Click on **Management Services**

Telnet Click on ☑

"Apply" and **"Save"** the configuration.

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

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

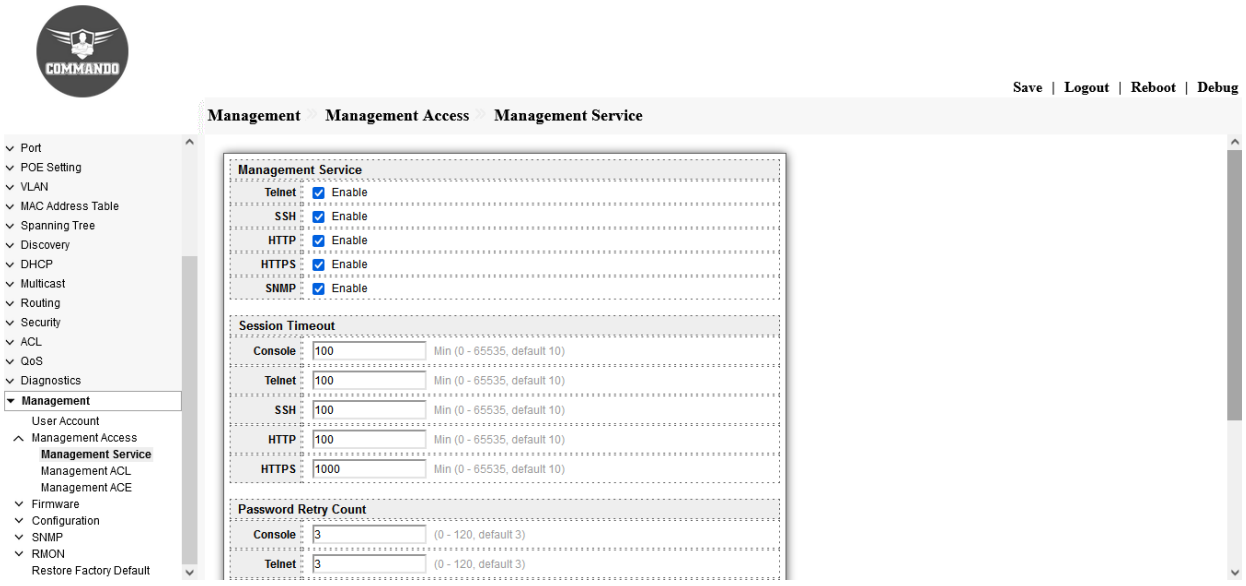
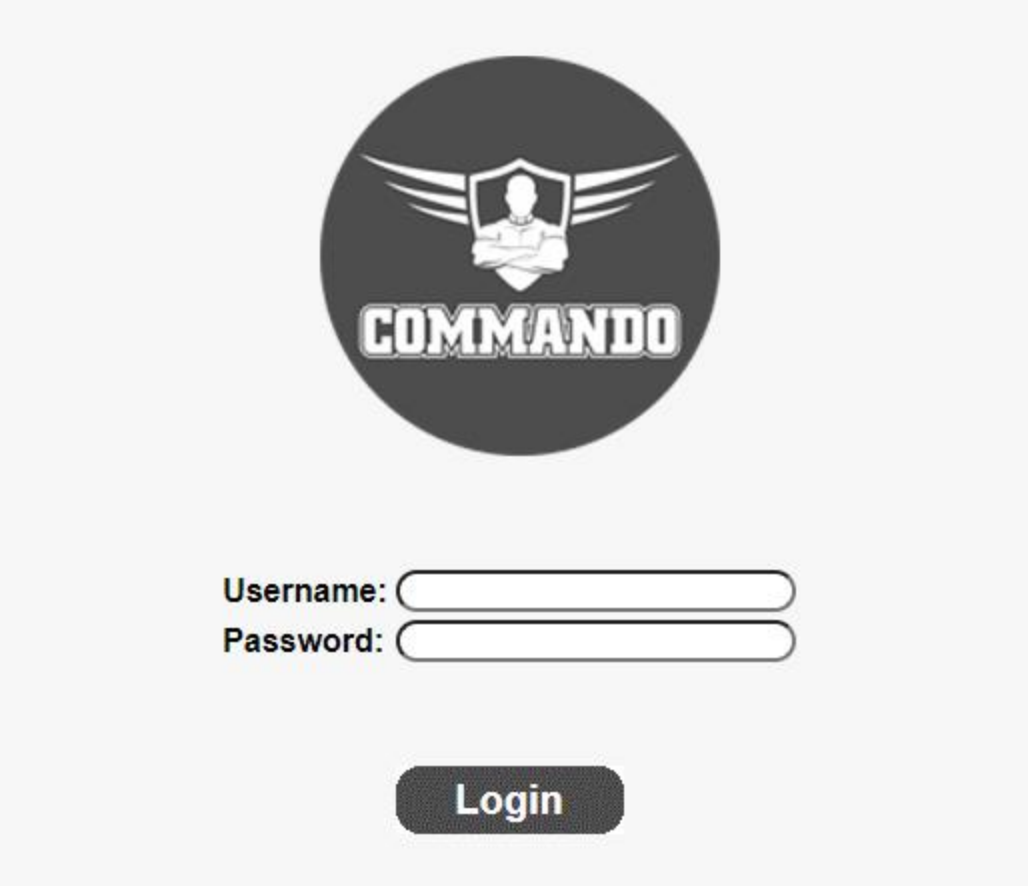


Fig-8. COMMANDO E3000 Switch Management Access service.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Web browse based graphical user interface (Web GUI)

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



© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Fig 9. Username and Password page of E3000 Series Switches

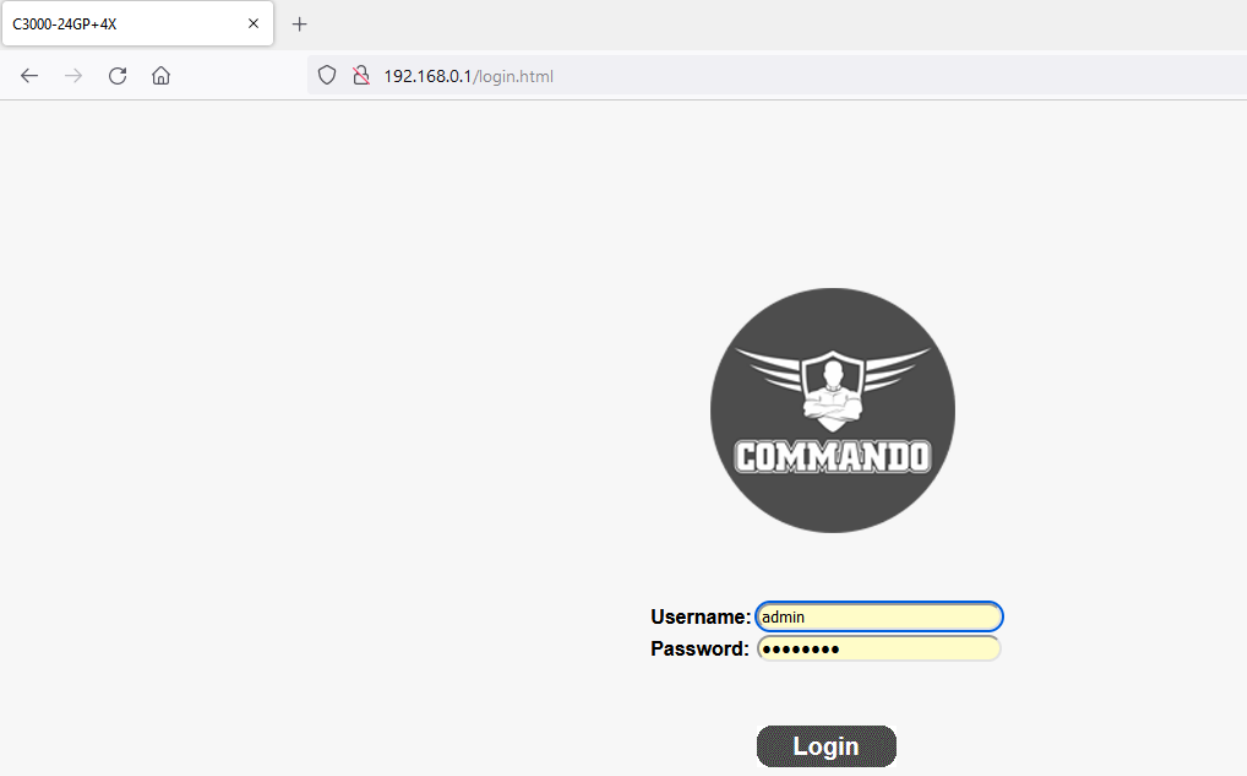


Fig 10. Default Login page of E3000 Series Switches

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

1. You can change default IP 192.168.0.1 to any desired IP address.

2. You can change Factory set username: admin and password: *******.

3. Factory set default Password is written on the Backside of device.

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

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

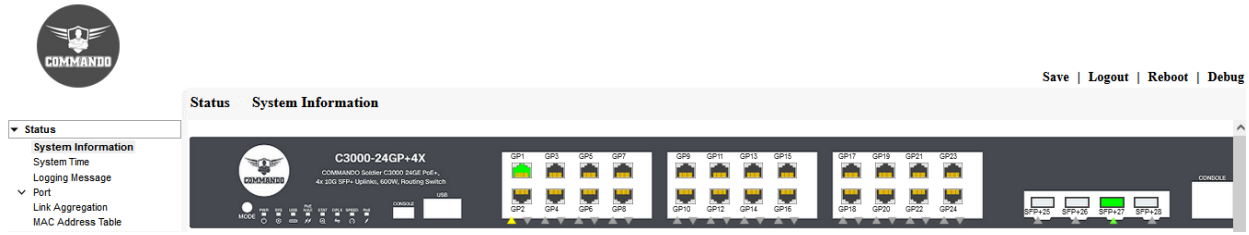


Fig 11. System Information page of E3000 Series Switches

Management via Telnet configuration in CLI

To Configure the switch with Telnet, users should type the CLI command telnet-server enable in the global mode as below:

Step 1: Enable telnet-server

Switch>**enable**

Switch#**configure terminal**

Switch(config)# **telnet-server enable**

Step 2: Run Telnet Client program (PuTTY)

The communication parameters configuration of the PuTTY Terminal with TELNET is shown below：
IP Address: **192.168.0.1**
Port: **23**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

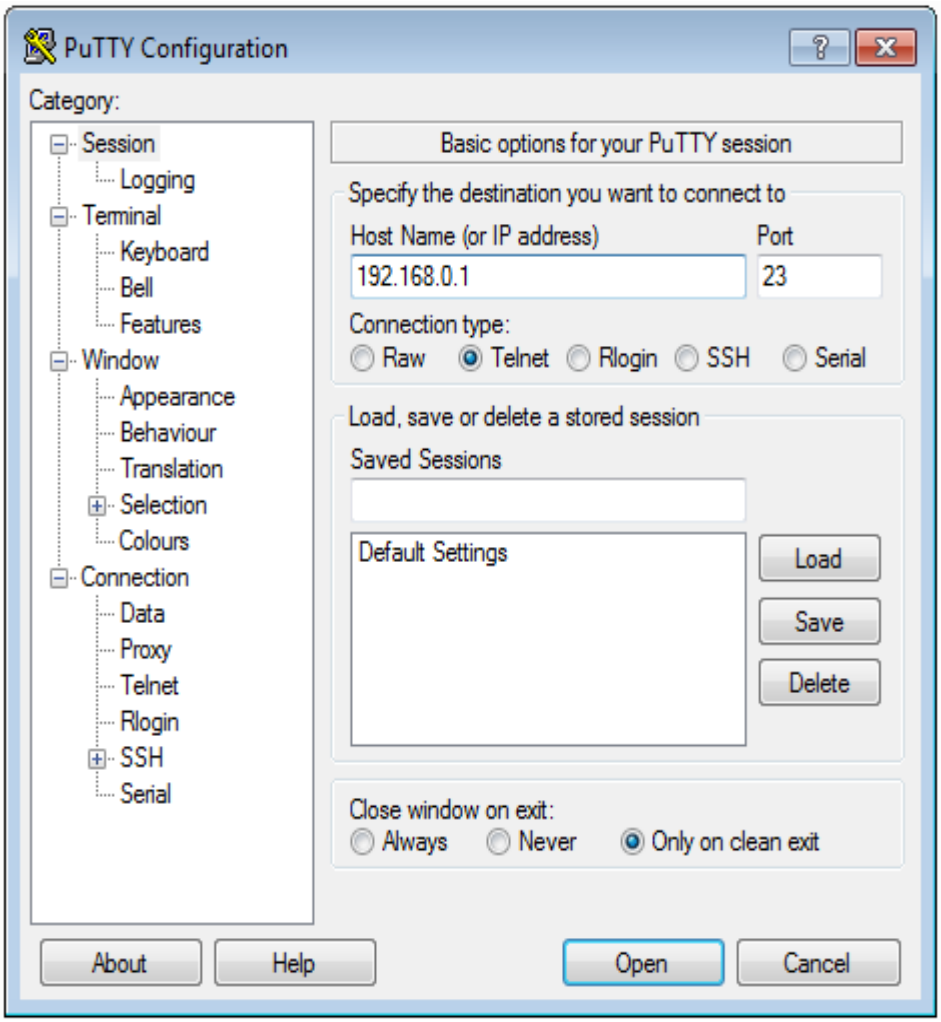


Fig-12. PuTTY configuration in PC for Telnet access

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

Username: **admin**

Password: ********

(Note: Password is mentioned on backside of device)

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

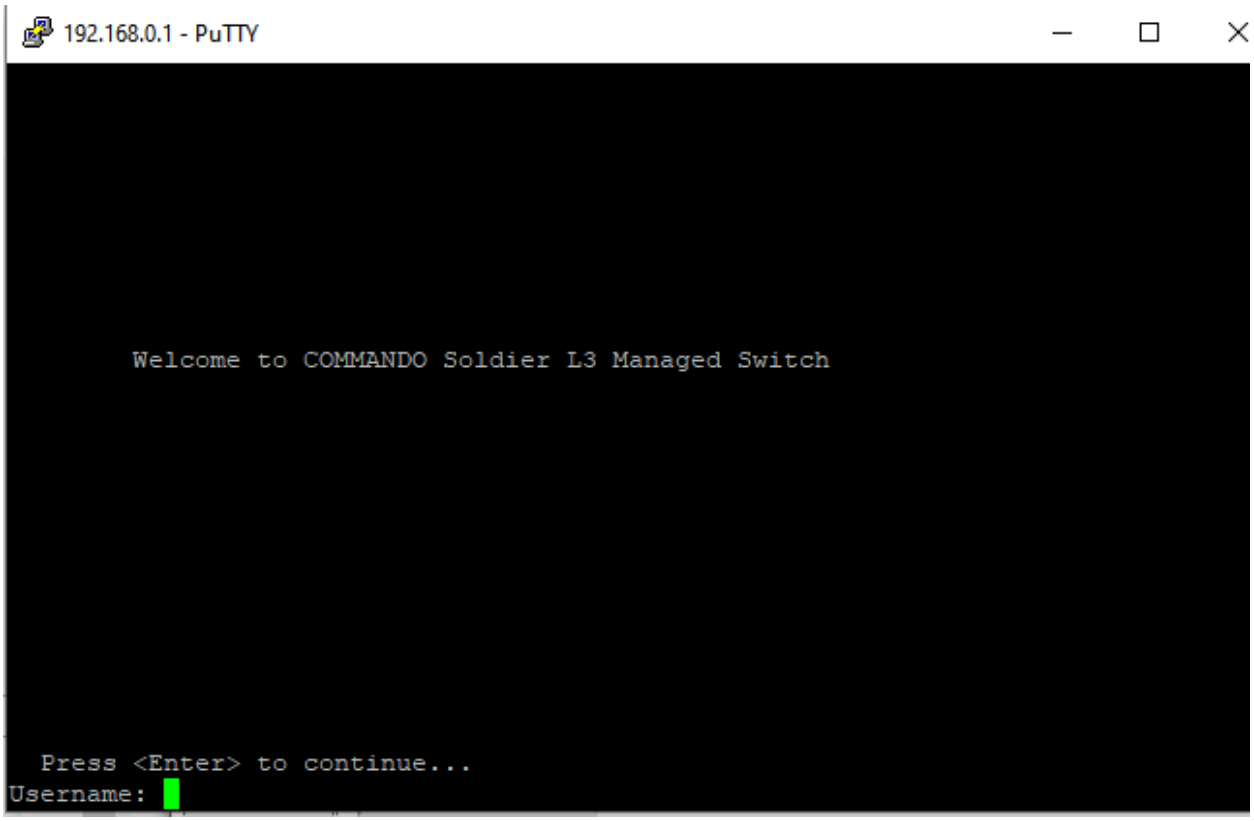


Fig-13. COMMANDO Series E3000 Switch CLI access via telnet

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1. ADMINISTRATION

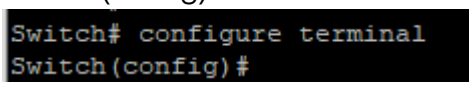
General commands used in E3000 Series Switches are described in the Administration. The switch administration is to perform some basic switch administration tasks. These commands are generally used for basic configuration of switch.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.1 CONFIGURE TERMINAL

Use **"configure terminal"** command to enter global configuration mode. In global configuration mode, the prompt will show as **"Switch(config)#"**.

Switch#**configure terminal**
Switch(config)#

Syntax	**Configure terminal**
Mode	Privileged EXEC
Example	This example shows how to enter global configuration mode. Switch#configure **terminal** Switch(config)# 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.2 CLEAR ARP

Use **"clear arp-cache"** command to clear all or specific one ARP entry. Clear the dynamic ARP learnt by the switch.

Switch#clear arp-cache

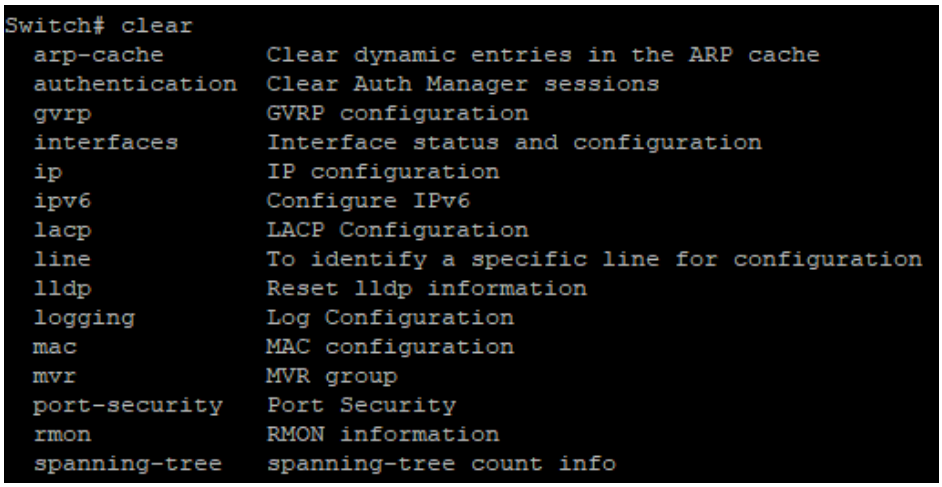
Syntax	clear arp-cache
Mode	User EXEC Privileged EXEC
Example	This example shows how to clear all arp entries. Switch#clear arp-cache Switch# sh arp VLAN Interface IP address HW address Status vlan 1 192.168.0.21 28:d2:44:0a:7e:9c Dynamic Total number of entries: 1 Switch# clear arp-cache Used to clear the non-aged out unavailable ARP entries

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.3 CLEAR Service

Use **"clear"** command to kill all existing sessions for the select service.

Switch# **clear (arp-cache | authentication | gvrp | interfaces | ip | ipv6 | lacp | line | lldp | logging | mac | mvr | port-security | rmon | spanning-tree)**

Syntax	**clear (arp-cache | authentication | gvrp | interfaces | ip | ipv6 | lacp | line | lldp | logging | mac | mvr | port-security | rmon | spanning-tree)**
Mode	Privileged EXEC
Example	 This example shows how to clear interfaces, Switch# **clear interfaces GigabitEthernet 1 counters**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show interfaces g1
GigabitEthernet1 is up
  Hardware is Gigabit Ethernet
  Auto-duplex, Auto-speed, media type is Copper
  back-pressure is enabled
     7561 packets input, 1062238 bytes, 0 discarded packets
     1493 broadcasts  1814 multicasts 4254 unicasts
     0 runts, 0 giants, 0 discarded packets
     0 input errors, 0 CRC, 0 frame
     1814 multicast, 0 pause input
     0 input packets with dribble condition detected
     last 5 minutes input rate 1688 bits/sec, 1 packets/sec

     7554 packets output, 1879752 bytes, 0 discarded packets
     2 broadcasts  3346 multicasts 4206 unicasts
     0 output errors, 0 collisions
     0 babbles, 0 late collision, 0 deferred
     0 PAUSE output
     last 5 minutes output rate 944 bits/sec, 1 packets/sec
Switch# clear interfaces g1 counters
Switch# show interfaces g1
GigabitEthernet1 is up
  Hardware is Gigabit Ethernet
  Auto-duplex, Auto-speed, media type is Copper
  back-pressure is enabled
     10 packets input, 640 bytes, 0 discarded packets
     2 broadcasts  0 multicasts 8 unicasts
     0 runts, 0 giants, 0 discarded packets
     0 input errors, 0 CRC, 0 frame
     0 multicast, 0 pause input
     0 input packets with dribble condition detected
     last 5 minutes input rate 1792 bits/sec, 2 packets/sec

     7 packets output, 515 bytes, 0 discarded packets
     0 broadcasts  1 multicasts 6 unicasts
     0 output errors, 0 collisions
     0 babbles, 0 late collision, 0 deferred
     0 PAUSE output
     last 5 minutes output rate 1032 bits/sec, 1 packets/sec
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.4 ENABLE

In User EXEC mode, user only allows to do a few actions. Most of commands are only available in privileged EXEC mode. Use **"enable"** command to enter the privileged mode to do more actions on switch. In privileged EXEC mode, use "exit" command is able to go back to user EXEC mode with original user privilege level. If you need to go back to user EXEC mode with different privilege level, use **"disable"** command to specify the privilege level you need. In privileged EXEC mode, the prompt will show**"Switch#".**

Switch>**enable** [*<1-15>*]
Switch#**disable** [*<1-14>*]
Note: Default Enable password is <Enter Button>

Syntax	**enable** [*<1-15>*] **disable** [*<1-14>*]
Parameter	*<1-15>* Specify privileged level to enable *<1-14>* Specify privileged level to disable
Default	Default privilege level is 15 if no privilege level is specified on enable command. Default privilege level is 1 if no privilege level is specified on disable command.

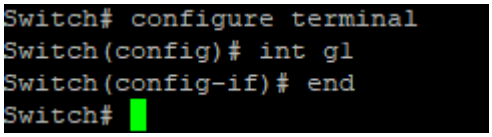
Example	This example shows how to enter privileged EXEC mode and show current privilege level.
	Switch>**enable**
	Password:
	Switch# **show privilege**
	`Switch> en`
	`Password:`
	`Switch# disable`
	`  <1-14>  Privilege level`
	`  <cr>`
	`Switch# show privilege`
	`Current CLI Username:  admin`
	`Current CLI Privilege: 15`
	
	Switch# **disable**
	Switch>

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.5 END

Use **“end”** command to return to privileged EXEC mode directly. Every mode except User EXEC mode has the **“end”** command.

Switch#**configure terminal**
Switch(config)# **interface GigabitEthernet 1**
Switch(config-if)# **end**

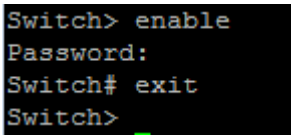
Syntax	**end**
Mode	Privileged EXEC Global Configuration Interface Configuration Line Configuration
Example	This example shows how to enter Interface Configuration mode and use end command to go back to privileged EXEC mode Switch#**configure terminal** Switch(config)# **interface GigabitEthernet 1** Switch(config-if)# **end** Switch# 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.6 EXIT

In User EXEC mode, **"exit"** command will close current CLI session. In other modes, **"exit"** command will go to the parent mode. And every mode has the **"exit"** command.

Switch# **exit**

Syntax	**exit**
Mode	User EXEC Privileged EXEC Global Configuration Interface Configuration Line Configuration
Example	This example shows how to enter privileged EXEC mode and use exit command to go back to user EXEC mode. Switch>**enable** Switch# **exit** Switch> 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.7 HISTORY

Use **“history”** command to specify the maximum commands history number for CLI running on console, telnet or ssh service. Every command input by user will record in history buffer. If all history commands exceed configured history number, older ones will be deleted from buffer. Use **“no history”** to disable the history feature. And use “show history” to show all history commands.

Switch#**configure terminal**
Switch(config)# **line console**
Switch(config-line)# **history 100**
Switch(config-line)# **exit**

Syntax	**history** *<1-256>* **no history**
Parameter	*<1-256>*Specify maximum CLI history entry number.
Default	Default maximum history entry number is 128.
Mode	Line Configuration
	This example shows how to change console history number to 100, telnet history number to 150 and ssh history number to 200. Switch#**configure terminal** Switch(config)# **line console** Switch(config-line)# **history 100** Switch(config-line)# **exit** Switch(config)# **line telnet** Switch(config-line)# **history 150** Switch(config-line)# **exit** Switch(config)# **line ssh** Switch(config-line)# **history 200** Switch(config-line)# **exit** This example shows how show line information. Switch# **show line**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# line telnet
Switch(config-line)# history 100
Switch(config-line)# exit
Switch(config)# exit
Switch# show line
Console ==============================
    Session Timeout : 10 (minutes)
    History Count   : 100
    Password Retry  : 3
    Silent Time     : 0 (seconds)
Telnet ===============================
    Telnet Server   : enabled
    Session Timeout : 10 (minutes)
    History Count   : 100
    Password Retry  : 3
    Silent Time     : 0 (seconds)
SSH ==================================
    SSH Server      : enabled
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
```

This example shows how show history commands.

Switch# show history

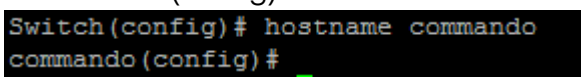
```
Switch# show history
Maximun History Count: 100
------------------------------------------------------------
1. exit
2. enable
3. exit
4. enable
5. configure
6. interface GigabitEthernet 1
7. end
8. exit
9. enable
10. exit
11. enable
12. configure
13. line console
14. history 100
15. exit
16. line telnet
17. history 100
18. exit
19. show line
20. show history
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.8 HOSTNAME

Use **"hostname"** command to modify hostname of the switch. The system name is also used to be CLI prompt. Specifies the host name for the switch. This command specifies or modifies the host name (Maximum length: 255 characters)

Switch#**configure terminal**
Switch(config)# **hostname** *{WORD}*

Syntax	**hostname** *{WORD}*
Parameter	*WORD* Specify the hostname of the switch.
Default	Default name string is **"Switch"**.
Mode	Global Configuration
Example	This example shows how to modify contact information Switch#**configure terminal** Switch(config)# **hostname commando** commando(config)# 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.9 INTERFACE

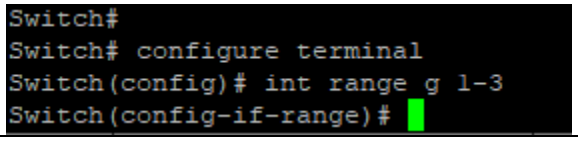
Some configurations are port based. To configure these configurations, we need to enter Interface Configuration mode to configure them. Use **"interface"** command to enter the Interface Configuration mode and select the port to be configured. In Interface Configuration mode, the prompt will show as **"Switch(config- if)#"**

Switch#**configure terminal**
Switch(config)# **interface** *{IF_PORTS}*
Switch(config)# **interface range** *{IF_PORT starting - IF_PORT ending }*

Syntax	**interface** *{IF_PORTS}* **interface range** *{IF_PORTS}*
Parameter	*IF_PORTS* Specify the port to select. This parameter allows partial port name and ignore case. For Example: GigabitEthernet 1, GigabitEthernet2, GigabitEthernet3 and so on If port range is specified, the list format is also available. For Example: gi1,3,5 gi2, gi1-3
Mode	Global Configuration
Usage	Some configurations are port based. In order to configure these configurations, we need to enter Interface Configuration mode to configure them. Use "interface" command to enter the Interface Configuration mode and select the port to be configured. In Interface Configuration mode, the prompt will show as **"Switch(config- if)#"**

Example	This example shows how to enter Interface Configuration mode
	Switch#**configure terminal**
	Switch(config)# **interface GigabitEthernet 1**
	Switch(config-if)#
	`Switch# configure`
	`Switch(config)# interface GigabitEthernet 1`
	`Switch(config-if)#`
	
	Switch#**configure terminal**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch(config)# interface range GigabitEthernet 1-3 Switch(config-if-range)# 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

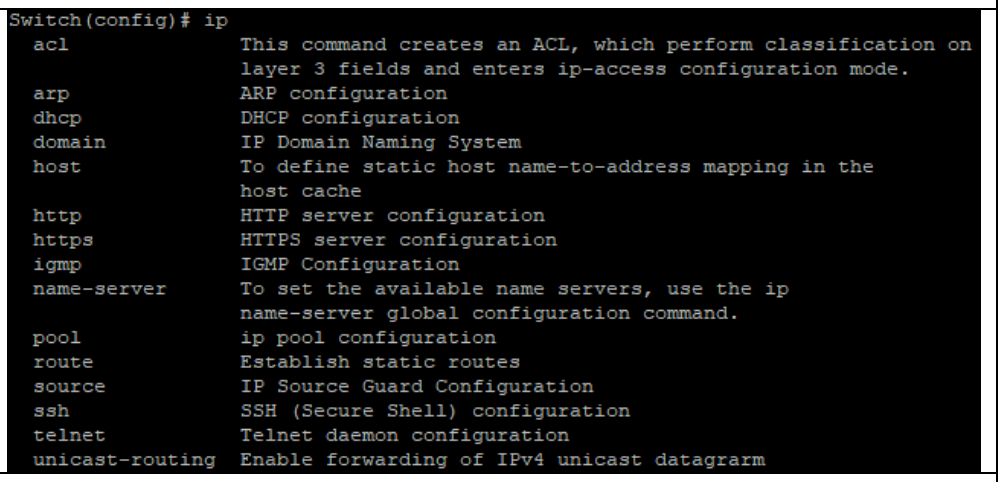
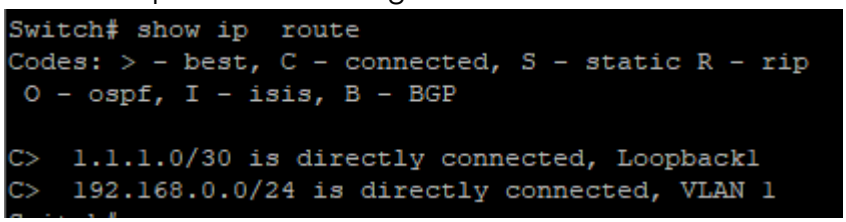
1.10 IP

Use **“ip”** command followed by combination to configure important E3000 series switches Functions as follows.

acl	This command creates an ACL, which perform classification on layer 3 fields and enters ip-access configuration mode.
arp	ARP configuration
dhcp	DHCP configuration
domain	IP Domain Naming System
host	To define static host name-to-address mapping in the host cache
http	HTTP server configuration
https	HTTPS server configuration
Igmp	IGMP Configuration
name-server	To set the available name servers, use the ip name-server global configuration command.
pool	ip pool configuration
route	Establish static routes
source	IP Source Guard Configuration
ssh	SSH (Secure Shell) configuration
telnet	Telnet daemon configuration
unicast-routing	Enable forwarding of IPv4 unicast datagrarm

Switch#**configure terminal**
Switch(config)# **ip (acl | arp | dhcp | domain | host | http | https | igmp | name-server | pool | route | source | ssh | telnet | unicast-routing**)

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Syntax	ip (acl | arp | dhcp | domain | host | http | https | igmp | name-server | pool | route | source | ssh | telnet | unicast-routing)
Parameter	
Default	NIL
Mode	Global Configuration
Example	This example shows routing table of E3000 series Switches 

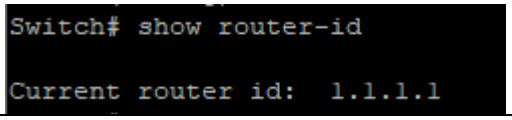
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.11 Router-id

Use **“router-id”** is a 32-bit IP address that uniquely identifies a router in an Autonomous System (AS).

Switch#**configure terminal**
Switch(config)# **router-id** *{A.B.C.D}*

Switch(config)# **no router-id**

Syntax	**router-id** *{A.B.C.D}* **no router-id**
Parameter	*A.B.C.D* Specify router ID IPv4 address for switch
Default	NA
Mode	Global Configuration
Example	This example shows how to modify the ipv4 address of the switch. Switch#**configure terminal** Switch(config)# **router-id 1.1.1.1** This example shows how to show current ipv4 router ID of the switch. 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.12 IP DHCP SNOOPING

Use **"ip dhcp snooping"** is a security feature that acts like a security program between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs the following activities: • Validates DHCP messages received from untrusted sources and filters out invalid messages.

Use **"no ip snooping"** command to disabled dhcp client and use static ip address.

Switch#**configure terminal**
Switch(config)# **ip dhcp snooping**

Switch(config)# **no ip dhcp snooping**

Syntax	**ip dhcp snooping** **no ip dhcp snooping**
Default	Default DHCP snooping is disabled.
Mode	Global Configuration

Example	This example shows how to enable dhcp snooping.
	Switch#**configure terminal**
	Switch(config)# **ip dhcp snooping**
	This example shows how to show current dhcp snooping state of the switch.
	Switch# **show ip dhcp snooping**
	`Switch# show ip dhcp snooping`
	
	`DHCP Snooping : enabled`
	`Enable on following Vlans : None`
	`circuit-id default format: vlan-port`
	`remote-id: : 8c:02:fa:05:00:04 (Switch Mac in Byte Order)`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.13 IPV6 AUTOCONFIG

Use **“ipv6 autoconfig”** command to enabled IPv6 auto configuration feature. Use **“no ipv6 autoconfig”**command to disabled IPv6 auto configuration feature.

Switch#**configure terminal**
Switch(config)# **ipv6 autoconfig**

Switch(config)# **no ipv6 autoconfig**

Syntax	**ipv6 autoconfig** **no ipv6 autoconfig**
Default	Default IPv6 auto config is enabled.
Mode	Global Configuration

Example	This example shows how to enable IPv6 auto config.
	Switch#**configure terminal**
	Switch(config)# **ipv6 autoconfig**
	This example shows how to show current IPv6 auto config state.
	Switch# **show ipv6 interface**
	`Switch# configure terminal`
	`Switch(config)# ipv6 autoconfig`
	`Switch(config)#`
	`Switch# show ipv6 interface`
	`VLAN 1 is up/up`
	`IPv6 is enabled, link-local address is fe80::8e02:faff:fe05:4`
	`IPv6 Forwarding is disabled`
	`No global unicast address is configured`
	`Joined group address(es):`
	`ff02::1:ff05:4`
	`ff02::1`
	`ff01::1`
	`ND DAD is enabled, number of DAD attempts: 1`
	`Stateless autoconfiguration is enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.14 IPV6 ADDRESS

Use **"ipv6 address"** command to specify static IPv6 address.

Switch#**configure terminal**
Switch(config)# **ipv6 address** *{X:X::X:X}* **prefix** *<0-128>*

Syntax	**ipv6 address** *X:X::X:X* **prefix** *<0-128>*
Parameter	**address***X:X::X:X* Specify IPv6 address for switch **prefix***<0-128>* Specify IPv6 prefix length for switch
Mode	Global Configuration

Example	This example shows how to add static ipv6 address of the switch.
	Switch#**configure terminal**
	Switch(config)# **ipv6 address 2001::1 prefix 64**
	`Switch# configure terminal`
	`Switch(config)#  ipv6 address`
	`  X:X::X:X  IPv6 address`
	`Switch(config)#  ipv6 address 2001::1 prefix`
	`  <0-128>  lengh value`
	`Switch(config)#  ipv6 address 2001::1 prefix 64`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.15 IPV6 DEFAULT-GATEWAY

Use **"ipv6 default-gateway"** command to modify default gateway IPv6.

Switch#**configure terminal**
Switch(config)# **ipv6 default-gateway** *{X:X::X:X}*

Syntax	**ipv6 default-gateway** *{X:X::X:X}*
Parameter	*X:X::X:X* Specify default gateway IPv6 address for switch
Mode	Global Configuration

Example	This example shows how to modify the ipv6 default gateway address of the switch.
	Switch#**configure terminal**
	Switch(config)# **ipv6 default-gateway 2002::1**
	`Switch# configure terminal`
	`Switch(config)# ipv6 default-gateway 2002::1`
	`Switch(config)#`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.16 IPV6 DHCP

Use **“ipv6 dhcp”** command to enabled dhcpv6 client to get IP address from remote DHCPv6 server. Use **“no ipv6 dhcp”** command to disabled dhcpv6 client and use static ipv6 address or ipv6 auto config address.

Switch#**configure terminal**
Switch(config)# **ipv6 dhcp**

Switch(config)# **no ipv6 dhcp**

Syntax	**ipv6 dhcp** **no ipv6 dhcp**
Default	Default DHCPv6 client is disabled.
Mode	Global Configuration

Example	This example shows how to enable dhcp client.
	Switch#**configure terminal**
	Switch(config)# **ipv6 dhcp**
	`Switch# configure terminal`
	`Switch(config)# ipv6 dhcp`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.17 IP SERVICE

This is one of very important command to enable/disable management access via CLI. Use **"ip (telnet | ssh | http | https)"** command to enable all kinds of management services. Such as telnet, ssh, http and https from CLI.

Switch#**configure terminal**
Switch(config)# **ip (telnet | ssh | http | https)**

Switch(config)# **no ip (telnet | ssh | http | https)**

Syntax	**ip (telnet | ssh | http | https)** **no ip (telnet | ssh | http | https)**
Parameter	telnet Enable/Disable telnet service ssh Enable/Disable ssh service http Enable/Disable http service https Enable/Disable https service
Default	Default telnet service is disabled. Default ssh service is disabled. Default http service is enabled. Default https service is disabled.
Mode	Global Configuration
Example	This example shows how to enable telnet service and show current telnet service status. Switch#**configure terminal** Switch(config)# **ip telnet** Telnet daemon enabled. Switch(config)# **exit** Switch# **show line telnet**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# ip telnet
Switch(config)# exit
Switch# show line telnet
Telnet ===============================
    Telnet Server    : enabled
    Session Timeout  : 10 (minutes)
    History Count    : 128
    Password Retry   : 3
    Silent Time      : 0 (seconds)
```

This example shows how to enable https service and show current https service status.

Switch#configure terminal

Switch(config)# ip https

Switch(config)# exit

Switch# show ip https

```
Switch# configure
Switch(config)# ip https
Switch(config)# exit
Switch# show ip https
   HTTPS daemon : enabled
Session Timeout : 10 (minutes)
```

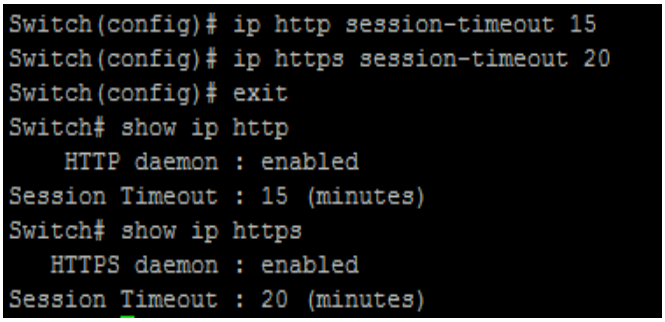
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.18 IP SESSION-TIMEOUT

Use **"ip session-timeout"** command to specify the session timeout value for http or https service. When user login into Web GUI and do not do any action after session timeout will be logged out.

Switch#**configure terminal**
Switch(config)# **ip (http | https) session-timeout** *<0-86400>*

Syntax	**ip (http | https) session-timeout** *<0-86400>*
Parameter	httpSpecify session timeout for http service. https Specify session timeout for https service. *<0-86400>*Specify session timeout minutes. 0 means never timeout.
Default	Default session timeout for http and https is 10 minutes.
Mode	Global Configuration

Example	This example shows how to change http session timeout to 15min and https session timeout to 20min
	Switch#**configure terminal**
	Switch(config)# **ip http session-timeout 15**
	Switch(config)# **ip https session-timeout 20**
	This example shows how to enable https service and show current https service status.
	Switch# **show ip http**
	Switch# **show ip https**
	 
	`Switch(config)# ip http session-timeout 15`
	`Switch(config)# ip https session-timeout 20`
	`Switch(config)# exit`
	`Switch# show ip http`
	`HTTP daemon : enabled`
	`Session Timeout : 15 (minutes)`
	`Switch# show ip https`
	`HTTPS daemon : enabled`
	`Session Timeout : 20 (minutes)`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.19 IP SSH

Use **"ip ssh"** command to generate the key files for ssh connection. Enables the SSH server on the switch. The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server.

Switch#**configure terminal**
Switch(config)# **ip ssh (v1|v2|all|port)**

Switch(config)# **no ip ssh (v1|v2|all|port**)

Syntax	**ip ssh (v1|v2|all|port)** **no ip ssh (v1|v2|all|port**)
Parameter	v1 Generate/Delete version 1 key files v2 Generate/Delete version 2 key files port tcp port number; default port 22 all Generate/Delete version 1 and 2 key files
Default	Version 2 key files will be generated by default
Mode	Global Configuration

Example	This example shows how to delete and re-generate ssh version 2 key files.
	Switch#**configure terminal**
	Switch(config)# **ip ssh v2**
	Switch# **show ip ssh**
	`Switch# sh ip ssh`
	`SSH config info:`
	`SSH Status : enable`
	`SSH Tcp Port : 22`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.20 LINE

Some configurations are line based. To configure these configurations, we need to enter Line Configuration mode to configure them. Use **"line"** command to enter the Line Configuration mode and select the line to be configured. In Line Configuration mode, the prompt will show as **"Switch(config-line)#"**

Switch#**configure terminal**
Switch(config)# **line (console | telnet | ssh)**

Syntax	**line (console | telnet | ssh)**
Parameter	console Console terminal line ssh Virtual terminal for secured remote console access (SSH) telnet Virtual terminal for remote console access (Telnet)
Mode	Global Configuration

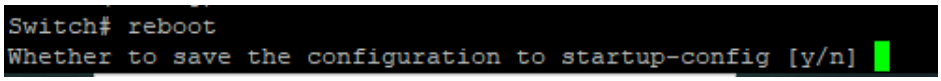
Example	This example shows how to enter Interface Configuration mode
	Switch# **configure**
	Switch(config)# **line console**
	Switch(config-line)#
	`Switch# configure`
	`Switch(config)# line console`
	`Switch(config-line)#`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.21 REBOOT

Use **"reboot"** command to make system hot restart. Switch will be Power OFF and again ON (Restart) with this command.

Switch#**reboot**

Syntax	**reboot**
Mode	Privileged EXEC
Example	This example shows how to restart the system Switch# **reboot** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.22 ENABLE PASSWORD

Use **"enable password"** command to edit password for each privilege level for enable authentication. Use **"no enable"** command to restore enable password to default empty value. The only way to show this configuration is using **"show running-config"** command.

Switch#**configure terminal**
Switch(config)# **enable [privilege** *<1-15>***] (password UNENCRYPY-PASSWORD | secret UNENCRYPY-PASSWORD | secret encrypted ENCRYPT-PASSWORD)**

Switch(config)# **no enable [privilege** *<0-15>***]**

Syntax	**enable [privilege** *<1-15>***] (password UNENCRYPT-PASSWORD | secret UNENCRYPT-PASSWORD | secret encrypted ENCRYPT-PASSWORD)** **no enable [privilege** *<0-15>***]**
Parameter	**privilege***<0-15>*Specify the privilege level to configure. If no privilege level is specified, default is 15. **password UNENCRYPT**-Specify password string and make it not encrypted. **secret UNENCRYPT- PASSWORD**Specify password string and make it encrypted. **secret encrypted ENCRYPT- PASSWORD** Enter an encrypted password. Use this keyword to enter a password that is already encrypted (for instance, a password that you copied from another the configuration file of another device).
Default	No default enable password for all privilege levels.
Mode	Global Configuration
Example	This example shows how to edit enable password for privilege level 15 Switch#configure terminal Switch(config)# **enable password** abc

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Username: admin
Password: ********
Switch# config t
Switch(config)# enable password abc
Switch(config)# end
Switch# exit
Switch> en
Password: ***
Switch#
```

Configuration of privileged level for enable passwords
This example shows how to set privilege level for enable password.
Switch#configure terminal
Switch(config)# enable privilege 15 secret xyz

```
Switch# config t
Switch(config)# enable privilege 15 secret xyz
Switch(config)# end
Switch# exit
Switch> enable 15
Equal to current privilege level 15
Password: ***
Switch#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.23 EXEC-TIMEOUT

Use **"exec-timeout"** command to specify the session timeout value for CLI running on console, telnet or ssh service. When user login into CLI and do not do any action after session timeout will be logged out from the CLI session. It basically sets the interval that the command interpreter waits until user input is detected.

Switch#**configure terminal**
Switch(config)# **line console**
Switch(config-line)# **exec-timeout** *<0-65535>*

Syntax	**exec-timeout** *<0-65535>*
Parameter	*<0-65535>*Specify session timeout minutes. 0 means never timeout
Default	Default session timeout for all lines are 10 minutes.
Mode	Line Configuration
Example	This example shows how to change console session timeout to 15min, telnet session timeout to 20min and ssh session timeout to 25min. Timeout after specified minutes (0 means no timeout) Switch#**configure terminal** Switch(config)# **line console** Switch(config-line)# **exec-timeout 15** Switch(config-line)# **exit** Switch(config)# **line telnet** Switch(config-line)# **exec-timeout 20** Switch(config-line)# **exit** Switch(config)# **line ssh** Switch(config-line)# **exec-timeout 25** Switch(config-line)# **exit** This example shows how show line information. Switch# **show line**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config-line)# line console
Switch(config-line)# exec-timeout 15
Switch(config-line)# exit
Switch(config)# line telnet
Switch(config-line)# exec-timeout 20
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# exec-timeout 25
Switch(config-line)# exit
Switch(config)# exit
Switch# show line
Console ==============================
    Session Timeout : 15 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
Telnet ===============================
    Telnet Server   : enabled
    Session Timeout : 20 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
SSH ==================================
    SSH Server      : enabled
    Session Timeout : 25 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.24 PASSWORD-THRESH

Sets the password intrusion threshold, which limits the number of failed logon attempts. When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the password-thresh command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state. Use **"password-thresh"** command to specify the password fail retry number for CLI running on console, telnet or ssh service. When user inputs password to login and authentication fails, the failed retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command **"silent-time".**

Switch#**configure terminal**
Switch(config)# **line console**
Switch(config-line)# **password-thresh 4**

Syntax	**password-thresh** *<0-120>*
Parameter	*<0-120>*Specify password fail retry number. 0 means no limit.
Default	Default password fail retry number is 3.
Mode	Line Configuration
Example	This example shows how to change console fail retry number to 4, telnet fail retry number to 5 and ssh fail retry number to 6. The number of allowed password attempts. (Range: 0-120; 0: no threshold) Switch#**configure terminal** Switch(config)# **line console** Switch(config-line)# **password-thresh 4** Switch(config-line)# **exit** Switch(config)# line **telnet** Switch(config-line)# **password-thresh 5** Switch(config-line)# **exit** Switch(config)# **line ssh** Switch(config-line)# **password-thresh 6** Switch(config-line)# **exit**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

This example shows how show line information.

Switch# show line

```
Switch(config)# line console
Switch(config-line)# password-thresh 4
Switch(config-line)# exit
Switch(config)# line telnet
Switch(config-line)# password-thresh 5
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# password-thresh 6
Switch(config-line)# exit
Switch(config)# exit
Switch# show line
Console ==============================
    Session Timeout : 15 (minutes)
    History Count   : 128
    Password Retry  : 4
    Silent Time     : 0 (seconds)
Telnet ===============================
    Telnet Server   : enabled
    Session Timeout : 20 (minutes)
    History Count   : 128
    Password Retry  : 5
    Silent Time     : 0 (seconds)
SSH ==================================
    SSH Server      : enabled
    Session Timeout : 25 (minutes)
    History Count   : 128
    Password Retry  : 6
    Silent Time     : 0 (seconds)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.25 PING

Ping (Packet Internet Groper) tests the connection between two network nodes by sending packets to a host and measure the round-trip time. Use **"ping"** command to do network ping diagnostic. Ping command is mainly used for sending ICMP query packet from the switches to remote devices, also for check the accessibility between the switch and the remote device.

Switch# **ping** *HOSTNAME* [**count** *<1-999999999>*]

Syntax	**ping** *HOSTNAME* [**count** *<1-999999999>*]
Parameter	*HOSTNAME* Specify IPv4/IPv6 address or domain name to ping. count *<1-999999999>* Specify how many times to ping.
Mode	User EXEC Privileged EXEC

Example	This example shows how to ping remote host 192.168.0.21
	Switch# **ping 192.168.0.21**
	`Switch# ping 192.168.0.21`
	`PING 192.168.0.21 (192.168.0.21): 56 data bytes`
	`64 bytes from 192.168.0.21: seq=0 ttl=128 time=0.000 ms`
	`64 bytes from 192.168.0.21: seq=1 ttl=128 time=0.000 ms`
	`64 bytes from 192.168.0.21: seq=2 ttl=128 time=0.000 ms`
	`64 bytes from 192.168.0.21: seq=3 ttl=128 time=0.000 ms`
	
	`--- 192.168.0.21 ping statistics ---`
	`4 packets transmitted, 4 packets received, 0% packet loss`
	`round-trip min/avg/max = 0.000/0.000/0.000 ms`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

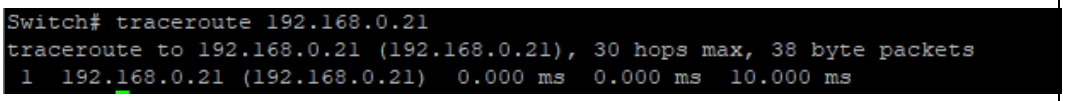
1.26 TRACEROUTE

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.

Use **"traceroute"** command to do network trace route diagnostic. Traceroute command is for testing the gateways through which the data packets travel from the source device to the destination device, so to check the network accessibility and locate the network failure.

Switch# **traceroute** *{A.B.C.D}* [**max_hop***<2-255>*]

Syntax	**Traceroute** *{A.B.C.D}* [**max_hop***<2-255>*]
Parameter	*A.B.C.D* Specify IPv4 to trace. **max_hop***<2-255>*Specify maximum hop to trace.
Mode	User EXEC Privileged EXEC

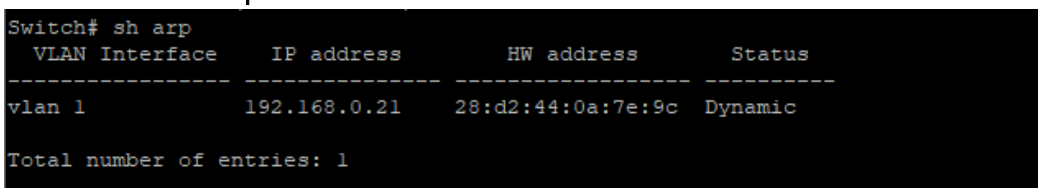
Example	This example shows how to trace route host 192.168.0.21.
	Switch# **traceroute 192.168.0.21**
	 
	`Switch# traceroute 192.168.0.21`
	`traceroute to 192.168.0.21 (192.168.0.21), 30 hops max, 38 byte packets`
	`1  192.168.0.21 (192.168.0.21)  0.000 ms  0.000 ms  10.000 ms`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.27 SHOW ARP

Use **"show arp"** command to displays entries in the ARP cache.

Switch# **show arp**

Syntax	**show arp**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show arp entries. Switch# **show arp** 

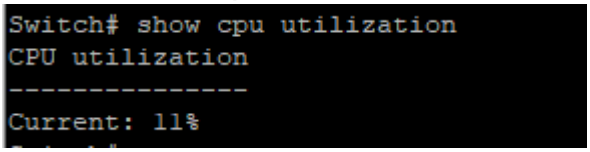
```
Switch# sh arp
  VLAN Interface    IP address        HW address       Status
---------------- --------------- ------------------ ----------
vlan 1            192.168.0.21    28:d2:44:0a:7e:9c  Dynamic

Total number of entries: 1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.28 SHOW CPU UTILIZATION

Use **“show cpu utilization”** command to show current CPU utilization.

Switch# **show cpu utilization**

Syntax	**show cpu utilization**
Mode	Privileged EXEC
Example	This example shows how to show current CPU utilization. Switch# **show cpu utilization** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.29 SHOW HISTORY

Use **"show history"** to show commands we input before.

Switch# **show history**

Syntax	**show history**
Mode	User EXEC Privileged EXEC Global Configuration

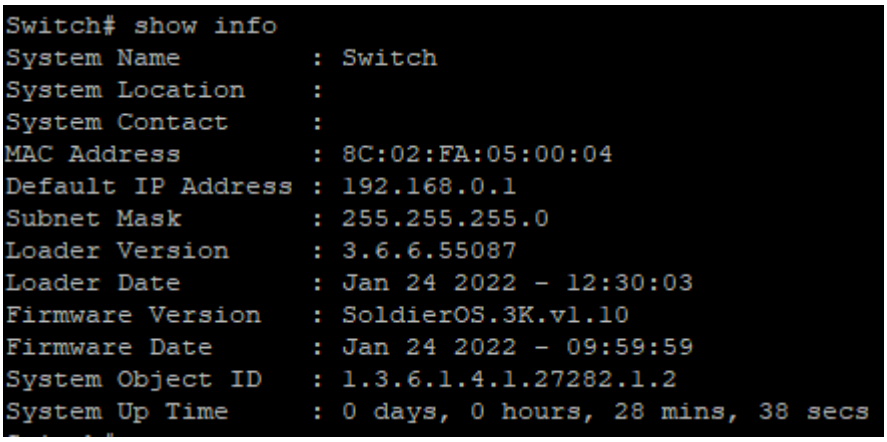
Example	This example shows how show history commands.
	Switch# **show history**
	`Switch# show history`
	`Maximun History Count: 128`
	`----------`
	`1. show cpu utilization`
	`2. hostname Switch`
	`3. config t`
	`4. hostname Switch`
	`5. wr`
	`6. show cpu utilization`
	`7. show history`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.30 SHOW INFO

Use **“show info”** command to show system summary information.

Switch#**show info**

Syntax	**show info**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show system version. Switch# **show info** 

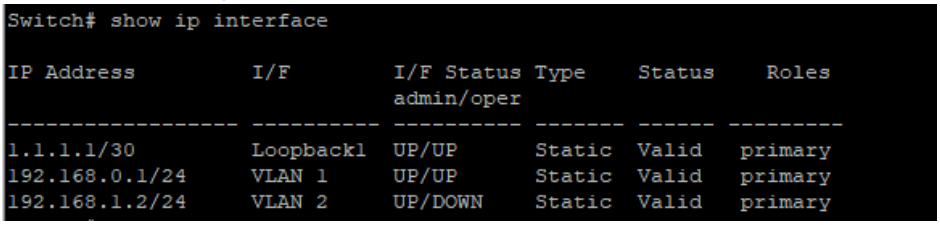
```
Switch# show info
System Name         : Switch
System Location     :
System Contact      :
MAC Address         : 8C:02:FA:05:00:04
Default IP Address  : 192.168.0.1
Subnet Mask         : 255.255.255.0
Loader Version      : 3.6.6.55087
Loader Date         : Jan 24 2022 - 12:30:03
Firmware Version    : SoldierOS.3K.v1.10
Firmware Date       : Jan 24 2022 - 09:59:59
System Object ID    : 1.3.6.1.4.1.27282.1.2
System Up Time      : 0 days, 0 hours, 28 mins, 38 secs
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.31 SHOW IP

Use **“show ip interface”** command to show system IPv4 address, net mask and default gateway.

Switch#**show ip interface**

Syntax	**show ip interface**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show current ipv4 address of the switch. Switch# **show ip interface** 

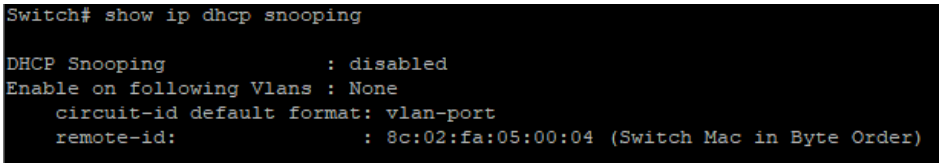
```
Switch# show ip interface

IP Address         I/F        I/F Status Type    Status    Roles
                              admin/oper
------------------ ---------- ---------- ------- ------ ---------
1.1.1.1/30         Loopback1  UP/UP      Static  Valid   primary
192.168.0.1/24     VLAN 1     UP/UP      Static  Valid   primary
192.168.1.2/24     VLAN 2     UP/DOWN    Static  Valid   primary
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.32 SHOW IP DHCP snooping

Use **“show ip dhcp snooping”** Shows the DHCP snooping configuration settings.

Switch#**show ip dhcp snooping**

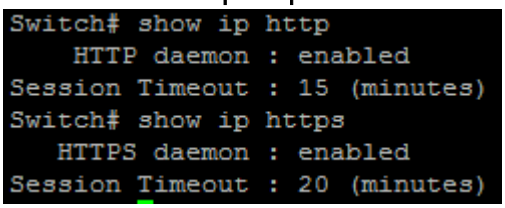
Syntax	**show ip dhcp snooping**
Mode	User EXEC Privileged EXEC
Example	This example shows Shows the DHCP snooping configuration settings Switch# **show ip dhcp snooping** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.33 SHOW IP HTTP

Use **"show ip http"** command to show HTTP/HTTPS information.

Switch#**show ip (http|https)**

Syntax	**show ip (http|https)**
Mode	Privileged EXEC
Example	This example shows how to show current ipv4 address of the switch. Switch# **show ip http** Switch# **show ip https** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.34 SHOW IPV6 Interface

Use **“show ipv6 interface”** command to show system IPv6 address, net mask, default gateway and auto config state.

Switch#**show ipv6 interface**

Syntax	**show ipv6 interface**
Mode	User EXEC Privileged EXEC

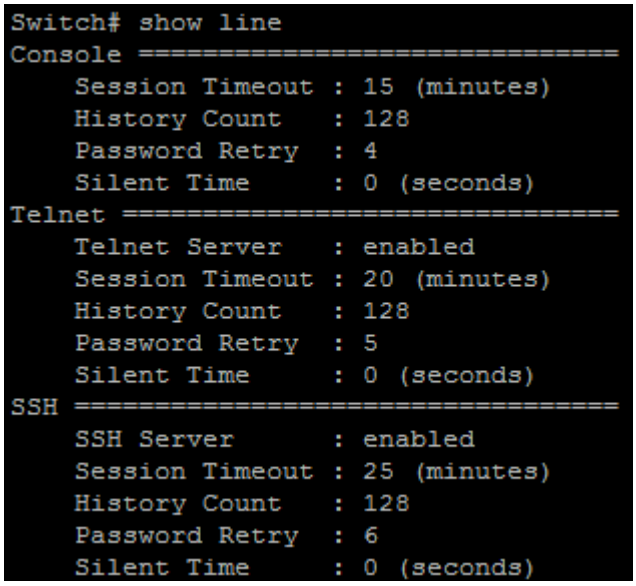
Example	This example shows how to show current ipv6 interface address of the switch.
	Switch# **show ipv6 interface**
	`Switch# show ipv6 interface`
	`VLAN 1 is up/up`
	`IPv6 is enabled, link-local address is fe80::8e02:faff:fe05:4`
	`IPv6 Forwarding is disabled`
	`No global unicast address is configured`
	`Joined group address(es):`
	`ff02::1:ff05:4`
	`ff02::1`
	`ff01::1`
	`ND DAD is enabled, number of DAD attempts: 1`
	`Stateless autoconfiguration is enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.35 SHOW LINE

Use **"show line"** command to show all line configurations including session timeout, history count, password retry number and silent time. For telnet and ssh, it also shows the service enable/disable state.

Switch#**show line [(console | telnet | ssh)]**

Syntax	**show line [(console | telnet | ssh)]**
Parameter	**console** Select console line to show. **telnet** Select telnet line to show. **Ssh** Select ssh line to show.
Mode	Privileged EXEC
Example	This example shows how show all lines' information. Switch# **show line** 

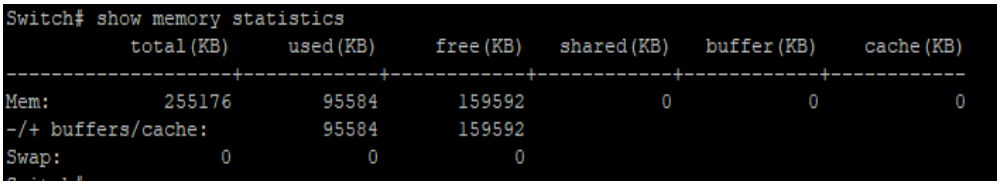
```
Switch# show line
Console ==============================
    Session Timeout : 15 (minutes)
    History Count   : 128
    Password Retry  : 4
    Silent Time     : 0 (seconds)
Telnet ===============================
    Telnet Server   : enabled
    Session Timeout : 20 (minutes)
    History Count   : 128
    Password Retry  : 5
    Silent Time     : 0 (seconds)
SSH ==================================
    SSH Server      : enabled
    Session Timeout : 25 (minutes)
    History Count   : 128
    Password Retry  : 6
    Silent Time     : 0 (seconds)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.36 SHOW MEMORY STATISTICS

Use **"show memory statistics"** command to show current memory utilization.

Switch#**show memory statistics**

Syntax	**show memory statistics**
Mode	Privileged EXEC
Example	This example shows how to show current system memory statistics. Switch# **show memory statistics** 

```
Switch# show memory statistics
             total(KB)      used(KB)      free(KB)    shared(KB)    buffer(KB)     cache(KB)
-------------------+-------------+-------------+-------------+-------------+-------------
Mem:          255176         95584        159592             0             0             0
-/+ buffers/cache:           95584        159592
Swap:              0             0             0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.37 SHOW PRIVILEGE

Use **"show privilege"** command to show the privilege level of the current user.

Switch#**show privilege**

Syntax	**show privilege**
Mode	User EXEC Privileged EXEC

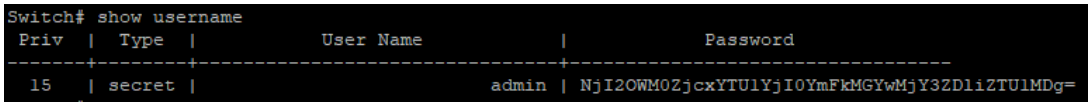
Example	This example shows how to show arp entries.
	Switch# **show privilege**
	`Switch# show privilege`
	`Current CLI Username:  admin`
	`Current CLI Privilege: 15`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.38 SHOW USERNAME

Use **“show username”**command shows all user accounts in local database.

Switch#**show username**

Syntax	**show username**
Mode	Privileged EXEC
Example	This example shows how to show existing user accounts. Switch# **show username** 

```
Switch# show username
 Priv  |  Type  |          User Name            |           Password
-------+--------+-------------------------------+----------------------------------
  15   | secret |                         admin | NjI2OWM0ZjcxYTU1YjI0YmFkMGYwMjY3ZD1iZTU1MDg=
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.39 SHOW USERS

Use **"show users"** command show information of all active users.

Switch#**show users**

Syntax	**show users**
Mode	Privileged EXEC

Example	This example shows how to show existing user accounts.
	Switch# **show users**
	`Switch# show users`
	`Username Protocol Location`
	`--- --- ---`
	`console 0.0.0.0`
	`admin telnet 192.168.0.22`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.40 SHOW VERSION

Use **"show version"** command to show loader and loader version and date and also display firmware version and date information of the switch.

Switch#**show version**

Syntax	**show version**
Mode	User EXEC Privileged EXEC

Example	This example shows how to show system version.
	Switch# **show version**
	`Switch# show version`
	`Loader Version : 3.6.6.55087`
	`Loader Date : Jan 24 2022 - 12:30:03`
	`Firmware Version : SoldierOS.3K.v1.10`
	`Firmware Date : Jan 24 2022 - 09:59:59`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.41 SILENT-TIME

Use **"silent time"** command to specify the silent time for CLI running on console, telnet or ssh service. When user inputs password to login and authentication fails, the failed retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command **"silent-time"**.

Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. The range is from 1 to 65535 seconds & by default it is disabled.

Switch#**configure terminal**
Switch(config)# **line {console|telnet|ssh|http}**
Switch(config-line)# **silent-time** *<0-65535>*

Syntax	**silent-time** *<0-65535>*
Parameter	*<0-65535>*Specify silent time with unit seconds. 0 means do not silent.
Default	Default silent time is 0.
Mode	Line Configuration
Example	This example shows how to change console silent time to 10, telnet silent time to 15 and ssh silent time to 20. Switch#**configure terminal** Switch(config)# **line console** Switch(config-line)# **silent-time 10** Switch(config-line)# **exit** Switch(config)# **line telnet** Switch(config-line)# **silent-time 15** Switch(config-line)# **exit** Switch(config)# **line ssh** Switch(config-line)# **silent-time 20** Switch(config-line)# **exit** This example shows how show line information. Switch# **show line**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# line console
Switch(config-line)#  silent-time 10
Switch(config-line)#  exit
Switch(config)# line telnet
Switch(config-line)# silent-time 15
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# silent-time 20
Switch(config-line)# exit
Switch(config)# exit
Switch# show line
Console ==============================
    Session Timeout : 15 (minutes)
    History Count   : 128
    Password Retry  : 4
    Silent Time     : 10 (seconds)
Telnet ==============================
    Telnet Server   : enabled
    Session Timeout : 20 (minutes)
    History Count   : 128
    Password Retry  : 5
    Silent Time     : 15 (seconds)
SSH ==================================
    SSH Server      : enabled
    Session Timeout : 25 (minutes)
    History Count   : 128
    Password Retry  : 6
    Silent Time     : 20 (seconds)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.42 SSL

Use **“ssl”** command to generate security certificate files such as RSA, DSA.

Switch#**ssl**

Syntax	**ssl**
Mode	Global Configuration
Example	This example shows how to generate certificate files. Switch# **ssl** Switch# **show flash**

```
Switch# ssl
Generating a 2048 bit RSA private key
.....................................................+++
.............+++
writing new private key to '/mnt/ssh/ssl_key.pem_tmp'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

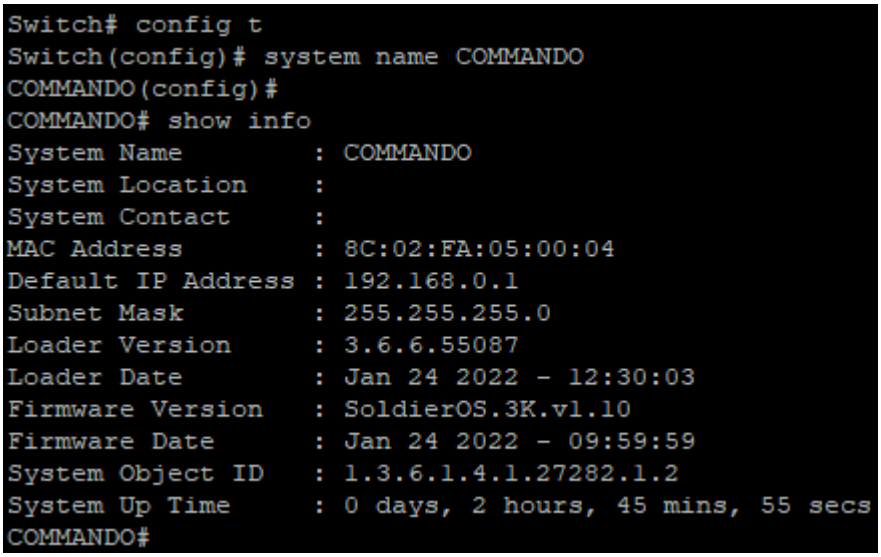
```
Switch# show flash
        File Name             File Size        Modified
------------------------ ---------------- ------------------------
 startup-config           1845             2022-01-01 00:45:26
 rsa2                     1679             2022-01-01 00:00:33
 dsa2                     668              2022-01-01 00:01:02
 ssl_cert                 1257             2022-01-01 02:39:46
 image0 (active)          8813783          2022-01-24 09:59:59
 image1 (backup)          0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.43 SYSTEM NAME

Use **“system name”** command to modify system name information of the switch. The system name is also used to be CLI prompt. System name and system description advertisement can also provide useful information for collecting network flow data. System description advertisement can include data such as the full name of the advertising device, hardware type of system, the version information of software operation system and so on.

Switch#**configure terminal**
Switch(config)#**system name** *{NAME}*

Syntax	**system name** *{NAME}*
Parameter NAME	*NAME* Specify system name string.
Default	Default name string is **“Switch”**.
Mode	Global Configuration
Example	This example shows how to modify contact information Switch#**configure terminal** Switch(config)# **system name** COMMANDO COMMANDO(config)# COMMANDO# **show info** 

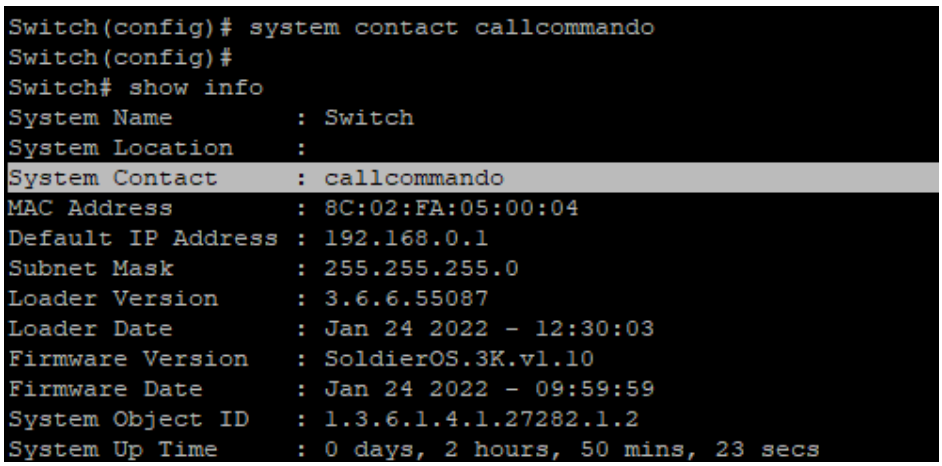
```
Switch# config t
Switch(config)# system name COMMANDO
COMMANDO(config)#
COMMANDO# show info
System Name         : COMMANDO
System Location     :
System Contact      :
MAC Address         : 8C:02:FA:05:00:04
Default IP Address  : 192.168.0.1
Subnet Mask         : 255.255.255.0
Loader Version      : 3.6.6.55087
Loader Date         : Jan 24 2022 - 12:30:03
Firmware Version    : SoldierOS.3K.v1.10
Firmware Date       : Jan 24 2022 - 09:59:59
System Object ID    : 1.3.6.1.4.1.27282.1.2
System Up Time      : 0 days, 2 hours, 45 mins, 55 secs
COMMANDO#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.44 SYSTEM CONTACT

Use **"system contact"** command to modify contact information of the switch. It is generally can be set for administrator responsible for the system troubleshooting and maintenance.

Switch#**configure terminal**
Switch(config)# **system contact** *{CONTACT}*

Syntax	**system contact** *{CONTACT}*
Parameter	*CONTACT* Specify contact string.
Default	Default contact string is **"Default Contact"**.
Mode	Global Configuration
Example	This example shows how to modify contact information Switch#**configure terminal** Switch(config)# **system contact** callcommando Switch# **show info** 

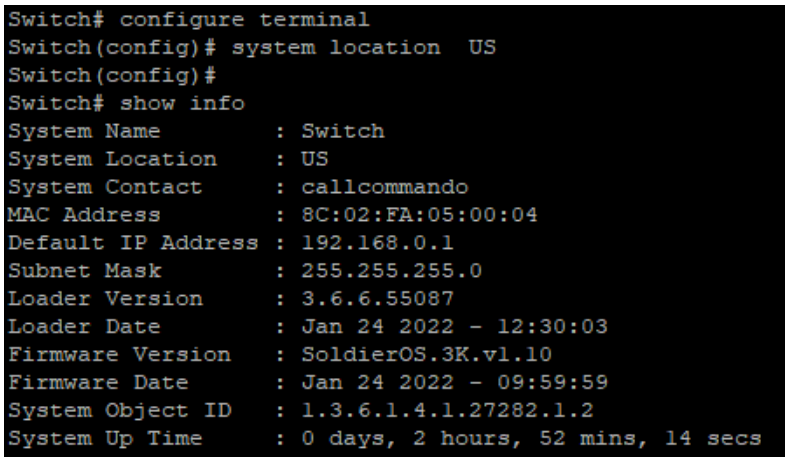
```
Switch(config)# system contact callcommando
Switch(config)#
Switch# show info
System Name         : Switch
System Location     :
System Contact      : callcommando
MAC Address         : 8C:02:FA:05:00:04
Default IP Address  : 192.168.0.1
Subnet Mask         : 255.255.255.0
Loader Version      : 3.6.6.55087
Loader Date         : Jan 24 2022 - 12:30:03
Firmware Version    : SoldierOS.3K.v1.10
Firmware Date       : Jan 24 2022 - 09:59:59
System Object ID    : 1.3.6.1.4.1.27282.1.2
System Up Time      : 0 days, 2 hours, 50 mins, 23 secs
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.45 SYSTEM LOCATION

Use **"system location"** command to modify location information of the switch. Specifies the system location.

Switch#**configure terminal**
Switch(config)# **system location** *{LOCATION}*

Syntax	**system location** *{LOCATION}*
Parameter	*LOCATION* Specify location string.
Default	Default location string is "**Default Location**".
Mode	Global Configuration
Example	This example shows how to modify contact information Switch#**configure terminal** Switch(config)# **system location** US This example shows how to show system location information Switch# **show info** 

```
Switch# configure terminal
Switch(config)# system location  US
Switch(config)#
Switch# show info
System Name         : Switch
System Location     : US
System Contact      : callcommando
MAC Address         : 8C:02:FA:05:00:04
Default IP Address  : 192.168.0.1
Subnet Mask         : 255.255.255.0
Loader Version      : 3.6.6.55087
Loader Date         : Jan 24 2022 - 12:30:03
Firmware Version    : SoldierOS.3K.v1.10
Firmware Date       : Jan 24 2022 - 09:59:59
System Object ID    : 1.3.6.1.4.1.27282.1.2
System Up Time      : 0 days, 2 hours, 52 mins, 14 secs
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.46 TERMINAL LENGTH

Use **“terminal length”** command to specify the maximum line number the terminal is able to print.

Switch# **terminal length** *<0-24>*

Syntax	**terminal length** *<0-24>*
Parameter	*<0-24>*Specify terminal length value. 0 means no limit.
Default	Default terminal length is 24.
Mode	User EXEC Privileged EXEC
Example	This example shows how to change terminal length. Switch# **terminal length 24**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.47 USERNAME

Use **"username"** command to add a new user account or edit an existing user account. And use **"no username"** to delete an existing user account. The user account is a local database for login authentication.

Switch#**configure terminal**
Switch(config)# **username** *WORD<0-32>*[**privilege (admin|user|<0-15>)] (nopassword | password UNENCRYPY-PASSWORD | secret UNENCRYPY-PASSWORD | secret encrypted ENCRYPT-PASSWORD)**

Switch(config)# **no username** *WORD<0-32>*

Syntax	**username** *WORD<0-32>*[**privilege (admin|user|<0-15>)] (nopassword | password UNENCRYPY-PASSWORD | secret UNENCRYPY-PASSWORD | secret encrypted ENCRYPT-PASSWORD)** **no username** *WORD<0-32>*
Parameter	**username** *WORD<0-32>* Specify username to add/delete/edit. **privilege** admin Specify privilege level to be admin (privilege 15) **privilege** userSpecify privilege level to be user (privilege 1) **privilege***<0-15>* Specify custom privilege level password. **UNENCRYPY- PASSWORD** Specify password string and make it not encrypted. **Secret UNENCRYPY- PASSWORD** Specify password string and make it encrypted. **secret encrypted ENCRYPT- PASSWORD** Enter an encrypted password. Use this keyword to enter a password that is already encrypted (for instance, a password that you copied from another the configuration file of another device).
Default	Default username **"admin"** has password **"commando"** with privilege 15.
Mode	Global Configuration

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Example	This example shows how to add a new user account. Switch#configure terminal Switch(config)# **username** test **secret** passwd This example shows how to show existing user accounts. Switch# **show username** 

```
Switch(config)# username test secret passwd
Switch(config)# exit
Switch# show username
 Priv  |  Type  |          User Name           |           Password
-------+--------+------------------------------+----------------------------------
  15   | secret |                        admin | NjI2OWM0ZjcxYTU1YjI0YmFkMGYwMjY3ZDliZTU1MDg=
  15   | secret |                         test | NzZhMjE3M2JlNjM5MzI1NGU3MmZmYTRkNmRmMTAzMGE=
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1.48 USB

Use **"usb"** command to enable Universal Serial Bus (USB) Storage feature which is used to store and deploy switch configurations and images from other USB Flash to the switch.

Switch#**usb**

Syntax	**usb**
Parameter	install Install remove Remove
Default	Default usb unistalled.
Mode	Global Configuration

Example	This example shows how to add and remove usb.
	Switch# **usb install**
	Switch# **usb remove**
	Switch# **show username**
	`Switch# usb`
	`  install  Install`
	`  remove  Remove`
	`Switch# usb install`
	`USB flash drive install Success.`
	
	`Switch# usb remove`
	`USB flash drive remove Success.`
	`Switch#`
	`Switch#`
	`Switch# show usb`
	`Please install the usb device first. Use <usb install> command.`
	
	Note: This command is very useful for upgrading the image and installing standard configure file or taking switch backup.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2. AAA (Authentication, Authorization, Accounting)

AAA is short for Authentication, Authorization and Accounting, it provides a consistency framework for the network management safely. According to the three functions of Authentication, Authorization, Accounting, the framework can meet the access control for the security network: which one can visit the network device, which access-level the user can have and the accounting for the network resource. The AAA feature allows you to verify the identity of grant access to and track the actions of users managing E3000 Series switches. The E3000 Series switches support Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (TACACS+) protocols.

The three security functions can be summarized as follows:

Authentication: Identifies users that request access to the network.

Authorization: Determines if users can access specific services.

Accounting: Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are applied as a method for controlling user access to specified services. When the switch attempts to authenticate a user request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The switch supports the following AAA features:

Accounting for IEEE 802.1X authenticated users that access the network through the switch. Accounting for users that access management interfaces on the switch through the console and Telnet. Accounting for commands that users enter at specific CLI privilege levels.

Authorization of users that access management interfaces on the switch through the console and Telnet. Based on the user ID and password combination that you provide, the E3000 Series switches perform local authentication or authorization using the local database or remote authentication or authorization using one or more AAA servers. A

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

preshared secret key provides security for communication between the E3000 Series switches and AAA servers. You can configure a common secret key for all AAA servers or for only a specific AAA server.

The accounting feature tracks and maintains a log of every management session used to access the E3000 Series switches. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

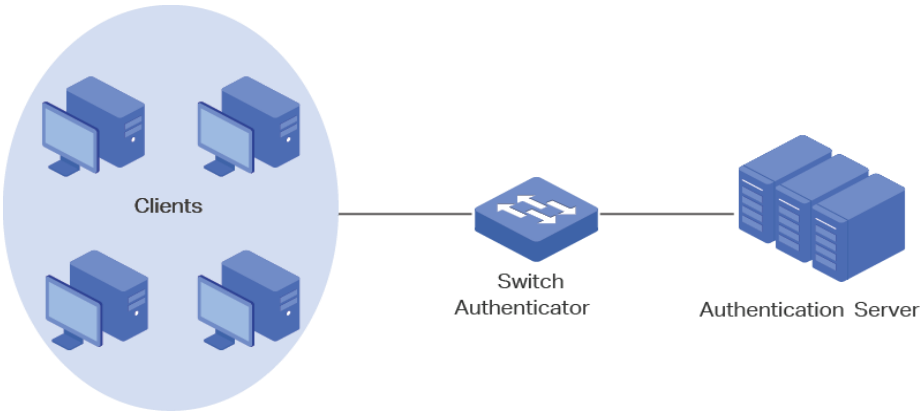


Fig 2.1.1 AAA E3000 Series Switches

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.1 AAA AUTHENTICATION

AAA security provides the following services:

1) Authentication - Identifies users, including login and password dialog, challenge and response, messaging support, and encryption depending on the security protocol that you select. Authentication is the process of verifying the identity of the person or device accessing the E3000 Series switches. This process is based on the user ID and password combination provided by the entity trying to access the E3000 switch. The E3000 Series switches allow you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

2) Authorization - Authorization Provides access controls.

AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in E3000 Series switches is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.

3) Accounting - Provides the method for collecting information, logging the information locally, and sending the information to the AAA server for billing, auditing, and reporting.

Login authentication is used when user try to login into the switch. Such as CLI login dialog and WEBUI login web page. Enable authentication is used only on CLI for user trying to switch from User EXEC mode to Privileged EXEC mode. Both support following authenticate methods. TACACS+ provides more control over the authorization of commands while in RADIUS, no external authorization of commands is supported. All the AAA packets are encrypted in TACACS+ while only the passwords are encrypted in RADIUS is more secure.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Each list allows you to combine these methods with different orders. For example, we want to authenticate login user with remote TACACS+ server, but server may be crashed. Therefore, we need a backup plan, such as another Radius server. So, we can configure the list with TACACS+ server as first authentication method and Radius server as second one.

Switch#**configure terminal**
Switch(config)# **aaa authentication (login | enable) (default |** *listname* **)** *[methodlist][methodlist] [methodlist] [methodlist]*
Switch(config)# **no aaa authentication (login | enable)** {listname}

Syntax	**aaa authentication (login | enable) (default |** *listname* **)** *methodlist [methodlist] [methodlist] [methodlist]* **no aaa authentication (login | enable)** {listname}
Parameter	**login** Add/Edit login authentication list
	enable Add/Edit enable authentication list
	default Edit default authentication list
	listname Specify the list name for authentication type
	methodlist Specify the authenticate method, including none, local enable, tacacs+, radius.
Default	Default authentication list name for type login is **"default"** and default method is **"local"**. Default authentication list name for type enable is **"default"** and default method is **"enable"**
Mode	Global Configuration
Example	This example shows how to add a login authentication list to authenticate with order tacacs+, radius, local. Switch(config)# **aaa authentication login test1 tacacs+ radius local** This example shows how to show existing login authentication lists Switch# **show aaa authentication login lists**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch(config)# exit
Switch# show aaa authentication login lists
 Login List Name    Authentication Method List
----------------- ------------------------------
         default   local
           test1   tacacs+  radius  local
```

Switch(config)# aaa authentication enable test1 tacacs+ radius enable

This example shows how to show existing enable authentication lists

Switch# show aaa authentication login lists Enable

```
Switch(config)# aaa authentication enable test1 tacacs+ radius enable
Switch(config)# exit
Switch# show aaa authentication login lists
 Login List Name    Authentication Method List
----------------- ------------------------------
         default   local
           test1   tacacs+  radius  local
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.2 LOGIN AUTHENTICATION

Different access methods are allowed to bind different login authentication lists. Use **"login authentication"** command to bind the list to specific line (console, telnet, ssh).

Switch#**configure terminal**
Switch#**line [console|telnet|ssh]**
Switch(config-line)# **login authentication** {listname}

Switch(config-line)# **no login authentication**

Syntax	**login authentication** {listname} **no login authentication**
Parameter	listname Specify the login authentication list name to use.
Default	Default login authentication list for each line is **"default"**.
Mode	Line Configuration
Example	This example shows how to create a new login authentication list and bind to telnet line. Switch(config)# **aaa authentication login test1 (tacacs+| radius | local | none |enable)** Switch(config)# **line telnet** Switch(config-line)# **login authentication test1** This example shows how to show line binding lists. Switch# **show line lists**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# aaa authentication login test1 tacacs+
Switch(config)# line telnet
Switch(config-line)# login authentication test1
Switch(config-line)# exit
Switch(config)# exit
Switch# show line lists
  Line Type   |     AAA Type      |  List Name
--------------+-------------------+-----------------
     console  |            login  | default
              |           enable  | default
      telnet  |            login  | test1
              |           enable  | test1
         ssh  |            login  | default
              |           enable  | default
        http  |            login  | test1
       https  |            login  | test2
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.3 IP HTTP LOGIN AUTHENTICATION

Different access methods are allowed to bind different login authentication lists. Use **"ip (http | https) login authentication"** command to bind the list to WEBUI access from http or https.

Switch#**configure terminal**
Switch(config)# **ip (http | https) login authentication** *{listname}*

Switch(config)# **no ip (http | https) login authentication**

Syntax	**ip (http | https) login authentication** *{listname}* **no ip (http | https) login authentication**
Parameter	**http**: Bind login authentication list to user access WEBUI with http protocol **https**: Bind login authentication list to user access WEBUI with https protocol *listname* Specify the login authentication list name to use.
Default	Default login authentication list for each line is **"default"**.
Mode	Global Configuration
Example	This example shows how to create two new login authentication lists and bind to http and https. Switch#**configure terminal** Switch(config)# **aaa authentication login test1 tacacs+ radius local** Switch(config)# **aaa authentication login test2 radius local** Switch(config)# **ip http login authentication test1** Switch(config)# **ip https login authentication test2** This example shows how to show line binding lists. Switch# **show line lists**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# aaa authentication login test2 radius local
Switch(config)# ip http login authentication test1
Switch(config)# ip https login authentication test2
Switch(config)# exit
Switch# show line lists
  Line Type   |    AAA Type      |  List Name
--------------+------------------+-----------------
     console  |           login  | default
              |          enable  | default
      telnet  |           login  | test1
              |          enable  | test1
         ssh  |           login  | default
              |          enable  | default
        http  |           login  | test1
       https  |           login  | test2
```

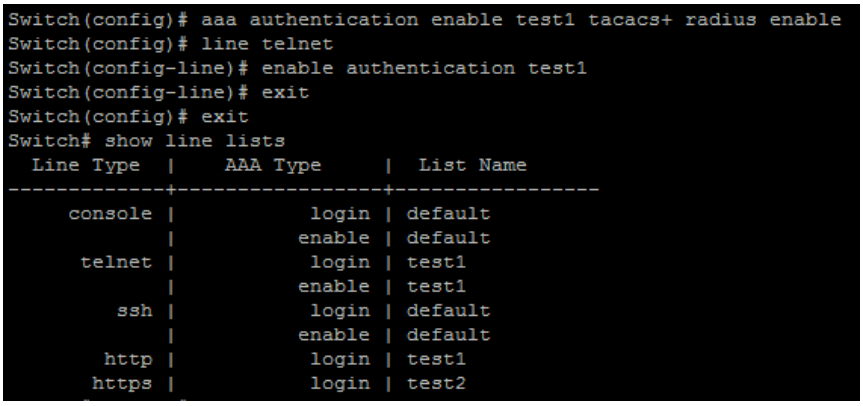
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.4 ENABLE AUTHENTICATION

Different access methods are allowed to bind different enable authentication lists. Use **"enable authentication"** command to bind the list to specific line (console, telnet, ssh).

Switch#**configure terminal**
Switch(config-line)# **enable authentication** {listname}

Switch(config-line)# **no enable authentication**

Syntax	**enable authentication** {listname} **no enable authentication**
Parameter	listname Specify the enable authentication list name to use.
Default	Default enable authentication list for each line is **"default"**.
Mode	Line Configuration
Example	This example shows how to create a new enable authentication list and bind to telnet line. Switch#**configure terminal** Switch(config)# **aaa authentication enable test1 tacacs+ radius enable** Switch(config)# **line telnet** Switch(config-line)# **enable authentication test1** 

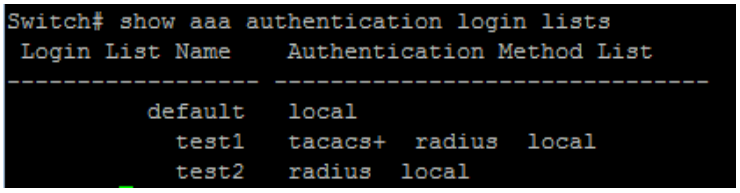
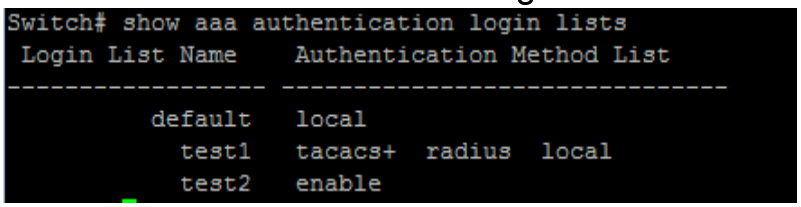
```
Switch(config)# aaa authentication enable test1 tacacs+ radius enable
Switch(config)# line telnet
Switch(config-line)# enable authentication test1
Switch(config-line)# exit
Switch(config)# exit
Switch# show line lists
  Line Type  |    AAA Type     |  List Name
-------------+-----------------+-----------------
     console |           login | default
             |          enable | default
      telnet |           login | test1
             |          enable | test1
         ssh |           login | default
             |          enable | default
        http |           login | test1
       https |           login | test2
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.5 SHOW AAA AUTHENTICATION

Use **"show aaa authentication"** command to show login authentication or Enable authentication method lists.

Switch#**show aaa authentication (login | enable) lists**

Syntax	**show aaa authentication (login | enable) lists**
Parameter	**login** Show login authentication list. **enable** Show enable authentication list.
Mode	Privileged EXEC
Example	This example shows how to show existing login authentication lists. Switch# **show aaa authentication login lists**  This example shows how to show existing enable authentication lists Switch# **show aaa authentication login lists** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.6 SHOW LINE LISTS

Use **“show line lists”** command to show all lines binding list of all.

Switch#**show line lists**

Syntax	**show line lists**
Mode	Privileged EXEC
Example	This example shows how to show line binding lists. Switch# **show line lists** Switch# show line lists Line Type | AAA Type | List Name console | login | default | enable | default telnet | login | test1 | enable | test1 ssh | login | default | enable | default http | login | test1 https | login | test2

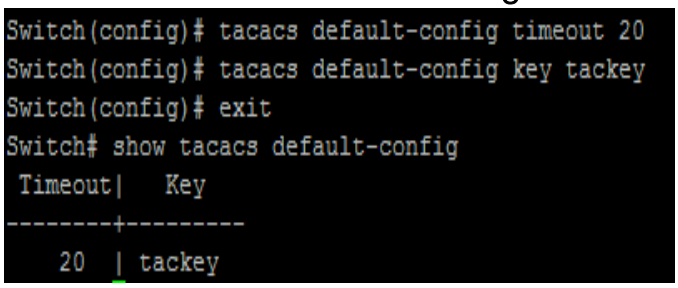
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.7 TACACS DEFAULT-CONFIG

Use **"tacacs default-config"** command to modify default values of TACACS+ Server. These default values will be used when user try to create a new TACACS+ Server and not assigned these values.

Switch#**configure terminal**
Switch(config)#**tacacs default-config [key TACACSKEY] [timeout** *<1-30>*]

Syntax	**tacacs default-config [key TACACSKEY] [timeout** *<1-30>*]
Parameter	**key TACACSKEY** Specify default tacacs+ server key string. **timeout***<1-30>* Specify default tacacs+ server timeout value.
Default	Default tacacs+ key is **"********"**. Default tacacs+ timeout is 5 seconds.
Mode	Global Configuration

Example	This example shows how modify default tacacs+ configuration
	Switch#**configure terminal**
	Switch(config)# **tacacs default-config timeout 20**
	Switch(config)# **tacacs default-config key tackey**
	This example shows how to show default tacacs+ configurations.
	
	Switch# **show tacacs default-config**
	 
	`Switch(config)# tacacs default-config timeout 20`
	`Switch(config)# tacacs default-config key tackey`
	`Switch(config)# exit`
	`Switch# show tacacs default-config`
	`Timeout|  Key`
	`--------+---------`
	`20  | tackey`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.8 TACACS HOST

Use **"TACACS+ host"** command to add or edit TACACS+ Server for Authentication, Authorization or accounting. Use **"no"** form to delete one or all TACACS+ servers from database.

Switch#**configure terminal**
Switch(config)# **tacacs host** *{HOSTNAME }*[**port** *<0-65535>*] [**key TACPLUSKEY**] [**priority***<0-65535>*][**timeout** *<1-30>]*
Switch(config)#**no tacacs** [**host** *{HOSTNAME }*]

Syntax	**tacacs host** *HOSTNAME* [**port** *<0-65535>*] [**key TACPLUSKEY**] [**priority***<0-65535>*] [**timeout** *<1-30>*] **no tacacs** [**host** *{HOSTNAME }*]
Parameter	*HOSTNAME* Specify tacacs+ server host name, both IP address and domain name are available. **port** *<0-65535>* Specify tacacs+ server udp port **key TACPLUSKEY** Specify tacacs+ server key string **priority** *<0-65535>* Specify tacacs+ server priority **timeout** *<1-30>* Specify tacacs+ server timeout value
Default	Default tacacs+ key is **"********"**. Default tacacs+ timeout is 5 seconds.
Mode	Global Configuration
Example	This example shows command execution. Switch# Switch# configure t Switch(config)# tacacs host change port 22 key TACACSKEY priority 45 timeout 5

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.9 SHOW TACACS DEFAULT-CONFIG

Use **"show tacacs default-config"** command to show TACACS+ default.

Switch#**show tacacs default-config**

Syntax	**show tacacs default-config**
Mode	Privileged EXEC

Example	This example shows how to show default tacacs+ configurations.
	Switch# **show tacacs default-config**
	`Switch# show tacacs default-config`
	`Timeout|  Key`
	`--------+---------`
	`20  | tackey`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.10 SHOW TACACS

Use **"show tacacs"** command to show existing TACACS+ servers.

Switch#**show tacacs**

Syntax	**show tacacs**
Mode	Privileged EXEC

Example	This example shows how to show existing tacacs+ server.
	Switch# **show tacacs**
	`Switch#  show tacacs`
	`Prio | Timeout |  IP Address  |  Port  |  Key`
	`------+---------+-----------------+-------+----------`
	`4 |  25  |  192.168.0.100 |  49  | TACACSKEY`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.11 SHOW Default-config

Use **"radius default-config"** command to modify default values of radius server. These default values will be used when user try to create a new radius server and not assigned these values.

Switch#**configure terminal**
Switch(config)#**radius default-config [key RADIUSKEY] [retransmit** *<1-10>*] [**timeout** *<1-30>*]

Syntax	**radius default-config [key RADIUSKEY] [retransmit** *<1-10>*] [**timeout** *<1-30>*]
Parameter	**key RADIUSKEY** Specify default radius server key string **retransmit** *<1-10>* Specify default radius server retransmit value **timeout** *<1-30>* Specify default radius server timeout value
Default	Default radius key is **"********"**. Default radius retransmit is 3 times. Default radius timeout is 3 seconds
Mode	Global Configuration

Example	This example shows how modify default radius configuration,
	Switch#**configure terminal**
	Switch(config)# **radius default-config timeout 20**
	Switch(config)# **radius default-config key radiuskey**
	Switch(config)# **radius default-config retransmit 5**
	This example shows how to show default radius configurations.
	Switch# **show radius default-config**
	`Switch(config)# radius default-config timeout 20`
	`Switch(config)# radius default-config key radiuskey`
	`Switch(config)# radius default-config retransmit 5`
	`Switch(config)# exit`
	`Switch# show radius default-config`
	`Retries| Timeout| Key`
	`--------+--------+---------`
	`5 | 20 | radiuskey`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.12 RADIUS HOST

Use **"radius host"** command to add or edit an existing radius server. Use **"no"** form to delete one or all radius servers from database.

Switch#**configure terminal**
Switch(config)# **radius host** *{HOSTNAME }* [**auth-port** *<0-65535>*] [**key RADIUSKEY**][**priority** *<0-65535>*] [**retransmit** *<1-10>*] [**timeout** *<1-30>*] [**type (login|802.1x|all)**]
Switch(config)# **no radius** [**host** *{HOSTNAME }*]

Syntax	**radius host HOSTNAME** [**auth-port** *<0-65535>*] [**key RADIUSKEY**][**priority** *<0-65535>*] [**retransmit** *<1-10>*] [**timeout** *<1-30>*] [**type (login|802.1x|all)**] **no radius** [**host** *HOSTNAME*]
Parameter	*HOSTNAME*Specify radius server host name, both IP address and domain name are available. **auth-port** *<0-65535>* Specify radius server udp port **key RADIUSKEY** Specify radius server key string **priority** *<0-65535>*Specify radius server priority **retransmit** *<1-10>* Specify radius server retransmit times **timeout** *<1-30>* Specify radius server timeout value
Default	Default radius timeout is 3 seconds.
Mode	Global Configuration

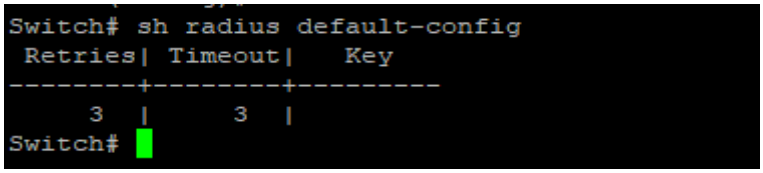
Example	This example shows how to create a new radius server
	Switch(config)# **radius host 192.168.1.111 auth-port 12345 key radiuskey priority100 retransmit 5 timeout 10 type all**
	This example shows how to show existing radius server.
	Switch# **show radius**
	`Switch(config)# radius host 192.168.1.111 auth-port 12345 key radiuskey priority 100 retransmit 5 timeout 10 type all`
	`Switch(config)# exit`
	`Switch# show radius`
	`Prio | IP Address | Auth-Port| Retries| Timeout| Type | Key`
	`100 | 192.168.1.111 | 12345 | 5 | 10 | All | radiuskey`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.13 SHOW RADIUS Default-config

Use **“show radius default-config”** command to show radius default configurations.

Switch#**show radius default-config**

Syntax	**show radius default-config**
Mode	Privileged EXEC
Example	This example shows how to show default radius configurations. Switch# **show radius default-config** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2.14 SHOW RADIUS

Use **"show radius"** command to show existing radius servers.

Switch#**show radius**

Syntax	**show radius**
Mode	Privileged EXEC

Example	This example shows how to show existing radius server.
	Switch# **show radius**
	`Switch# show radius`
	`Prio | IP Address | Auth-Port| Retries| Timeout| Type | Key`
	`100 | 192.168.1.111 | 12345 | 5 | 10 | All | radiuskey`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3. ACL (ACCESS CONRTOL LIST)

An ACL is a sequential collection of permits and deny conditions that apply to packets. Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a switch and permit or deny packets crossing specified interfaces. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can use ACLs on all packets it forwards.

You configure access lists on a switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic.

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies permit or deny and a set of conditions the packet must satisfy to match the ACE. The meaning of permit or deny depends on the context in which the ACL is used.
The switch supports IP ACLs and Ethernet (MAC) ACLs:

1) IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
2) Ethernet ACLs filter non-IP traffic.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

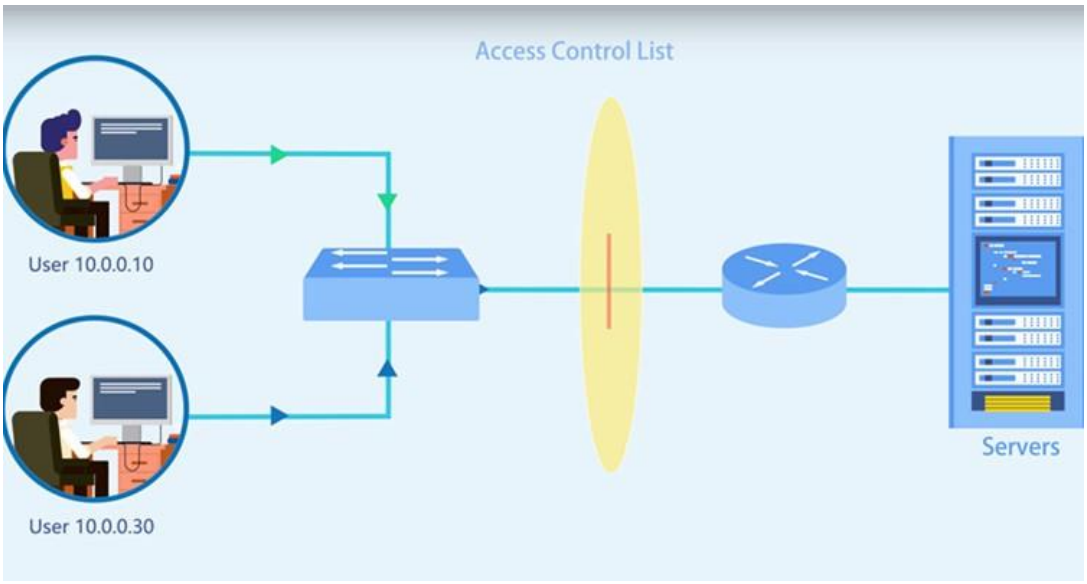


Fig 3.1.1 IP ACL E3000 series Switches

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.1 MAC ACL

MAC ACLs are ACLs that filter traffic using information in the Layer 2 header of each packet. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at the router interfaces.

Use the mac acl command to create a MAC access list and to enter mac-acl configuration mode. The name of ACL must be unique that cannot have same name with other ACL or QoS policy. Once an ACL is created, an implicit **"deny any"** ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

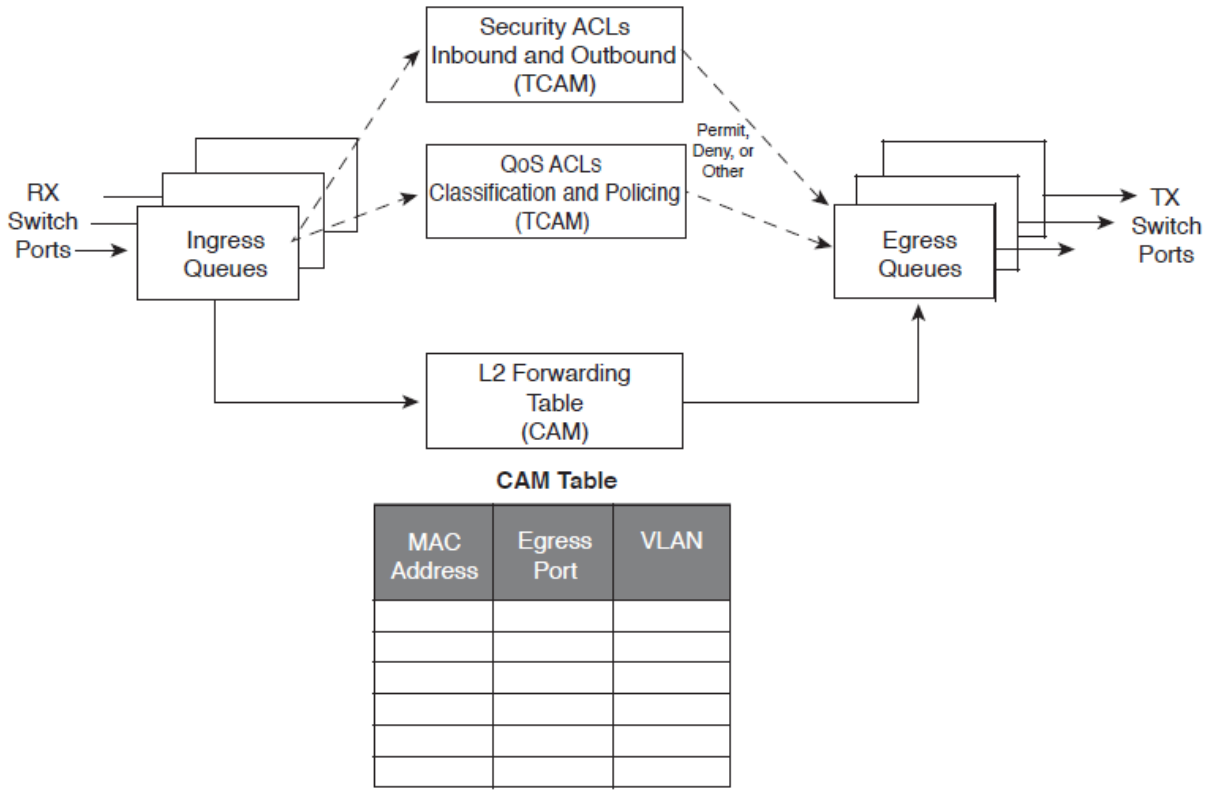


Fig 3.2.1 MAC ACL E3000 series Switches

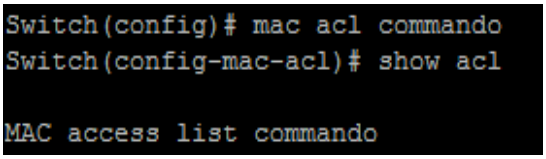
Switch#**configure terminal**

Switch(config)# **mac acl** *{NAME }*

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Switch(config)#**no mac acl** *{NAME }*

Syntax	**mac acl** *{NAME }* **no mac acl** *{NAME }*
Parameter	*NAME* Specify the name of MAC ACL
Mode	Global Configuration

Example	The example shows how to create a mac acl. You can verify settings by the following show acl command
	Switch#**configure terminal**
	Switch(config)# **mac acl** test
	Switch(mac-acl)# **show acl**
	 
	`Switch(config)# mac acl commando`
	`Switch(config-mac-acl)# show acl`
	
	`MAC access list commando`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.2 PERMIT (MAC)

Use the permit command to add permit conditions for a mac ACE that bypass those packets hit the ACE.

The **"sequence"** also represents hit priority when ACL bind to an interface. An ACE does not specify **"sequence"** index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE.

Switch#**configure terminal**
Switch(config)# **mac acl** *{NAME }*
Switch(config-mac-acl)# **[sequence** *<1-2147483647>***]** **permit (A:B:C:D:E:F /A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan** *<1-4094>***] [cos** *<0-7><0-7>***][ethtype** *<0x0600-0xFFFF>***]**

Switch(config-mac-acl)#**no sequence** *<1-2147483647>*

Syntax	**[sequence** *<1-2147483647>***] permit (A:B:C:D:E:F/A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan** *<1-4094>***] [cos** *<0-7><0-7>***][ethtype <0x0600-0xFFFF>]** **no sequence** *<1-2147483647>*
Parameter	*<1-2147483647>* b (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. **(A:B:C:D:E:F/A:B:C:D:E:F|any)**Specify the source MAC address and mask of packet or any MAC address. **(A:B:C:D:E:F/A:B:C:D:E:F|any)**Specify the destination MAC address and mask of packet or any MAC address. **[vlan***<1-4094>***]** (Optional) Specify the vlan ID of packet. **[cos***<0-7><0-7>***]**(Optional) Specify the Class of Service value and mask of packet. **[ethtype***<0x0600-0xFFFF>***]** (Optional) Specify Ethernet protocol number of packet.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Mode	MAC ACL Configuration

Example	The example shows how to add an ACE that permit packets with source MAC address 22:33:44:55:66:77. VLAN 3 and Ethernet type 1999. You can verify settings by the following show acl command,
	Switch#**configure terminal**
	Switch(config)# **mac acl test**
	Switch(mac-acl)# **sequence** 999 **permit** 22:33:44:55:66:77/ FF:FF:FF:FF:FF:FF **any vlan** 3 **ethtype** 0x2800
	Switch(mac-al)# **show acl**
	`Switch(config)# mac acl commando`
	`Switch(config-mac-acl)# sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 0x2800`
	`Switch(config-mac-acl)# show acl`
	
	`MAC access list commando`
	`sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 0x2800`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.3 DENY (MAC)

Use the deny command to add deny conditions for a mac ACE that drop those packets hit the ACE. The **"sequence"** also represents hit priority when ACL bind to an interface. An ACE does not specify **"sequence"** index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE. Use **"shutdown"** to shutdown interface while ACE hit.

Switch#**configure terminal**
Switch(config)# **mac acl** *{NAME }*
Switch(config-mac-acl)# **[sequence** *<1-2147483647>***]** **deny** **(A:B:C:D:E:F/ A:B:C:D:E:F|any)** **(A:B:C:D:E:F/A:B:C:D:E:F|any)** **[vlan** *<1-4094>***]** **[cos** *<0-7><0-7>***]** **[ethtype** *<0x0600-0xFFFF>***]** **[shutdown]**

Switch(config-mac-acl)# **no sequence** *<1-2147483647>*

Syntax	**[sequence** *<1-2147483647>***]** **deny** **(A:B:C:D:E:F/A:B:C:D:E:F|any)** **(A:B:C:D:E:F/A:B:C:D:E:F|any)** **[vlan** *<1-4094>***]** **[cos** *<0-7><0-7>***]** **[ethtype** *<0x0600-0xFFFF>***]** **[shutdown]** **no sequence** *<1-2147483647>*
Parameter	*<1-2147483647>* (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. **(A:B:C:D:E:F/A:B:C:D:E:F|any)**Specify the source MAC address and mask of packet or any MAC address. **(A:B:C:D:E:F/A:B:C:D:E:F|any)**Specify the destination MAC address and mask of packet or any MAC address. **[vlan***<1-4094>***]** (Optional) Specify the vlan ID of packet. **[cos***<0-7><0-7>***]**(Optional) Specify the Class of Service value and mask of packet. **[ethtype***<0x0600-0xFFFF>***]**(Optional) Specify Ethernetprotocol number of packet

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	[shutdown](Optional) Shutdown interfaces while ACE hit.
Mode	MAC ACL Configuration
Example	The example shows how to add an ACE that denies packets with destination MAC address aa:bb:cc:xx:xx:xx and VLAN 9. You can verify settings by the following show acl command Switch#configure terminal Switch(config)# mac acl test Switch(mac-acl)# sequence 30 permit any any Switch(mac-acl)# deny any aa:bb:cc:00:0:00/FF:FF:FF:00:00:00 vlan 9 shutdown Switch(mac-acl)# show acl Switch(config)# mac acl commando Switch(config-mac-acl)# sequence 30 permit any any Switch(config-mac-acl)# deny any aa:bb:cc:00:0:00/FF:FF:FF:00:00:00 vlan 9 shutdown Switch(config-mac-acl)# show acl MAC access list commando sequence 30 permit any any sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 0x2800 sequence 1019 deny any AA:BB:CC:00:00:00/FF:FF:FF:00:00:00 vlan 9 shutdown

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.4 IP ACL

Use the ip acl command to create an IPv4 access list and to enter ip-acl configuration mode. The name of ACL must be unique that cannot have same name with other ACL or QoS policy. Once an ACL is created, an implicit **"deny any"** ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

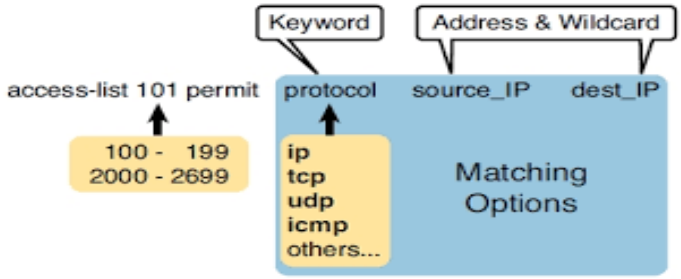


Fig 3.4.1 IP ACL with permit and deny.

Switch#**configure terminal**
Switch(config)# **ip acl** *{NAME}*

Switch(config)# **no ip acl** *{NAME}*

Syntax	**ip acl** *{NAME}* **no ip acl** *{NAME}*
Parameter	*NAME* Specify the name of IPv4 ACL
Mode	Global Configuration

Example	The example shows how to create an IP ACL. You can verify settings by the following show acl command
	Switch#**configure terminal**
	Switch(config)#**ip acl iptest**
	Switch(config-ip-acl)# **do show acl**
	`Switch(config)# ip acl iptest`
	`Switch(config-ip-acl)# show acl`
	
	`IP access list iptest`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.5 PERMIT (IP)

Use the permit command to add permit conditions for an IP ACE that bypasses those packets hit the ACE. The **"sequence"** also represents hit priority when ACL bind to an interface. An ACE does not specify **"sequence"** index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE.

Switch#**configure terminal**

Switch(config)# **ip acl** *{NAME}*

Switch(config-ip-acl)#**permit ip** 192.168.1.0/255.255.255.0 **any permit icmp any any echo-request any**

Syntax	[sequence *<1-2147483647>*] permit (*<0- 255>*|ipinip|egp|igp |hmp|rdp|ipv6| ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip) (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any)[(dscp|precedence) VALUE]] [sequence*<1-2147483647>*]permit icmp(A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) (*<0-255>*|echo-reply|destination-unreachable|source-quench|echo- request|router-advertisement|router-solicitation|time- exceeded|timestamp|timestamp-reply|traceroute|any) (*<0- 255>*|any) [(dscp|precedence) VALUE] [sequence*<1-2147483647>*] permit tcp (A.B.C.D/A.B.C.D|any) (*<0-65535>* |echo|discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois|tacacs-ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANG E|any) (A.B.C.D/A.B.C.D|any) (*<0-65535>*|echo|discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois| tacacs-ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_R

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	ANGE|any)[match-all TCP_FLAG][(dscp|precedence) VALUE] [sequence *<1-2147483647>*]permit udp (A.B.C.D/A.B.C.D|any) (*<0-65535>*|echo|discard| time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|snmp| snmptrap|who|syslog|talk|rip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) *<0-65535>*|echo |discard|time|nameserver|tacacsds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns| snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE] no sequence *<1-2147483647>*
Parameter	*<1-2147483647>* (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. (A.B.C.D/A.B.C.D|any) Specify the source IPv4 address and mask of packet or any IPv4 address. (A.B.C.D/A.B.C.D|any) Specify the destination IPv4 address and mask of packet or any IPv4 address. [dscp VALUE](Optional) Specify the DSCP of packet. [precedence VLAUE](Optional) Specify the IP precedence of packet. icmp-type Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type. icmp-code Specify ICMP message code for filtering ICMP packet. l4-source-port Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. l4-destination-port Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. match-all Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin,-urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
Mode	IP ACL Configuration
Example	The example shows how to add a set of ACEs. You can verify settings by the following show acl command. This command shows how to permit a source IP address subnet.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch#**configure terminal**
	Switch(config)# **ip acl** *{commando}*
	Switch(config-ip-acl)#**permit ip** 192.168.1.0/255.255.255.0 **any**
	This command shows how to permit ICMP echo-request packet with any IP address.
	Switch(config-ip-acl)#**permit icmp any any** echo-request **any**
	This command shows how to permit any IP address HTTP packets with DSCP 5.
	Switch(config-ip-acl)#**permit tcp any any any** www **dscp** 5
	This command shows how to permit any source IP address SNMP packet connect to destination IP address 192.168.1.1.
	Switch(config-ip-acl)#**permit udp any any** 192.168.1.1/255.255.255.255 **snmp**
	Switch(config-ip-acl)#**show acl**
	`Switch(config-ip-acl)# permit ip 192.168.1.0/255.255.255.0 any`
	`Switch(config-ip-acl)# permit icmp any any echo-request any`
	`Switch(config-ip-acl)# permit tcp any any any www dscp 5`
	`Switch(config-ip-acl)# permit udp any any 192.168.1.1/255.255.255.255 snmp`
	`Switch(config-ip-acl)# show acl`
	
	`IP access list iptest`
	`sequence 1 permit ip 192.168.1.0/255.255.255.0 any`
	`sequence 21 permit icmp any any echo-request any`
	`sequence 41 permit tcp any any any www dscp 5`
	`sequence 61 permit udp any any 192.168.1.1/255.255.255.255 snmp`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.6 DENY (IP)

Use the deny command to add deny conditions for an IP ACE that drop those packets hit the ACE. The **"sequence"** also represents hit priority when ACL bind to an interface. An ACE does not specify **"sequence"** index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE. Use **"shutdown"** to shutdown interface while ACE hit.

Switch#**configure terminal**

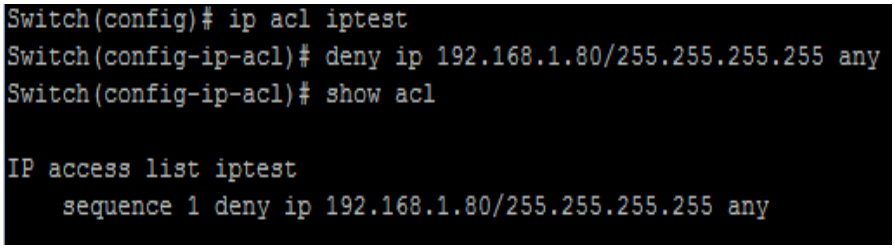
Switch(config)# **ip acl** {iptest}
Switch(config-ip-acl)#**deny ip** 192.168.1.80/255.255.255.255 **any**

Syntax	[sequence *<1-2147483647>*] deny(*<0-255>*|ipinip|egp|igp|hmp|rdp|ipv6|ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip) (A.B.C.D/A.B.C.D|any)(A.B.C.D/A.B.C.D|any)[(dscp|precedence) VALUE]] [shutdown] [sequence *<1-2147483647>*] deny icmp (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any)(*<0-255>*|echo-reply|destination-unreachable| source-quench|echo-request|router-advertisement|router- solicitation| time-exceeded|timestamp| timestamp-reply|traceroute|any) (<0-255>|any) [(dscp|precedence) VALUE] [shutdown] [sequence *<1-2147483647>*]deny tcp (A.B.C.D/A.B.C.D|any) (*<0-65535>*|echo| discard|daytime|ftp- data|ftp|telnet|smtp|time|hostname|whois|tacacs-ds| domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip| PORT_RANGE|any)(<0-65535>|echo|discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois| (A.B.C.D/A.B.C.D|any) (*<0-65535>*|echo|discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois|tacacsds|domain|www|pop2|pop3|syslog|talk| klogin|kshell|sunrpc|drip|PORT_RANGE|any) [match-all TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	[sequence *<1-2147483647>*] deny udp (A.B.C.D/A.B.C.D|any)(*<0-65535>*|echo|discard|time|nameserver|tacacs- ds|domain|bootps| bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|snmptrap|who|syslog| talk|rip|PORT_RANGE|any)(A.B.C.D/A.B.C.D|any)(*<0-65535>*|echo|discard|time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp| sunrpc|ntp|netbiosns|snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE] [shutdown] no sequence *<1-2147483647>*
Parameter	*<1-2147483647>* (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. (A.B.C.D/A.B.C.D|any)Specify the source IPv4 address and mask of packet or any IPv4 address. (A.B.C.D/A.B.C.D|any)Specify the destination IPv4 address and mask of packet or any IPv4 address. [dscp VALUE](Optional) Specify the DSCP ofpacket. [precedence VLAUE](Optional) Specify the IP precedence of packet. icmp-typeSpecify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type. icmp-code Specify ICMP message code for filtering ICMP packet. l4-source-portSpecify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. l4-destination-portSpecify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. match-allSpecify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin,-urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack). [shutdown](Optional) Shutdown interface while ACE hit.
Mode	IP ACL Configuration
Example	The example shows how to add an ACE that denies packets with source IP address 192.168.1.80. You can verify settings by the following show acl command

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch#configure terminal Switch(config)# ip acl iptest Switch(config-ip-acl)#deny ip 192.168.1.80/255.255.255.255 any Switch(config-ip-acl)#show acl 

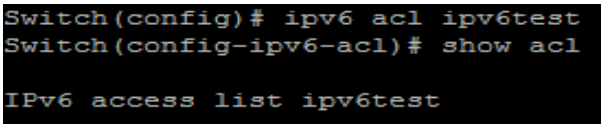
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.7 IPV6 ACL

Use the ipv6 acl command to create an IPv6 access list and to enter ipv6-acl configuration mode. The name of ACL must be unique that cannot have same name with other ACL or QoS policy. Once an ACL is created, an implicit **"deny any"** ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

Switch#**configure terminal**
Switch(config)# **ipv6 acl** *{NAME}*

Switch(config)# **no ipv6 acl** *{NAME}*

Syntax	**ipv6 acl** *{NAME}* **no ipv6 acl** *{NAME}*
Parameter	*NAME* Specify the name of IPv6 ACL
Mode	Global Configuration
Example	The example shows how to create an IPv6 ACL. You can verify settings by the following show acl command Switch#**configure terminal** Switch(config)#**ipv6 acl** ipv6test Switch(config-ipv6-acl)# **show acl** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.8 PERMIT (IPV6)

Use the permit command to add permit conditions for an IPv6 ACE that bypasses those packets hit the ACE. The **"sequence"** also represents hit priority when ACL bind to an interface. An ACE does not specify **"sequence"** index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE.

Switch#**configure terminal**
Switch(config)# **ipv6 acl** {ipv6test}
Switch(config-ipv6-acl)#**permit ipv6** fe80:1122:3344:5566::1/64 **any**

Syntax	[sequence *<1-2147483647>*] permit (*<0-255>*|ipv6) (X:X::X:X/*<0-128>*|any) (X:X::X:X/*<0-128>*|any)[(dscp|precedence) VALUE] [sequence <1-2147483647>] permit icmp (X:X::X:X/*<0- 128>*|any) (X:X::X:X/*<0-128>*|any) (*<0-255*>|destination- unreachable|packet-too-big| time-exceeded|parameter-problem|echo-request|echo-reply| mld-query|mld-report|mldv2-report|mld-done| router- solicitation|router-advertisement|nd-ns|nd-na|any) (*<0- 255>*|any)[(dscp|precedence) VALUE] [sequence *<1-2147483647>*] permit tcp (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|daytime|ftp-data|ftp|telnet|smtp| time|hostname|whois|tacacs- ds|domain|www|pop2|pop3|syslog| talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|daytime|ftp- data|ftp| telnet|smtp|time|hostname|whois|tacacs-ds|domain|www|pop2| pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)[match-all TCP_FLAG] [(dscp|precedence) VALUE] [sequence *<1-2147483647>*] permit udp (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|time|nameserver|tacacs-ds|domain|

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	bootps|bootpc|tftp|sunrpc|ntp|netbios- ns|snmp|snmptrap|who|syslog| talk|rip|PORT_RANGE|any) (X:X::X:X/ *<0-128>*|any) (*<0-65535>*|echo|discard|time|nameserver|tacacs-ds|domain| bootps|bootpc|tftp|sunrpc|ntp|netbios-ns| snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE] no sequence *<1-2147483647>*
Parameter	*<1-2147483647>*(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. (X:X::X:X/<0-128>|any) Specify the source IPv6 address and prefix of packet or any IPv6 address. (X:X::X:X/<0-128>|any) Specify the destination IPv6 address and prefix of packet or any IPv6 address. [dscp VALUE](Optional) Specify the DSCP of packet. [precedence VLAUE](Optional) Specify the IP precedence of packet. icmp-type Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type. icmp-code Specify ICMP message code for filtering ICMP packet. l4-source-port Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. l4-destination-port Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. match-all Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
Mode	IPv6 ACL Configuration
Example	The example shows how to add a set of ACEs. You can verify settings by the following show acl command. This command shows how to permit a source IP address subnet. Switch#configure terminal Switch(config)# ipv6 acl {commando} Switch(ipv6-acl)# permit ipv6 fe80:1122:3344:5566::1/64 any

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch(ipv6-acl)# show acl Switch(config-ipv6-acl)# permit ipv6 fe80:1122:3344:5566::1/64 any Switch(config-ipv6-acl)# show acl IPv6 access list ipv6test sequence 1 permit ipv6 fe80:1122:3344:5566::1/64 any

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.9 DENY (IPV6)

Use the deny command to add deny conditions for an IPv6 ACE that drop those packets hit the ACE. The **"sequence"** also represents hit priority when ACL bind to an interface. An ACE does not specify **"sequence"** index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE. Use **"shutdown"** to shutdown interface while ACE hit.

Switch#**configure terminal**
Switch(config)# **ipv6 acl** {ipv6test}
Switch(config-ipv6-acl)# **permit ipv6** fe80:1122:3344:5566::1/64 **any**

Syntax	[sequence *<1-2147483647>*] deny (*<0-255>*|ipv6) (X:X::X:X/*<0-128>*|any) (X:X::X:X/*<0-128>*|any) [(dscp|precedence) VALUE] [shutdown] [sequence <1-2147483647>] deny icmp (X:X::X:X/*<0-128>*|any) (X:X::X:X/*<0-128>*|any) (*<0-255>*|destination- unreachable|packet-too-big| time-exceeded|parameter-problem|echo-request|echo-reply| mld-query|mld-report|mldv2-report|mld-done| router- solicitation|router-advertisement|nd-ns|nd-na|any) (*<0- 255>*|any)[(dscp|precedence) VALUE] [shutdown] [sequence *<1-2147483647>*] deny tcp (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|daytime|ftp-data|ftp|telnet|smtp| time|hostname|whois|tacacs-ds|domain|www|pop2|pop3|syslog| talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|daytime|ftp- data|ftp| telnet|smtp|time|hostname|whois|tacacs-ds|domain|www|pop2| pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) [match-all TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	[sequence *<1-2147483647>*] deny udp (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|time|nameserver|tacacs-ds|domain| bootps|bootpc|tftp|sunrpc|ntp|netbios- ns|snmp|snmptrap|who|syslog| talk|rip|PORT_RANGE|any) (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|time|nameserver|tacacs-ds|domain| bootps|bootpc|tftp|sunrpc|ntp|netbios-ns| snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE] [shutdown] no sequence *<1-2147483647>*
Parameter	Parameter *<1-2147483647>*(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. (A.B.C.D/A.B.C.D|any) Specify the source IPv4 address and mask of packet or any IPv4 address. (A.B.C.D/A.B.C.D|any) Specify the destination IPv4 address and mask of packet or any IPv4 address. [dscp VALUE](Optional) Specify the DSCP of packet. [precedence VLAUE](Optional) Specify the IP precedence of packet. icmp-type Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type. icmp-code Specify ICMP message code for filtering ICMP packet. l4-source-port Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. l4-destination-port Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. match-all Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack). [shutdown](Optional) Shutdown interface while ACE hit.
Mode	IP ACL Configuration
Example	The example shows how to add an ACE that denies packets with destination IP address fe80::abcd. You can verify settings by the following show acl command

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch#configure terminal
	Switch(config)# ipv6 acl {ipv6test}
	Switch(config-ip-acl)#deny ipv6 any fe80::abcd/128
	Switch(config-ip-acl)#show acl
	`Switch(config)# ipv6 acl ipv6test`
	`Switch(config-ipv6-acl)# deny ipv6 any fe80::abcd/128`
	`Switch(config-ipv6-acl)# show acl`
	
	`IPv6 access list ipv6test`
	`sequence 1 permit ipv6 fe80:1122:3344:5566::1/64 any`
	`sequence 21 deny ipv6 any fe80::abcd/128`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.10 BIND ACL

Use the **(mac|ip|ipv6) acl** *{NAME }* command to bind an ACL to interfaces. An interface can bind only one ACL or QoS policy. Use the no form of this command to return to unbind an ACL from interface.

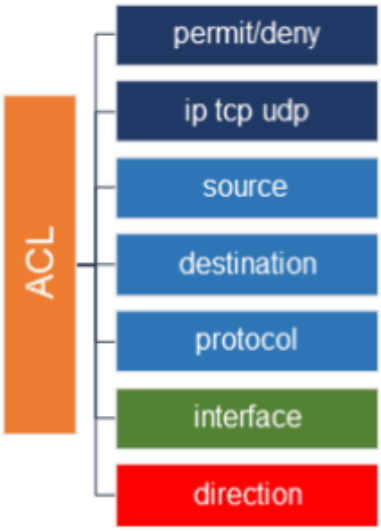


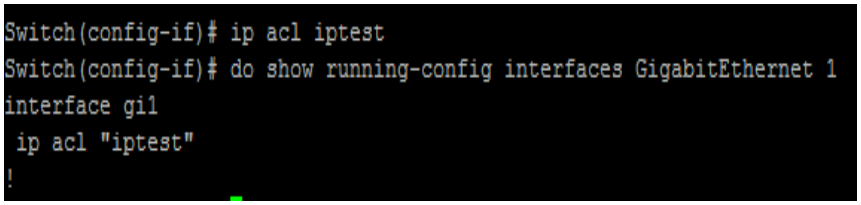
Fig 3.10.1 E3000 Series Switches bind an ACL to interface

Switch#**configure terminal**
Switch(config)# **(mac|ip|ipv6) acl** *{NAME }*

Switch(config)# **[no] (mac|ip|ipv6) acl** *{NAME}*

Syntax	**(mac|ip|ipv6) acl** *{NAME }* **[no] (mac|ip|ipv6) acl** *{NAME}*
Parameter	*(mac|ip|ipv6)* Specify a type of ACL to binding to interface **NAME** Specify the name of ACL
Mode	Interface Configuration
Example	The example shows how to bind an existed ACL to interface. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

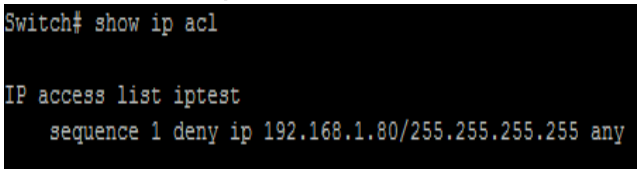
	Switch(config-if)# **ip acl** iptest Switch(config-if)# **do show running-config interfaces GigabitEthernet 1**  Switch(config-if)# ip acl iptest Switch(config-if)# do show running-config interfaces GigabitEthernet 1 interface gi1 ip acl "iptest" !

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.11 SHOW ACL

Use the show acl command to show created ACLs. You can specify macip or ipv6 to show specific type ACL or specify unique name string to show ACL with the name.

Switch#**show acl**
Switch#**show (mac|ip|ipv6) acl**
Switch#**show (mac|ip|ipv6) acl** (NAME)

Syntax	**show acl** **show (mac|ip|ipv6) acl** **show (mac|ip|ipv6) acl NAME**
Parameter	**(mac|ip|ipv6)**Specify a type of ACL to show *NAME* Specify the name of ACL
Mode	Global Configuration Context Configuration
Example	The example shows how to show all IP ACL. Switch# **show ip acl** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

3.12 SHOW ACL UTILIZATION

Use the show acl utilization command to show the usage of PIE of ASIC. When an ACL bind to interface, it needs ASIC resource to help to filter packet. An ASIC has limited resource. This command help user to know the PIE usage of AISC.

Switch#**show acl utilization**

Syntax	**show acl utilization**
Mode	Global Configuration

Example	The example shows how to show utilization
	Switch# **show acl utilization**
	`Switch# show acl utilization`
	`Type: System Reserve usage: 256`
	`Type: MAC-based VLAN usage: 512`
	`Type: Auth usage: 128`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

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 manager implementation that delegates responsibility for authentication to one or more authentication providers. 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. Use MAC-based authentication to authenticate devices based on their physical media access control (MAC) address. 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. WEB-Based Local Account can be defined as the process of verifying someone's identity by using pre-required details (Commonly username and password).

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 through the network.
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.

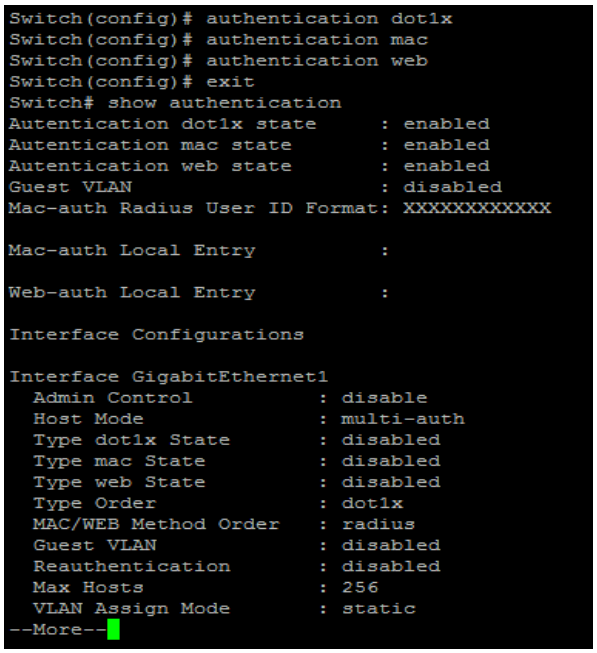
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.1 AUTHENTICATION

Use **"authentication"** command to enable the global setting of 802.1x/MAC/WEB authentication network access control. Use the **"no"** form of this command to disable 802.1x/MAC/WEB authentication.

Switch#**configure terminal**
Switch(config)#**authentication (dot1x|mac|web)**

Switch(config)#**no authentication (dot1x|mac|web)**

Syntax	**authentication (dot1x|mac|web)** **no authentication (dot1x|mac|web)**
Example	The following example shows how to enable 802.1x/MAC/WEB authentication. Switch#**configure terminal** Switch(config)# **authentication dot1x** Switch(config)# **authentication mac** Switch(config)# **authentication web** Switch# **show authentication** 

```
Switch(config)# authentication dot1x
Switch(config)# authentication mac
Switch(config)# authentication web
Switch(config)# exit
Switch# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : disabled
Mac-auth Radius User ID Format: XXXXXXXXXXXX

Mac-auth Local Entry          :

Web-auth Local Entry          :

Interface Configurations

Interface GigabitEthernet1
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.2 AUTHENTICATION (INTERFACE)

Use **"authentication"** interface command to enable the port setting of 802.1x/MAC/WEB authentication network access control. Use the **"no"** form of this command to disable 802.1x/MAC/WEB authentication.

Switch#**configure terminal**
Switch(config)#**authentication (dot1x|mac|web)**

Switch(config)#**no authentication (dot1x|mac|web)**

Syntax	**authentication (dot1x|mac|web)** **no authentication (dot1x|mac|web)**
Default	Default is disabled for all type
Mode	Interface Configuration
Example	The following example shows how to enable 802.1x/MAC/WEB authentication. Switch#**configure terminal** Switch(config)# **interface GigabitEthernet 1** Switch(config-if)# **authentication dot1x** Switch(config-if)# **authentication mac** Switch(config-if)# **authentication web** Switch# **show authentication interface GigabitEthernet 1**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# authentication dot1x
Switch(config-if)# authentication mac
Switch(config-if)# authentication web
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control           : disable
  Host Mode               : multi-auth
  Type dot1x State        : enabled
  Type mac State          : enabled
  Type web State          : enabled
  Type Order              : dot1x
  MAC/WEB Method Order    : radius
  Guest VLAN              : disabled
  Reauthentication        : disabled
  Max Hosts               : 256
  VLAN Assign Mode        : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout      : 60
    Quiet Period          : 60
  802.1x Parameters
    EAP Max Request       : 2
    EAP TX Period         : 30
    Supplicant Timeout    : 30
    Server Timeout        : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.3 AUTHENTICATION MAC RADIUS

Use **"authentication mac radius"** command to configure the radius user id format used by MAC authentication Radius method.

Switch#**configure terminal**
Switch(config)#**authentication mac radius [mac-case (lower|upper)] [mac delimiter(colon|dot|hyphen|none) [gap (2|4|6)]]**

Syntax	**authentication mac radius [mac-case (lower|upper)] [mac delimiter(colon|dot|hyphen|none) [gap (2|4|6)]]**
Parameter	**mac-case (lower|upper)** Select radius user id to be upper case or lower case.mac-delimiter(colon|dot|hyphen|none) Select radius user id delimiter colon: XX:XX:XX:XX:XX:XX dot: XX.XX.XX.XX.XX.XX hyphen: XX-XX-XX-XX-XX-XX none: XXXXXXXXXXXX gap (2|4|6) Select delimiter gap 2: XX-XX-XX-XX-XX-XX 4: XXXX-XXXX-XXXX 6: XXXXXX-XXXXXX
Default	Default radius id format is upper case with none delimiter.
Mode	Global Configuration
Example	The following example shows how to configure MAC authentication radius id format to be upper case with colon delimiter every 2 chars Switch#**configure terminal** Switch(config)# **authentication mac radius mac-case upper** Switch(config)# **authentication mac radius mac-delimiter colon gap 2** Switch# **show authentication**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# authentication mac radius mac-case upper
Switch(config)# authentication mac radius mac-delimiter colon gap 2
Switch(config)# exit
Switch# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : disabled
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX

Mac-auth Local Entry          :

Web-auth Local Entry          :

Interface Configurations

Interface GigabitEthernet1
  Admin Control           : disable
  Host Mode               : multi-auth
  Type dot1x State        : enabled
  Type mac State          : enabled
  Type web State          : enabled
  Type Order              : dot1x
  MAC/WEB Method Order    : radius
  Guest VLAN              : disabled
  Reauthentication        : disabled
  Max Hosts               : 256
  VLAN Assign Mode        : static
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.4 AUTHENTICATION MAC LOCAL

Use **"authentication mac local"** command to add local MAC authentication hosts in database. This local host database is used when MAC authentication method is configured as **"local"**. The MAC authentication module will find host in this local database and authenticated it. Use the no form of this command to delete local host from database.

Switch#**configure terminal**
Switch(config)#**authentication mac local mac-addr control auth** [**vlan** *<1-4094>*] [**reauth-period** *<300-4294967294>*] [**inactive-timeout** *<60-65535>*]
Switch(config)#**authentication mac local mac-addr control unauth**

Switch(config)#**no authentication mac local mac-addr**

Syntax	**authentication mac local mac-addr control auth** [**vlan** *<1-4094>*] [**reauth-period** *<300-4294967294>*] [**inactive-timeout** *<60-65535>*] **authentication mac local mac-addr control unauth** Switch(config)#**no authentication mac local mac-addr**
Parameter	**mac-addr** MAC Authentication local MAC address. **control auth** Host with this MAC address will be authorized. **control unauth** Host with this MAC address will be force-unauthorized **vlan** *<1-4094>*MAC Authentication host assigned VLAN. **reauth-period** *<300-4294967294>*MAC Authentication host reauthentication period inactive-timeout. *<60-65535>*MAC authentication host inactive timeout.
Default	Default is no local MAC Authentication entry.
Mode	Global Configuration
Example	The following example shows how to add a new local mac authentication host. Switch#**configure terminal** Switch(config)# **authentication mac local 00:11:22:33:00:01 control auth vlan 3 reauth-period 500 inactive-timeout 300** Switch# **show authentication**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# authentication mac local 00:11:22:33:00:01 control auth vlan 3 reauth-period 500
Switch(config)# exit
Switch# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : disabled
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX

Mac-auth Local Entry          :
                                        Reauth     Inactive
MAC Address         Control       VLAN  Period     Timeout
------------------ ------------- ------ ---------- ---------
00:11:22:33:00:01   Authorized    3      500        N/A

Web-auth Local Entry          :

Interface Configurations

Interface GigabitEthernet1
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.5 AUTHENTICATION GUEST-VLAN

Use **“authentication guest-vlan”** command to enable the global setting of guest VLAN and specify guest VLAN ID. Use the **“no”** form of this command to disable guest VLAN.

Switch#**configure terminal**
Switch(config)#**authentication guest-vlan** *<1-4094>*
Switch(config)#**no authentication guest-vlan**

Syntax	**authentication guest-vlan** *<1-4094>* **no authentication guest-vlan**
Parameter	*<1-4094>*Guest VLAN ID
Default	Default guest VLAN is disabled
Mode	Global Configuration
Example	The following example shows how to create guest VLAN. Switch#**configure terminal** Switch(config)# **vlan 3** Switch(config-vlan)# **exit** Switch(config)# **authentication guest-vlan 3** Switch# **show authentication**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# vlan 3
Switch(config-vlan)# exit
Switch(config)# authentication guest-vlan 3
Switch(config)# exit
Switch# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : enabled (3)
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX

Mac-auth Local Entry          :
                                          Reauth     Inactive
MAC Address         Control        VLAN   Period     Timeout
------------------- -------------- ------ ---------- ---------
00:11:22:33:00:01   Authorized     3      500        N/A

Web-auth Local Entry          :

Interface Configurations

Interface GigabitEthernet1
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.6 AUTHENTICATION GUEST-VLAN (INTERFACE)

Use **"authentication guest-vlan"** command to enable the port setting of guest VLAN. Use the **"no"** form of this command to disable guest VLAN.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)#**authentication guest-vlan**

Switch(config-if)#**no authentication guest-vlan**

Syntax	**authentication guest-vlan** **no authentication guest-vlan**
Default	Default guest VLAN is disabled
Mode	Interface Configuration

Example	The following example shows how to enable guest VLAN.
	Switch#configure terminal
	Switch(config)# **interface** GigabitEthernet1
	Switch(config-if)# **authentication guest-vlan**
	`Switch# configure`
	`Switch(config)# interface GigabitEthernet 1`
	`Switch(config-if)# authentication guest-vlan`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.7 AUTHENTICATION HOST-MODE

Use **"authentication host-mode"** command to configure the port, Authentication host mode. Use the **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config)#**authentication host-mode (multi-auth|multi-host|single-host)**

Switch(config)#**no authentication host-mode**

Syntax	**authentication host-mode (multi-auth|multi-host|single-host)** **no authentication host-mode**
Parameter	**multi-auth** Multiple Authentication Mode. In this mode, every client needs to pass authenticate procedure individually. **multi-host** Multiple Host Mode. In this mode, only one client needs to be authenticated and other clients will get the same access accessibility. **single-host** Single Host Mode. In this mode, only one host is allowed to be authenticated. It is the same as multi-auth mode with max hosts number configure to be 1.
Default	Default is multi-auth mode.
Mode	Interface Configuration
Example	The following example shows how to modify port host mode to multi-host. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication host-mode multi-host** Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control           : auto
  Host Mode               : multi-host
  Type dot1x State        : disabled
  Type mac State          : disabled
  Type web State          : disabled
  Type Order              : dot1x
  MAC/WEB Method Order    : radius
  Guest VLAN              : disabled
  Reauthentication        : enabled
  Max Hosts               : 256
  VLAN Assign Mode        : static
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout      : 60
    Quiet Period          : 300
  802.1x Parameters
    EAP Max Request       : 1
    EAP TX Period         : 10
    Supplicant Timeout    : 120
    Server Timeout        : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.8 AUTHENTICATION MAX-HOSTS

Use **"authentication max-hosts"** command to configure the port max hosts number for multi-auth mode. The host exceed the max host number is not allowed to create authentication session and do authenticating. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)#**authentication max-hosts** *<1-256>*

Switch(config-if)#**no authentication max-hosts**

Syntax	**authentication max-hosts** *<1-256>* **no authentication max-hosts**
Parameter	*<1-256>* Available max host number in multi-auth mode.
Default	Default max host number is 256
Mode	Interface Configuration
Example	The following example shows how to change port max host's number. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication max-hosts** 100 Switch# **show authentication interface GigabitEthernet** 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication max-hosts 100
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-host
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 60
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 10
    Supplicant Timeout   : 120
    Server Timeout       : 30
  Web-auth Parameters
    Login Attempt        : 3
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.9 AUTHENTICATION METHOD

Use **“authentication method”** command to configure the port authentication method order.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)# **authentication method local radius**

Syntax	**authentication method (local [radius] | radius [local])** **no authentication order**
Parameter	Local Use local account to authenticate Radius Use remote RADIUS server to authenticate
Default	Default is RADIUS method in first place and no other method.
Mode	Interface Configuration
Example	The following example shows how to modify port authentication order to local and then RADIUS. Switch#**configure terminal** Switch(config)# **interface GigabitEthernet 2** Switch(config-if)# **authentication method local radius** Switch# **show authentication interface GigabitEthernet 2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication method local radius
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 100
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.10 AUTHENTICATION ORDER

Use **"authentication order"** command to configure the port authentication type order. Use the **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)# **authentication order (dot1x [mac] [web] | mac [dot1x] [web] | web)**

Switch(config-if)# **no authentication order**

Syntax	**authentication order (dot1x [mac] [web] | mac [dot1x] [web] | web)** **no authentication order**
Parameter	**dot1x** Authenticating user by IEEE 802.1X **mac** Authenticating user by mac-based authentication **web** Authenticating user by web-based authentication
Default	Default is dot1x type in first place and no other types.
Mode	Interface Configuration
Example	The following example shows how to modify port authentication order to dot1x, mac and web. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication order dot1x mac web** Switch# **show authentication interface GigabitEthernet 2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication order dot1x mac web
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 100
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.11 AUTHENTICATION PORT-CONTROL

Use **"authentication port-control"** command to enable the port authentication control mode. Use the **"no"** form of this command to disable authentication port control

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)# **authentication port-control (auto|force-auth|force-unauth)**

Switch(config-if)# **no authentication port-control**

Syntax	**authentication port-control (auto|force-auth|force-unauth)** **no authentication port-control**
Parameter	**Auto** Need passing authentication procedure to get network accessibility **force-auth** Port is force authorized and all clients have network accessibility. **force-unauth** Port is force unauthorized and all clients have no network accessibility.
Mode	Interface Configuration
Example	The following example shows how to configure port control to auto mode. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication port-control auto** Switch# **show authentication interface GigabitEthernet 1**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication port-control auto
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 100
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.12 AUTHENTICATION RADIUS-ATTRIBUTES VLAN

Use **"authentication radius-attributes vlan"** command to configure the port RADIUS VLAN assign mode. Use the **"no"** form of this command to disable the port RADIUS VLAN assign.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)# **authentication radius-attributes vlan (reject | static)**

Switch(config-if)# **no authentication radius-attributes vlan**

Syntax	**authentication radius-attributes vlan (reject | static)** **no authentication radius-attributes vlan**
Parameter	**reject** If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized. **static** If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.
Default	Default radius attributes VLAN assign mode is static.
Mode	Interface Configuration
Example	The following example shows how to configure port VLAN assign to reject mode. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication radius-attributes vlan reject** Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication radius-attributes vlan reject
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.13 AUTHENTICATION REAUTH

Use **"authentication reauth"** command to enable the port reauthentication. Use the **"no"** form of this command to disable reauthentication.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)# **authentication reauth**

Switch(config-if)# **no authentication reauth**

Syntax	**authentication reauth** **no authentication reauth**
Mode	Interface Configuration
Example	The following example shows how to enable port reauthentication. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication reauth** Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication reauth
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.14 AUTHENTICATION TIMER INACTIVE

Use **"authentication timer inactive"** command to configure the port inactive timeout value. Sometimes, we may assign a long aging time for a host, but in fact, it is not active. This inactive timeout will detect the host is active or not. If the host is inactive exceed this timeout, it should be removed. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)# **authentication timer inactive** *<60-65535>*

Switch(config-if)# **no authentication timer inactive**

Syntax	**authentication timer inactive** *<60-65535>* **no authentication timer inactive**
Parameter	<60-65535>Interval in seconds after which if there is no activity from the client then it will be unauthorized
Default	Default inactive timeout is 60 seconds.
Mode	Interface Configuration
Example	The following example shows how to configure port inactive period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication timer inactive** 300 Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication timer inactive 300
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control           : auto
  Host Mode               : multi-auth
  Type dot1x State        : disabled
  Type mac State          : disabled
  Type web State          : disabled
  Type Order              : dot1x mac web
  MAC/WEB Method Order    : local radius
  Guest VLAN              : disabled
  Reauthentication        : enabled
  Max Hosts               : 100
  VLAN Assign Mode        : reject
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout      : 300
    Quiet Period          : 60
  802.1x Parameters
    EAP Max Request       : 2
    EAP TX Period         : 30
    Supplicant Timeout    : 30
    Server Timeout        : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.15 AUTHENTICATION TIMER QUIET

Use **"authentication timer quiet"** command to configure the port quiet period value. After authenticating fail many times and the port is guest VLAN disabled, the port/host will enter lock state until quiet period expired. In lock state, the port/host is not allowed to do authenticating. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)# **authentication timer quiet** *<0-65535>*

Switch(config-if)# **no authentication timer quiet**

Syntax	**authentication timer quiet** *<0-65535>* **no authentication timer quiet**
Parameter	*<0-65535>*Interval in seconds to wait following a failed authentication exchange
Default	Default quiet period is 60 seconds.
Mode	Interface Configuration
Example	The following example shows how to configure port quiet period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication timer quiet** 300 Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication timer quiet 300
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.16 AUTHENTICATION TIMER REAUTH

Use **"authentication timer reauth"** command to configure the port reauthentication period value with unit second if the reauthentication time is not assigned by local database or remote authentication server. On the other hand, if the reauthentication time is assigned by local database or remote server, this configured reauthentication time will be ignored. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-name}
Switch(config-if)# **authentication timer reauth** *<300-4294967294>*

Switch(config-if)# **no authentication timer reauth**

Syntax	**authentication timer reauth** *<300-4294967294>* **no authentication timer reauth**
Parameter	*<300-4294967294>*Time in seconds after which an automatic re-authentication should be initiated
Default	Default reauthentication period is 3600 seconds.
Mode	Interface Configuration
Example	The following example shows how to configure port reauthentication period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication timer reauth** 300 Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication timer reauth 300
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.17 AUTHENTICATION WEB LOCAL

Use **"authentication web local"** command to add local account in database. This local account database is used when web authentication method is configured as **"local"**. The web authentication module will find account in this local database and authenticated it. Use the **"no"** form of this command to delete local account from database.

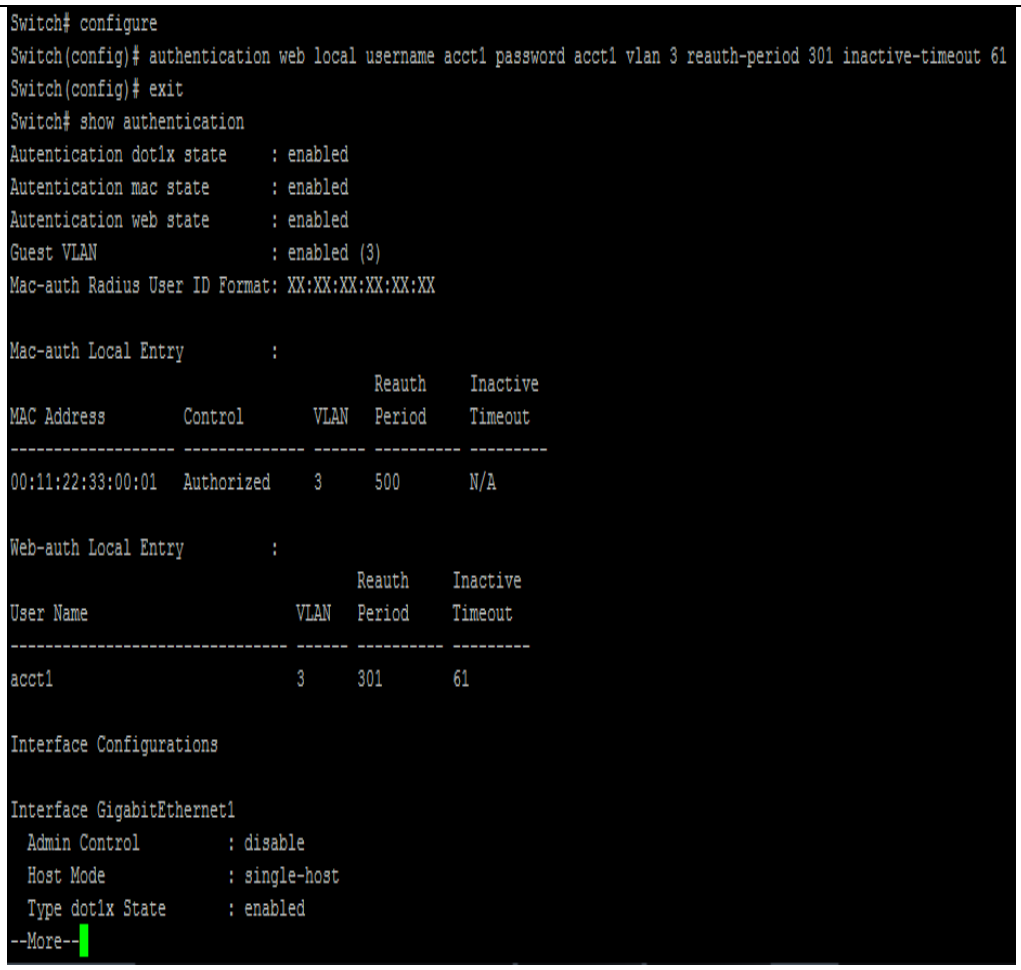
Switch#**configure terminal**

Switch(config)# **authentication web local username USERNAME password (encryptedCRYPT-PASSWORD | PASSWORD) [vlan** *<1-4094>*] [**reauth-period** *<300-4294967294>*] [**inactive-timeout** *<60-65535>*]

Switch(config)# **no authentication web local username USERNAME**

Syntax	**authentication web local username** USERNAME **password (encrypted** CRYPT-PASSWORD **|** PASSWORD**)** [**vlan** *<1-4094>*] [**reauth-period** *<300-4294967294>*] [**inactive-timeout** *<60-65535>*] **no authentication web local username USERNAME**
Parameter	**USERNAME** Local account username **Encrypted CRYPT-PASSWORD** Encrypted password. **PASSWORD** Un-encrypted password. **vlan** *<1-4094>* Assigned VLAN of this local account reauth-period **Re-authentication period** *<300-4294967294>* of this local account inactive-timeout. **Inactive timeout** *<60-65535>* of this local account.
Mode	Global Configuration
Example	The following example shows how to add/delete a new local account. Switch#**configure terminal** Switch(config)# **authentication web local username acct1 password acct1 vlan 3reauth-period 301 inactive-timeout 61** Switch# **show authentication**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.



© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.18 AUTHENTICATION WEB MAX-LOGIN-ATTEMPTS

Use **"authentication web max-login-attempts"** command to configure the port WEB authentication max login attempt number. After login fail number exceed, the host will enter Lock state and is not able to authenticate until quiet period exceed. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-id}
Switch(config-if)# **authentication web max-login-attempts (infinite|***<3-10>***)**

Switch(config-if)# **no authentication web max-login-attempts**

Syntax	**authentication web max-login-attempts (infinite|***<3-10>***)** **no authentication web max-login-attempts**
Parameter	**infinite** Do not care user login fail number *<3-10>* Allow user login fail number
Default	Default max login attempt number is 3.
Mode	Interface Configuration
Example	The following example shows how to configure port max login attempt number. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication web max-login-attempts** 5 Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication web max-login-attempts 5
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.19 CLEAR AUTHENTICATION SESSIONS

Use **"clear authentication sessions"** command to delete existing authentication sessions. If no parameter is specified, all sessions will be deleted. After authentication session is deleted, host need to do authentication procedure again.

Switch# **clear authentication sessions**
Switch# **clear authentication sessions interfaces** *{IF_PORTS}*
Switch# **clear authentication sessions mac** *{mac-addr}*
Switch# **clear authentication sessions session-id** *{WORD}*
Switch# **clear authentication sessions type (dot1x|mac|web)**

Syntax	**clear authentication sessions** **clear authentication sessions interfaces** *{IF_PORTS}* **clear authentication sessions mac** *{mac-addr}* **clear authentication sessions session-id** *{WORD}* **clear authentication sessions type (dot1x|mac|web)**
Parameter	**interfaces** *IF_PORTS* Clear sessions on specific interface **mac** *mac-addr* Clear session with specific MAC address **session-id** *WORD* Clear session with specific session ID type **(dot1x|mac|web)type** Clear session with specific authentication
Mode	Privileged EXEC
Example	The following example shows how to clear all authentication sessions. Switch# **clear authentication sessions** Switch# **show authentication sessions**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.20 DOT1X

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol). Use **"dot1x"** command to enable the global setting of 802.1x. The **"authentication dot1x"** command has the same effect as this one. This command is a backward compatible command. Use the **"no"** form of this command to disable 802.1 x authentications.

Switch#**configure terminal**
Switch(config)# **dot1x**

Switch(config)# **no dot1x**

Syntax	**dot1x** **no dot1x**
Default	Default 802.1x is disabled
Mode	Global Configuration
Example	The following example shows how to enable 802.1 x authentications. Switch#**configure terminal** Switch(config)# **dot1x** Switch# **show authentication**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# dot1x
Switch(config)# exit
Switch# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : enabled (3)
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX

Mac-auth Local Entry          :
                                          Reauth     Inactive
MAC Address         Control        VLAN   Period     Timeout
------------------- -------------- ------ ---------- ---------
00:11:22:33:00:01   Authorized     3      500        N/A

Web-auth Local Entry          :
                                        Reauth     Inactive
User Name                         VLAN  Period     Timeout
--------------------------------- ------ ---------- ---------
acct1                             3      301        61

Interface Configurations

Interface GigabitEthernet1
  Admin Control          : disable
  Host Mode              : single-host
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.21 DOT1X GUEST-VLAN

Use **"dot1x guest-vlan"** command to enable the global setting of guest VLAN and specify guest VLAN ID. It set the guest VLAN of the specified port. Use the **"no"** form of this command to disable guest VLAN.

Switch#**configure terminal**
Switch(config)# **dot1x guest-vlan** *<1-4094>*

Switch(config)# **no dot1x guest-vlan**

Syntax	**dot1x guest-vlan** *<1-4094>* **no dot1x guest-vlan**
Parameter	*<1-4094>*Guest VLAN ID
Default	Default guest VLAN is disabled
Mode	Global Configuration
Example	The following example shows how to create guest VLAN. Switch#**configure terminal** Switch(config)# **vlan 3** Switch(config-vlan)# **exit** Switch(config)# **dot1x guest-vlan 3** Switch# **show authentication**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# vlan 3
Switch(config-vlan)# exit
Switch(config)# dot1x guest-vlan 3
Switch(config)# exit
Switch# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : enabled (3)
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX

Mac-auth Local Entry          :
                                                Reauth     Inactive
MAC Address         Control         VLAN        Period     Timeout
------------------- --------------- ----------- ---------- ---------
00:11:22:33:00:01   Authorized      3           500        N/A

Web-auth Local Entry          :

Interface Configurations

Interface GigabitEthernet1
  Admin Control           : disable
  Host Mode               : single-host
  Type dot1x State        : enabled
  Type mac State          : enabled
  Type web State          : enabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.22 DOT1X MAX-REQ

Use **"dot1x max-req"** command to configure the port 802.1x max EAP request value. The max request is the maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-id}
Switch(config-if)# **dot1x max-req** *<1-10>*

Switch(config-if)# **no dot1x max-req**

Syntax	**dot1x max-req** *<1-10>* **no dot1x max-req**
Parameter	*<1-10>* The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.
Default	Default EAP max request number is 2.
Mode	Interface Configuration
Example	The following example shows how to configure port 802.1x EAP TX period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x max-req 1** Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x max-req 1
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 10
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.23 DOT1X PORT-CONTROL

Use **"dot1x port-control"** command to enable the port authentication control mode. The **"authentication port-control"** command has the same effect. Use the **"no"** form of this command to disable authentication port control.

Switch#**configure terminal**
Switch(config)# **interface** {interface-id}
Switch(config-if)# **dot1x port-control (auto|force-auth|force-unauth)**

Switch(config-if)# **no dot1x port-control**

Syntax	**dot1x port-control (auto|force-auth|force-unauth)** **no dot1x port-control**
Parameter	**Auto** Need passing authentication procedure to get network accessibility **force-auth** Port is force authorized and all clients have network accessibility. **force-unauth** Port is force unauthorized and all clients have no network accessibility.
Mode	Interface Configuration
Example	The following example shows how to configure port control to auto mode. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x port-control auto** Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x port-control auto
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 10
    Supplicant Timeout   : 120
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.24 DOT1X REAUTH

Use **“dot1x reauth”** command to enable the port reauthentication. The **“authentication reauth”** command has the same effect, it is a backward compatible command

Switch#**configure terminal**
Switch(config)# **interface** {interface-id}
Switch(config-if)# **dot1x reauth**

Switch(config-if)# **no dot1x reauth**

Syntax	**dot1x reauth** **no dot1x reauth**
Mode	Interface Configuration
Example	The following example shows how to enable port reauthentication. Switch#**configure terminal** Switch(config)# **interface** {interface-id} Switch(config-if)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x reauth** Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x reauth
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 10
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.25 DOT1X TIMEOUT REAUTH-PERIOD

Use **"dot1x timout reauth"** command to configure the port reauthentication period value with unit second if the reauthentication time is not assigned by local database or remote authentication server. On the other hand, if the reauthentication time is assigned by local database or remote server, this configured reauthentication time will be ignored. The **"authentication timer reauth"** command has the same effect, and it is a backward compatible command. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-id}
Switch(config-if)# **dot1x timeout reauth-period** *<300-4294967294>*

Switch(config-if)# **no dot1x timeout reauth-period**

Syntax	**dot1x timeout reauth-period** <300-4294967294> **no dot1x timeout reauth-period**
Parameter	*<300-4294967294>*Time in seconds after which an automatic re-authentication should be initiated
Default	Default reauthentication period is 3600 seconds. Mode Interface Configuration
Mode	Interface Configuration
Example	The following example shows how to configure port 802.1x reauthentication period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout reauth-period** 300 Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x timeout reauth-period 300
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 60
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 10
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.26 DOT1X TIMEOUT QUIET-PERIOD

Use **"dot1x timeout quiet-period"** command to configure the port quiet period value. The **"authentication timer quiet"** command has the same effect and it is backward compatible command.After authenticating fail many times and the port is guest VLAN disabled, the port/host will enter lock state until quiet period expired. In lock state, the port/host is not allowed to do authenticating. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-id}
Switch(config-if)# **dot1x timeout quiet-period** *<0-65535>*

Switch(config-if)# **no dot1x timeout quiet-period**

Syntax	**dot1x timeout quiet-period** *<0-65535>* **no dot1x timeout quiet-period**
Parameter	*<0-65535>*Interval in seconds to wait following a failed authentication exchange
Default	Default quiet period is 60 seconds.
Mode	Interface Configuration
Example	The following example shows how to configure port 802.1x quiet period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout quiet-period** 300 Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x timeout quiet-period 300
Switch(config-if)# exit
Switch(config)# exit
Switch#  show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control           : disable
  Host Mode               : multi-auth
  Type dot1x State        : disabled
  Type mac State          : disabled
  Type web State          : disabled
  Type Order              : dot1x
  MAC/WEB Method Order    : radius
  Guest VLAN              : disabled
  Reauthentication        : disabled
  Max Hosts               : 256
  VLAN Assign Mode        : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout      : 60
    Quiet Period          : 300
  802.1x Parameters
    EAP Max Request       : 2
    EAP TX Period         : 10
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.27 DOT1X TIMEOUT SERVER-TIMEOUT

Use **"dot1x timeout server-timeout"** command to configure the port 802.1x server timeout value. The server timeout is the number of seconds that lapses before the device resends a request to the authentication server.

Switch#**configure terminal**
Switch(config)# **interface** {interface-id}
Switch(config-if)# **dot1x timeout server-timeout** *<1-65535>*

Switch(config-if)# **no dot1x timeout server-timeout**

Syntax	**dot1x timeout server-timeout** *<1-65535>* **no dot1x timeout server-timeout**
Parameter	*<1-65535>* Number of seconds that lapse before the device resends a request to the authentication server.
Default	Default server timeout is 30 seconds.
Mode	Interface Configuration
Example	The following example shows how to configure port 802.1x server timeout. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout supp-timeout** 150 Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x timeout supp-timeout 150
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control           : disable
  Host Mode               : multi-auth
  Type dot1x State        : disabled
  Type mac State          : disabled
  Type web State          : disabled
  Type Order              : dot1x
  MAC/WEB Method Order    : radius
  Guest VLAN              : disabled
  Reauthentication        : disabled
  Max Hosts               : 256
  VLAN Assign Mode        : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout      : 60
    Quiet Period          : 60
  802.1x Parameters
    EAP Max Request       : 2
    EAP TX Period         : 30
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.28 DOT1X TIMEOUT SUPP-TIMEOUT

Use "**dot1x timeout supp-timeout"** command to configure the port supplicant timeout value. The supplicant timeout is the number of seconds that lapses before EAP requests are resent to the supplicant. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-id}
Switch(config-if)# **dot1x timeout supp-timeout** *<1-65535>*

Switch(config-if)# **no dot1x timeout supp-timeout**

Syntax	**dot1x timeout supp-timeout** *<1-65535>* **no dot1x timeout supp-timeout**
Parameter	*<1-65535>* Number of seconds that lapses before EAP requests are resent to the supplicant
Default	Default supplicant timeout is 30 seconds.
Mode	Interface Configuration
Example	The following example shows how to configure port 802.1x supplicant timeout. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout supp-timeout** 120 Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x timeout supp-timeout 120
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control           : disable
  Host Mode               : multi-auth
  Type dot1x State        : disabled
  Type mac State          : disabled
  Type web State          : disabled
  Type Order              : dot1x
  MAC/WEB Method Order    : radius
  Guest VLAN              : disabled
  Reauthentication        : disabled
  Max Hosts               : 256
  VLAN Assign Mode        : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout      : 60
    Quiet Period          : 60
  802.1x Parameters
    EAP Max Request       : 2
    EAP TX Period         : 30
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.29 DOT1X TIMEOUT TX-PERIOD

Use **"dot1x timeout tx-period"** command to configure the port 802.1x EAP TX period value. The TX period is the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request. Use **"no"** form of this command to restore default value.

Switch#**configure terminal**
Switch(config)# **interface** {interface-id}
Switch(config-if)# **dot1x timeout tx-period** *<1-65535>*

Switch(config-if)# **no dot1x timeout tx-period**

Syntax	**dot1x timeout tx-period** *<1-65535>* **no dot1x timeout tx-period**
Parameter	*<1-65535>* Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
Default	Default EAP TX period is 30 seconds.
Mode	Interface Configuration
Example	The following example shows how to configure port 802.1x EAP TX period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout tx-period** 10 Switch# **show authentication interface** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x timeout tx-period 10
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 10
    Supplicant Timeout   : 120
    Server Timeout       : 30
  Web-auth Parameters
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.30 SHOW AUTHENTICATION

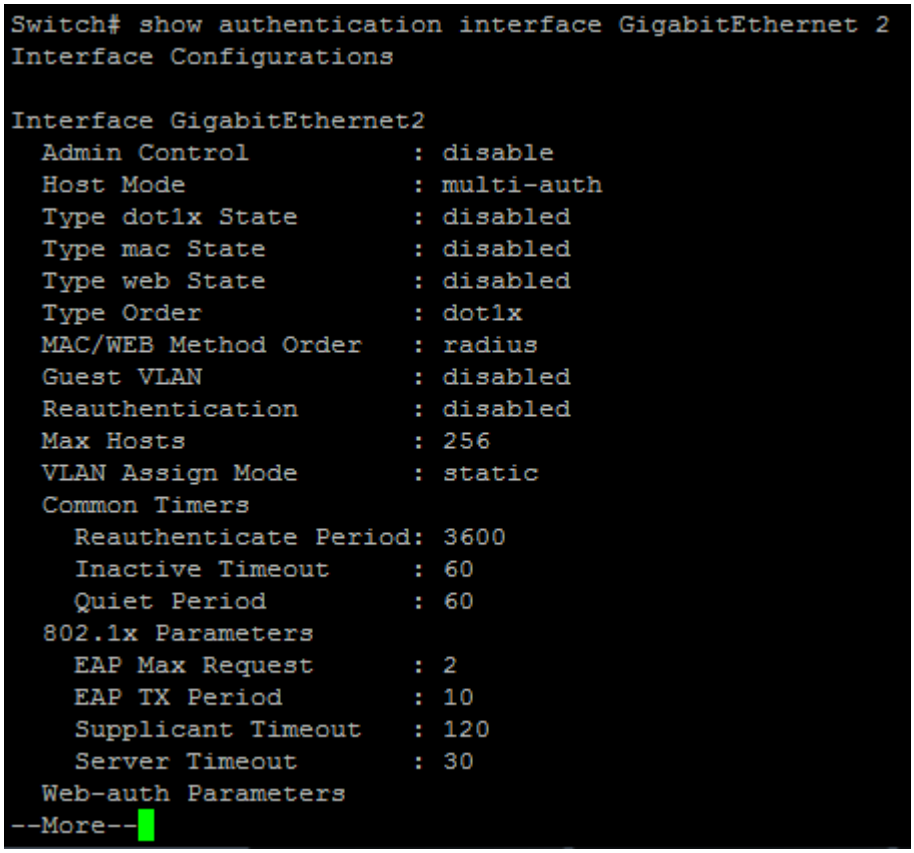
Use "**show authentication**" command to show all authentication manager configurations. Use "**show authentication interface**" command to show authentication manager configuration of specific port.

Switch# **show authentication**
Switch# **show authentication interfaces** *{IF_PORTS}*

Syntax	**show authentication** **show authentication interfaces** *{IF_PORTS}*
Parameter	**Interfaces** *IF_PORTS* Specify port list to show port configurations
Mode	Privileged EXEC
Example	This example shows how to show the mac authentication configurations of port GigabitEthernet 1. Switch# **show authentication**

```
Switch# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : enabled (3)
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX

Mac-auth Local Entry          :
                                          Reauth     Inactive
MAC Address         Control        VLAN   Period     Timeout
------------------- -------------- ------ ---------- ---------
00:11:22:33:00:01   Authorized     3      500        N/A

Web-auth Local Entry          :

Interface Configurations

Interface GigabitEthernet1
  Admin Control           : disable
  Host Mode               : single-host
  Type dot1x State        : enabled
  Type mac State          : enabled
  Type web State          : enabled
  Type Order              : dot1x
  MAC/WEB Method Order    : radius
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch# **show authentication interface GigabitEthernet 2** 

```
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control           : disable
  Host Mode               : multi-auth
  Type dot1x State        : disabled
  Type mac State          : disabled
  Type web State          : disabled
  Type Order              : dot1x
  MAC/WEB Method Order    : radius
  Guest VLAN              : disabled
  Reauthentication        : disabled
  Max Hosts               : 256
  VLAN Assign Mode        : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout      : 60
    Quiet Period          : 60
  802.1x Parameters
    EAP Max Request       : 2
    EAP TX Period         : 10
    Supplicant Timeout    : 120
    Server Timeout        : 30
  Web-auth Parameters
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4.31 SHOW AUTHENTICATION SESSIONS

Use **"show authentication sessions"** command to show authentication detail session information.

Switch# **show authentication sessions [detail]**
Switch# **show authentication sessions interface** *{IF_PORTS}*
Switch# **show authentication sessions session-id** *{WORD}*
Switch# **show authentication session type (dot1x|mac|web)**

Syntax	**show authentication sessions [detail]** **show authentication sessions interface** *{IF_PORTS}* **show authentication sessions session-id** *{WORD}* **show authentication session type (dot1x|mac|web)**
Parameter	**detail** Show session detail information. **Interface** *IF_PORTS* Show session detail information of specific port **session-id** *WORD* Show session detail information of specific session id **Type (dot1x|mac|web)** Show session detail information of specific authentication type
Mode	Privileged EXEC
Example	This example shows how to show current authentication session brief and detail information. Switch# **show authentication sessions** Switch# **show authentication sessions detail**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

5. DIAGNOSTIC

E3000 Series Switches Diagnostics offer proactive diagnostics and real-time alerts and provides higher network availability and increased operational efficiency. Log files of a switch are classified into user log files and diagnostic log files. A diagnostic log file records the service processing flow and fault information. These logs sent to the log buffer, console, or terminal monitors. You can set up a switch to automatically transfer diagnostic information to a remote server. If a fault occurs, you can provide troubleshooting and support.

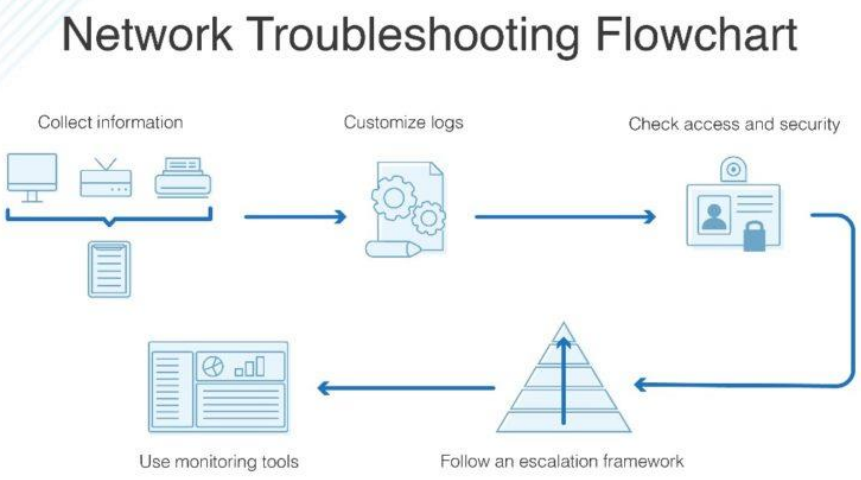


Fig 5.1.1 Network Troubleshooting Flowchart

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

5.1 SHOW CABLE-DIAG

To show the estimated copper cable length attached to a specific interface, use the command show cable-diag in the Privileged EXEC mode. For the proper information of the cable length, the interface must be active and linked up.

Switch#**show cable-diag interfaces** *{IF_NMLPORTS}*

Syntax	**show cable-diag interfaces** *{IF_NMLPORTS}*
Parameter	Interfaces *{IF_NMLPORTS}* Display the cable diagnostic information of the copper media for an interface ID or a list of interfaces IDs.
Mode	Privileged EXEC

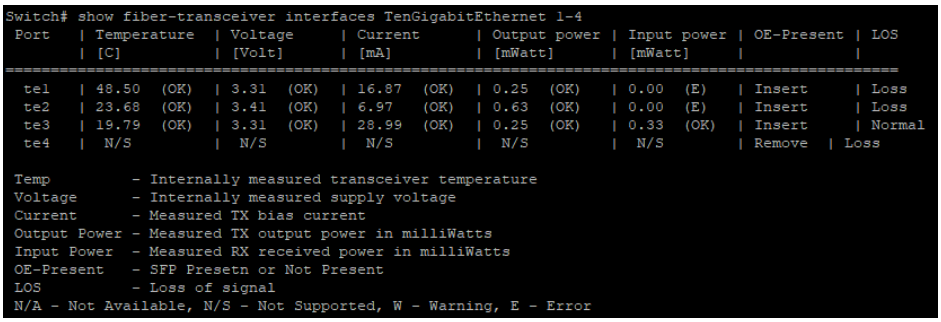
Example	The following example shows the result of cable diagnostic for the interface GigabitEthernet 7
	Switch# **show cable-diag interfaces GigabitEthernet 7**
	`Switch# show cable-diag interfaces GigabitEthernet 7`
	`Port | Speed | Local pair | Pair length | Pair status`
	`gi7 | auto | Pair A | 22.00 | Normal`
	`Pair B | 22.00 | Normal`
	`Pair C | 22.00 | Normal`
	`Pair D | 22.00 | Normal`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

5.2 SHOW FIBER-TRANSCEIVER

To show the diagnostic information of the fiber transceivers use the command. show fiber-transceiver in the Privilege EXEC mode.

Switch#**show fiber-transceiver interfaces** *{IF_NMLPORTS}*

Syntax	**show fiber-transceiver interfaces** *{IF_NMLPORTS}*
Parameter	**interfaces***{IF_NMLPORTS}* Display the o diagnostic information of the fiber transceiver for an interface ID or a list of interface IDs
Mode	Privileged EXEC
Example	The following example shows the diagnostic information for the interface SFP inserted. Switch# **show fiber-transceiver interfaces TenGigabitEthernet 1-4** 

```
Switch# show fiber-transceiver interfaces TenGigabitEthernet 1-4
 Port    | Temperature  | Voltage      | Current      | Output power | Input power | OE-Present | LOS
         | [C]          | [Volt]       | [mA]         | [mWatt]      | [mWatt]     |            |
=============================================================================================
  te1    | 48.50  (OK)  | 3.31  (OK)   | 16.87  (OK)  | 0.25  (OK)   | 0.00  (E)   | Insert     | Loss
  te2    | 23.68  (OK)  | 3.41  (OK)   | 6.97   (OK)  | 0.63  (OK)   | 0.00  (E)   | Insert     | Loss
  te3    | 19.79  (OK)  | 3.31  (OK)   | 28.99  (OK)  | 0.25  (OK)   | 0.33  (OK)  | Insert     | Normal
  te4    |  N/S         |  N/S         |  N/S         |  N/S         |  N/S        | Remove  | Loss

 Temp         - Internally measured transceiver temperature
 Voltage      - Internally measured supply voltage
 Current      - Measured TX bias current
 Output Power - Measured TX output power in milliWatts
 Input Power  - Measured RX received power in milliWatts
 OE-Present   - SFP Presetn or Not Present
 LOS          - Loss of signal
 N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6. DHCP (Dynamic Host Configuration Protocol)

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. Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring IP address, gateways, and other IP related things automatically to connected hosts. You can customize the DHCP pool subnet and address range to provide simultaneous access to a greater number of clients.

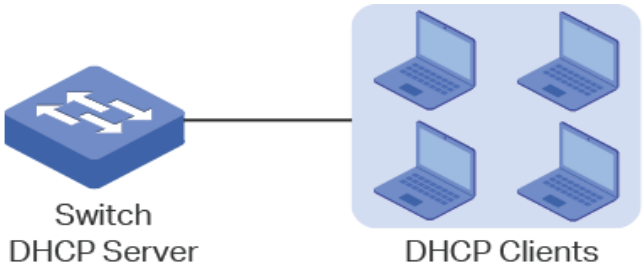


Fig 6.1 E3000 Series Switches DHCP server

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.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

DHCP Option 82

DHCP 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. DHCP provides a relay mechanism for sending information about its DHCP clients or the relay agent itself to the DHCP server. Also known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.

DHCP Snooping must be enabled for Option 82 information to be inserted into request packets. When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information may specify the MAC address or IP address of the requesting device (that is, the switch in this context). By default, the switch also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the port and VLAN ID. This allows DHCP client-server exchange messages to be forwarded between the server and client without having to flood them to the entire VLAN. If DHCP Snooping Information Option 82 is enabled on the switch, information may be inserted into a DHCP request packet received over any VLAN (depending on DHCP snooping filtering rules). The information inserted into the relayed packets includes the circuit-id and remote-id, as well as the gateway Internet address. When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

replace it with the switch's relay information. DHCP Snooping Information Option 82 and DHCP Relay Information Option 82 cannot both be enabled at the same time.

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. The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping (or using the static bindings configured with IP Source Guard). DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

DHCP Snooping Process

Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or fire wall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped. Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier. The rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped. When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

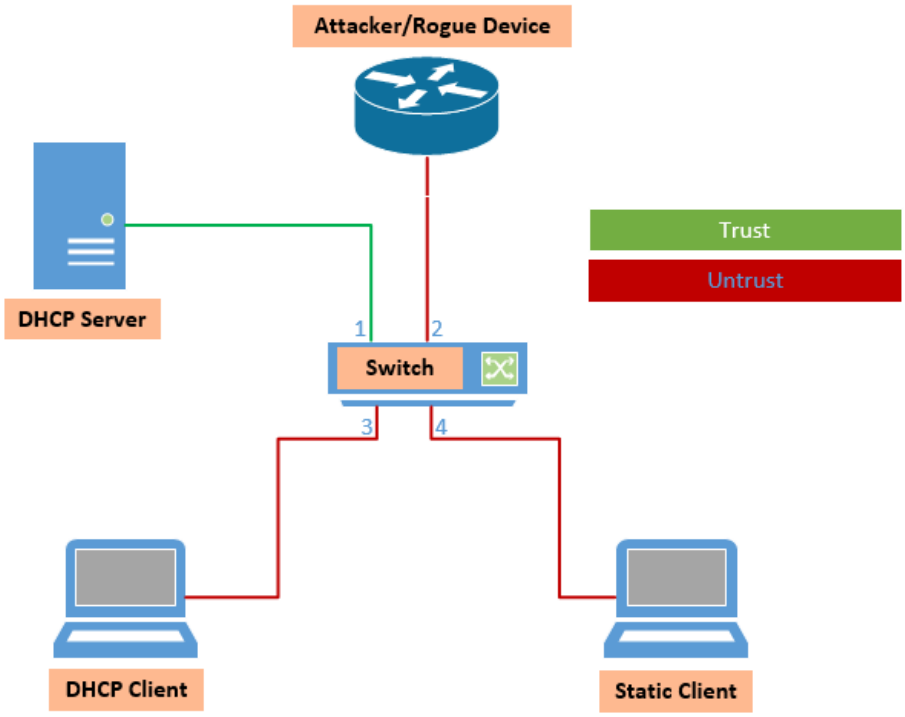


Fig 6.2 E3000 Series Switches DHCP Snooping

DHCP snooping causes a switch to examine DHCP messages and filter those considered to be inappropriate. DHCP snooping also builds a table of IP address and port mappings, based on legitimate DHCP messages, called the DHCP snooping binding table. The DHCP snooping binding table can then be used by DAI and by the IP Source Guard feature. Use DHCP snooping and IP Source Guard to prevent DHCP DoS and man-in-the-middle attacks. 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. 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. 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.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

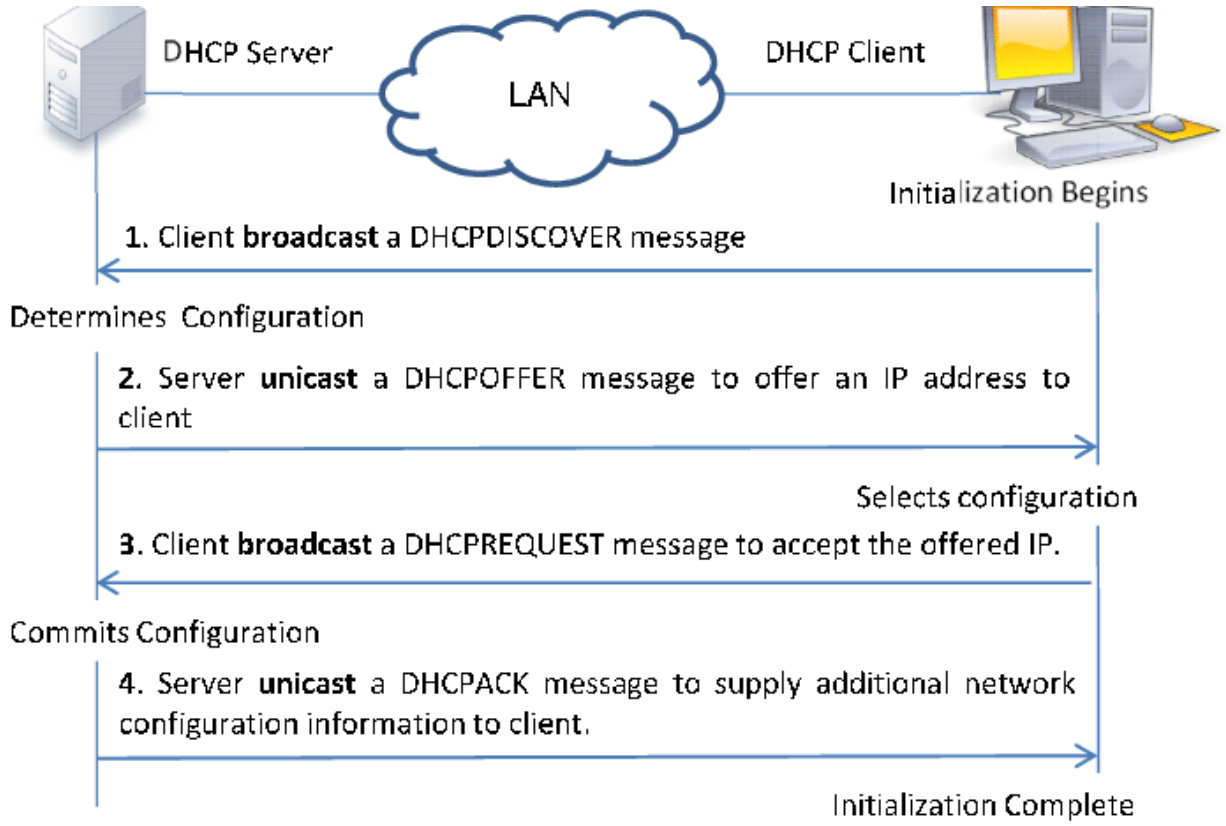


Fig 6.3 DHCP Messages

DHCP snooping defeats attacks for ports it considers to be untrusted. DHCP snooping allows all DHCP messages on trusted ports, but it filters DHCP messages on untrusted ports. It operates based on the premise that only DHCP clients should exist on untrusted ports; as a result, the switch filters incoming DHCP messages those are only sent by servers. So, from a design perspective, unused and unsecured user ports would be configured as untrusted to DHCP snooping. DHCP snooping also needs to examine the DHCP client messages on untrusted ports, because other attacks can be made using DHCP client messages. DHCP servers identify clients based on their stated client hardware address as listed in the DHCP request. A single device could pose as multiple devices by sending repeated DHCP requests, each with a different DHCP client hardware address. The legitimate DHCP server, thinking the requests are from different hosts, assigns an IP address for each request. The DHCP server will soon assign all IP addresses available for the subnet, preventing legitimate users from being

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

assigned an address. For untrusted ports, DHCP snooping uses the following general logic for filtering the packets:

1. It filters all messages sent exclusively by DHCP servers.
2. The switch checks DHCP *release* and *decline* messages against the DHCP snooping binding table; if the IP address in those messages is not listed with the port in the DHCP snooping binding table, the messages are filtered.
3. Optionally, it compares a DHCP request's client hardware address value with the source MAC address inside the Ethernet frame.

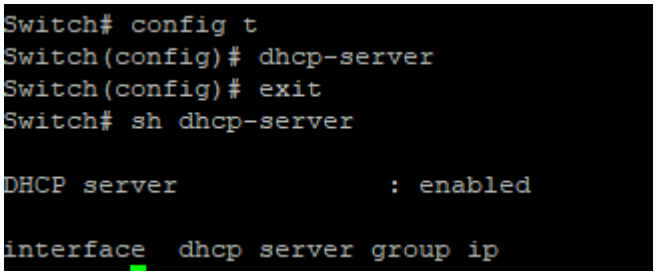
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.1 DHCP Server

Use the dhcp-server command to enable DHCP Server function. Use the **"no"** form of this command to disable.

Switch#**configure terminal**
Switch(config)#**dhcp-server**

Switch(config)# **no dhcp-server**

Syntax	**dhcp-server** **no dhcp-server**
Default	DHCP server is disabled
Mode	Global Configuration
Example	The example shows how to enable DHCP Server. You can verify settings by the following **show dhcp-server** command. Switch#configure terminal Switch(config)#**dhcp-server** Switch# **show dhcp-server** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.2 DHCP Port setting

Use the dhcp-relay command to enable DHCP relay on Switch port. Enabling port to carry DHCP information. Use the **"no"** form of this command to disable.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-Id}
Switch(config-if)#**dhcp-relay**

Switch(config-if)# **no dhcp-relay**

Syntax	**dhcp-relay** **no dhcp-relay**
Default	DHCP relay on port is disabled
Mode	Interface Configuration

Example	The example shows how to port to carry DHCP information.
	You can verify settings by the following **show run** command.
	Switch#**configure terminal**
	Switch(config)#**interface range** g1-24
	Switch(config-if-range)#**dhcp-relay**
	`Switch# config t`
	`Switch(config)# int range g1-24`
	`Switch(config-if-range)# dhcp-relay`
	Switch#**show run**
	`interface gi3`
	`  dhcp-relay`
	`!`
	`interface gi4`
	`  dhcp-relay`
	`!`
	`interface gi5`
	`  dhcp-relay`
	`!`
	`interface gi6`
	`  dhcp-relay`
	`!`
	`interface gi7`
	`  dhcp-relay`
	`!`
	`interface gi8`
	`  dhcp-relay`
	`!`
	`interface gi9`
	`  dhcp-relay`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.3 DHCP IP Pool Setting

Use the **ip pool** command to create DHCP Pool. Use the **"no"** form of this command to disable.

Switch#**configure terminal**
Switch(config)# **ip pool** *{Pool-Name}*
Switch(config-ip-pool-Pool-Name)# **gateway** *{Gateway-IP-address}*
Switch(config-ip-pool-Pool-Name)# **dns primary-ip** *{Primary DNS-IP-address}*
Switch(config-ip-pool-Pool-Name)# **dns second-ip** *{Secondary DNS-IP-address}*
Switch(config-ip-pool-Pool-Name)# **lease** *{Lease time}*
Switch(config-ip-pool-Pool-Name)# **section** *{Section-Number} {Pool Starting-IP-address} {Pool End-IP-address}*

Switch(config)# **no ip pool** *{Pool-Name}*

Syntax	**ip pool** **no ip pool**
Default	DHCP pool is disabled
Mode	Global Configuration

Example	The example shows how to create DHCP Pool.
	You can verify settings by the following **show run** command.
	Switch#**configure terminal**
	Switch(config)# **ip pool** COMMANDO
	Switch(config-ip-pool-COMMANDO)# **gateway** 192.168.0.1/24
	Switch(config-ip-pool-COMMANDO)# **dns primary-ip** 8.8.8.8
	Switch(config-ip-pool-COMMANDO)# **dns second-ip** 8.8.4.4
	Switch(config-ip-pool-COMMANDO)# **lease** 2:0:0
	Switch(config-ip-pool-COMMANDO)# **section** **1** 192.168.0.101 192.168.0.200
	`Switch# config t`
	`Switch(config)# ip pool COMMANDO`
	`Switch(config-ip-pool-COMMANDO)# gateway 192.168.0.1/24`
	`Switch(config-ip-pool-COMMANDO)# dns primary-ip 8.8.8.8`
	`Switch(config-ip-pool-COMMANDO)# dns second-ip 8.8.4.4`
	`Switch(config-ip-pool-COMMANDO)# lease 2:0:0`
	`Switch(config-ip-pool-COMMANDO)# section 1 192.168.0.101 192.168.0.200`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.4 DHCP VLAN Interface Group setting

Use the **dhcp-server group** command to enable VLAN Interface Group setting. Enabling Vlan carry DHCP information. Use the **"no"** form of this command to disable. Following commands are for Management Vlan. By default, VLAN 1 is a Management Vlan in E3000 Series Switches.

Switch#**configure terminal**

Switch(config)#**dhcp-server group** *{Group-ID}*

Switch(config)#**dhcp-server group** *{Group-ID}* **ip** *{Gateway-IP Address}*

Switch(config)# **no dhcp-server group** *{Group-ID}*

Following commands are for Non-Management VLAN
Switch#**configure terminal**

Switch(config)#**interface vlan{Vlan-ID}**

Switch(config-if)#**dhcp-server group** *{Group-ID}*

Switch(config)#**dhcp-server group** *{Group-ID}* **ip** *{Gateway-IP Address}*

Switch(config-if)#**no dhcp-server group** *{Group-ID}*

Syntax	**dhcp-server group** **no dhcp-server group**
Default	DHCP VLAN Interface Group setting is disabled
Mode	In Global configuration for Management VLAN. VLAN Interface Configuration for other than management VLAN.
Example	The example shows how to set DHCP VLAN Interface Group setting for Management VLAN . You can verify settings by the following **show run** command. Switch#**configure terminal**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Switch(config)# dhcp-server group 1
Switch(config)# dhcp-server group 1 ip 192.168.0.1

```
Switch# config t
Switch(config)# dhcp-server group 1
Switch(config)# dhcp-server group 1 ip 192.168.0.1
```

The example shows how to set DHCP VLAN Interface Group setting for other than management VLAN.
Switch#configure terminal
Switch(config)#interface vlan2

Switch(config-if)# dhcp-server group 1

Switch(config)# dhcp-server group 1 ip 192.168.0.1

```
Switch# config t
Switch(config)# interface vlan2
Switch(config-if)# dhcp-server group 2
```

Verifying the DHCP Server
Switch# sh dhcp-server

```
Switch# sh dhcp-server

DHCP server              : enabled
DHCP server group 1 ip : 192.168.0.1

interface  dhcp server group ip
 interface vlan 1 server group  :  1,
```

Verifying the DHCP Client

Switch# show dhcp-client
Note: Only Static binded clients are shown.

```
Switch# sh dhcp-client

dhcp-client bind table info:
     MAC Address            ipAddress       VlanId      UserName
  -----------------    -----------------    -------    ----------
  28:D2:44:0A:7E:9C    192.168.0.10         1       COMMANDO

Total 1 entry.
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.5 IP DHCP SNOOPING

Use the ip dhcp snooping command to enable DHCP Snooping function. Use the **"no"** form of this command to disable.

Switch#**configure terminal**
Switch(config)# **ip dhcp snooping**

Switch(config)# **no ip dhcp snooping**

Syntax	**ip dhcp snooping** **no ip dhcp snooping**
Default	DHCP snooping is disabled
Mode	Global Configuration

Example	The example shows how to enable DHCP Snooping on VLAN 1. You can verify settings by the following show ip dhcp snooping command.
	Switch#**configure terminal**
	Switch(config)# **ip dhcp snooping**
	Switch(config)# **ip dhcp snooping vlan 1**
	Switch# **show ip dhcp snooping**
	`Switch# configure`
	`Switch(config)# ip dhcp snooping`
	`Switch(config)# ip dhcp snooping vlan 1`
	`Switch(config)# exit`
	`Switch# show ip dhcp snooping`
	
	`DHCP Snooping : enabled`
	`Enable on following Vlans : 1`
	`circuit-id default format: vlan-port`
	`remote-id: : 00:e0:4c:00:00:00 (Switch Mac in Byte Order)`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.6 IP DHCP SNOOPING VLAN

Use the **ip dhcp snooping vlan** command to enable VLANs on DHCP Snooping function. Use the **"no"** form of this command to disable VLANs on DHCP Snooping function.

Switch#**configure terminal**
Switch(config)# **ip dhcp snooping vlan** *{VLAN-LIST}*

Syntax	**ip dhcp snooping vlan** *{VLAN-LIST}*
Parameter	*VLAN-LIST* Specify VLAN ID or a range of VLANs to enable or disable dynamic Arp inspection
Default	Default is disabled on all VLANs
Mode	Global Configuration

Example	The example shows how to enable VLAN 1-100 on DHCP Snooping, and then disable VLAN 30-40 on DHCP Snooping. You can verify settings by the following show ip dhcp snooping command.
	Example 1:
	Switch#**configure terminal**
	Switch(config)# **vlan** 1-100
	Switch(config)# **exit**
	Switch(config)# **ip dhcp snooping**
	Switch(config)# **ip dhcp snooping vlan** 1-100
	
	Switch# **show ip dhcp snooping**
	`Switch(config)# vlan 1-100`
	`Switch(config-vlan)# exit`
	`Switch(config)# ip dhcp snooping`
	`Switch(config)# ip dhcp snooping vlan 1-100`
	`Switch(config)# exit`
	`Switch# show ip dhcp snooping`
	
	`DHCP Snooping : enabled`
	`Enable on following Vlans : 1-100`
	`circuit-id default format: vlan-port`
	`remote-id: : 00:e0:4c:00:00:00 (Switch Mac in Byte Order)`
	
	Example 2:
	Switch#**configure terminal**
	Switch(config)# **no ip dhcp snooping vlan** 30-40

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch(config)# **show ip dhcp snooping**
	`Switch(config)# no ip dhcp snooping vlan 30-40`
	`Switch(config)# exit`
	`Switch# show ip dhcp snooping`
	
	`DHCP Snooping : enabled`
	`Enable on following Vlans : 1-29,41-100`
	`circuit-id default format: vlan-port`
	`remote-id: : 00:e0:4c:00:00:00 (Switch Mac in Byte Order)`

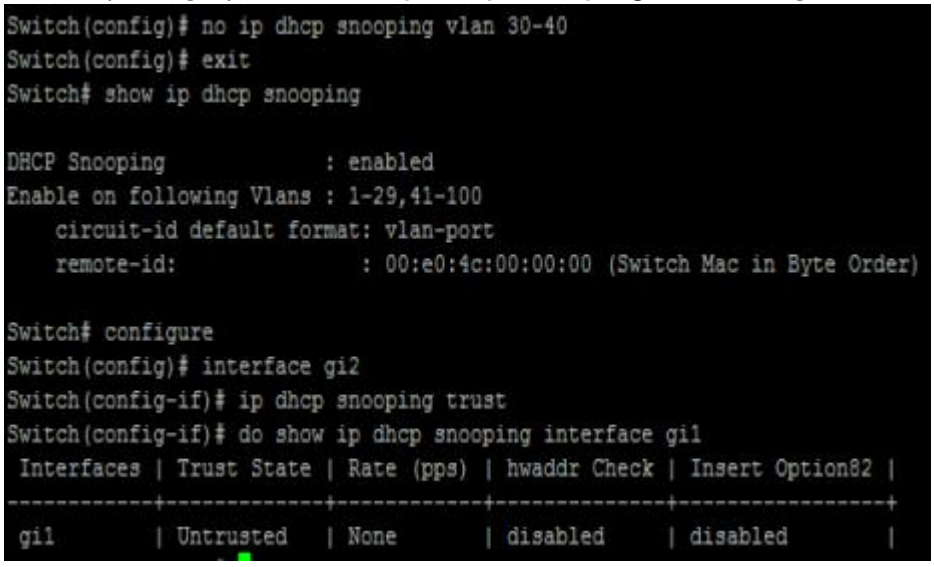
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.7 IP DHCP SNOOPING TRUST

Use the **ip dhcp snooping trust** command to set trusted interface. The switch does not check DHCP packets that are received on the trusted interface; it simply forwards it. Use the **"no"** form of this command to set untrusted interface.

Switch#**configure terminal**
Switch(config)# **ip dhcp snooping trust**

Switch(config)# **no ip dhcp snooping trust**

Syntax	**ip dhcp snooping trust** **no ip dhcp snooping trust**
Default	DHCP snooping trust is disabled
Mode	Interface Configuration
Example	The example shows how to set interface gi1 to trust. You can verify settings by the following show ip dhcp snooping interface command. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **ip dhcp snooping trust** Switch(config-if)# **do show ip dhcp snooping interface** gi1 

```
Switch(config)# no ip dhcp snooping vlan 30-40
Switch(config)# exit
Switch# show ip dhcp snooping

DHCP Snooping             : enabled
Enable on following Vlans : 1-29,41-100
    circuit-id default format: vlan-port
    remote-id:              : 00:e0:4c:00:00:00 (Switch Mac in Byte Order)

Switch# configure
Switch(config)# interface gi2
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# do show ip dhcp snooping interface gi1
 Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
------------+-------------+------------+--------------+-----------------+
 gi1        | Untrusted   | None       | disabled     | disabled        |
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.8 IP DHCP SNOOPING VERIFY

Use the **ip dhcp snooping verify** command to verify MAC address function on interface. The **"mac-address"** drop DHCP packets that address and ethernet source mac is not match.

Switch#**configure terminal**
Switch(config)#**interface** *{Interface-ID}*
Switch(config-if)# **ip dhcp snooping verify mac-address**
Switch(config-if)# **no ip dhcp snooping verify mac-address**

Syntax	**ip dhcp snooping verify mac-address** **no ip dhcp snooping verify mac-address**
Default	DHCP snooping verify mac-address is disabled
Mode	Interface Configuration

Example	The example shows how to set interface gi1 to validate **"mac- address"**. You can verify settings by the following show ip dhcp snooping interface command.
	Switch#**configure terminal**
	Switch(config)# **interface** gi2
	Switch(config-if)# **ip dhcp snooping verify mac-address**
	Switch(config-if)# **do show ip dhcp snooping interface** gi2
	`Switch(config)# interface gi2`
	`Switch(config-if)# ip dhcp snooping verify mac-address`
	`Switch(config-if)# do show ip dhcp snooping interface gi2`
	`Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |`
	`gi2 | Trusted | None | enabled | disabled |`

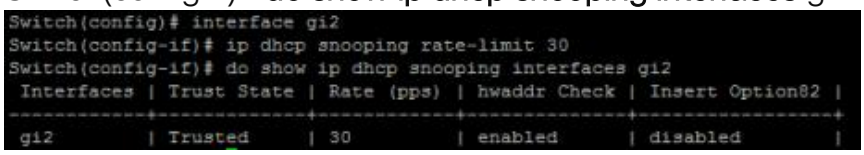
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.9 IP DHCP SNOOPING RATE-LIMIT

Use the **ip dhcp snooping rate-limit** command to set rate limitation on interface. The switch drop DHCP packets after receives more than configured rate of packets per second. Use the **"no"** form of this command to return to default settings.

Switch#**configure terminal**
Switch(config)#**interface** *{Interface-ID}*
Switch(config-if)# **ip dhcp snooping rate-limit** *<1-300>*

Switch(config-if)# **no ip dhcp snooping rate-limit**

Syntax	**ip dhcp snooping rate-limit** *<1-300>* **no ip dhcp snooping rate-limit**
Parameter	*<1-300>* Set 1 to 300 PPS of DHCP packet rate limitation
Default	Default is un-limited of DHCP packet
Mode	Interface Configuration
Example	The example shows how to set rate limit to 30 pps on interface gi1. You can verify settings by the following show ip dhcp snooping interface command. Switch#configure terminal Switch(config)# **interface** gi2 Switch(config-if)# **ip dhcp snooping rate-limit** 30 Switch(config-if)# **do show ip dhcp snooping interfaces** gi2 

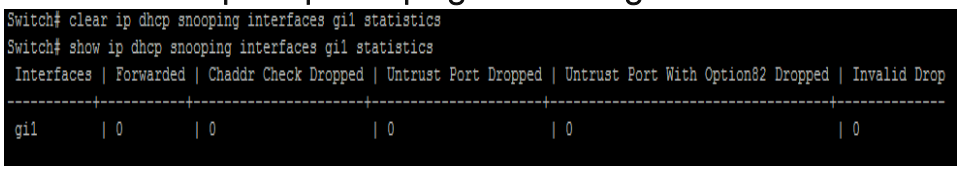
```
Switch(config)# interface gi2
Switch(config-if)# ip dhcp snooping rate-limit 30
Switch(config-if)# do show ip dhcp snooping interfaces gi2
 Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
------------+-------------+------------+--------------+-----------------+
 gi2        | Trusted     | 30         | enabled      | disabled        |
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.10 CLEAR IP DHCP SNOOPING STATISTICS

Use the **clear ip dhcp snooping interfaces statistics** command to clear statistics that are recorded on interface.

Switch# **clear ip dhcp snooping interfaces** *{IF_PORTS}* **statistics**

Syntax	**clear ip dhcp snooping interfaces** *{IF_PORTS}***statistics**
Parameter	*IF_PORTS* specifies ports to clear statistics
Mode	Privileged EXEC
Example	The example shows how to clear statistics on interface gi1. You can verify settings by the following show ip DHCP Snooping interface statistics command. Switch# **clear ip dhcp snooping interfaces gi1 statistics** Switch# **show ip dhcp snooping interfaces gi1 statistics** 

```
Switch# clear ip dhcp snooping interfaces gi1 statistics
Switch# show ip dhcp snooping interfaces gi1 statistics
 Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped | Untrust Port With Option82 Dropped | Invalid Drop
------------+-----------+----------------------+----------------------+------------------------------------+--------------
 gi1        | 0         | 0                    | 0                    | 0                                  | 0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.11 SHOW IP DHCP SNOOPING

Use the show IP DHCP snooping command to show settings of DHCP Snooping.

Switch#**show ip dhcp snooping**

Syntax	**show ip dhcp snooping**
Mode	Privileged EXEC

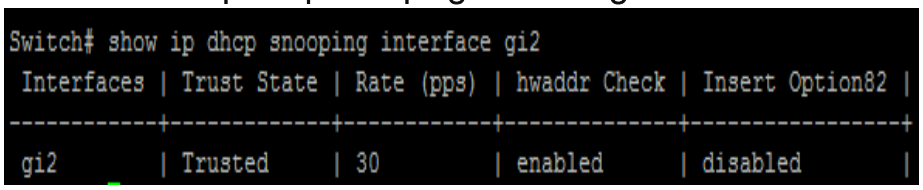
Example	The example shows how to show settings of DHCP Snooping
	Switch# **show ip dhcp snooping**
	`Switch# show ip dhcp snooping`
	
	`DHCP Snooping : enabled`
	`Enable on following Vlans : 1-29,41-100`
	`circuit-id default format: vlan-port`
	`remote-id: : 00:e0:4c:00:00:00 (Switch Mac in Byte Order)`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.12 SHOW IP DHCP SNOOPING INTERFACE

Use the show ip dhcp snooping interfaces command to show settings or statistics of interface.

Switch# **show ip dhcp snooping interfaces** *{IF_PORTS}*
Switch# **show ip dhcp snooping interfaces** *{IF_PORTS}* **statistics**

Syntax	**show ip dhcp snooping interfaces** *{IF_PORTS}* **show ip dhcp snooping interfaces** *{IF_PORTS}* **statistics**
Parameter	*IF_PORTS* specifies ports to show statistics
Mode	Privileged EXEC
Example	The example shows how to show settings of interface gi1. Switch# **show ip dhcp snooping interface gi2** 

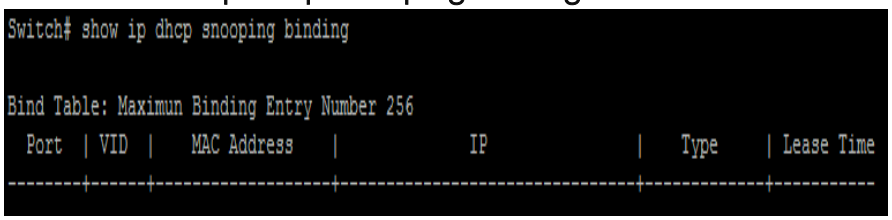
```
Switch# show ip dhcp snooping interface gi2
 Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
------------+-------------+------------+--------------+-----------------+
 gi2        | Trusted     | 30         | enabled      | disabled        |
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.13 SHOW IP DHCP SNOOPING BINDING

Use the **show ip dhcp snooping binding** command to show binding entries that learned by DHCP Snooping.

Switch# **show ip dhcp snooping binding**

Syntax	**show ip dhcp snooping binding**
Mode	Privileged EXEC
Example	The example shows how to show binding entries that learned by DHCP Snooping. Switch# **show ip dhcp snooping binding** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.14 IP DHCP SNOOPING OPTION

Use the **ip dhcp snooping option** command to enable that insert option82 content into packet. Use the **"no"** form of this command to disable.

Switch#**configure terminal**
Switch(config)#**interface** *{Interface-ID}*
Switch(config-if)# **ip dhcp snooping option**

Switch(config-if)# **no ip dhcp snooping option**

Syntax	**ip dhcp snooping option** **no ip dhcp snooping option**
Default	DHCP snooping option82 is disabled
Mode	Interface Configuration

Example	The example shows how to enable option82 insertion. You can verify settings by the following show ip dhcp snooping interface command.
	Switch#**configure terminal**
	Switch(config)# **interface** gi2
	Switch(config-if)# **ip dhcp snooping option**
	Switch(config-if)# **do show ip dhcp snooping interfaces gi2**
	`Switch(config)# interface gi2`
	`Switch(config-if)# ip dhcp snooping option`
	`Switch(config-if)# do show ip dhcp snooping interfaces gi2`
	`Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |`
	`gi2 | Trusted | 30 | enabled | enabled |`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.15 IP DHCP SNOOPING OPTION ACTION

Use the **ip dhcp snooping option action** command to set the action when receive packets that with option82 content. Use the **"no"** form of this command to default setting.

Switch#**configure terminal**
Switch(config)#**interface** *{Interface-ID}*
Switch(config-if)#**ip dhcp snooping option action (drop|keep|replace)**

Switch(config-if)#**no ip dhcp snooping option action**

Syntax	**ip dhcp snooping option action (drop|keep|replace)** **no ip dhcp snooping option action**
Parameter	**Drop** Drop packets with option82 that are received from untrusted port. **Keep** Keep original option82 content in packet. **Replace** Replace option82 content by switch setting.
Default	DHCP snooping option82 is drop
Mode	Interface Configuration

Example	The example shows how to set action to replace option82 content. You can verify settings by the following show running-config command.
	Switch#**configure terminal**
	switch(config)# **interface gi2**
	switch(config-if)# **ip dhcp snooping option action replace**
	`Switch(config)# interface gi2`
	`Switch(config-if)# ip dhcp snooping option action replace`
	`Switch(config-if)# do show ip dhcp snooping interfaces gi2`
	`Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |`
	`gi2 | Trusted | 30 | enabled | enabled |`

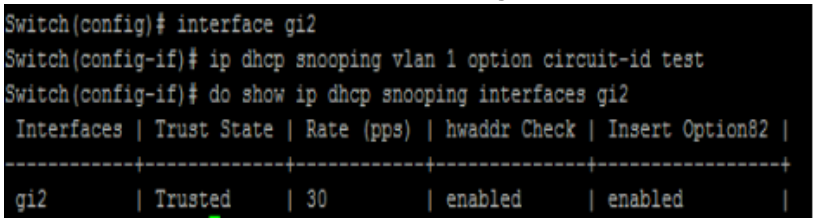
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.16 IP DHCP SNOOPING OPTION CIRCUIT-ID

Use the **ip dhcp snooping option circuit-id** command to set user-defined circuit-id string. Circuit-id is per port per VLAN setting. If a VLAN is not found user-defined circuit-id then use per port circuit-id string. Use the **"no"** form of this command to default setting.

Switch#**configure terminal**
Switch(config-if)# **ip dhcp snooping [vlan** *<1-4094>*] **option circuit-id** *{STRING}*

Switch(config-if)# **no ip dhcp snooping [vlan** *<1-4094>*] **option circuit-id**

Syntax	**ip dhcp snooping [vlan** *<1-4094>*] **option circuit-id** *STRING* **no ip dhcp snooping [vlan** *<1-4094>*] **option circuit-id**
Parameter	**Vlan***<1-4094>*VLAN ID to set user defined circuit-id string **STRING** Circuit-id string, 1 to 63 ASCII characters, no spaces.
Default	Default circuit-id is port id + vlan id in byte format.
Mode	Interface Configuration
Example	The example shows how to set a user-defined circuit-id string on interface gi1 and VLAN 1. You can verify settings by the following show running-config command. Switch#**configure terminal** switch(config)# **interface** gi2 switch(config-if)# **ip dhcp snooping vlan** 1 **option circuit-id** test 

```
Switch(config)# interface gi2
Switch(config-if)# ip dhcp snooping vlan 1 option circuit-id test
Switch(config-if)# do show ip dhcp snooping interfaces gi2
 Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
------------+-------------+------------+--------------+-----------------+
 gi2        | Trusted     | 30         | enabled      | enabled         |
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.17 IP DHCP SNOOPING OPTION REMOTE-ID

Use the **ip dhcp snooping option remote-id** command to set user-defined remote-id string. Remote-id is a global and unique string. Use the **"no"** form of this command to default setting.

Switch#**configure terminal**
Switch(config)# **ip dhcp snooping option remote-id** *{STRING}*

Switch(config)# **no ip dhcp snooping option remote-id**

Syntax	**ip dhcp snooping option remote-id** *{STRING}* **no ip dhcp snooping option remote-id**
Parameter	*STRING* Remote-id string, 1 to 63 ASCII characters, no spaces.
Default	Default remote-id is the switch MAC address in byte order
Mode	Global Configuration

Example	The example shows how to set a user-defined remote-id string on switch. You can verify settings by the following show ip dhcp snooping option remote- id.
	Switch#**configure terminal**
	Switch(config)# **ip dhcp snooping option remote-id test_remote**
	switch(config)# **do show ip dhcp snooping option remote-id**
	`Switch(config)# ip dhcp snooping option remote-id test_remote`
	`Switch(config)# do show ip dhcp snooping option remote-id`
	`Remote ID: test_remote`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.18 SHOW IP DHCP SNOOPING OPTION

Use the **show ip dhcp snooping option** remote-id command to show remote-id string.

Switch#**show ip dhcp snooping option remote-id**

Syntax	**show ip dhcp snooping option remote-id**
Mode	Privileged EXEC

Example	The example shows how to show remote-id string
	Switch# **show ip dhcp snooping option remote-id**
	`Switch# config t`
	`Switch(config)# ip dhcp snooping  option remote-id COMMANDO`
	`Switch(config)#`
	`Switch# show ip dhcp snooping option remote-id`
	`Remote ID: COMMANDO`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.19 IP DHCP SNOOPING DATABASE

Use the **ip dhcp snooping database** command to enable DHCP Snooping database agent. The "**flash**" means that write backup file to switch local drive. The **"tftp"** means that write backup file to remote TFTP server. Use the **"no"** form of this command to disable.

Switch#**configure terminal**
Switch(config)# **ip dhcp snooping database flash**
Switch(config)# **ip dhcp snooping database tftp (**A.B.C.D|HOSTNAME**)** *{NAME}*

Switch(config)# **no ip dhcp snooping database**

Syntax	**ip dhcp snooping database flash** **ip dhcp snooping database tftp (A.B.C.D|HOSTNAME)** *{NAME}* **no ip dhcp snooping database**
Parameter	(A.B.C.D|HOSTNAME)Specify the IP address or hostname of remote TFTP server *NAME* Input name of backup file
Default	DHCP snooping database is disabled
Mode	Global Configuration
Example	The example shows how to enable DHCP Snooping database agent and write backup file to remote TFTP server with file name "backup_file". You can verify settings by the following show ip dhcp snooping database command. Switch#**configure terminal** Switch(config)# **ip dhcp snooping database tftp** 192.168.1.50 **backup_file** Switch(config)# **do show ip dhcp snooping database**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# ip dhcp snooping database tftp 192.168.1.50 backup_file
Switch(config)# do show ip dhcp snooping database

Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 295

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :     1
Successful Transfers :     0   Failed Transfers :     0
Successful Reads     :     0   Failed Reads     :     0
Successful Writes    :     0   Failed Writes    :     0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.20 IP DHCP SNOOPING DATABASE WRITE-DELAY

Use the **ip dhcp snooping database write-delay** command to modify the write-delay timer. Use the **"no"** form of this command to default setting.

Switch#**configure terminal**
Switch(config)# **ip dhcp snooping database write-delay***<15-86400>*

Switch(config)# **no ip dhcp snooping database write-delay**

Syntax	**ip dhcp snooping database write-delay***<15-86400>* **no ip dhcp snooping database write-delay**
Parameter	*<15-86400>*Specifies the seconds of timeout. Specify the duration for which the transfer should be delayed after the binding database changes
Default	DHCP snooping database write-delay is 300 seconds
Mode	Global Configuration
Example	The example shows how to set write-delay timer to 60 seconds. You can verify settings by the following show ip dhcp snooping database command. Switch#**configure terminal** Switch(config)# **ip dhcp snooping database write-delay** 60 Switch(config)# **do show ip dhcp snooping database**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# ip dhcp snooping database write-delay 60
Switch(config)# do show ip dhcp snooping database

Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 300 seconds

Agent Running : Running
Delay Timer Expiry : 60 seconds
Abort Timer Expiry : 86

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :     1
Successful Transfers :     0   Failed Transfers :     0
Successful Reads     :     0   Failed Reads     :     0
Successful Writes    :     0   Failed Writes    :     0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.21 IP DHCP SNOOPING DATABASE TIMEOUT

Use the **ip dhcp snooping database timeout** command to modify the timeout timer. Use the **"no"** form of this command to default setting.

Switch#**configure terminal**
Switch(config)# **ip dhcp snooping database timeout** *<0-86400>*

Switch(config)# **no ip dhcp snooping database timeout**

Syntax	**ip dhcp snooping database timeout** *<0-86400>* **no ip dhcp snooping database timeout**
Parameter	*<15-86400>*Specifies the seconds of timeout. Specify (in seconds)how long to wait for the database transfer process to finish before stopping the process. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely
Default	DHCP snooping database timeout is 300 seconds
Mode	Global Configuration
Example	The example shows how to set timeout timer to 60 seconds. You can verify settings by the following show ip dhcp snooping database command. Switch#**configure terminal** Switch(config)# **ip dhcp snooping database timeout 60** Switch(config)#**do show ip dhcp snooping**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# ip dhcp snooping database timeout 60
Switch(config)# do show ip dhcp snooping database

Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 60 seconds

Agent Running : Running
Delay Timer Expiry : 60 seconds
Abort Timer Expiry : 0

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :     1
Successful Transfers :     0   Failed Transfers :     0
Successful Reads     :     0   Failed Reads     :     0
Successful Writes    :     0   Failed Writes    :     0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.22 CLEAR IP DHCP SNOOPING DATABASE STATISTICS

Use the **clear ip dhcp snooping database statistics** command to clear statistics of DHCP Snooping database.

Switch# **clear ip dhcp snooping database statistics**

Syntax	**clear ip dhcp snooping database statistics**
Mode	Privileged EXEC

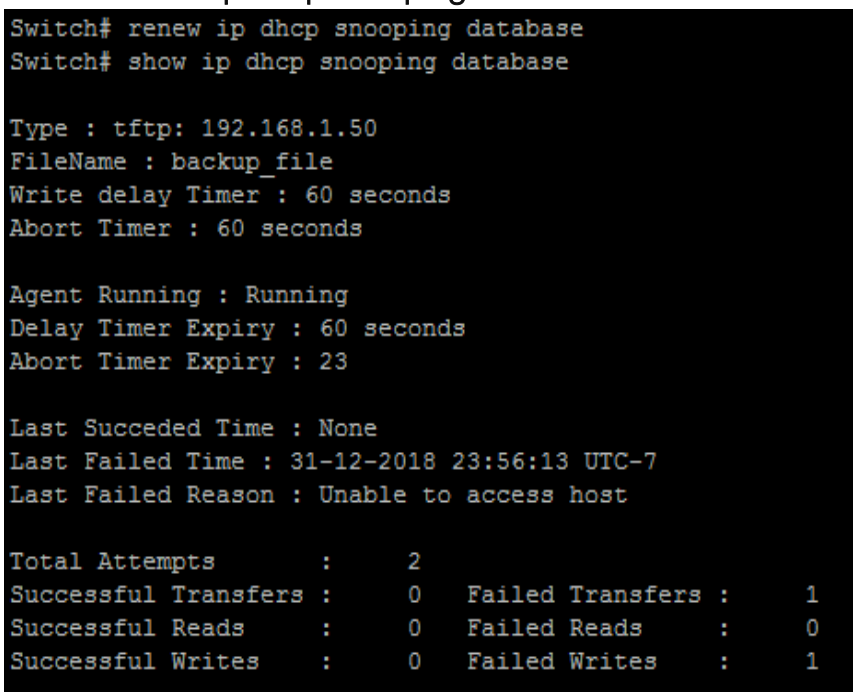
Example	The example shows how to clear statistics of DHCP Snooping agent. You can verify settings by the following show ip dhcp snooping database command.
	switch# **clear ip dhcp snooping database statistics**
	switch# **show ip dhcp snooping database**
	`Switch# clear ip dhcp snooping database statistics`
	`Switch# show ip dhcp snooping database`
	
	`Type : tftp: 192.168.1.50`
	`FileName : backup_file`
	`Write delay Timer : 60 seconds`
	`Abort Timer : 60 seconds`
	
	`Agent Running : None`
	`Delay Timer Expiry : Not Running`
	`Abort Timer Expiry :Not Running`
	
	`Last Succeded Time : None`
	`Last Failed Time : None`
	`Last Failed Reason :`
	
	`Total Attempts : 0`
	`Successful Transfers : 0 Failed Transfers : 0`
	`Successful Reads : 0 Failed Reads : 0`
	`Successful Writes : 0 Failed Writes : 0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.23 RENEW IP DHCP SNOOPING DATABASE

Use the **renew ip dhcp snooping database** command to renew DHCP Snooping database from backup file.

Switch# **renew ip dhcp snooping database**

Syntax	**renew ip dhcp snooping database**
Mode	Privileged EXEC
Example	The example shows how to renew DHCP Snooping database. You can verify settings by the following show ip dhcp snooping database and show ip dhcp snooping binding command. Switch# **renew ip dhcp snooping database** Switch# **show ip dhcp snooping database** 

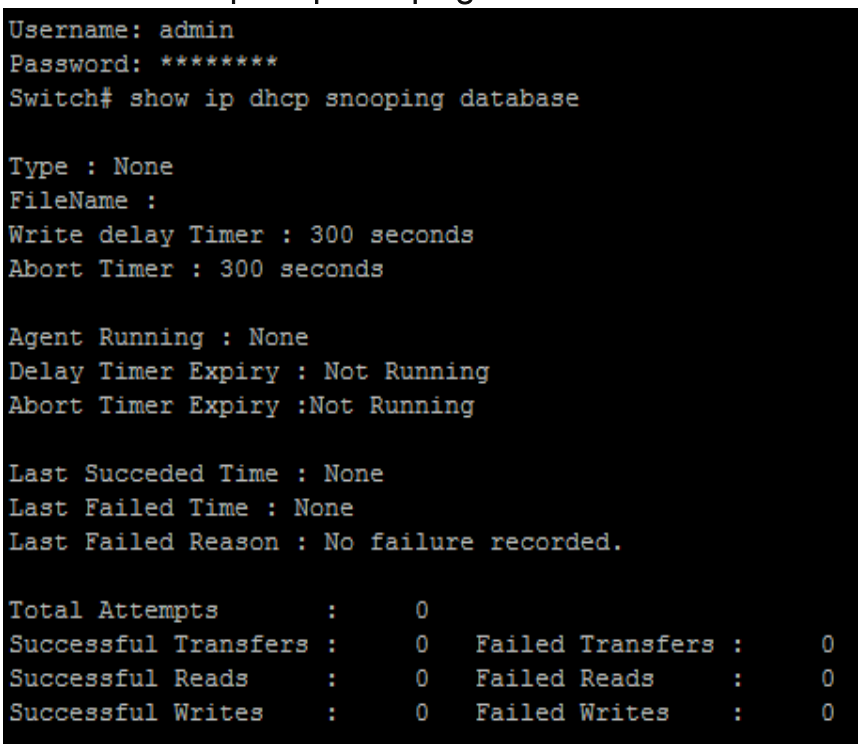
```
Switch# renew ip dhcp snooping database
Switch# show ip dhcp snooping database

Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 60 seconds

Agent Running : Running
Delay Timer Expiry : 60 seconds
Abort Timer Expiry : 23

Last Succeded Time : None
Last Failed Time : 31-12-2018 23:56:13 UTC-7
Last Failed Reason : Unable to access host

Total Attempts       :     2
Successful Transfers :     0   Failed Transfers :     1
Successful Reads     :     0   Failed Reads     :     0
Successful Writes    :     0   Failed Writes    :     1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

6.24 SHOW IP DHCP SNOOPING DATABASE

Use the **show ip dhcp snooping database** command to show settings of DHCP Snooping agent.

Switch# **show ip dhcp snooping database**

Syntax	**show ip dhcp snooping database**
Mode	Privileged EXEC
Example	The example shows how to show settings of DHCP Snooping agent. Switch # **show ip dhcp snooping database** 

```
Username: admin
Password: ********
Switch# show ip dhcp snooping database

Type : None
FileName :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : None
Delay Timer Expiry : Not Running
Abort Timer Expiry :Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :     0
Successful Transfers :     0   Failed Transfers :     0
Successful Reads     :     0   Failed Reads     :     0
Successful Writes    :     0   Failed Writes    :     0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

7. DOS Denial-of-Service (DoS)

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (ie. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- Buffer overflow attacks – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks.
- ICMP flood – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- SYN flood – sends a request to connect to a server, but never complete. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

Other DoS attacks simply exploit vulnerabilities that cause the target networks or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the network, so that it can't be accessed or used.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

7.1 DOS

To enable the specific Denial of Service (DoS) protection, use the command **dos** in the Global Configuration mode. Otherwise, use the no form of the command to disable the specific DoS protection.

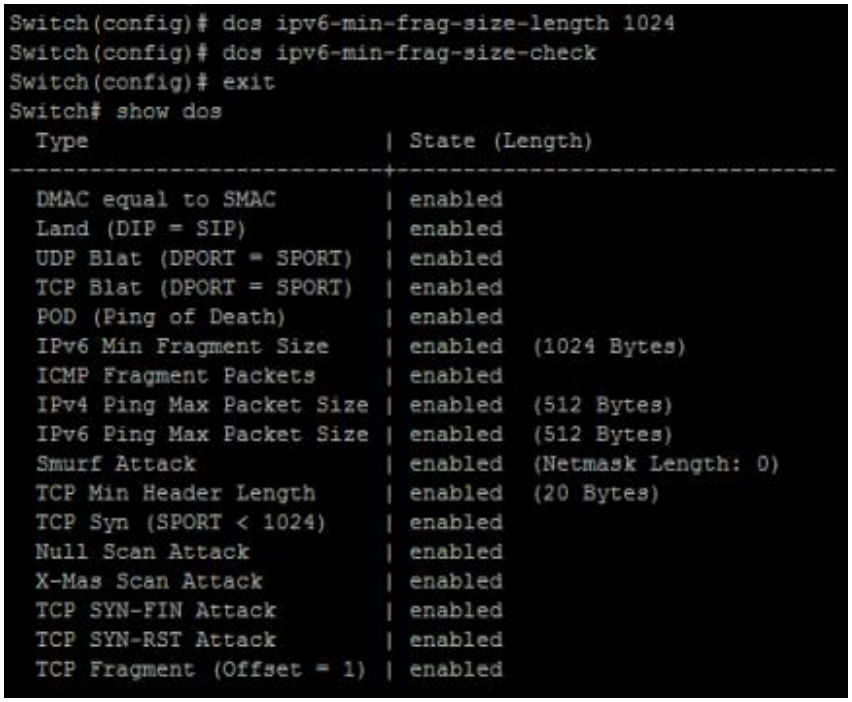
Switch#**configure terminal**
Switch(config)# **dos ipv6-min-frag-size-length 1024**
Switch(config)# **dos ipv6-min-frag-size-check**

Syntax	**dos (daeqsa-deny|icmp-frag-pkts-deny|icmpv4-ping-max-check |icmpv6-ping-max-check|ipv6-min-frag-size-check|land- deny|nullscan-deny|pod-deny|smurf-deny|syn-sportl1024-deny|synfin-deny|synrst-deny|tcp-frag-off-min-check|tcpblat-deny|tcphdr-min-check|udpblat-deny|xmas-deny)** **dos icmp-ping-max-length MAX_LEN** **dos ipv6-min-frag-size-length MIN_LEN** **dos smurf-netmask MASK** **dos tcphdr-min-length HDR_MIN_LEN** **no dos (tcp-frag-off-min-check|synrst-deny|synfin-deny|xma- deny |nullscan-deny|syn-sportl1024-deny|tcphdr-min-check|smurf-deny|icmpv6-ping-max-check|icmpv4-ping-max-check|icmp-frag- pkts-deny|ipv6-min-frag-size-check|pod-deny|tcpblat- deny|udpblat-deny|land-deny|daeqsa-deny)**
Parameter	**daeqsa-deny** Drops the packets if the destination MAC address is equal to the source MAC address. **icmp-frag-pkts-deny** Drops the fragmented ICMP packets. **icmpv4-ping-max-** check Checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size defined by the command dos icmp-ping-max-length MAX_LEN

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	icmpv6-ping-max- check Checks the maximum size of ICMPv6 ping packets and drops the packets larger than the maximum packet size defined by the command dos icmp-ping-max- length MAX_LEN. **ipv6-min-frag-** size-check Checks the minimum size of IPv6 fragments and drops the packets smaller than the minimum size defined by the command dos ipv6-min-frag-size-length MIN_LEN. **land-deny** Drops the packets if the source IP address is equal to the destination IP address. **nullscan-deny** Drops the packets with NULL scan. **pod-deny** Avoids ping of death attack. **smurf-deny** Avoids smurf attack. **syn-sportl1024-deny** Drops SYN packets with sport less than 1024. **synfin-deny** Drops the packets with SYN and FIN bits set. **synrst-deny** Drops the packets with SYN and RST bits set. **tcp-frag-off-min-** check Drops the TCP fragment packets with offset equals to one. **tcpblat-deny** Drops the packages if the TCP source port is equal to the TCP destination port. **tcphdr-min-check** Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size defined by the command dos tcphdr-min-length HDR_MIN_LEN. **udpblat-deny** Drops the packets if the UDP source port equals to the UDP destination port. **xmas-deny** Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set. **icmp-ping-max-** length MAX_LEN Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes. **ipv6-min-frag-** size-length MIN_LEN Specify the minimum size of IPv6 fragments. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes. **smurf-netmask** MASK Specify the netmask of smurf attack. The length range is from 0 to 323 bytes, and default length is 0 bytes. **tcphdr-min-length** HDR_MIN_LEN Specify the minimum TCP header length. The length range is from 0 to 31 bytes, and default length is 20 bytes.
Default	All of DoS protections are enabled by default. The default parameter

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	are: - The maximum size of ICMP ping packages is 512 bytes - The minimum size of IPv6 fragments is 1240 bytes. - The Smurf netmask length is 0 bytes. - The minimum TCP header length is 20 bytes
Mode	Global Configuration
Example	The following example sets the minimum fragment size to 1024 bytes and enables the minimum size of IPv6 fragments validation. Switch#**configure terminal** Switch(config)# **dos ipv6-min-frag-size-length** 1024 Switch(config)# **dos ipv6-min-frag-size-check** 

```
Switch(config)# dos ipv6-min-frag-size-length 1024
Switch(config)# dos ipv6-min-frag-size-check
Switch(config)# exit
Switch# show dos
  Type                       | State (Length)
-----------------------------+--------------------------------
  DMAC equal to SMAC         | enabled
  Land (DIP = SIP)           | enabled
  UDP Blat (DPORT = SPORT)   | enabled
  TCP Blat (DPORT = SPORT)   | enabled
  POD (Ping of Death)        | enabled
  IPv6 Min Fragment Size     | enabled  (1024 Bytes)
  ICMP Fragment Packets      | enabled
  IPv4 Ping Max Packet Size  | enabled  (512 Bytes)
  IPv6 Ping Max Packet Size  | enabled  (512 Bytes)
  Smurf Attack               | enabled  (Netmask Length: 0)
  TCP Min Header Length      | enabled  (20 Bytes)
  TCP Syn (SPORT < 1024)     | enabled
  Null Scan Attack           | enabled
  X-Mas Scan Attack          | enabled
  TCP SYN-FIN Attack         | enabled
  TCP SYN-RST Attack         | enabled
  TCP Fragment (Offset = 1)  | enabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

7.2 DOS (INTERFACE)

To enable the DoS on the specific interface, use the command **dos** in the Interface Configuration mode. Otherwise, use the **"no"** form of the command to disable the DoS on the interface.

Switch#**configure terminal**
Switch(config)# **interface** *{interface-ID}*
Switch(config-if)# **dos**

Switch(config-if)# **no dos**

Syntax	**dos** **no dos**
Default	DoS protection is disabled on each interface.
Mode	Interface Configuration
Example	The following example enables the DoS on the interface GigabitEthernet 2. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dos** `Switch(config)# interface GigabitEthernet 2` `Switch(config-if)# dos` `Switch(config-if)# exit` `Switch(config)# exit` `Switch# show dos interfaces GigabitEthernet 2` ` Port	DoS Protection` `----------+---------------` ` gi2	enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

7.3 SHOW DOS

To show the DoS protection configuration, use the command **show dos** in the Privileged EXEC mode. For the status of DoS protection on each interface, use the command show dos interface in the Privileged EXEC mode.

Switch# **show dos**
Switch# **show dos interface** *{IF_PORTS}*

Syntax	**show dos** **show dos interface** *{IF_PORTS}*
Parameter	**interface***{IF_PORTS}* An interface ID or the list of interface IDs
Mode	Privileged EXEC
Example	The following example shows the global DoS protection configuration. Switch# **show dos**

```
Switch# show dos
  Type                        | State (Length)
------------------------------+---------------------------------
  DMAC equal to SMAC          | enabled
  Land (DIP = SIP)            | enabled
  UDP Blat (DPORT = SPORT)    | enabled
  TCP Blat (DPORT = SPORT)    | enabled
  POD (Ping of Death)         | enabled
  IPv6 Min Fragment Size      | enabled  (1024 Bytes)
  ICMP Fragment Packets       | enabled
  IPv4 Ping Max Packet Size   | enabled  (512 Bytes)
  IPv6 Ping Max Packet Size   | enabled  (512 Bytes)
  Smurf Attack                | enabled  (Netmask Length: 0)
  TCP Min Header Length       | enabled  (20 Bytes)
  TCP Syn (SPORT < 1024)      | enabled
  Null Scan Attack            | enabled
  X-Mas Scan Attack           | enabled
  TCP SYN-FIN Attack          | enabled
  TCP SYN-RST Attack          | enabled
  TCP Fragment (Offset = 1)   | enabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

8. DYNAMIC ARP INSPECTION

A switch can use DAI (Dynamic ARP Inspection) to prevent certain types of attacks that leverage the use of IP ARP messages. DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

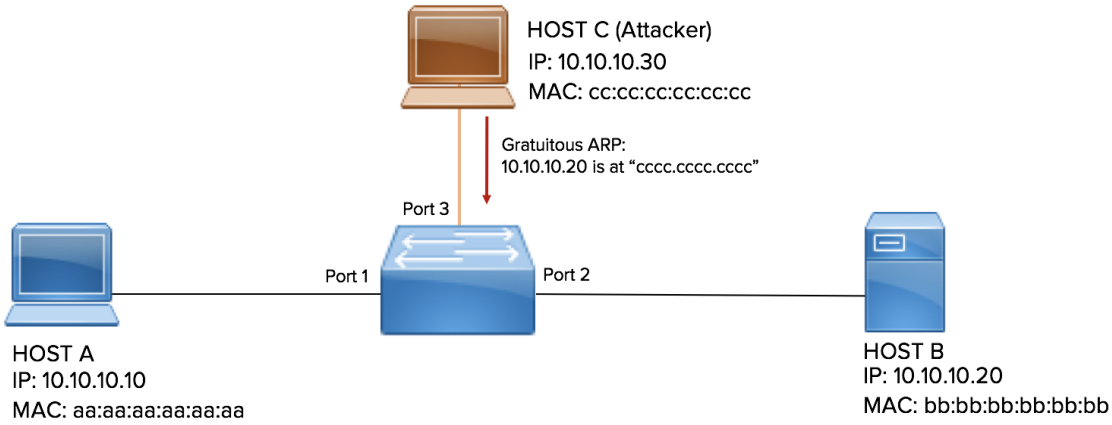


Fig 8.1 Dynamic ARP Inspection Setup

DAI ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination.
- Drops invalid ARP packets

DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid. DAI can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

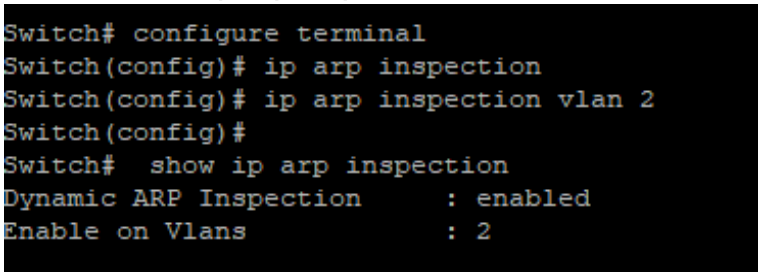
8.1 IP ARP INSPECTION

Use the **ip arp inspection** command to enable Dynamic Arp Inspection function. Use the **"no"** form of this command to disable.

Switch#**configure terminal**
Switch(config)#**ip arp inspection**

Switch(config)#**no ip arp inspection**

Syntax	**ip arp inspection** **no ip arp inspection**
Default	Dynamic Arp inspection is disabled
Mode	Global Configuration

Example	The example shows how to enable Dynamic Arp Inspection on VLAN 2. You can verify settings by the following show ip arp inspection command.
	Switch#**configure terminal**
	Switch(config)# **ip arp inspection**
	Switch(config)# **ip arp inspection vlan** 2
	
	switch# **show ip arp inspection**
	 
	`Switch# configure terminal`
	`Switch(config)# ip arp inspection`
	`Switch(config)# ip arp inspection vlan 2`
	`Switch(config)#`
	`Switch#  show ip arp inspection`
	`Dynamic ARP Inspection     : enabled`
	`Enable on Vlans            : 2`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

8.2 IP ARP INSPECTION VLAN

Use the **ip arp inspection vlan** command to enable VLANs on Dynamic Arp Inspection function. Use the **"no"** form of this command to disable VLANs on Dynamic Arp Inspection function.

Switch#**configure terminal**

Switch(config)# **ip arp inspection vlan** *{VLAN-LIST}*

Switch(config)# **no ip arp inspection vlan** *{VLAN-LIST}*

Syntax	**ip arp inspection vlan** *{VLAN-LIST}* **no ip arp inspection vlan** *{VLAN-LIST}*
Parameter	*VLAN-LIST*Specify VLAN ID or a range of VLANs to enable or disable dynamic Arp inspection
Default	Default is disabled on all VLANs
Mode	Global Configuration

Example	The example shows how to enable VLAN 1-100 on Dynamic Arp Inspection, and then disable VLAN 30-40 on Dynamic Arp Inspection. You can verify settings by the following show ip arp inspection command.
	Switch#**configure terminal**
	Switch(config)# **vlan** 1-100
	Switch(config)# **ip arp inspection**
	Switch(config)# **ip arp inspection vlan** 1-100
	Switch# **show ip arp inspection**
	`Switch# configure terminal`
	`Switch(config)# vlan 1-100`
	`Switch(config-vlan)# exit`
	`Switch(config)#  ip arp inspection`
	`Switch(config)#  ip arp inspection vlan 1-100`
	`Switch(config)# exit`
	`Switch# show ip arp inspection`
	`Dynamic ARP Inspection     : enabled`
	`Enable on Vlans            : 1-100`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

8.3 IP ARP INSPECTION TRUST

Use the **ip arp inspection trust** command to set trusted interface. The switch does not check ARP packets that are received on the trusted interface; it simply forwards it. Use the **"no"** form of this command to set untrusted interface.

Switch#**configure terminal**
Switch(config)# **Ip arp inspection trust**

Switch(config)# **no ip arp inspection trust**

Syntax	**ip arp inspection trust** **no ip arp inspection trust**
Default	Dynamic Arp inspection trust is disabled
Mode	Interface Configuration

Example	The example shows how to set interface gi1 to trust. You can verify settings by the following show ip arp inspection interface command.
	Switch#**configure terminal**
	Switch(config)# **interface gi2**
	Switch(config)# **ip arp inspection trust**
	
	Switch#**show ip arp inspection interface** gi2
	`Switch# configure terminal`
	`Switch(config)#  interface g2`
	`Switch(config-if)# ip arp inspection trust`
	`Switch(config-if)#`
	`Switch# show ip arp inspection interface g2`
	`Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |`
	`gi2 | Trusted | None | disabled | disabled | disabled/disabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

8.4 IP ARP INSPECTION VALIDATE

Use the **ip arp inspection validate** command to enable validate function on interface. The **"src-mac"** drop ARP requests and reply to packets that arp-sender-mac and ethernet-source-mac is not match. The **"dst-mac"** drops ARP reply packets that arp-target-mac and ethernet-dst-mac is not match. The **"ip"** drop ARP request and reply to packets that sender-ip is invalid such as broadcast multicast all zero IP address and drop ARP reply packets that target-ip is invalid. The **"allow-zeros"** means won't drop all zero IP address. Use the **"no"** form of this command to disable validation.

Switch#**configure terminal**

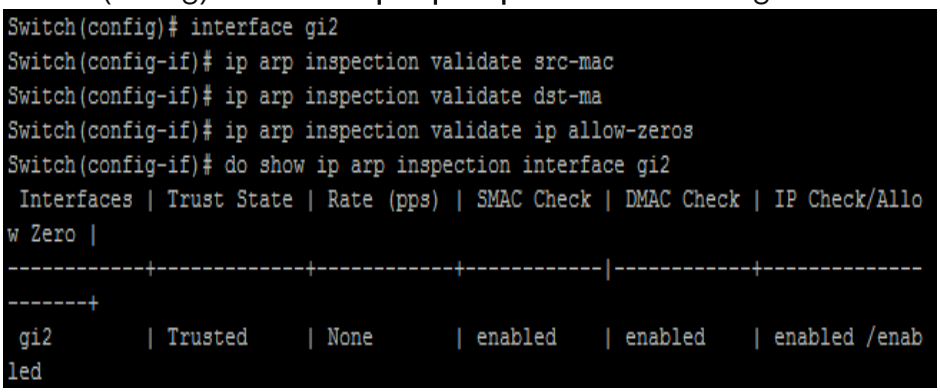
Switch(config)# **ip arp inspection validate src-mac**

Switch(config)# **ip arp inspection validate dst-mac**
Switch(config)# **ip arp inspection validate ip [allow-zeros]**

Switch(config)# **no ip arp inspection validate src-mac**
Switch(config)# **no ip arp inspection validate dst-mac**
Switch(config)# **no ip arp inspection validate ip [allow-zeros]**

Syntax	**ip arp inspection validate src-mac** **ip arp inspection validate dst-mac** **ip arp inspection validate ip [allow-zeros]** **no ip arp inspection validate src-mac** **no ip arp inspection validate dst-mac** **no ip arp inspection validate ip [allow-zeros]**
Default	Default is disabled of all validation
Mode	Interface Configuration
Example	The example shows how to set interface gi1 to validate **"src-mac"**,**"dst-mac"** and **"ip"**,**"allow zeros"**. You can verify settings by the following show ip arp inspection interface command. Switch#**configure terminal** Switch(config)# **interface** gi2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch(config-if)# ip arp inspection validate src-mac Switch(config-if)# ip arp inspection validate dst-ma Switch(config-if)# ip arp inspection validate ip allow-zeros Switch(config)# do show ip arp inspection interface gi2 

```
Switch(config)# interface gi2
Switch(config-if)# ip arp inspection validate src-mac
Switch(config-if)# ip arp inspection validate dst-ma
Switch(config-if)# ip arp inspection validate ip allow-zeros
Switch(config-if)# do show ip arp inspection interface gi2
 Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allo
w Zero |
------------+------------+------------+------------|------------+-------------
--------+
 gi2        | Trusted    | None       | enabled    | enabled    | enabled /enab
led
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

8.5 IP ARP INSPECTION RATE-LIMIT

Use the **ip arp inspection rate-limit** command to set rate limitation on interface. The switch drop ARP packets after receives more than configured rate of packets per second. Use the **"no"** form of this command to return to default settings.

Switch#**configure terminal**
Switch(config)# **ip arp inspection rate-limit** *<1-50>*

Switch(config)# **no ip arp inspection rate-limit**

Syntax	**ip arp inspection rate-limit** *<1-50>* **no ip arp inspection rate-limit**
Parameter	*<1-50>*Set 1 to 50 PPS of DHCP packet rate limitation
Default	Default is un-limited of ARP packet
Mode	Interface Configuration

Example	The example shows how to set rate limit to 30 pps on interface gi2. You can verify settings by the following show ip arp inspection interface command.
	Switch#**configure terminal**
	Switch(config)# **interface** gi2
	Switch(config)# **ip arp inspection rate-limit** 30
	Switch(config)# **do show ip arp inspection interface** gi2
	`Switch(config)# interface gi2`
	`Switch(config-if)# ip arp inspection rate-limit 30`
	`Switch(config-if)# do show ip arp inspection interface gi2`
	`Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |`
	`gi2 | Trusted | 30 | enabled | enabled | enabled /enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

8.6 CLEAR IP ARP INSPECTION STATISTICS

Use the **clear ip arp inspection interfaces statistics** command to clear statistics that are recorded on interface.

Switch#**clear ip arp inspection interfaces** *{IF_PORTS}* **statistics**

Syntax	**clear ip arp inspection interfaces** *{IF_PORTS}* **statistics**
Parameter	*IF_PORTS* specifies ports to clear statistics
Mode	Privileged EXEC

Example	The example shows how to clear statistics on interface gi1. You can verify settings by the following show ip arp inspection interface statistics command.
	switch# **clear ip arp inspection interfaces gi2 statistics**
	switch# **show ip arp inspection interfaces gi2**
	`Switch# show ip arp inspection interface g2`
	`Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |`
	`gi2 | Trusted | None | disabled | disabled | disabled/disabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

8.7 SHOW IP ARP INSPECTION

Use the **show ip arp inspection** command to show settings of Dynamic Arp Inspection.

Switch#**show ip arp inspection**

Syntax	**show ip dhcp snooping**
Mode	Privileged EXEC

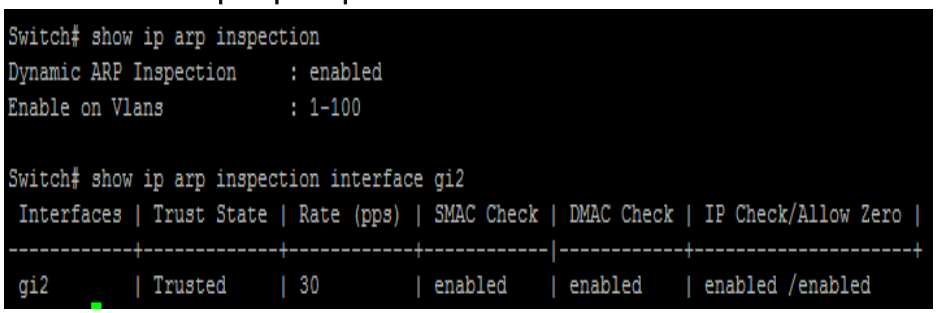
Example	The example shows how to show settings of Dynamic Arp Inspection
	Switch# **show ip arp inspection**
	`Switch#  show ip arp inspection`
	`Dynamic ARP Inspection      : enabled`
	`Enable on Vlans             : 1-100`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

8.8 SHOW IP ARP INSPECITON INTERFACE

Use the **show ip arp inspection interfaces** command to show settings or statistics of interface.

Switch#**show ip arp inspection interfaces** *{IF_PORTS}*
Switch#**show ip arp inspection interfaces** *{IF_PORTS}* **statistics**

Syntax	**show ip arp inspection interfaces** *{IF_PORTS}* **show ip arp inspection interfaces** *{IF_PORTS}***statistics**
Parameter	*IF_PORTS* specifies ports to show statistics
Mode	Privileged EXEC
Example	switch# **show ip arp inspection** 

```
Switch# show ip arp inspection
Dynamic ARP Inspection     : enabled
Enable on Vlans            : 1-100

Switch# show ip arp inspection interface gi2
 Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |
------------+------------+-------------+------------|------------+---------------------+
 gi2        | Trusted    | 30          | enabled    | enabled    | enabled /enabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

9. GVRP (GARP VLAN Registration Protocol)

GVRP, i.e. GARP VLAN Registration Protocol, is an application of GARP (Generic Attribute Registration Protocol). GARP is mainly used to establish an attribute transmission mechanism to transmit attributes, to ensure protocol entities registering and deregistering the attribute. According to different transmission attributes, GARP can be divided to many application protocols, such as GMRP and GVRP. Therefore, GVRP is a protocol which transmits VLAN attributes to the whole layer 2 network through GARP protocol. GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information to automatically register VLAN members on interfaces across the network. GVRP defines a way for switches to exchange VLAN information to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration. GVRP cannot be enabled for ports set to Access mode

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

9.1 GVRP (GLOBAL)

GARP VLAN Registration Protocol (GVRP) is a Generic Attribute Registration Protocol (GARP) application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

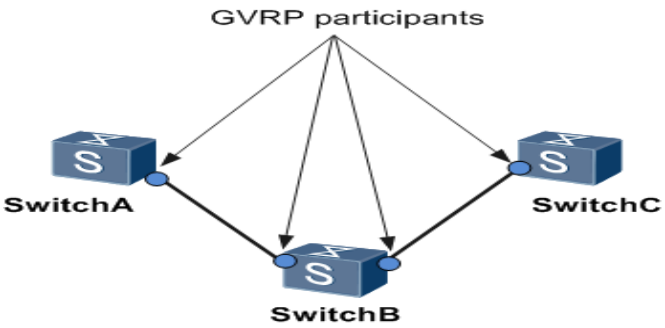


Fig 9.1 GVRP Participant List

With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports. You must enable GVRP globally before any GVRP processing occurs on the switch. Enabling GVRP globally enables GVRP to perform VLAN pruning on IEEE 802.1Q trunk links. Pruning occurs only on GVRP-enabled trunks.

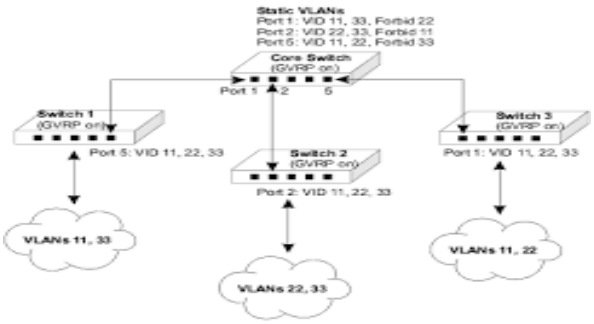


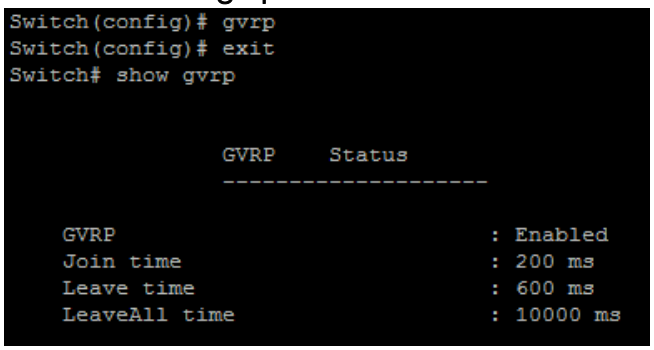
Fig 9.2 GVRP VLAN sharing

Disable **gvrp** will clear all learned dynamic vlan entry and do not learn dynamic vlan anymore. Use **'show gvrp'** to show configuration.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Switch#configure terminal
Switch(config)# gvrp

Switch(config)# no gvrp

Syntax	gvrp {timer} no gvrp
Default	GVRP is disabled
Mode	Global Configuration
Example	The following example specifies that set global gvrp test. Switch#configure terminal Switch(config)# gvrp Switch# show gvrp 

```
Switch(config)# gvrp
Switch(config)# exit
Switch# show gvrp


               GVRP    Status
               --------------------


    GVRP                           : Enabled
    Join time                      : 200 ms
    Leave time                     : 600 ms
    LeaveAll time                  : 10000 ms
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

9.2 GVRP (INTERFACE)

The **'no gvrp'** will remove dynamic port from vlan. **'gvrp'** must work at port mode is trunk.

Switch#**configure terminal**
Switch(config)# **gvrp**

Switch(config)# **no gvrp**
Switch# **show gvrp configuration interfaces** gi2

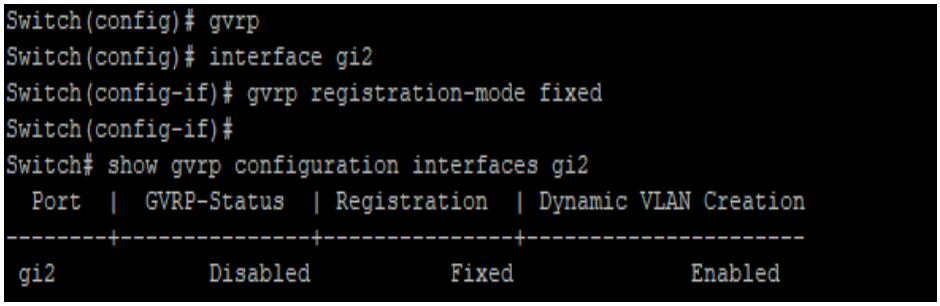
Syntax	**gvrp** **no gvrp**
Default	GVRP is disabled on interface
Mode	Interface mode
Example	The following example specifies that set port gvrp test. The port gvrp enable must set port mode is trunk firstly. Switch#**configure terminal** Switch(config)#**interface** gi2 Switch(config-if)# **switchport mode trunk** Switch(config)#**gvrp** Switch# **show gvrp configuration interfaces** gi2 `Switch(config)# interface gi2` `Switch(config-if)# switchport mode trunk` `Switch(config-if)# exit` `Switch(config)# gvrp` `Switch(config)# exit` `Switch# show gvrp configuration interfaces gi2` ` Port	GVRP-Status	Registration	Dynamic VLAN Creation` `--------+--------------+--------------+---------------------` ` gi2 Disabled Normal Enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

9.3 GVRP REGISTRATION-MODE

When set registration-mode is fixed or forbidden, will remove the port from vlan which is dynamic port and not learning vlan.

Switch#**configure terminal**
Switch(config#**interface** *{interface-ID}*
Switch(config-if)# **gvrp registration-mode (normal | fixed | forbidden)**

Syntax	**gvrp registration-mode (normal | fixed | forbidden)**
Parameter	**(normal | fixed | forbidden)** normal: register dynamic vlan, and transmit all vlan attribute. fixed: do not register dynamic vlan, and only transmit static vlan attribute. forbidden: do not register dynamic vlan, and only transmit default vlan attribute.
Mode	Interface mode
Example	The following example specifies that set gvrp registration mode test. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **gvrp registration-mode fixed** Switch# **show gvrp configuration interfaces** gi2 

```
Switch(config)# gvrp
Switch(config)# interface gi2
Switch(config-if)# gvrp registration-mode fixed
Switch(config-if)#
Switch# show gvrp configuration interfaces gi2
  Port  |  GVRP-Status  | Registration  | Dynamic VLAN Creation
--------+---------------+---------------+---------------------
 gi2           Disabled          Fixed             Enabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

9.4 GVRP VLAN-CREATE-FORBID

'gvrp vlan-creation-forbid' will not remove dynamic port from vlan immediate.

Switch#**configure terminal**
Switch(config#**interface** *{interface-ID}*
Switch(config-if)# **gvrp vlan-creation-forbid**

Switch(config-if)# **no gvrp vlan-creation-forbid**

Syntax	**gvrp vlan-creation-forbid** **no gvrp vlan-creation-forbid**
Mode	Interface mode
Example	The following example specifies that set port gvrp vlan-creation-forbid test. Switch#**configure terminal** Switch(config)#**interface** gi2 Switch(config-if)# **gvrp vlan-creation-forbid** Switch(config-if)#**exit** Switch# **show gvrp configuration interfaces** gi2 `Switch# configure terminal` `Switch(config)# interface gi2` `Switch(config-if)# gvrp vlan-creation-forbid` `Switch(config-if)#` `Switch# show gvrp configuration interfaces gi2` ` Port	GVRP-Status	Registration	Dynamic VLAN Creation` `--------+---------------+---------------+---------------------` `gi2 Disabled Fixed Disabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

9.5 CLEAR GVRP STATISTICS

This command will clear the ports error statistics or statistics info.

Switch# **clear gvrp (error-statistics | statistics) [interfaces** *{IF_PORTS}*]

Syntax	**clear gvrp (error-statistics | statistics) [interfaces** *{IF_PORTS}*]
Parameter	(error-statistics | statistics) [interfaces IF_PORTS] Error-statistics: error gvrp packet statistics Statistics: gvrp event message statistics Specifies posts to clear statistics
Mode	Privileged EXEC

Example	The following example specifies that clear gvrp error statistics and statistics test.
	Switch# **clear gvrp statistics**
	Switch# **clear gvrp error-statistics**
	`Switch#  clear gvrp statistics`
	`Switch# clear gvrp error-statistics`
	`Switch# sh gvrp statistics`
	`Port id          :  gil`
	`Total RX         :    0`
	`JoinEmpty RX     :    0`
	`JoinIn RX        :    0`
	`Empty RX         :    0`
	`LeaveIn RX       :    0`
	`LeaveEmpty RX    :    0`
	`LeaveAll RX      :    0`
	`Total TX         :    0`
	`JoinEmpty TX     :    0`
	`JoinIn TX        :    0`
	`Empty TX         :    0`
	`LeaveIn TX       :    0`
	`LeaveEmpty TX    :    0`
	`LeaveAll TX      :    0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

9.6 SHOW GVRP STATISTICS

This command will display the ports error statistics or statistics info.

Switch# **show gvrp (statistics | error-statistics) [interfaces** *{IF_PORTS}*]

Syntax	**show gvrp (statistics | error-statistics) [interfaces** *{IF_PORTS}*]
Parameter	none Display all ports (statistics| error- statistics) [interfaces *IF_PORTS*] **statistics** – GVRP statistics error-statistics GVRP error statistics Specifies posts
Default	Display all ports statistics info
Mode	Privileged EXEC

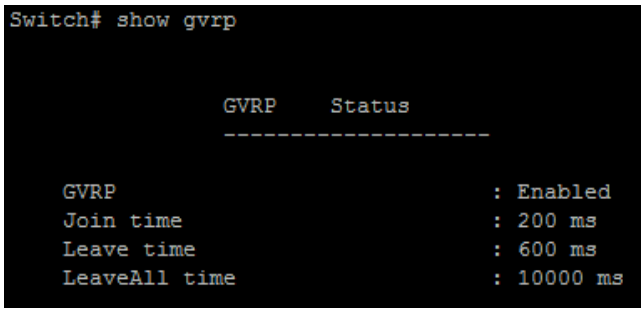
Example	The following example specifies that display gvrp error statistics and statistics test.
	Switch# **show gvrp statistics**
	`Switch# sh gvrp statistics`
	`Port id : gil`
	`Total RX : 0`
	`JoinEmpty RX : 0`
	`JoinIn RX : 0`
	`Empty RX : 0`
	`LeaveIn RX : 0`
	`LeaveEmpty RX : 0`
	`LeaveAll RX : 0`
	`Total TX : 0`
	`JoinEmpty TX : 0`
	`JoinIn TX : 0`
	`Empty TX : 0`
	`LeaveIn TX : 0`
	`LeaveEmpty TX : 0`
	`LeaveAll TX : 0`
	
	`Port id : gi2`
	`Total RX : 0`
	`JoinEmpty RX : 0`
	`JoinIn RX : 0`
	`Empty RX : 0`
	`LeaveIn RX : 0`
	`LeaveEmpty RX : 0`
	`LeaveAll RX : 0`
	`Total TX : 0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

9.7 SHOW GVRP

This command will display the gvrp global info.

Switch# **show gvrp**

Syntax	**show gvrp**
Mode	Privileged EXEC
Example	The following example specifies that display gvrp test. Switch# **show gvrp** 

```
Switch# show gvrp

               GVRP    Status
               --------------------

   GVRP                          : Enabled
   Join time                     : 200 ms
   Leave time                    : 600 ms
   LeaveAll time                 : 10000 ms
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

9.8 SHOW GVRP CONFIGURATION

This command will display the ports configuration info.

Switch# **show gvrp configuration**

Syntax	**show gvrp configuration [interface** *{IF_PORTS}***]**
Parameter	**none [interfaces** *IF_PORTS***]** Display all ports configuration Display Specifies posts configuration
Mode	Privileged EXEC
Example	The following example specifies that display gvrp port configuration test. Switch# **show gvrp configuration** `Switch# show gvrp configuration` ` Port	GVRP-Status	Registration	Dynamic VLAN Creation` `--------+---------------+---------------+----------------------` `gi1 Disabled Normal Enabled` `gi2 Disabled Fixed Disabled` `gi3 Disabled Normal Enabled` `gi4 Disabled Normal Enabled` `gi5 Disabled Normal Enabled` `gi6 Disabled Normal Enabled` `gi7 Disabled Normal Enabled` `gi8 Disabled Normal Enabled` `gi9 Disabled Normal Enabled` `gi10 Disabled Normal Enabled` `gi11 Disabled Normal Enabled` `gi12 Disabled Normal Enabled` `gi13 Disabled Normal Enabled` `gi14 Disabled Normal Enabled` `gi15 Disabled Normal Enabled` `gi16 Disabled Normal Enabled` `gi17 Disabled Normal Enabled` `gi18 Disabled Normal Enabled` `gi19 Disabled Normal Enabled` `gi20 Disabled Normal Enabled` `gi21 Disabled Normal Enabled` `gi22 Disabled Normal Enabled` `--More--`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10. IGMP SNOOPING

Internet Group Management Protocol (IGMP) snooping constrains the flooding of IPv4 multicast traffic on VLANs on a device. With IGMP snooping enabled, the device monitors IGMP traffic on the network and uses what it learns to forward multicast traffic to only the downstream interfaces that are connected to interested receivers. The device conserves bandwidth by sending multicast traffic only to interfaces connected to devices that want to receive the traffic, instead of flooding the traffic to all the downstream interfaces in a VLAN.

Benefits of IGMP Snooping

- Optimized bandwidth utilization—IGMP snooping's main benefit is to reduce flooding of packets. The device selectively forwards IPv4 multicast data to a list of ports that want to receive the data instead of flooding it to all ports in a VLAN.
- Improved security—Prevents denial of service attacks from unknown sources.

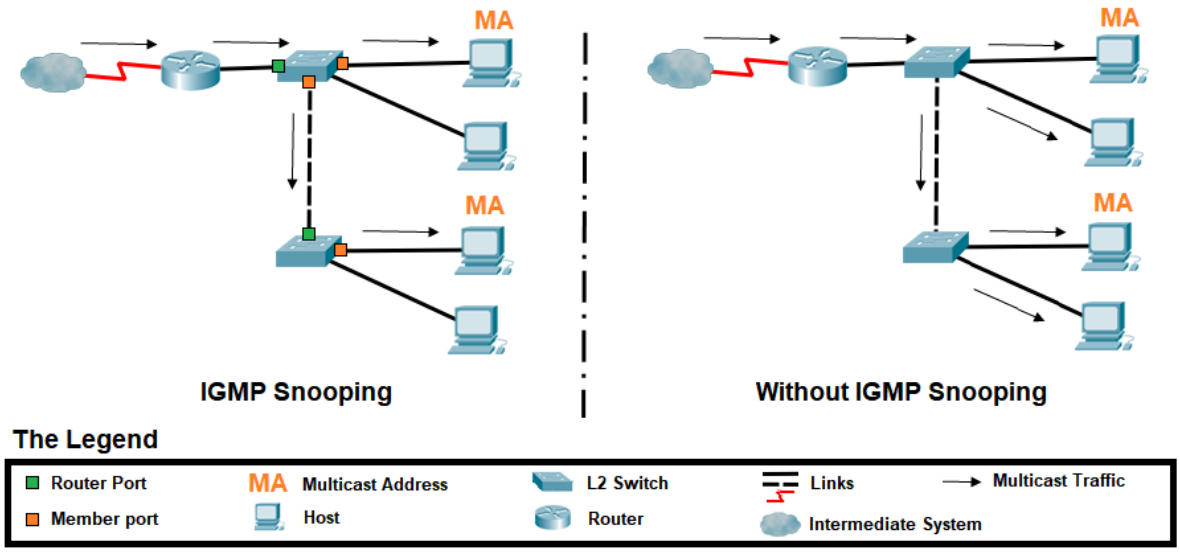


Fig 10.1 IGMP Snooping Optimized bandwidth utilization

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.1 IP IGMP SNOOPING

How IGMP Snooping Works?

Devices usually learn unicast MAC addresses by checking the source address field of the frames they receive and then send any traffic for that unicast address only to the appropriate interfaces. However, a multicast MAC address can never be the source address for a packet. As a result, when a device receives traffic for a multicast destination address, it floods the traffic on the relevant VLAN, sending a significant amount of traffic for which there might not necessarily be interested receivers.

IGMP snooping prevents this flooding. When you enable IGMP snooping, the device monitors IGMP packets between receivers and multicast routers and uses the content of the packets to build a multicast forwarding table—a database of multicast groups and the interfaces that are connected to members of the groups. When the device receives multicast packets, it uses the multicast forwarding table to selectively forward the traffic to only the interfaces that are connected to members of the appropriate multicast groups.

IGMP Message Types

Multicast routers use IGMP to learn which groups have interested listeners for each of their attached physical networks. In any given subnet, one multicast router acts as an IGMP querier. The IGMP querier sends out the following types of queries to hosts:

- General query—Asks whether any host is listening to any group.
- Group-specific query — (IGMPv2 and IGMPv3 only) Asks whether any host is listening to a specific multicast group. This query is sent in response to a host leaving the multicast group and allows the router to quickly determine if any remaining hosts are interested in the group.
- Group-and-source-specific query — (IGMPv3 only) Asks whether any host is listening to group multicast traffic from a specific multicast source. This query is sent in response to a host indicating that it is no longer interested in receiving group multicast traffic from the multicast source and allows the router to quickly

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

determine any remaining hosts are interested in receiving group multicast traffic from that source.

Hosts that are multicast listeners send the following kinds of messages:

- Membership report—Indicates that the host wants to join a particular multicast group.
- Leave report — (IGMPv2 and IGMPv3 only) Indicates that the host wants to leave a particular multicast group.

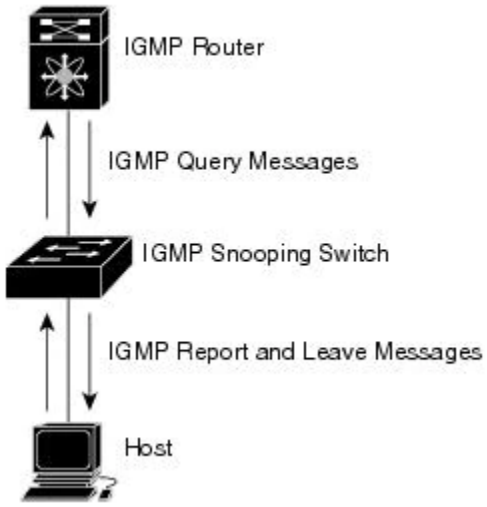


Fig 10.2 IGMP Messages

How Hosts Join and Leave Multicast Groups?

Hosts can join multicast groups in two ways:

- By sending an unsolicited IGMP join message to a multicast router that specifies the IP multicast group the host wants to join.
- By sending an IGMP join message in response to a general query from a multicast router.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

A multicast router continues to forward multicast traffic to a VLAN provided that at least one host on that VLAN responds to the periodic general IGMP queries. For a host to remain a member of a multicast group, it must continue to respond to the periodic general IGMP queries.

Hosts can leave a multicast group in either of two ways:

- By not responding to periodic queries within a particular interval of time, which is considered a "silent leave." This is the only leave method for IGMPv1 hosts.
- By sending a leave report. This method can be used by IGMPv2 and IGMPv3 hosts.

Use the ip igmp snooping command to enable IGMP snooping function. Use the no form of this command to disable. You can verify settings by the show ip igmp snooping command.

Switch#configure terminal
Switch(config)# ip igmp snooping

Switch(config)# no ip igmp snooping

Syntax	ip igmp snooping no ip igmp snooping
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping test. Switch#configure terminal Switch(config)# ip igmp snooping Switch(config)# no ip igmp snooping Switch #show ip igmp snooping

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)#  ip igmp snooping
Switch(config)#
Switch# show ip igmp snooping


               IGMP Snooping Status
               --------------------

    Snooping                          : Enabled
    Report Suppression                : Enabled
    Operation Version                 : v2
    Forward Method                    : mac
    Unknown IP Multicast Action       : Flood


               Packet Statistics
    Total RX                          :  0
    Valid RX                          :  0
    Invalid RX                        :  0
    Other RX                          :  0
    Leave RX                          :  0
    Report RX                         :  0
    General Query RX                  :  0
    Specail Group Query RX            :  0
    Specail Group & Source Query RX   :  0
    Leave TX                          :  0
    Report TX                         :  0
    General Query TX                  :  0
    Specail Group Query TX            :  0
    Specail Group & Source Query TX   :  0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.2 IGMP SNOOPING REPORT-SUPPRESSION

Use the ip **igmp snooping report-suppression** command to enable IGMP snooping report-suppression function. Use **"no"** form of this command to disable. Disable report-suppression will forward all received reports to the VLAN router ports. You can verify settings by the **"show ip igmp snooping"** snooping command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping report-suppression**

Switch(config)# **no ip igmp snooping report-suppression**

Syntax	**ip igmp snooping report-suppression** **no ip igmp snooping report-suppression**
Default	Default is enabled
Mode	Global Configuration
Example	The following example specifies that disable ip igmp snooping report-suppression test. Switch#**configure terminal** Switch(config)# **ip igmp snooping report-suppression** Switch #**show ip igmp snooping**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)#  ip igmp snooping report-suppression
Switch(config)#
Switch# show ip igmp snooping


               IGMP Snooping Status
               --------------------

    Snooping                          : Enabled
    Report Suppression                : Enabled
    Operation Version                 : v2
    Forward Method                    : mac
    Unknown IP Multicast Action       : Flood


               Packet Statistics
    Total RX                           :  0
    Valid RX                           :  0
    Invalid RX                         :  0
    Other RX                           :  0
    Leave RX                           :  0
    Report RX                          :  0
    General Query RX                   :  0
    Specail Group Query RX             :  0
    Specail Group & Source Query RX    :  0
    Leave TX                           :  0
    Report TX                          :  0
    General Query TX                   :  0
    Specail Group Query TX             :  0
    Specail Group & Source Query TX    :  0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.3 IP IGMP SNOOPING VERSION

Use the **ip igmp snooping version** command to change IGMP support version. Only basic mode is supported in v3. When change version from v3 to v2, all querier version will update to version 2. You can verify settings by the show ip igmp snooping command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping version** (2|3)

Syntax	**ip igmp snooping version (2|3)**
Parameter	(2|3)IGMP version 2 or IGMP version 3 basic mode
Default	Default is version 2
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping version 3. Switch#**configure terminal** Switch(config)# **ip igmp snooping version 3**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)#  ip igmp snooping version 3
Switch(config)#
Switch# show ip igmp snooping


               IGMP Snooping Status
               --------------------

    Snooping                        : Enabled
    Report Suppression              : Enabled
    Operation Version               : v3
    Forward Method                  : mac
    Unknown IP Multicast Action     : Flood


               Packet Statistics
    Total RX                          :  0
    Valid RX                          :  0
    Invalid RX                        :  0
    Other RX                          :  0
    Leave RX                          :  0
    Report RX                         :  0
    General Query RX                  :  0
    Specail Group Query RX            :  0
    Specail Group & Source Query RX   :  0
    Leave TX                          :  0
    Report TX                         :  0
    General Query TX                  :  0
    Specail Group Query TX            :  0
    Specail Group & Source Query TX   :  0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.4 IP IGMP SNOOPING UNKNOWN-MULTICAST ACTION

When igmp and mld snooping disabled, it can't set action router-port. When disable igmp snooping &mld snooping, it set unknown multicast action flood. When action is router-port to flood or drop, it will delete the unknown multicast group entry. Use the ip igmp snooping unknown-multicast action command to change action. Use the **"no"** form of this command to restore to default. You can verify settings by the show ip igmp snooping command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping unknown-multicast action (drop | flood |router-port)**

Switch(config)# **no ip igmp snooping unknown-multicast action**

Syntax	**ip igmp snooping unknown-multicast action (drop | flood |router-port)** **no ip igmp snooping unknown-multicast action**
Parameter	**(drop | flood | router- port)** Drop, flood in vlan or forward to router port of unknown multicast packet
Default	Default is flood.
Mode	Global Configuration
Example	The following example specifies that set ip igmp unknown multicast action router-port test. Switch#**configure terminal** Switch(config)# **ip igmp snooping** Switch(config)# **ip igmp snooping unknown-multicast action router-port** Switch#**show ip igmp snooping**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)#  ip igmp snooping unknown-multicast action router-port
Switch(config)#
Switch# show ip igmp snooping


              IGMP Snooping Status
              --------------------

   Snooping                       : Enabled
   Report Suppression             : Enabled
   Operation Version              : v3
   Forward Method                 : mac
   Unknown IP Multicast Action    : Router-Port


              Packet Statistics
   Total RX                        :  0
   Valid RX                        :  0
   Invalid RX                      :  0
   Other RX                        :  0
   Leave RX                        :  0
   Report RX                       :  0
   General Query RX                :  0
   Specail Group Query RX          :  0
   Specail Group & Source Query RX  :  0
   Leave TX                        :  0
   Report TX                       :  0
   General Query TX                :  0
   Specail Group Query TX          :  0
   Specail Group & Source Query TX  :  0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.5 IP IGMP SNOOPING QUERIER

When enable **ip igmp vlan querier**, there will process router select, the select successful will send general and specific query. Use the ip igmp snooping querier command to add querier. Use the **"no"** form of this command to delete querier. You can verify settings by the show ip igmp snooping querier command.

Switch#**configure terminal**
Switch(config)#**ip igmp snooping vlan** *{VLAN-LIST}***querier [version (2|3)]**

Switch(config)#**no ip igmp snooping [vlan** *<VLAN-LIST>***] querier**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}***querier [version (2|3)]** **no ip igmp snooping [vlan** *<VLAN-LIST>***] querier**
Parameter	*VLAN-LIST* specifies VLAN ID list to set(2|3)Query version 2 or 3
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping querier test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan** 2 **querier version** 3

```
Switch# configure terminal
Switch(config)#  ip igmp snooping vlan 2 querier version 3
Switch(config)#
Switch# sh ip igmp snooping querier


 VID  |    State    |    Status   | Version   | Querier IP
------+-------------+-------------+-----------+-------------------
    1 |  Disabled   | Non-Querier |   No      |    ------
    2 |   Enabled   |   Querier   |   v3      |    ------

Total Entry 2
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.6 IP IGMP SNOOPING VLAN

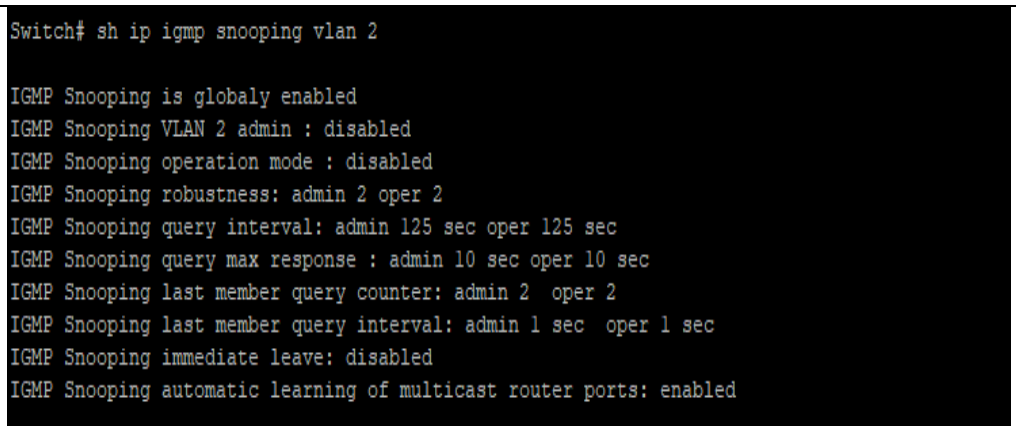
Internet Group Management Protocol (IGMP) snooping streamlines multicast traffic handling for VLANs. IGMP snooping allows a switch to only forward multicast traffic to the links that have solicited them. Snooping is therefore especially useful for bandwidth-intensive IP multicast applications such as IPTV. Disable will clear all ip igmp snooping dynamic group and dynamic router port and make all static ip igmp group invalid of this vlan. It will not learn dynamic group and router port by igmp message anymore. Use the ip igmp snooping vlan command to enable IGMP on VLAN. Use the **"no"** form of this command to disable. You can verify settings by the show ip igmp snooping vlan command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **no ip igmp snooping vlan** *{VLAN-LIST}*
Parameter	*VLAN-LIST* specifies VLAN ID list to set
Default	Default is disabled for all VLANs
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping vlan test. Switch#**configure terminal** Switch(config)# **ip igmp snooping** Switch(config)# **ip igmp snooping vlan 2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.7 IP IGMP SNOOPING VLAN FASTLEAVE

Use the **ip igmp snooping vlan fastleave** command to enable fastleave function. Group will remove port immediately when receive leave packet. Use the **"no"** form of this command to disable. You can verify settings by the show ip igmp snooping vlan command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **fastleave**

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **fastleave**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **fastleave** **no ip igmp snooping vlan** *{VLAN-LIST}* **fastleave**
Parameter	*VLAN-LIST* specifies VLAN ID list to set
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping vlan fastleave test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 fastleave** Switch#**show ip igmp snooping**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 fastleave
Switch(config)#
Switch# sh ip igmp snooping


              IGMP Snooping Status
              --------------------

   Snooping                       : Enabled
   Report Suppression             : Enabled
   Operation Version              : v3
   Forward Method                 : mac
   Unknown IP Multicast Action    : Router-Port


              Packet Statistics
   Total RX                        :  1
   Valid RX                        :  0
   Invalid RX                      :  0
   Other RX                        :  0
   Leave RX                        :  0
   Report RX                       :  0
   General Query RX                :  0
   Specail Group Query RX          :  0
   Specail Group & Source Query RX  :  0
   Leave TX                        :  0
   Report TX                       :  0
   General Query TX                :  0
   Specail Group Query TX          :  0
   Specail Group & Source Query TX  :  0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.8 IP IGMP SNOOPING VLAN LAST-MEMBER-QUERY-COUNT

Use the **ip igmp snooping vlan last-member-query-count** command to change how many query packets will send. Use the **"no"** form of this command to restore to default. You can verify settings by the show ip igmp snooping vlan command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-count** *<1-7>*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-count**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-count** *<1-7>* **no ip igmp snooping vlan** *{VLAN-LIST}***last-member-query-count**
Parameter	*VLAN-LIST* last-member-query-count *<1-7>*specifies VLAN ID list to set specifies
Default	Default is 2
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping vlan last-member-query-count test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp snooping vlan 1 last-member-query-count 5**
	`Switch# configure t`
	`Switch(config)#  ip igmp snooping vlan 1 last-member-query-count 5`
	`Switch(config)#`
	`Switch# sh ip igmp snooping vlan 1`
	
	`IGMP Snooping is globaly enabled`
	`IGMP Snooping VLAN 1 admin : enabled`
	`IGMP Snooping operation mode : enabled`
	`IGMP Snooping robustness: admin 2 oper 2`
	`IGMP Snooping query interval: admin 125 sec oper 125 sec`
	`IGMP Snooping query max response : admin 10 sec oper 10 sec`
	`IGMP Snooping last member query counter: admin 5  oper 2`
	`IGMP Snooping last member query interval: admin 1 sec  oper 1 sec`
	`IGMP Snooping immediate leave: enabled`
	`IGMP Snooping automatic learning of multicast router ports: enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.9 IP IGMP SNOOPING VLAN LAST-MEMBER-QUERY-INTERVAL

Use the **ip igmp snooping vlan last-member-query-interval** command to set interval between each query packet. Use the **"no"** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}***last-member-query-interval** *<1-60>*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-interval**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-interval** *<1- 60>* **no ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-interval**
Parameter	*VLAN-LIST* last-member-query-interval *<1-60>* specifies VLAN ID list to set specifies last member query interval to set
Default	Default is 1
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping vlan last-member-query-interval test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp snooping vlan 1 last-member-query-interval 3**
	`Switch# configure t`
	`Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3`
	`Switch(config)#`
	`Switch# sh ip igmp snooping vlan 1`
	
	`IGMP Snooping is globaly enabled`
	`IGMP Snooping VLAN 1 admin : enabled`
	`IGMP Snooping operation mode : enabled`
	`IGMP Snooping robustness: admin 2 oper 2`
	`IGMP Snooping query interval: admin 125 sec oper 125 sec`
	`IGMP Snooping query max response : admin 10 sec oper 10 sec`
	`IGMP Snooping last member query counter: admin 5 oper 2`
	`IGMP Snooping last member query interval: admin 3 sec oper 1 sec`
	`IGMP Snooping immediate leave: enabled`
	`IGMP Snooping automatic learning of multicast router ports: enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.10 IP IGMP SNOOPING VLAN QUERY-INTERVAL

Use the **ip igmp snooping vlan query-interval** command to set interval between each query. Use the **"no"** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **query-interval** *<30-18000>*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***query-interval**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}***query-interval** *<30-18000>* **no ip igmp snooping vlan** *{VLAN-LIST}***query-interval**
Parameter	*VLAN-LIST* query-interval specifies VLAN ID list to set *<30-18000>* specifies query interval to set
Default	Default is 125
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping vlan query-interval test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan** 1 **query-interval** 100

```
Switch# configure t
Switch(config)# ip igmp snooping vlan 1 query-interval 100
Switch(config)#
Switch# sh ip igmp snooping vlan 1

IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : enabled
IGMP Snooping operation mode : enabled
IGMP Snooping robustness: admin 2 oper 2
IGMP Snooping query interval: admin 100 sec oper 125 sec
IGMP Snooping query max response : admin 10 sec oper 10 sec
IGMP Snooping last member query counter: admin 5  oper 2
IGMP Snooping last member query interval: admin 3 sec  oper 1 sec
IGMP Snooping immediate leave: enabled
IGMP Snooping automatic learning of multicast router ports: enabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.11 IP IGMP SNOOPING VLAN RESPONSE-TIME

Use the **ip igmp snooping vlan response-time** command to set response time. Use the **"no"** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}*> **response-time** *<5-20>*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***response-time**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}***response-time** *<5-20>* **no ip igmp snooping vlan** *{VLAN-LIST}* **response-time**
Parameter	*VLAN-LIST*specifies VLAN ID list to set. **response-time***<5-20>*specifies a response time to set
Default	Default is 10
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping vlan response- time test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp snooping vlan** 1 **response-time** 12
	Switch#**show ip igmp snooping vlan** 1
	`Switch# configure t`
	`Switch(config)# ip igmp snooping vlan 1 response-time 12`
	`Switch(config)#`
	`Switch# sh ip igmp snooping vlan 1`
	
	`IGMP Snooping is globaly enabled`
	`IGMP Snooping VLAN 1 admin : enabled`
	`IGMP Snooping operation mode : enabled`
	`IGMP Snooping robustness: admin 2 oper 2`
	`IGMP Snooping query interval: admin 100 sec oper 125 sec`
	`IGMP Snooping query max response : admin 12 sec oper 10 sec`
	`IGMP Snooping last member query counter: admin 5  oper 2`
	`IGMP Snooping last member query interval: admin 3 sec  oper 1 sec`
	`IGMP Snooping immediate leave: enabled`
	`IGMP Snooping automatic learning of multicast router ports: enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.12 IP IGMP SNOOPING VLAN ROBUSTNESS-VARIABLE

Use the **ip igmp snooping vlan robustness-variable** command to times to retry. Use the **"no"** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **robustness-variable** *<1-7>*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **robustness-variable**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **robustness-variable** *<1-7>* **no ip igmp snooping vlan** *{VLAN-LIST}* **robustness-variable**
Parameter	*VLAN-LIST* specifies VLAN ID list to set. robustness-variable *<1-7>* specifies a robustness value to set
Default	Default is 2
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping vlan parameters test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp snooping vlan 1 robustness-variable 2**
	`Switch(config)# ip igmp snooping vlan 1 robustness-variable 2`
	`Switch(config)# exit`
	`Switch# show ip igmp snooping vlan 1`
	
	`IGMP Snooping is globaly disabled`
	`IGMP Snooping VLAN 1 admin : disabled`
	`IGMP Snooping operation mode : disabled`
	`IGMP Snooping robustness: admin 2 oper 2`
	`IGMP Snooping query interval: admin 100 sec oper 125 sec`
	`IGMP Snooping query max response : admin 12 sec oper 10 sec`
	`IGMP Snooping last member query counter: admin 2  oper 2`
	`IGMP Snooping last member query interval: admin 1 sec  oper 1 sec`
	`IGMP Snooping immediate leave: disabled`
	`IGMP Snooping automatic learning of multicast router ports: enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.13 IP IGMP SNOOPING VLAN ROUTER

Use the **ip igmp snooping vlan router** command to enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF. Use the **"no"** form of this command to disable. You can verify settings by the **show ip igmp snooping vlan** command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **router learn pim-dvmrp**

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **router learn pim-dvmrp**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **router learn pim-dvmrp** **no ip igmp snooping vlan** *{VLAN-LIST}* **router learn pim-dvmrp**
Parameter	*VLAN-LIST* specifies VLAN ID list to set
Default	Default is enabled
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping vlan router test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 router learn pim-dvmrp** Switch# **show ip igmp snooping router**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure t
Switch(config)# ip igmp snooping vlan 1 router learn pim-dvmrp
Switch(config)#
Switch# show ip igmp snooping router

Dynamic Router Table
 VID  |  Port   | Expiry Time(Sec)
------+---------+-----------------


Total Entry 0


Static Router Table
 VID  | Port Mask
------+-----------------------


Total Entry 0


Forbidden Router Table
 VID  | Port Mask
------+-----------------------


Total Entry 0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.14 IP IGMP SNOOPING VLAN FORBIDDEN-PORT

Use the **ip igmp snooping vlan forbidden-port** command to add static non-forwarding port, all known vlan 1 ipv4 group will remove the forbidden ports. Use the **"no"** form of this command to delete forbidden port. You can verify settings by the **show ip igmp snooping forward-all** command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-port** *IF_PORTS*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-port** *IF_PORTS*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-port** *IF_PORTS* **no ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-port** *IF_PORTS*
Parameter	*VLAN-LIST* specifies VLAN ID list to set *IF_PORTS* specifies a port list to set or remove
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping static/forbidden port test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp snooping vlan 1 forbidden-port** gi3-4
	Switch# **show ip igmp snooping forward-all**
	`Switch# configure t`
	`Switch(config)# ip igmp snooping vlan 1 forbidden-port gi3-4`
	`Switch(config)#`
	`Switch# show ip igmp snooping forward-all`
	
	`IGMP Snooping VLAN : 1`
	`IGMP Snooping static port : None`
	`IGMP Snooping forbidden port : gi3-4`
	
	`IGMP Snooping VLAN : 2`
	`IGMP Snooping static port : None`
	`IGMP Snooping forbidden port : None`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.15 IP IGMP SNOOPING VLAN STATIC-PORT

Use the **ip igmp snooping vlan static-port** command to add static forwarding port, all known vlan 1 ipv4 group will add the static ports. Use the **"no"** form of this command to delete static port. You can verify settings by the **show ip igmp snooping forward-all** command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **static-port** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **static-port** *{IF_PORTS}*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **static-port** *{IF_PORTS}* **no ip igmp snooping vlan** *{VLAN-LIST}* **static-port** *{IF_PORTS}*
Parameter	*VLAN-LIST* specifies VLAN ID list to set *IF_PORTS* specifies a port list to set or remove
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping static port test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp snooping vlan 1 static-port gi1-2**
	Switch# **show ip igmp snooping forward-all**
	`Switch(config)# ip igmp snooping vlan 1 static-port gi1-2`
	`Switch(config)# exit`
	`Switch# show ip igmp snooping forward-all`
	
	`IGMP Snooping VLAN : 1`
	`IGMP Snooping static port : gi1-2`
	`IGMP Snooping forbidden port : gi3-4`
	
	`IGMP Snooping VLAN : 2`
	`IGMP Snooping static port : None`
	`IGMP Snooping forbidden port : None`
	
	`IGMP Snooping VLAN : 5`
	`IGMP Snooping static port : None`
	`IGMP Snooping forbidden port : None`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.16 IP IGMP SNOOPING VLAN FORBIDDEN-ROUTER-PORT

Use the **ip igmp snooping vlan forbidden-router-port** command to add static forbidden router port. This will also remove port from static router port. The forbidden router port will not forward receive query packet. Use the **"no"** form of this command to delete forbidden router port. You can verify settings by the show ip igmp snooping router command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-router-port** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-router-port** *{IF_PORTS}*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-router-port** *{IF_PORTS}* **no ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-router-port** *{IF_PORTS}*
Parameter	*VLAN-LIST* specifies VLAN ID list to set *IF_PORTS* specifies a port list to set or remove
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping forbidden test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 forbidden-router-port gi2** Switch# **show ip igmp snooping router**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure t
Switch(config)# ip igmp snooping vlan 1 forbidden-router-port gi2
Switch(config)#
Switch# show ip igmp snooping router

Dynamic Router Table
 VID  |  Port   | Expiry Time(Sec)
------+---------+-----------------


Total Entry 0


Static Router Table
 VID  | Port Mask
------+-----------------------


Total Entry 0


Forbidden Router Table
 VID  | Port Mask
------+-----------------------
    1 | gi2


Total Entry 1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.17 IP IGMP SNOOPING VLAN STATIC-ROUTER-PORT

Use the **ip igmp snooping vlan static-router-port** command to add static router port. All query packets will forward to this port. Use the **"no"** form of this command to delete static router port. You can verify settings by the **show ip igmp snooping router** command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}***static-router-port** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***static-router-port** *{IF_PORTS}*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}***static-router-port** *{IF_PORTS}* **no ip igmp snooping vlan** *{VLAN-LIST}***static-router-port** *{IF_PORTS}*
Parameter	*VLAN-LIST* specifies VLAN ID list to set *IF_PORTS* specifies a port list to set or remove
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping static test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 static-router-port gi1-2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure t
Switch(config)# ip igmp snooping vlan 1 static-router-port gil-2
Switch(config)#
Switch# show ip igmp snooping router

Dynamic Router Table
 VID  |  Port   | Expiry Time(Sec)
------+---------+-----------------


Total Entry 0


Static Router Table
 VID  | Port Mask
------+-----------------------
    1 | gil-2


Total Entry 1


Forbidden Router Table
 VID  | Port Mask
------+-----------------------


Total Entry 0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.18 IP IGMP SNOOPING VLAN STATIC-GROUP

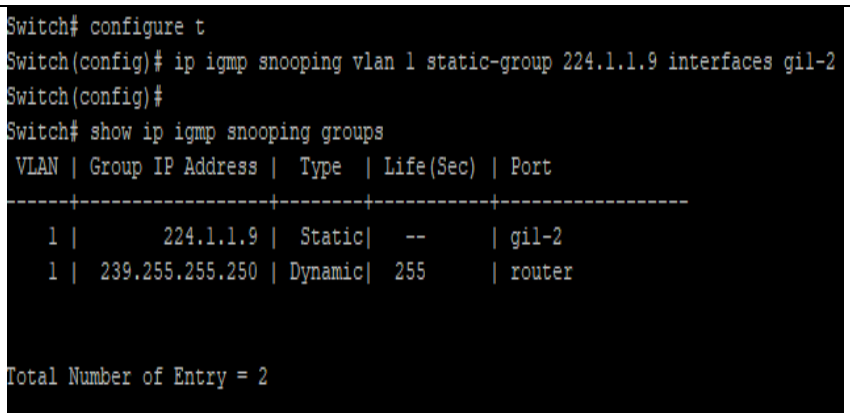
Use the **ip igmp snooping vlan static-group** command to add a static group. The static group will not learn other dynamic ports. If the dynamic group exists, then the static group will overlap the dynamic group. The static group set to valid unless igmp snooping global and vlan enable. Use the **"no"** form of this command to delete a port in static group. If remove the last member of static group, the static group will be delete. You can verify settings by the **show ip igmp snooping group** command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}***static-group** [<ip-addr>] **interfaces** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***static-group** [<ip-addr>] **interfaces** *{IF_PORTS}*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}***static-group** [<ip-addr>] **interfaces** *{IF_PORTS}* **no ip igmp snooping vlan** *{VLAN-LIST}***static-group** [<ip-addr>] **interfaces** *{IF_PORTS}*
Parameter	*VLAN-LIST* specifies VLAN ID list to set *ip-addr* specifies multicast group ipv4 address *IF_PORTS* specifies port list to set or remove
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping static group test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan** 1 **static-group** 224.1.1.9 **interfaces** gi1-2 Switch# **show ip igmp snooping groups**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.



© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.19 IP IGMP SNOOPING VLAN GROUP

Use the **"no ip igmp snooping vlan group"** command to delete a group which could be static or dynamic. You can verify settings by the **show ip igmp snooping group** command.

Switch#**configure terminal**
Switch(config)# **ip igmp snooping vlan {VLAN-LIST}static-group <ip-addr> interfaces GigabitEthernet** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan {VLAN-LIST}static-group <ip-addr> interfaces GigabitEthernet** *{ IF_PORTS}*

Syntax	**ip igmp snooping vlan {VLAN-LIST}static-group <ip-addr> interfaces GigabitEthernet** *{ IF_PORTS}* **no ip igmp snooping vlan {VLAN-LIST}static-group <ip-addr> interfaces GigabitEthernet** *{ IF_PORTS}*
Parameter	VLAN-LIST specifies VLAN ID list to set ip-addr specifies multicast group ipv4 address
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping static group test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp snooping vlan** 1 **static-group** 224.1.1.9 **interfaces GigabitEthernet** 1
	Switch#**show ip igmp snooping groups**
	`Switch# configure t`
	`Switch(config)# ip igmp snooping vlan 1 static-group 224.1.1.9 interfaces GigabitEthernet 1`
	`Switch(config)#`
	`Switch# show ip igmp snooping groups`
	`VLAN | Group IP Address | Type | Life(Sec) | Port`
	`------+-----------------+--------+-----------+-----------------`
	`1 | 224.1.1.9 | Static| -- | gil-2`
	`1 | 239.255.255.250 | Dynamic| 142 | router`
	`Total Number of Entry = 2`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.20 PROFILE RANGE

Use the profile command to generate IGMP profile. You can verify settings by the show ip igmp profile command

Switch#**configure terminal**
Switch(config)# **ip igmp profile** *{Profile-No}*
Switch(config-igmp-profile)#**profile range ip** *<ip-addr>* **[ip-addr] action (permit | deny)**

Syntax	**profile range ip** <ip-addr> **[ip-addr] action (permit | deny)**
Parameter	**<ip-addr>[ip-addr](permit | deny)** Start ipv4 multicast address End ipv4 multicast address **Permit:** allow Multicast address range ip address learning **deny:** do not allow Multicast address range ip address learning
Mode	igmp profile configuration mode

Example	The following example specifies that set ip igmp profile test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp profile 1**
	Switch(config-igmp-profile)# **profile range ip** 224.1.1.1 224.1.1.8 **action permit**
	`Switch# configure t`
	`Switch(config)#  ip igmp profile 1`
	`Switch(config-igmp-profile)# profile range ip 224.1.1.1 224.1.1.8 action permit`
	`Switch(config-igmp-profile)#`
	`Switch# sh ip igmp profile`
	`IP igmp profile index: 1`
	`IP igmp profile action: permit`
	`Range low ip: 224.1.1.1`
	`Range high ip: 224.1.1.8`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.21 IP IGMP PROFILE

Use the **ip igmp profile** command to enter profile configuration. Use the **"no"** form of this command to delete profile. You can verify settings by the show ip igmp profile command.

Switch#**configure terminal**
Switch(config)# **ip igmp profile** *<1-128>*

Switch(config)# **no ip igmp profile** *<1-128>*

Syntax	**ip igmp profile** *<1-128>* **no ip igmp profile** *<1-128>*
Parameter	*<1-128>*specifies profile ID
Mode	Global Configuration

Example	The following example specifies that set ip igmp profile test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp profile 1**
	`Switch# configure t`
	`Switch(config)#  ip igmp profile 1`
	`Switch(config-igmp-profile)#`
	`Switch# sh ip igmp profile`
	`IP igmp profile index: 1`
	`IP igmp profile action: permit`
	`Range low ip: 224.1.1.1`
	`Range high ip: 224.1.1.8`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.22 IP IGMP FILTER

Use the **ip igmp filter** command to bind a profile for port. When the port binds a profile, then the port learning group will update, if the group is not matching the profile rule it will remove the port from the group. Static group is excluded. Use the **"no"** form of this command to delete profile. You can verify settings by the **show ip igmp filter** command.

Switch#**configure terminal**
Switch(config)# **interface** *{Interface-ID}*
Switch(config-if)#**ip igmp filter** *<1-128>*

Switch(config-if)#**no ip igmp filter**

Syntax	**ip igmp filter** *<1-128>* **no ip igmp filter**
Parameter	*<1-128>*specifies profile ID
Mode	Port Configuration
Example	The following example specifies that set ip igmp filter test. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)#**ip igmp filter** 1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure t
Switch(config)#  interface g2
Switch(config-if)# ip igmp filter 1
Switch(config-if)#
Switch# sh ip igmp filter
Port ID  |  Profile ID
---------+--------------
     gi1 : None
     gi2 : 1
     gi3 : None
     gi4 : None
     gi5 : None
     gi6 : None
     gi7 : None
     gi8 : None
     gi9 : None
    gi10 : None
    gi11 : None
    gi12 : None
    gi13 : None
    gi14 : None
    gi15 : None
    gi16 : None
    gi17 : None
    gi18 : None
    gi19 : None
    gi20 : None
    gi21 : None
    gi22 : None
    gi23 : None
    gi24 : None
    gi25 : None
    gi26 : None
    gi27 : None
    gi28 : None
    lag1 : None
    lag2 : None
    lag3 : None
    lag4 : None
    lag5 : None
    lag6 : None
    lag7 : None
    lag8 : None
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.23 IP IGMP MAX-GROUPS

Use the ip igmp max-groups command to limit port learning max group number. When the port has reach limitation, new group will not add this port. Static group is excluded. Use the **"no"** form of this command to restore to default. You can verify settings by the show ip igmp max-groups command.

Switch#**configure terminal**
Switch(config)# **interface** *{Interface-ID}*
Switch(config-if)#**ip igmp max-groups** *<0-1024>*

Switch(config-if)#**no ip igmp max-groups**

Syntax	**ip igmp max-groups** *<0-1024>* **no ip igmp max-groups**
Parameter	*<0-1024>* The maximum number of IGMP groups that an interface can join.
Default	Default is 1024
Mode	Port Configuration
Example	The following example specifies that set ip igmp max-groups test. Switch#**configure terminal** Switch(config)# **interface** g2 Switch(config-if)#**ip igmp max-groups 10**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# ip igmp max-groups 10
Switch(config-if)# exit
Switch(config)# exit
Switch# show ip igmp max-group
Port ID  |  Max Group
---------+-------------
     gi1 : 256
     gi2 : 10
     gi3 : 256
     gi4 : 256
     gi5 : 256
     gi6 : 256
     gi7 : 256
     gi8 : 256
     gi9 : 256
    gi10 : 256
    gi11 : 256
    gi12 : 256
    gi13 : 256
    gi14 : 256
    gi15 : 256
    gi16 : 256
    gi17 : 256
    gi18 : 256
    gi19 : 256
    gi20 : 256
    gi21 : 256
    gi22 : 256
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.24 IP IGMP MAX-GROUPS ACTION

Use the ip igmp max-groups action command to set the action when the numbers of groups reach the limitation. Use the **"no"** form of this command to restore to default. You can verify settings by the show ip igmp max-groups command.

Switch#**configure terminal**
Switch(config)# **interface** *{Interface-ID}*
Switch(config-if)# **ip igmp max-groups action (deny | replace)**

Syntax	**ip igmp max-groups action (deny | replace)**
Parameter	**(deny | replace) Deny:** current port igmp group arrived max-groups, don't add group. **Replace:** current port igmp group arrived max-groups, remove port for rand group, and add port to new group.
Default	Default action is deny
Mode	Port Configuration

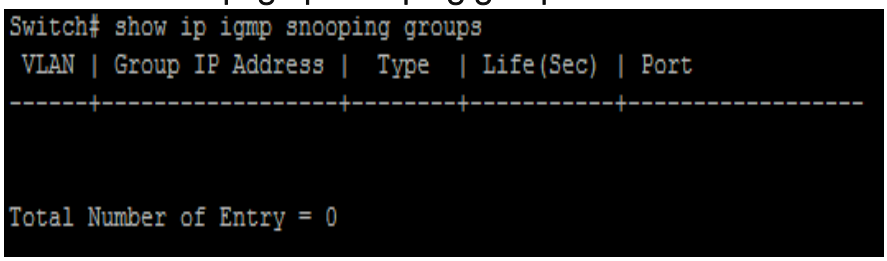
Example	The following example specifies that set action replace test.
	Switch#**configure terminal**
	Switch(config)#**interface** g2
	Switch(config-if)#**ip igmp max-groups action replace**
	
	Switch# **show ip igmp max-group action interfaces** GigabitEthernet 2
	`Switch# configure terminal`
	`Switch(config)# interface g2`
	`Switch(config-if)# ip igmp max-groups action replace`
	`Switch(config-if)#`
	`Switch# show ip igmp max-group action interfaces GigabitEthernet 2`
	`Port ID | Max-groups Action`
	`---------+--------------------`
	`gi2 : replace`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.25 CLEAR IP IGMP SNOOPING GROUPS

This command will clear the ip igmp groups for dynamic or static or all of type. You can verify settings by the show ip igmp snooping groups command.

Switch# clear ip igmp snooping groups [(dynamic | static)]

Syntax	clear ip igmp snooping groups [(dynamic | static)]
Parameter	none Clear ip igmp groups include dynamic and static (dynamic | static) Ip igmp group type is dynamic or static
Mode	Privileged EXEC
Example	The following example specifies that clear ip igmp snooping groups test. Switch# clear ip igmp snooping groups Switch# show ip igmp snooping groups 

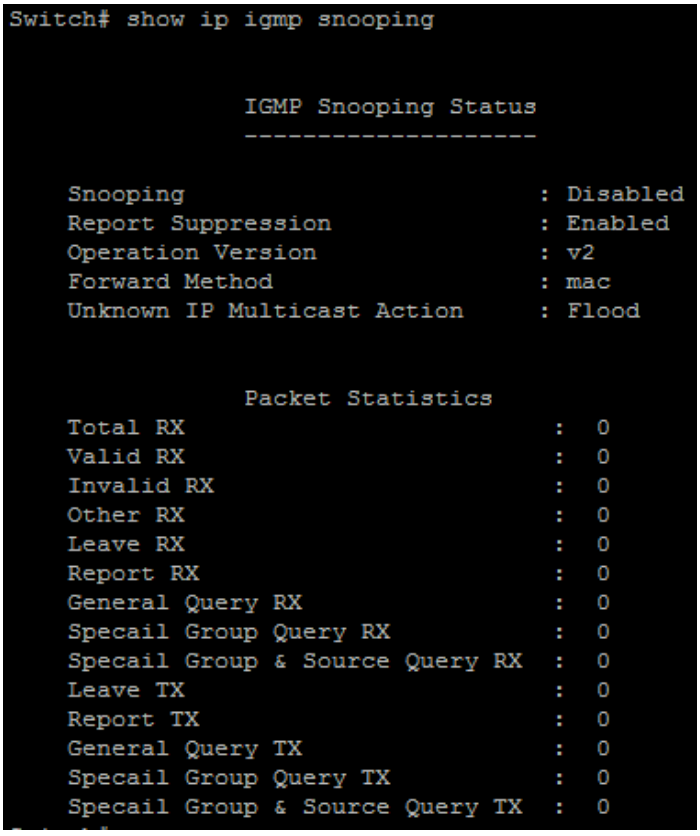
```
Switch# show ip igmp snooping groups
 VLAN | Group IP Address |  Type  | Life(Sec) | Port
------+------------------+--------+-----------+-----------------


Total Number of Entry = 0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.26 CLEAR IP IGMP SNOOPING STATISTICS

This command will clear the igmp statistics. You can verify settings by the show ip igmp snooping command.

Switch# clear ip igmp snooping statistics

Syntax	clear ip igmp snooping statistics
Mode	Privileged EXEC
Example	The following example specifies that clear ip igmp snooping statistics test. Switch# clear ip igmp snooping statistics Switch# show ip igmp snooping 

```
Switch# show ip igmp snooping


                IGMP Snooping Status
                --------------------

    Snooping                          : Disabled
    Report Suppression                : Enabled
    Operation Version                 : v2
    Forward Method                    : mac
    Unknown IP Multicast Action       : Flood


                Packet Statistics
    Total RX                          :  0
    Valid RX                          :  0
    Invalid RX                        :  0
    Other RX                          :  0
    Leave RX                          :  0
    Report RX                         :  0
    General Query RX                  :  0
    Specail Group Query RX            :  0
    Specail Group & Source Query RX   :  0
    Leave TX                          :  0
    Report TX                         :  0
    General Query TX                  :  0
    Specail Group Query TX            :  0
    Specail Group & Source Query TX   :  0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.27 SHOW IP IGMP SNOOPING GROUPS COUNTERS

This command will display the **ip igmp snooping group counters** include static group.

Switch# **show ip igmp snooping group counters**

Syntax	**show ip igmp snooping group counters**
Mode	Privileged EXEC

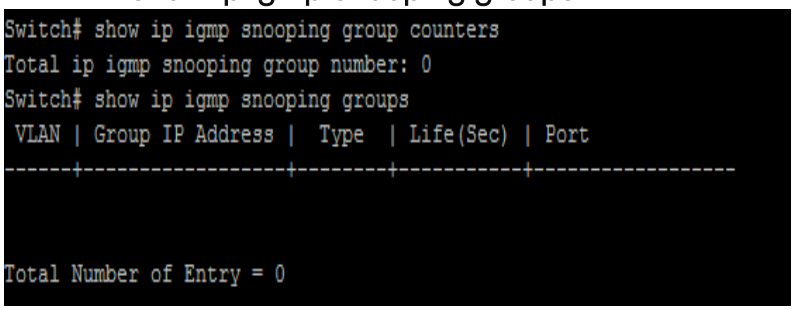
Example	The following example specifies that display ip igmp snooping group counter test.
	Switch# **show ip igmp snooping group counters**
	`Switch# show ip igmp snooping group counters`
	`Total ip igmp snooping group number: 0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.28 SHOW IP IGMP SNOOPING GROUPS

This command will display the ip igmp groups for dynamic or static or all of type.

Switch# **show ip igmp snooping groups [(dynamic | static)]**

Syntax	**show ip igmp snooping groups [(dynamic | static)]**
Parameter	**none** Show ip igmp groups include dynamic and static **(dynamic | static)** Display Ip igmp group type is dynamic or static
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping groups. Switch**# show ip igmp snooping groups**  Switch# show ip igmp snooping group counters Total ip igmp snooping group number: 0 Switch# show ip igmp snooping groups VLAN | Group IP Address | Type | Life(Sec) | Port ------+-----------------+--------+-----------+----------------- Total Number of Entry = 0

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.29 SHOW IP IGMP SNOOPING ROUTER

This command will display the ip igmp router info.

Switch# **show ip igmp snooping router [(dynamic | forbidden |static)]**

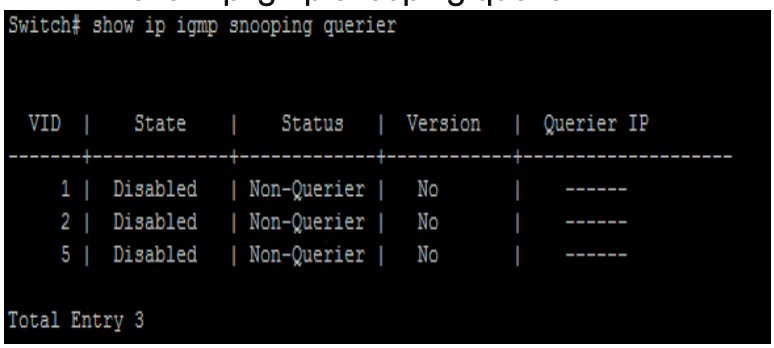
Syntax	**show ip igmp snooping router [(dynamic | forbidden |static)]**
Parameter	**none** Show ip igmp router include dynamic and static and forbidden **(dynamic | forbidden | static)** Display Ip igmp router info for different type
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping router. Switch# **show ip igmp snooping router** `Switch# show ip igmp snooping router` `Dynamic Router Table` ` VID	Port	Expiry Time(Sec)` `------+---------+-----------------`  `Total Entry 0`  `Static Router Table` ` VID	Port Mask` `------+------------------------` ` 1	gi1-2`  `Total Entry 1`  `Forbidden Router Table` ` VID	Port Mask` `------+------------------------`  `Total Entry 0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.30 SHOW IP IGMP SNOOPING QUERIER

This command will display all the static vlan ip igmp, querier info.

Switch# **show ip igmp snooping querier**

Syntax	**show ip igmp snooping querier**
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping querier test. Switch# **show ip igmp snooping querier** 

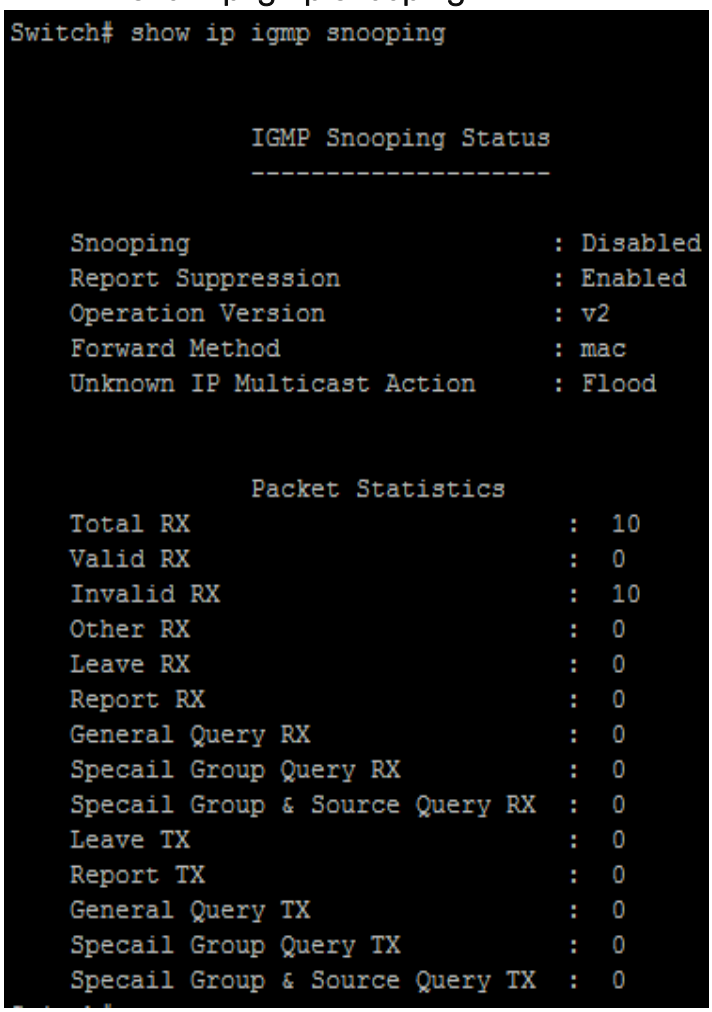
```
Switch# show ip igmp snooping querier


  VID  |    State    |    Status   | Version   |  Querier IP
-------+-------------+-------------+-----------+-------------------
     1 |  Disabled   | Non-Querier |   No      |    ------
     2 |  Disabled   | Non-Querier |   No      |    ------
     5 |  Disabled   | Non-Querier |   No      |    ------

Total Entry 3
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.31 SHOW IP IGMP SNOOPING

This command will display ip igmp snooping global info.

Switch# **show ip igmp snooping**

Syntax	**show ip igmp snooping**
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping test. Switch# **show ip igmp snooping** 

```
Switch# show ip igmp snooping


                IGMP Snooping Status
                --------------------

    Snooping                        : Disabled
    Report Suppression              : Enabled
    Operation Version               : v2
    Forward Method                  : mac
    Unknown IP Multicast Action     : Flood


                Packet Statistics
    Total RX                         :  10
    Valid RX                         :  0
    Invalid RX                       :  10
    Other RX                         :  0
    Leave RX                         :  0
    Report RX                        :  0
    General Query RX                 :  0
    Specail Group Query RX           :  0
    Specail Group & Source Query RX  :  0
    Leave TX                         :  0
    Report TX                        :  0
    General Query TX                 :  0
    Specail Group Query TX           :  0
    Specail Group & Source Query TX  :  0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.32 SHOW IP IGMP SNOOPING VLAN

This command will display ip igmp snooping vlan info.

Switch# **show ip igmp snooping vlan** *[VLAN-LIST]*

Syntax	**show ip igmp snooping vlan** [*VLAN-LIST*]
Parameter	**none** Show all ip igmp snooping vlan info *[VLAN-LIST]* Show specifies vlan ip igmp snooping info
Mode	Privileged EXEC

Example	The following example specifies that show ip igmp snooping vlan test.
	Switch# **show ip igmp snooping vlan** 1
	`Switch# show ip igmp snooping vlan 1`
	
	`IGMP Snooping is globaly disabled`
	`IGMP Snooping VLAN 1 admin : enabled`
	`IGMP Snooping operation mode : disabled`
	`IGMP Snooping robustness: admin 2 oper 2`
	`IGMP Snooping query interval: admin 100 sec oper 125 sec`
	`IGMP Snooping query max response : admin 12 sec oper 10 sec`
	`IGMP Snooping last member query counter: admin 2  oper 2`
	`IGMP Snooping last member query interval: admin 1 sec  oper 1 sec`
	`IGMP Snooping immediate leave: disabled`
	`IGMP Snooping automatic learning of multicast router ports: enabled`

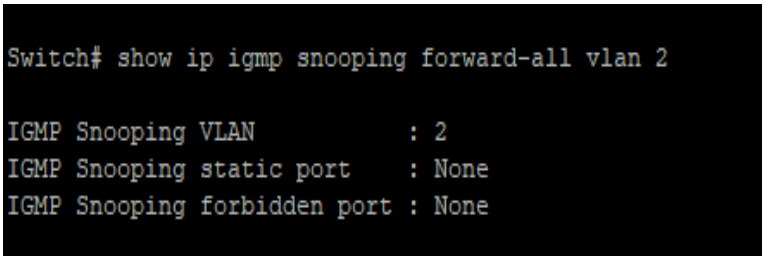
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.33 SHOW IP IGMP SNOOPING FORWARD-ALL

This command will display ip igmp snooping forward all info.

Switch#**show ip igmp snooping forward-all** ***[vlan*** *VLAN-LIST]*

Syntax	**show ip igmp snooping forward-all** [**vlan** *VLAN-LIST*]
Parameter	**none** Show all ip igmp snooping vlan forward-all info [**vlan** *VLAN-LIST*] Show specifies vlan of ip igmp forward info.
Mode	Privileged EXEC

Example	The following example specifies that show ip igmp snooping forward-all test.
	Switch# **show ip igmp snooping forward-all vlan 2**
	 
	`Switch# show ip igmp snooping forward-all vlan 2`
	`IGMP Snooping VLAN : 2`
	`IGMP Snooping static port : None`
	`IGMP Snooping forbidden port : None`

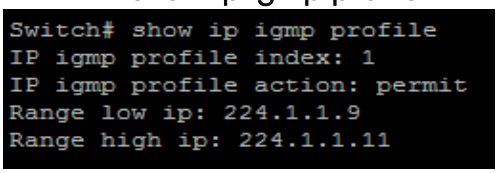
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.34 SHOW IP IGMP PROFILE

This command will display ip igmp profile info.

Switch# **show ip igmp profile** *[<1-128>]*

Syntax	**show ip igmp profile** [*<1-128>*]
Parameter	**none** Show all ip igmp snooping profile info [*<1-128>*] Show specifies index profile info
Mode	Privileged EXEC

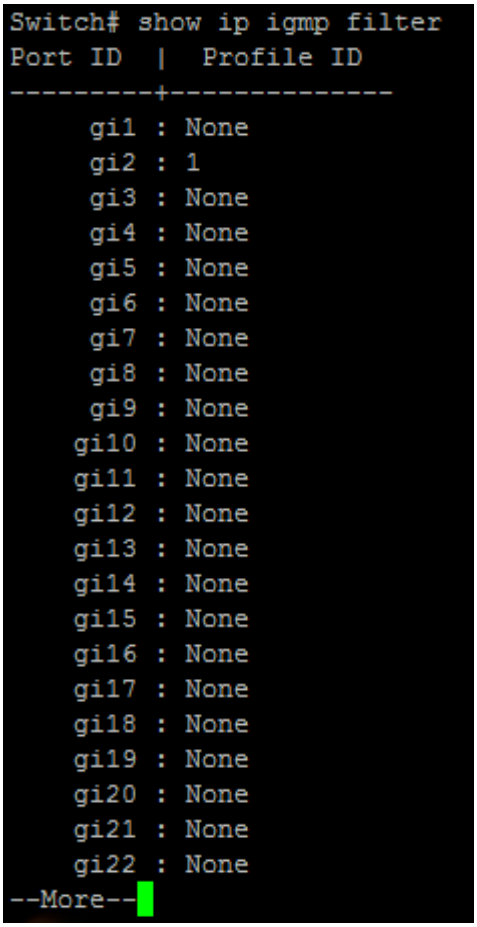
Example	The following example specifies that show ip igmp profile test.
	Switch# **show ip igmp profile**
	 
	`Switch# show ip igmp profile`
	`IP igmp profile index: 1`
	`IP igmp profile action: permit`
	`Range low ip: 224.1.1.9`
	`Range high ip: 224.1.1.11`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.35 SHOW IP IGMP FILTER

This command will display ip igmp port filter info.

Switch# **show ip igmp filter** *[interfaces IF_PORTS]*

Syntax	**show ip igmp filter** [**interfaces** *IF_PORTS*]
Parameter	**none** Show all port filter [**interfaces***IF_PORTS*] Show specifies ports filter
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp filter test. Switch# **show ip igmp filter** 

```
Switch# show ip igmp filter
Port ID  |  Profile ID
---------+--------------
     gi1 : None
     gi2 : 1
     gi3 : None
     gi4 : None
     gi5 : None
     gi6 : None
     gi7 : None
     gi8 : None
     gi9 : None
    gi10 : None
    gi11 : None
    gi12 : None
    gi13 : None
    gi14 : None
    gi15 : None
    gi16 : None
    gi17 : None
    gi18 : None
    gi19 : None
    gi20 : None
    gi21 : None
    gi22 : None
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.36 SHOW IP IGMP MAX-GROUP

This command will display ip igmp port max-group.

Switch# **show ip igmp max-group** ***[interfaces** IF_PORTS]*

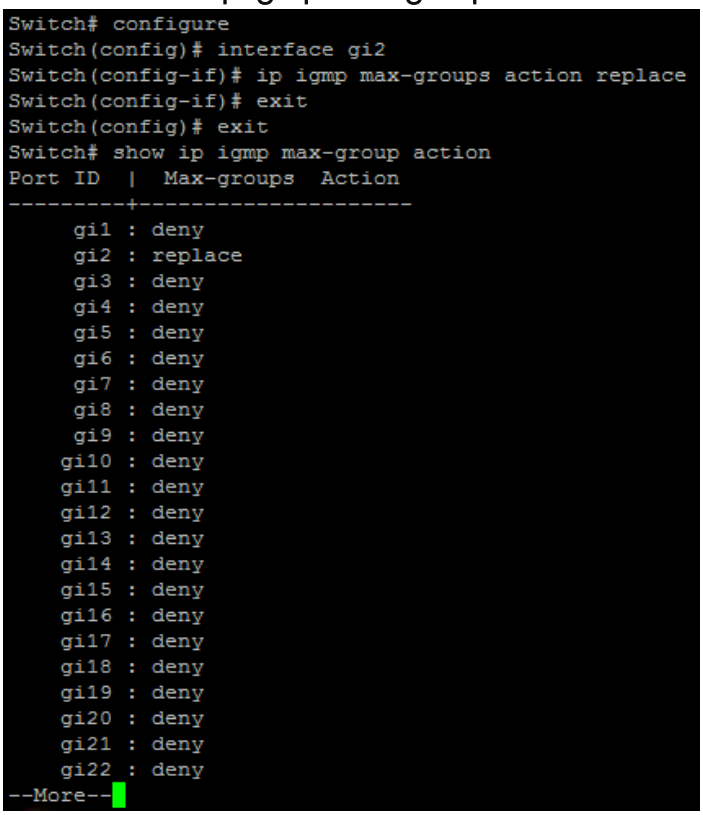
Syntax	**show ip igmp max-group** [**interfaces** *IF_PORTS*]
Parameter	**none** Show all port max-group ***[interfaces** IF_PORTS]* Show interfaces
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp max-group test. Switch#**configure terminal** Switch(config)#**interface** *{Interface-ID}* Switch(config-if)#**ip igmp max-groups** 50 Switch# **show ip igmp max-group** `Switch(config)# interface GigabitEthernet 2` `Switch(config-if)# ip igmp max-groups 50` `Switch(config-if)# exit` `Switch(config)# exit` `Switch# show ip igmp max-group` `Port ID	Max Group` `---------+--------------` `gi1 : 256` `gi2 : 50` `gi3 : 256` `gi4 : 256` `gi5 : 256` `gi6 : 256` `gi7 : 256` `gi8 : 256` `gi9 : 256` `gi10 : 256` `gi11 : 256` `gi12 : 256` `gi13 : 256` `gi14 : 256` `gi15 : 256` `gi16 : 256` `gi17 : 256` `gi18 : 256` `gi19 : 256` `gi20 : 256` `gi21 : 256` `gi22 : 256`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

10.37 SHOW IP IGMP MAX-GROUP ACTION

This command will display ip igmp port max-group action.

Switch# **show ip igmp max-group action** ***[interfaces*** *IF_PORTS]*

Syntax	**show ip igmp max-group action** [**interfaces** *IF_PORTS*]
Parameter	**none** Show all port max-group action [**interfaces***IF_PORTS*] Show specifies ports max-group action
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp max-group action test. Switch#**configure terminal** Switch(config)#**interface** gi2 Switch(config-if)#**ip igmp max-groups action replace** Switch# **show ip igmp max-group action** 

```
Switch# configure
Switch(config)# interface gi2
Switch(config-if)# ip igmp max-groups action replace
Switch(config-if)# exit
Switch(config)# exit
Switch# show ip igmp max-group action
Port ID   |  Max-groups  Action
---------+---------------------
     gi1 : deny
     gi2 : replace
     gi3 : deny
     gi4 : deny
     gi5 : deny
     gi6 : deny
     gi7 : deny
     gi8 : deny
     gi9 : deny
    gi10 : deny
    gi11 : deny
    gi12 : deny
    gi13 : deny
    gi14 : deny
    gi15 : deny
    gi16 : deny
    gi17 : deny
    gi18 : deny
    gi19 : deny
    gi20 : deny
    gi21 : deny
    gi22 : deny
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

11. 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. Any IP traffic coming into the interface with a source IP address other than that assigned (via DHCP or static configuration) will be filtered out on the untrusted Layer 2 ports.

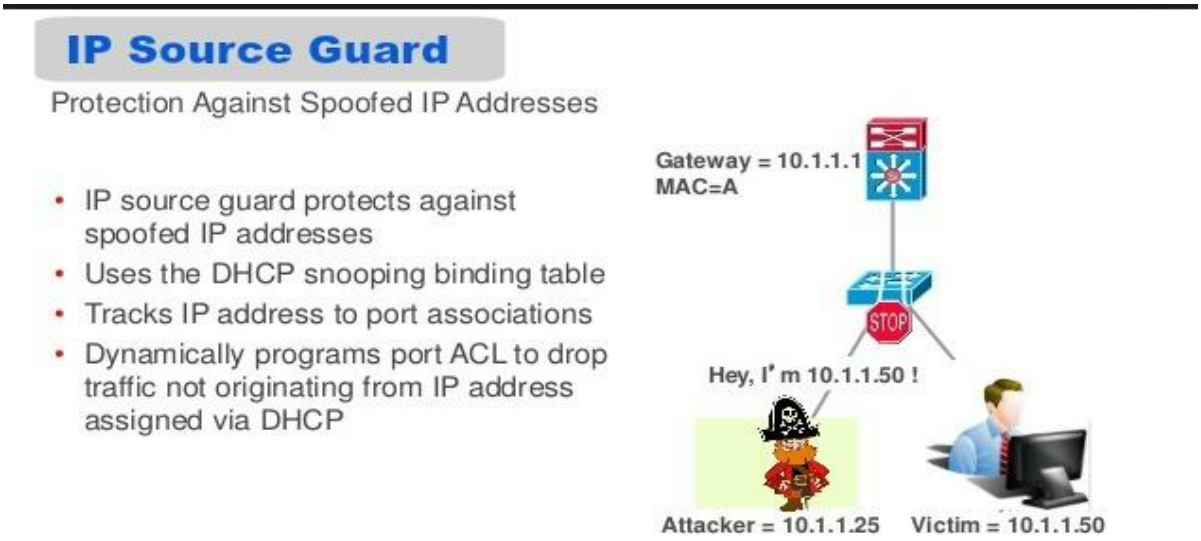


Fig 11.1 IP Source Guard Concept

The IP Source Guard feature is enabled in combination with the DHCP snooping feature on untrusted Layer 2 interfaces. It builds and maintains an IP source binding table that is learned by DHCP snooping or manually configured (static IP source bindings). An entry in the IP source binding table contains the IP address and the associated MAC and VLAN numbers. The IP Source Guard is supported on Layer 2 ports only, including access and trunk ports.

IP Source Guard prevents IP and/or MAC address spoofing attacks on untrusted layer two interfaces. When IP source guard is enabled, all traffic is blocked except for DHCP

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

packets. Once the host gets an IP address through DHCP, only the DHCP-assigned source IP address is permitted. You can also configure a static binding instead of using DHCP.

Comparison between DAI and IP Source Guard:

Dynamic ARP Inspection	IP Source Guard
- DHCP Snooping creates IP to MAC bindings - DAI Intercepts all ARP requests - Intercepted ARP is validated against IP to MAC binding - Does not switch ARP packets with invalid source address - Used primarily to prevent MITM attacks	- Initially all traffic blocked - Snoops DHCP Address - Creates IP to MAC binding - Installs per port VACL to deny traffic other than snooped source - Protects against IP and MAC spoofing - Will not prevent a MITM attack
Dynamic ARP Inspection	IP Source Guard

Fig 11.2 Comparison between DAI and IP Source Guard

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

11.1 IP SOURCE VERIFY

Uses the ip source verify command to enable IP Source Guard function. Default IP Source Guard filter source IP address. The **"mac-and-ip"** filters not only source IP address but also source MAC address. Use the no form of this command to disable. You can verify settings by the show ip source interfaces command.

Switch#**configure terminal**
Switch(config)# **interface** *{Interface-ID}*
Switch(config-if)# **ip source verify** ***[mac-and-ip]***

Switch(config-if)# **no ip source verify**

Syntax	**ip source verify** ***[mac-and-ip]*** **no ip source verify**
Parameter	**mac-and-ip** Verify by mac and ip address bundle
Default	IP Source Guard is disabled on interface. Default is that verifying ip address only.
Mode	Port Configuration
Example	The example shows how to enable IP Source Guard with source IP address filtering on interface gi1. Switch#configure terminal Switch(config)# **interface** gi2 Switch(config-if)# **ip source verify** Switch(config-if)# **ip source verify mac-and-ip** Switch(config-if)# **do show ip source interfaces gi1-2** `Switch(config)# interface gi2` `Switch(config-if)# ip source verify mac-and-ip` `Switch(config-if)# do show ip source interfaces gi1-2` ` Port	Status	Max Entry	Current Entry` `--------+----------------+-----------+---------------` ` gi1	disabled	No Limit	0` ` gi2	Verify MAC+IP	No Limit	0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

11.2 IP SOURCE BINDING

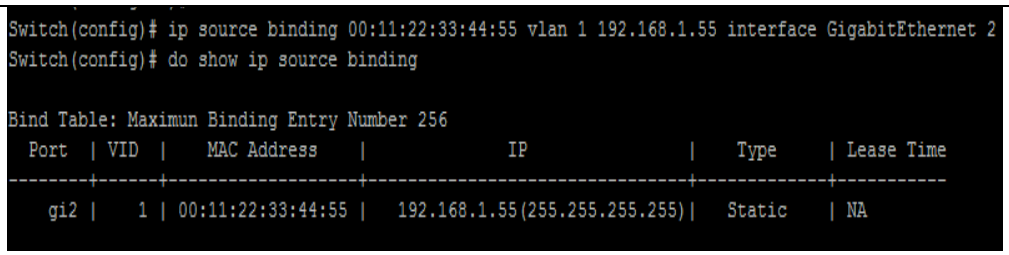
Use the ip source binding command to create a static IP source binding entry has an IP address, its associated MAC address, VLAN ID interface. Use the **"no"** form of this command to delete static entry. You can verify settings by the **"show ip source binding"**command.

Switch#**configure terminal**
Switch(config)# **ip source binding** {A:B:C:D:E:F} **vlan** *<1-4094> (*A.B.C.D) **interface** *{IF_PORT}*

Switch(config)# **no ip source binding** {A:B:C:D:E:F} **vlan** *<1-4094> (*A.B.C.D) **interface** *{IF_PORT}*

Syntax	**ip source binding** {A:B:C:D:E:F} **vlan** *<1-4094> (*A.B.C.D) **interface** *{IF_PORT}* **no ip source binding** {A:B:C:D:E:F} **vlan** *<1-4094> (*A.B.C.D) **interface** *{IF_PORT}*
Parameter	A:B:C:D:E:F Specify a MAC address of a binding entry VLAN *<1-4094>*Specify a VLAN ID of a binding entry A.B.C.D Specify IP address and MASK of a binding entry. *IF_PORT* Specify interface of a binding entry.
Mode	Global Configuration
Example	The example shows how to add a static IP source binding entry. Switch#**configure terminal** Switch(config)# **ip source binding** 00:11:22:33:44:55 **vlan** 1 192.168.1.55 **interface** GigabitEthernet 1 Switch(config)# **do show ip source binding**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

11.3 SHOW IP SOURCE INTERFACE

Use the show ip source interface command to show settings of IP Source Guard of interface.

Switch# **show ip source interfaces** *{IF_PORTS}*

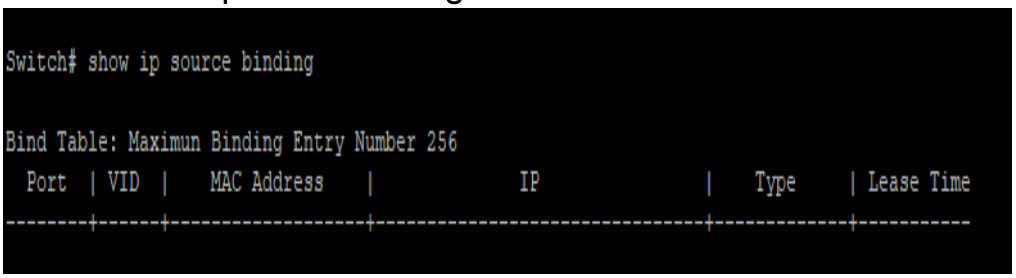
Syntax	**show ip source interfaces** *IF_PORTS*
Parameter	*IF_PORTS* specifies ports to show
Mode	Privileged EXEC
Example	The example shows how to show settings of IP Source Guard of interface gi1 Switch# **show ip source interfaces gi2** `Switch# show ip source interfaces gi2` ` Port	Status	Max Entry	Current Entry` `--------+----------------+-----------+--------------` ` gi2	disabled	No Limit	0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

11.4 SHOW IP SOURCE BINDING

Use the show ip source binding command to show binding entries of IP Source Guard.

Switch# **show ip source binding** *[(dynamic|static)]*

Syntax	**show ip source binding [(dynamic|static)]**
Parameter	dynamic Show entries that added by DHCP snooping learn static Show entries that added by user
Mode	Privileged EXEC
Example	The example shows how to show static binding entries of IP Source Guard. Switch# **show ip source binding** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

12. LINK AGGREGATION

Use the link aggregation feature to aggregate one or more Ethernet interfaces to form a logical point-to-point link, known as a LAG, virtual link, or bundle. The MAC client can treat this virtual link like a single link. Link aggregation increases bandwidth, provides graceful degradation as failure occurs, and increases availability. It provides network redundancy by load-balancing traffic across all available links. If one of the links fails, the system automatically load-balances traffic across all remaining links.

LACP, a subcomponent of IEEE 802.3ad, provides additional functionality for link aggregation groups (LAGs). When LACP is not enabled, a local LAG might attempt to transmit packets to a remote single interface, which causes the communication to fail. When LACP is enabled, a local LAG cannot transmit packets unless a LAG with LACP is also configured on the remote end of the link.

A typical LAG deployment includes aggregate trunk links between an access switch and a distribution switch or customer edge (CE) device.

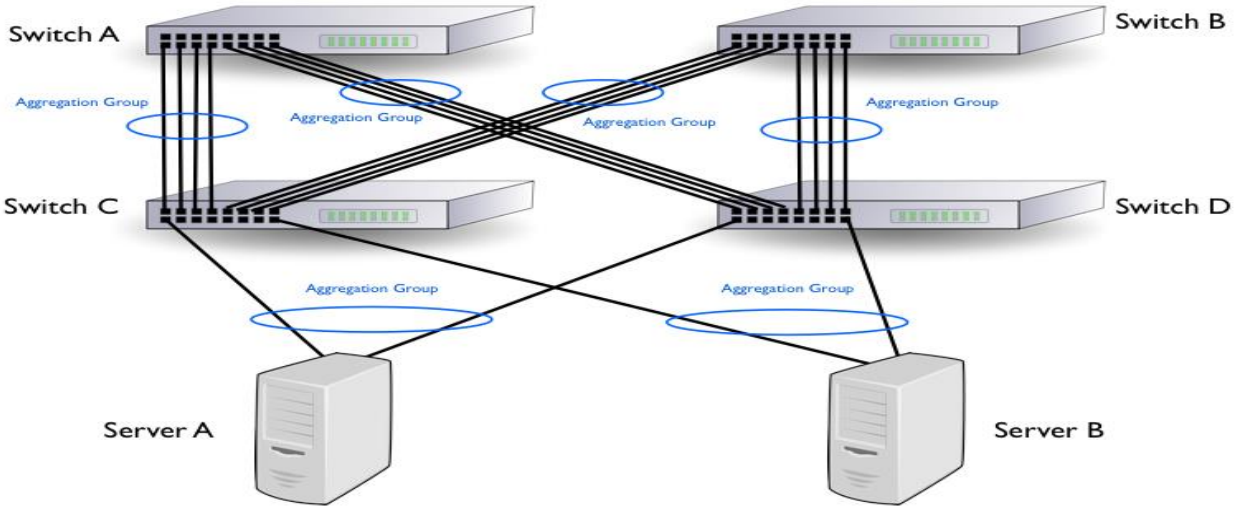


Fig 12.1 Link aggregation Concept

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

12.1 LAG

Link aggregation group function allows you to aggregate multiple physical ports into one logic port to increase bandwidth. This command makes normal port join into the specific LAG logic port with static or dynamic mode. Use **"no lag"** to leave the LAG logic port.

Switch#**configure terminal**
Switch(config)# **lag load-balance (src-dst-mac | src-dst-mac-ip)**
Switch(config)# **interface** *{Inteface-ID}*
Switch(config-if)# **lag** *<1-8>* **mode (static | active | passive)**

Switch(config-if)# **no lag**

Note:Use static mode to enable LAG on Ports.

Syntax	**lag** *<1-8>* **mode (static | active | passive)** **no lag**
Parameter	*<1-8>* Specify the LAG id for the interface **static** Specify the LAG to be static mode and join the interface into this LAG. **active** Specify the LAG to be dynamic mode and join the interface into this LAG with LACP active port. **passive** Specify the LAG to be dynamic mode and join the interface into this LAG with LACP passive port
Mode	Interface Configuration
Example	This example shows how to create a dynamic LAG and join fa1-fa3 to this LAG. Switch#**configure terminal** Switch(config)# **lag load-balance src-dst-mac-ip** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **lag** 1 **mode static** Switch(config)# **interface** GigabitEthernet 3 Switch(config-if)# **lag** 1 **mode static** To show current LAG status. Use command **show lag**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Switch# **show lag**

```
Switch# show lag
Load Balancing: src-dst-mac-ip.

 Group ID |  Type  |          Ports
----------+--------+-----------------------------------------
   1      | Static |  Active: gil,gi3
   2      | ------ |
   3      | ------ |
   4      | ------ |
   5      | ------ |
   6      | ------ |
   7      | ------ |
   8      | ------ |
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

12.2 LAG LOAD-BALANCE

Link aggregation **group** port should transmit packets spread to all ports to balance traffic loading. There are two algorithms supported and this command allows you to select the algorithm.

Switch#**configure terminal**
Switch(config)# **lag load-balance (src-dst-mac | src-dst-mac-ip)**

Switch(config)# **no lag load-balance**

Syntax	**lag load-balance (src-dst-mac | src-dst-mac-ip)** **no lag load-balance**
Parameter	**src-dst-mac** Specify algorithm to balance traffic by using source and destination MAC address for all packets. **src-dst-mac-ip** Specify algorithm to balance traffic by using source and destination IP address for IP packets and using source and destination MAC address for non-IP packets.
Default	Default load balance algorithm is src-dst-mac
Mode	Global Configuration

Example	This example shows how to change load balance algorithm to src-dst-mac-ip.
	Switch#**configure terminal**
	Switch(config)# **lag load-balance src-dst-mac-ip**
	To show current load balance algorithm use **show lag.**
	Switch# **show lag**
	`Switch# configure terminal`
	`Switch(config)# lag load-balance src-dst-mac-ip`
	`Switch(config)#`
	`Switch# show lag`
	`Load Balancing: src-dst-mac-ip.`
	`Group ID | Type | Ports`
	`1 | Static | Active: gi1,gi3`
	`2 | ------ |`
	`3 | ------ |`
	`4 | ------ |`
	`5 | ------ |`
	`6 | ------ |`
	`7 | ------ |`
	`8 | ------ |

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

12.3 LACP

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

Two types of LAGs are supported:

Static LAG: A LAG is static if the LACP is disabled on it. The group of ports assigned to a static LAG are always active members.

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

Load Balancing Traffic forwarded to a LAG is load-balanced across the active member ports, thus achieving an effective bandwidth close to the aggregate bandwidth of all the active member ports of the LAG. Traffic load balancing over the active member ports of a LAG is managed by a hash-based distribution function that distributes Unicast and Multicast traffic based on Layer 2 or Layer 3 packet header information.

The device supports two modes of load balancing:

MAC Addresses: Based on the Destination and Source MAC addresses of all packets.

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

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

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

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

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.

Switch#**configure terminal**
Switch(config)# **lag load-balance (src-dst-mac | src-dst-mac-ip)**
Switch(config)# **interface** *{Inteface-ID}*
Switch(config-if)# **lag** *<1-8>* **mode (static | active | passive)**

Switch(config-if)# **no lag**

Note:Use active and passive mode to enable LACP on Ports.

Syntax	**lag** *<1-8>* **mode (static | active | passive)** **no lag**
Parameter	*<1-8>* Specify the LAG id for the interface **static** Specify the LAG to be static mode and join the interface into this LAG. **active** Specify the LAG to be dynamic mode and join the interface into this LAG with LACP active port. **passive** Specify the LAG to be dynamic mode and join the interface into this LAG with LACP passive port
Mode	Interface Configuration
Example	This example shows how to create a dynamic LAG and join fa1-fa3 to this LAG. Switch#**configure terminal** Switch(config)# **lag load-balance src-dst-mac-ip** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **lag 1 mode active** Switch(config)# **interface** GigabitEthernet 3 Switch(config-if)# **lag 1 mode active**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

This example shows how to show current LAG status.

Switch# **show lag**

```
Switch#  sh lag
Load Balancing: src-dst-mac-ip.

 Group ID |  Type  |          Ports
----------+--------+-----------------------------------------
   1      |  LACP  |  Active: gi1,gi3
   2      | ------ |
   3      | ------ |
   4      | ------ |
   5      | ------ |
   6      | ------ |
   7      | ------ |
   8      | ------ |
```

Switch# **show lacp neighbor**

```
Switch# sh lacp neighbor
  <cr>
  detail  Detailed neighbor information
Switch# sh lacp neighbor
Flags:  S - Device is sending Slow LACPDUs
        F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:

                LACP port                       Admin  Oper   Port    Port
Port      Flags   Priority  Dev ID         Age    key    Key    Number  State
gi1       SA      1         8c02.fa02.003e  75s    0x3e8  0x3e8  0x1     0x3d
gi3       SA      1         8c02.fa02.003e  74s    0x3e8  0x3e8  0x5     0x3d
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

12.3 LACP PORT-PRIORITY

LACP port priority is used for two connected DUT to select aggregation ports. Lower port priority value has higher priority. And the port with higher priority will be selected into LAG first.

Switch#**configure terminal**
Switch(config)# **interface** { Inteface-ID}
Switch(config-if)# **lacp port-priority***<1-65535>*

Switch(config-if)# **no lacp port-priority**

Syntax	**lacp port-priority***<1-65535>* **no lacp port-priority**
Parameter	*<1-65535>*Specify port priority value
Default	Default port priority is 1.
Mode	Interface Configuration
Example	This example shows how to configure interface GigabitEthernet 3 with lacp port priority to 1. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 3 Switch(config-if)# **lacp port-priority** 1 Switch# **show lacp neighbor detail**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# sh lacp neighbor detail
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode        P - Device is in Passive mode

Channel group 1

Partner's information


          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
gi1       32768, 8c02.fa02.003e 0x1             70s         SA

          LACP Partner         Partner         Partner
          Port Priority        Oper Key        Port State
          1                    0x3e8           0x3d

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No            No

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
gi3       32768, 8c02.fa02.003e 0x5             69s         SA

          LACP Partner         Partner         Partner
          Port Priority        Oper Key        Port State
          1                    0x3e8           0x3d

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No            No
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

12.4 LACP SYSTEM-PRIORITY

LACP system priority is used for two connected DUT to select master switch. Lower system priority value has higher priority. And the DUT with higher priority can decide which ports are able to join the LAG. Use **"no lacp system-priority"** to restore to the default priority value.

Switch#**configure terminal**
Switch(config)# **lacp system-priority** *<1-65535>*

Switch(config)# **no lacp system-priority**

Syntax	**lacp system-priority** *<1-65535>* **no lacp system-priority**
Parameter	*<1-65535>*Specify system priority value
Default	Default system priority is 32768.
Mode	Global Configuration
Example	This example shows how to configure lacp system priority to 32768. Switch#**configure terminal** Switch(config)# **lacp system-priority** 32768 Switch# **show lacp neighbor detail**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# sh lacp neighbor detail
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode        P - Device is in Passive mode

Channel group 1

Partner's information


          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
gi1       32768, 8c02.fa02.003e 0x1             72s         SA

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          1                     0x3e8           0x3d

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No            No

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
gi3       32768, 8c02.fa02.003e 0x5             71s         SA

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          1                     0x3e8           0x3d

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No            No
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

12.5 LACP TIMEOUT

LACP need to send LACP packet to partner switch to check the link status. This command configures the interval of sending LACP packets.

Switch#**configure terminal**
Switch(config)# **interface** *{Inteface-ID}*
Switch(config-if)# **lacp timeout (long | short)**

Switch(config-if)# **no lacp timeout**

Syntax	**lacp timeout (long | short)** **no lacp timeout**
Parameter	**long** Send LACP packet every 30 seconds. **short** Send LACP packet every 1 second
Default	Default LACP timeout is long.
Mode	Interface Configuration
Example	This example shows how to configure interface GigabitEthernet 3 lacp timeout to long. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 3 Switch(config-if)# **lacp timeout long** Switch# **show lacp internal detail**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# sh lacp internal detail
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode        P - Device is in Passive mode
Channel group 1

Actor (internal) information


          Actor                Actor                      Actor
Port      System ID            Port Number     Age        Flags
gil       32768, 00e0.4c00.0000 0x1                       SA

          LACP Actor           Actor           Actor
          Port Priority        Oper Key        Port State
          1                    0x3e8           0x3d

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No            No

          Actor                Actor                      Actor
Port      System ID            Port Number     Age        Flags
gi3       32768, 00e0.4c00.0000 0x3                       SA

          LACP Actor           Actor           Actor
          Port Priority        Oper Key        Port State
          1                    0x3e8           0x3d

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No            No
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

12.6 SHOW LACP

Use **"show lacp sys-id"** command to displays the system identifier that is being used by LACP. The system identifier is made up of the LAPC system priority and the switch MAC address.

Use **"show lacp counter"** command to display LACP statistic information. Use **"show lacp internal"** command to display local information.

Use **"show lacp neighbor"** command to display remote Information State of the specific port. These are the allowed values:

bndl Port is attached to an aggregator and bundled with other ports.

Susp Port is in a suspended state; it is not attached to any aggregator.

hot-sby Port is in a hot-standby state.

1indiv Port is incapable of bundling with any other port.

1indep Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).

Down-Port is down.

State variables for the port, encoded as individual bits within a single octet with these meanings:

- bit0 LACP_Activity
- bit1 LACP_Timeout
- bit2 Aggregation
- bit3 Synchronization
- bit4 Collecting
- bit5 Distributing
- bit6 Defaulted
- bit7 Expired

Switch# **show lacp sys-id**
Switch# **show lacp** [*<1-8>*] **counters**
Switch# **show lacp** [*<1-8>*] **(internal | neighbor) [detail]**

Syntax	**show lacp sys-id**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	show lacp [*<1-8>*] counters show lacp [*<1-8>*] (internal | neighbor) [detail]
Mode	Privileged EXEC
Example	This example shows how to show LACP statistics. Switch# show lacp counters

```
Switch# sh lacp counters
            LACPDUs       LACPDUs
Port       Sent   Recv     Pkts Err
-------------------------------------
Channel group 1
gi1        46     32       0
gi3        45     33       0
```

Switch# show lacp internal

```
Switch# show lacp internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode        P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
gi1       SA      bndl      1             0x3e8     0x3e8   0x1         0x3d
gi3       SA      bndl      1             0x3e8     0x3e8   0x3         0x3d
```

This example shows how to show LACP remote information.

Switch# show lacp neighbor

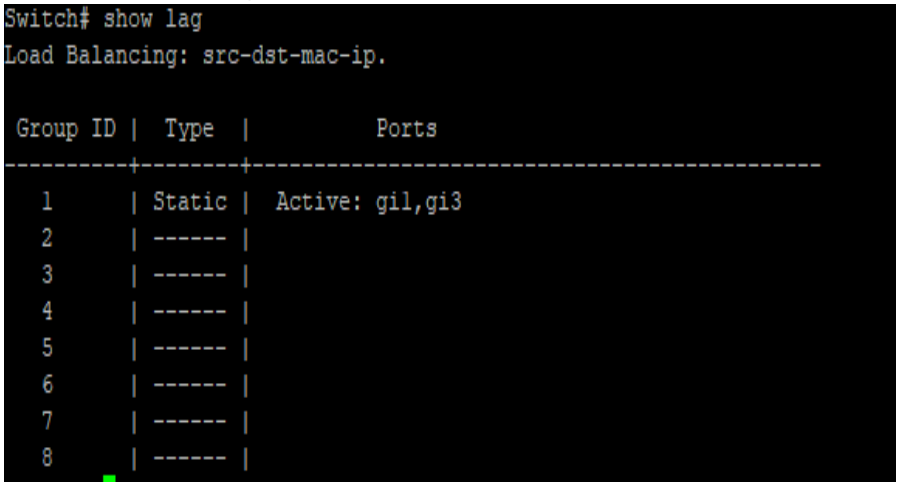
```
Switch# show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs
        F - Device is sending Fast LACPDUs
        A - Device is in Active mode        P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:

                LACP port                       Admin  Oper   Port    Port
Port      Flags   Priority  Dev ID          Age    key    Key    Number  State
gi1       SA      1         8c02.fa02.003e  69s    0x3e8  0x3e8  0x1     0x3d
gi3       SA      1         8c02.fa02.003e  68s    0x3e8  0x3e8  0x5     0x3d
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

12.7 SHOW LAG

Use **“show lag”** command to show current LAG load balance algorithm and members active/inactive status.

Switch# **show lag**

Syntax	**show lag**
Mode	Privileged EXEC
Example	This example shows how to show current LAG status. Switch# **show lag** 

```
Switch# show lag
Load Balancing: src-dst-mac-ip.

 Group ID |  Type  |          Ports
----------+--------+-----------------------------------------------
    1     | Static |  Active: gil,gi3
    2     | ------ |
    3     | ------ |
    4     | ------ |
    5     | ------ |
    6     | ------ |
    7     | ------ |
    8     | ------ |
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13. LLDP

LLDP (Link Layer Discovery Protocol) is an IEEE (Institute of Electrical and Electronics Engineers) standard protocol (IEEE 802.1AB) 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 (Local Area Network) through periodic retransmissions out each port every 30 seconds by default.

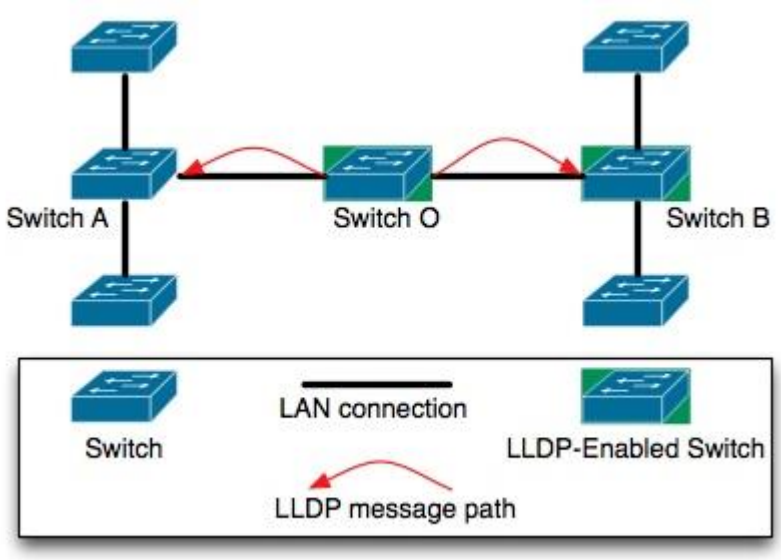


Fig 13.1 Link Layer Discovery Protocol Concept

With all kinds of devices connecting to the network these days, installing, tracking and managing each of them can be quite difficult in large networks. There are many applications for LLDP. Some of them are as follows

- To automate the deployment of access devices like IP Phones, Wireless Access Points, etc.
- To help troubleshoot network attached devices.
- To automate firmware management
- To discover the type and location (switch port) of a network device, connected anywhere on the network.
- To build a complete network topology (which is also automatically updated after adds/moves/changes).

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

- To identify and place a device (like IP phone) on the correct VLAN meant for it, automatically.
- To identify how a device can be powered up (from the main line, from an external source, etc.) and how much power it needs.
- To get information like hardware revision, firmware version, serial no, manufacturer/model name, etc. from LLDP supported devices connected to the network.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.1 LLDP

Use **"lldp"** command to enable LLDP RX/TX ability. The LLDP enable status is displayed by **"show lldp"** command. Use the **"no"** form of this command to disable the LLDP. When LLDP is disabled, the behavior of receiving LLDP PDU would be decided by **"lldp"** command.

Switch# **configure terminal**
Switch (config)#**lldp**

Switch (config)#**no lldp**

Syntax	**lldp** **no lldp**
Mode	Global Configuration
Example	The following example sets LLDP enable/disable. Switch# **configure terminal** Switch (config)# **lldp** Switch# **show lldp**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# lldp
Switch(config)#
Switch# show lldp

 State: Enabled
 Timer: 30 Seconds
 Hold multiplier: 4
 Reinit delay: 2 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Flooding

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
      gi1 |  RX,TX |                |192.168.0.1
      gi2 |  RX,TX |                |192.168.0.1
      gi3 |  RX,TX |                |192.168.0.1
      gi4 |  RX,TX |                |192.168.0.1
      gi5 |  RX,TX |                |192.168.0.1
      gi6 |  RX,TX |                |192.168.0.1
      gi7 |  RX,TX |                |192.168.0.1
      gi8 |  RX,TX |                |192.168.0.1
      gi9 |  RX,TX |                |192.168.0.1
     gi10 |  RX,TX |                |192.168.0.1
     gi11 |  RX,TX |                |192.168.0.1
     gi12 |  RX,TX |                |192.168.0.1
     gi13 |  RX,TX |                |192.168.0.1
     gi14 |  RX,TX |                |192.168.0.1
     gi15 |  RX,TX |                |192.168.0.1
     gi16 |  RX,TX |                |192.168.0.1
     gi17 |  RX,TX |                |192.168.0.1
     gi18 |  RX,TX |                |192.168.0.1
     gi19 |  RX,TX |                |192.168.0.1
     gi20 |  RX,TX |                |192.168.0.1
     gi21 |  RX,TX |                |192.168.0.1
     gi22 |  RX,TX |                |192.168.0.1
     gi23 |  RX,TX |                |192.168.0.1
     gi24 |  RX,TX |                |192.168.0.1
     gi25 |  RX,TX |                |192.168.0.1
     gi26 |  RX,TX |                |192.168.0.1
     gi27 |  RX,TX |                |192.168.0.1
     gi28 |  RX,TX |                |192.168.0.1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.2 LLDP RX

Use **"lldprx"** command to enable the LLDP PDU RX ability. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to disable the RX ability.

Switch# **configure terminal**
Switch(config)#**interface** *{Interface-ID}*
Switch(config-if)# **lldprx**

Switch(config-if)# **no lldprx**

Syntax	**lldprx** **no lldprx**
Mode	Port Configuration
Example	This example sets port gi1 to enable LLDP TX, port gi2 to disable RX but enable TX, port gi3 to enable RX but disable TX, port gi4 to disable RX and TX. Switch# **configure terminal** Switch(config)# **interface range g1-10** Switch(config-if-range)# **lldp rx** Switch(config-if-range)# **lldp tx** Switch# **show lldp interfaces g1-10**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# interface range gl-10
Switch(config-if-range)#  lldp rx
Switch(config-if-range)#  lldp tx
Switch(config-if-range)#
Switch# show lldp interfaces  gl-10

 State: Enabled
 Timer: 30 Seconds
 Hold multiplier: 4
 Reinit delay: 2 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Flooding

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
      gil |  RX,TX |                |192.168.0.1
      gi2 |  RX,TX |                |192.168.0.1
      gi3 |  RX,TX |                |192.168.0.1
      gi4 |  RX,TX |                |192.168.0.1
      gi5 |  RX,TX |                |192.168.0.1
      gi6 |  RX,TX |                |192.168.0.1
      gi7 |  RX,TX |                |192.168.0.1
      gi8 |  RX,TX |                |192.168.0.1
      gi9 |  RX,TX |                |192.168.0.1
     gil0 |  RX,TX |                |192.168.0.1

Port ID: gil
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.3 LLDP TX-INTERVAL

Use **"lldptx-interval"** command to configure the LLDP TX interval. It should be noticed that both **"lldptx-interval"** and **"lldptx-delay"** affects the LLDP PDU TX time. The larger value of the two configurations decides the TX interval. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to restore the interval to default value.

Switch# **configure terminal**
Switch(config)# **lldp tx-interval** *<5-32768>*

Switch(config)# **no lldp tx-interval**

Syntax	**lldptx-interval** *<5-32768>* **no lldptx-interval**
Parameter	*<5-32768>*Specify the LLDP PDU TX interval in unit of second
Default	Default TX interval is 30 seconds
Mode	Global Configuration

Example	This example sets LLDP TX interval to 100 seconds.
	Switch# **configure terminal**
	Switch(config)# **lldp tx-interval 100**
	Switch# **show lldp**
	`Switch# configure terminal`
	`Switch(config)# lldp tx-interval 100`
	`Switch(config)#`
	`Switch# show lldp`
	
	`State: Enabled`
	`Timer: 100 Seconds`
	`Hold multiplier: 4`
	`Reinit delay: 2 Seconds`
	`Tx delay: 2 Seconds`
	`LLDP packet handling: Flooding`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.4 LLDP REINIT-DELAY

Use **"lldpreinit-delay"** to configure the LLDP re-initials delay. This delay avoids LLDP generate too many PDU if the port is up and down frequently. The delay starts to count when the port links down. The port would not generate LLDP PDU until the delay counts to zero. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to restore the delay to default value.

Switch# **configure terminal**
Switch(config)# **lldp reinit-delay** *<1-10>*

Switch(config)# **no lldp reinit-delay**

Syntax	**Lldp reinit-delay** *<1-10>* **no lldp reinit-delay**
Parameter	*<1-10>*Specify the LLDP re-initial delay time in unit of second.
Default	Default reinital delay is 2 seconds
Mode	Global Configuration

Example	This example sets LLDP re-initial delay to 5 seconds.
	Switch# **configure terminal**
	Switch(config)# **lldp reinit-delay** 5
	Switch# **show lldp**
	`Switch# configure terminal`
	`Switch(config)# lldp reinit-delay 5`
	`Switch(config)#`
	`Switch# show lldp`
	
	`State: Enabled`
	`Timer: 100 Seconds`
	`Hold multiplier: 4`
	`Reinit delay: 5 Seconds`
	`Tx delay: 2 Seconds`
	`LLDP packet handling: Flooding`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.5 LLDP HOLDTIME-MULTIPLIER

Use **"lldp holdtime-multiplier"** command to configure the LLDP PDU hold multiplier that decides time-to-live (TTL) value sent in LLDP advertisements: TTL = (tx-interval * holdtime-multiplier). The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to restore the multiplier to default value.

Switch# **configure terminal**
Switch(config)# **lldp holdtime-multiplier** *<2-10>*

Switch(config)# **no holdtime-multiplier**

Syntax	**lldp holdtime-multiplier** *<2-10>* **no holdtime-multiplier**
Parameter	*<2-10>*Specify the LLDP hold time multiplier
Default	lldpholdtime-multiplier 4
Mode	Global Configuration

Example	This example sets LLDP hold time multiplier to 3.
	Switch# **configure terminal**
	Switch(config)# **lldp holdtime-multiplier 3**
	Switch# **show lldp**
	`Switch# configure terminal`
	`Switch(config)# lldp holdtime-multiplier 3`
	`Switch(config)#`
	`Switch# show lldp`
	
	`State: Enabled`
	`Timer: 100 Seconds`
	`Hold multiplier: 3`
	`Reinit delay: 5 Seconds`
	`Tx delay: 2 Seconds`
	`LLDP packet handling: Flooding`

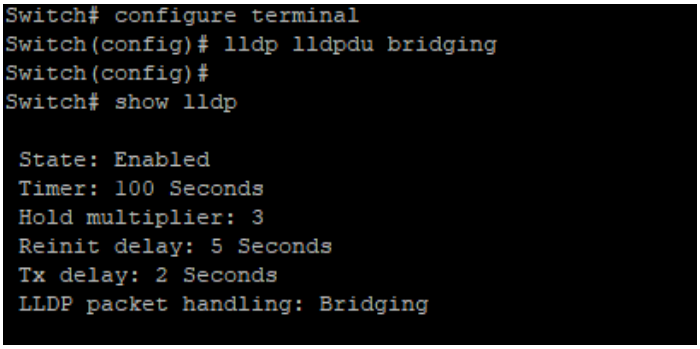
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.6 LLDP LLDPDU

Use **"lldp lldpdu"** command to configure the LLDP PDU handling behavior when LLDP is globally disabled. It should be noticed that if LLDP is globally enabled and per port LLDP RX status is configured to disabled, the received LLDP PDU would be dropped instead of taking the global disable behavior. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to restore the behavior to default.

Switch# **configure terminal**

Switch(config)# **lldp lldpdu (filtering|flooding|bridging)**

Syntax	**lldp lldpdu (filtering|flooding|bridging)**
Parameter	**bridging** When LLDP is globally disabled, LLDP packets are bridging (bridging LLDP PDU to VLAN member ports). **filtering** When LLDP is globally disabled, LLDP packets are filtered (deleted). **flooding** When LLDP is globally disabled, LLDP packets are flooded (forwarded to all interfaces).
Default	Default LLDP PDU handling behavior when LLDP disabled is flooding
Mode	Global Configuration
Example	This example sets LLDP disable action to bridging. Switch# **configure terminal** Switch(config)# **lldp lldpdu bridging** Switch# **show lldp** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.7 LLDP MED

Use **"lldp med"** to configure the LLDP MED enable status. If LLDP MED is enabled, LLDP MED capability TLV and other selected MED TLV would be attached. The configuration could be shown by **"show lldp med"** command. Use the **"no"** form of this command to disable the LLDP MED status.

Switch# **configure terminal**
Switch(config)# **interface** *{Interfac-ID}*
Switch(config-if)# **lldp med**

Switch(config-if)# **no lldp med**

Syntax	**lldp med** **no lldp med**
Default	lldp med
Mode	Port Configuration
Example	This example sets port gi1 to enable LLDP MED, port gi2 to disable LLDP MED. Switch# **configure terminal** Switch(config)# **interface range** g1-10 Switch(config-if-range)# **lldp med** Switch# **show lldp interfaces** g 1-10 **med**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# interface range g1-10
Switch(config-if-range)#  lldp med
Switch(config-if-range)#
Switch# show lldp interfaces g 1-10 med

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |          Yes |            Yes |       No |        No |      No
    gi2 |          Yes |            Yes |       No |        No |      No
    gi3 |          Yes |            Yes |       No |        No |      No
    gi4 |          Yes |            Yes |       No |        No |      No
    gi5 |          Yes |            Yes |       No |        No |      No
    gi6 |          Yes |            Yes |       No |        No |      No
    gi7 |          Yes |            Yes |       No |        No |      No
    gi8 |          Yes |            Yes |       No |        No |      No
    gi9 |          Yes |            Yes |       No |        No |      No
   gi10 |          Yes |            Yes |       No |        No |      No
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.8 LLDP MED FAST-START-REPEAT-COUNT

Use **"lldp med fast-start-repeat-count"** command to configure the LLDP PDU fast start TX repeat count. When port links up, it will send LLDP PDU immediately to notify link partner. The number of LLDP PDU sends when it links up depends on fast-start-repeat-count configuration. The LLDP PDU fast-start transmits in interval of one second. The fast start behavior works no matter LLDP MED is enabled or not. The configuration could be shown by **"show lldp med"** command. Use the **"no"** form of this command to restore count to default.

Switch# **configure terminal**
Switch(config)# **lldp med fast-start-repeat-count** *<1-10>*

Switch(config)# **no lldp med fast-start-repeat-count**

Syntax	**lldp med fast-start-repeat-count** *<1-10>* **no lldp med fast-start-repeat-count**
Parameter	*<1-10>* LLDP PDU fast start TX repeat counts.
Default	Default fast start TX repeat count is 3
Mode	Global Configuration
Example	This example sets fast start repeat count to 10. Switch# **configure terminal** Switch(config)# **lldp med fast-start-repeat-count** 10 Switch# **show lldp med**

```
Switch# configure terminal
Switch(config)# lldp med fast-start-repeat-count 10
Switch(config)#
Switch# show lldp med

 Fast Start Repeat Count: 10

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |          Yes |            Yes |       No |        No |      No
    gi2 |          Yes |            Yes |       No |        No |      No
    gi3 |          Yes |            Yes |       No |        No |      No
    gi4 |          Yes |            Yes |       No |        No |      No
    gi5 |          Yes |            Yes |       No |        No |      No
    gi6 |          Yes |            Yes |       No |        No |      No
    gi7 |          Yes |            Yes |       No |        No |      No
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.9 LLDP MED LOCATION

Use **"lldp med location"** command to configure the LLDP MED location data. The **"coordinate", "civic-address", "ecs-elin"** locations are independent, so at most three location TLVs could be sent if their data are not empty. The configuration of location could be shown by **"show lldp interface PORT med"** command. Use the **"no"** form of this command to clear location data.

Switch# **configure terminal**
Switch(config)#**interface** *{Interface-ID}*
Switch(config-if)# **lldp med location (coordination|civic-address|ecs-elin) ADDR**

Switch(config-if)# **no lldp med location (coordination|civic-address|ecs-elin)**

Syntax	**lldp med location (coordination|civic-address|ecs-elin) ADDR** **no lldp med location (coordination|civic-address|ecs-elin)**
Parameter	Co-ordination civic-address ecs-elin ADDR Location type to be configured. "ecs-elin" is abbreviation of emergency call service – emergency location identifier number Specify the location data. Input format is hexadecimal values without colon (for example: 1234AB). For coordination location type, the length of ADDR is 16 bytes. For civic-address, the length is 6 to 160 bytes. For ecs-elin, the length is 10 to 25 bytes.
Default	**Default** Deafult is no location data.
Mode	Mode Port Configuration
Example	This example sets location data for interface gi1. Switch# **configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **lldp med location coordinate 112233445566778899AABBCCDDEEFF00** Switch(config-if)# **lldp med location civic-address 112233445566** Switch(config-if)# **lldp med location ecs-elin 11223344556677889AA** Switch# **show lldp interfaces gi1 med**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# lldp med location coordinate 1122334455667788 99AABBCCDDEEFF00
Switch(config-if)# lldp med location civic-address 112233445566
Switch(config-if)# lldp med location ecs-elin 1122334455667788 99AA
Switch(config-if)# end
Switch# show lldp interfaces gi1 med

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |          Yes |            Yes |       No |        No |     N/A

Port ID: gi1
Network policies:
Location:
Coordinates: 1122334455667788 99AABBCCDDEEFF00
Civic-address: 112233445566
Ecs-elin: 1122334455667788 99AA
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.10 LLDP MED NETWORK-POLICY

Use **"lldp med network-policy"** command to configure the LLDP MED Network policy table and add a network policy entry that can be bind to ports. If LLDP MED network policy voice auto mode is enabled, **"voice"** type network policy cannot be created since it is in auto mode. The network policy table configuration could be shown by **"show lldp med"** command.

Use the **"no"** form of this command to remove network policy entry of specific index. A network policy can be removed only when it is not bind to any port.

Switch# **configure terminal**
Switch(config)# **lldp med network-policy** *<1-32>* **app (voice|voice-signaling|guest-voice|guest-voice-signaling|softphone-voice |video-conferencing| streaming- video |video-signaling) vlan** *<1-4094>* **vlan-type (tag|untag) priority** *<0- 7>* **dscp** *<0-63>*

Switch(config)# **no lldp med network-policy** *<1-32>*

Syntax	**lldp med network-policy** *<1-32>* **app (voice|voice-signaling|guest-voice|guest-voice-signaling|softphone-voice|video-conferencing|streaming- video|video-signaling) vlan** *<1-4094>* **vlan-type (tag|untag) priority** *<0- 7>* **dscp** *<0-63>* **no lldp med network-policy** *<1-32>*
Parameter	*<1-32>*Specify the network policy index. **voice-signaling** Specify the network policy application type. *<1-4094>*Specify the VLAN IDtag untag Specify the VLAN tag status *<0-7>*Specify the L2 priority <*0-63>*Specify the DSCP value
Mode	Global Configuration
Example	This example create 2 network policies. Switch# **configure terminal** Switch(config)# **lldp med network-policy** 1 **app voice-signaling vlan** 2 **vlan-type tag priority** 3 **dscp** 4 Switch(config)# **lldp med network-policy** 32 **app video- conferencing**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

vlan 5 vlan-type tag priority 1 dscp 63

Switch# show lldp med

```
Switch(config)# lldp med network-policy 1 app voice-signaling vlan 2 vlan-type tag priority 3 dscp 4
Switch(config)# lldp med network-policy 32 app video-conferencing vlan 5 vlan-type tag priority 1 dscp 63
Switch(config)# exit
Switch# show lldp med

 Fast Start Repeat Count: 10

Network policy 1
------------------
Application type: Voice Signaling
VLAN ID: 2 tagged
Layer 2 priority: 3
DSCP: 4

Network policy 32
------------------
Application type: Conferencing
VLAN ID: 5 tagged
Layer 2 priority: 1
DSCP: 63

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |          Yes |            Yes |       No |        No |     N/A
    gi2 |           No |            Yes |       No |        No |     N/A
    gi3 |          Yes |            Yes |       No |        No |     N/A
    gi4 |          Yes |            Yes |       No |        No |     N/A
    gi5 |          Yes |            Yes |       No |        No |     N/A
    gi6 |          Yes |            Yes |       No |        No |     N/A
    gi7 |          Yes |            Yes |       No |        No |     N/A
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.11 LLDP MED NETWORK-POLICY (INTERFACE)

Use **"lldp med network-policy"** command to bind the network policy to port interface. The bonded network policy of one port should be with different types. If network policy TLV is selected over a port, the bonded network policies would be attached in LLDP MED PDU. The configuration of network policy binding could be shown by **"show lldp med" command.**

Switch# **configure terminal**
Switch(config)# **interface** *{Interface-ID ranges}*

Switch(config-if-range)#**lldp med network-policy (add|remove)** *<1-32>*

Syntax	**lldp med network-policy (add|remove)** *<1-32>*
Parameter	**add**Add network policy binding for ports. **remove**Remove network policy binding for ports. *<1-32>* Specify the network policy index
Mode	Port Configuration
Example	This example binds network policy for interface gi1 and gi2. Switch# **show lldp med** Switch# **configure terminal** Switch(config)# **interface range** g1-10 Switch(config-if-range)#**lldp med network-policy add** 1 Switch# **show lldp interfaces** g1-10 **med**

```
Switch# configure terminal
Switch(config)# interface range gi1-10
Switch(config-if-range)# lldp med network-policy add 1
Switch(config-if-range)#
Switch# show lldp interfaces gi1-10 med

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |          Yes |            Yes |       No |        No |      No
    gi2 |          Yes |            Yes |       No |        No |      No
    gi3 |          Yes |            Yes |       No |        No |      No
    gi4 |          Yes |            Yes |       No |        No |      No
    gi5 |          Yes |            Yes |       No |        No |      No
    gi6 |          Yes |            Yes |       No |        No |      No
    gi7 |          Yes |            Yes |       No |        No |      No
    gi8 |          Yes |            Yes |       No |        No |      No
    gi9 |          Yes |            Yes |       No |        No |      No
   gi10 |          Yes |            Yes |       No |        No |      No
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.12 LLDP MED TLV-SELECT

Use **"lldp med tlv-select"** command to configure the LLDP MED TLV selection. It should be noticed that even no MED TLV is selected, MED capability TLV would be attached if LLDP MED is enable. The configuration could be shown by **"show lldp med"** command. Use the **"no"** form of this command to remove all selected MED TLV over the dedicated ports.

Switch# **configure terminal**
Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)# **lldp med tlv-select MEDTLV [MEDTLV] [MEDTLV] [MEDTLV]**

Switch(config-if)# **no lldp med tlv-select**

Syntax	**lldp med tlv-select MEDTLV [MEDTLV] [MEDTLV] [MEDTLV]** **no lldp med tlv-select**
Parameter	**MEDTLV MED** optional TLV. Available optional TLVs are : network-policy, location, poe-pse, inventory.
Default	network-policy TLV
Mode	Port Configuration
Example	This example sets port gi1-2 to select LLDP MED network policy, location, POE-PSE, inventory TLVs, and it sets port gi3-4 to un-select all LLDP MED TLVs. Switch# **configure terminal** Switch(config)# **interface** g1 Switch(config-if)# **lldp med tlv-select network-policy location inventory** Switch(config)# **interface** g2 Switch(config-if)# **no lldp med tlv-select** Switch# **show lldp interfaces** g1-2 **med**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)#  interface g1
Switch(config-if)# lldp med tlv-select network-policy location inventory
Switch(config-if)# exit
Switch(config)#  interface g2
Switch(config-if)#  no lldp med tlv-select
Switch(config-if)#
Switch#  show lldp interfaces g1-2 med

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    g1 |          Yes |            Yes |      Yes |       Yes |      No
    g2 |          Yes |             No |       No |        No |      No
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.13 LLDP TLV-SELECT

Use **"lldptlv-select"** command to attach selected TLV in PDU. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to remove all selected TLV.

Switch# **configure terminal**
Switch(config)# **interface** *{Interface-ID ranges}*

Switch(config-if-range)# **lldp tlv-select TLV** [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV]

Switch(config-if-range)# **no lldp tlv-select**

Syntax	**Lldp tlv-select TLV [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV]** **no lldp tlv-select**
Parameter	**TLV** Specify the selected optional TLV. Available optional TLVs are : sys-name (system name), sys-desc (system description), sys-cap (system capability), mac-phy (802.3 MAC-PHY), lag (802.3 link aggregation), max- frame-size (802.3 max frame size), and management- addr (management address).
Mode	Port Configuration
Example	This example selects system name, system description, system capability, 802.3 MAC-PHY, 802.3 link aggregation, 802.3 max frame size, and management address TLVs for interface gi1 and gi3. Switch# **configure terminal** Switch(config)# **interface range** g 1,3 Switch(config-if-range)# **lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size** Switch(config-if-range)# **end** Switch# **show lldp interfaces** g 1,3

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)#  interface range g 1,3
<s-name sys-desc sys-cap mac-phy lag max-frame-size
Switch(config-if-range)#
Switch#  show lldp interfaces g 1,3

 State: Enabled
 Timer: 100 Seconds
 Hold multiplier: 3
 Reinit delay: 5 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Bridging

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
      gi1 |  RX,TX | PD, SN, SD, SC |192.168.0.1
      gi3 |  RX,TX | PD, SN, SD, SC |192.168.0.1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.14 LLDP TLV-SELECT PVID

Use **"lldptlv-select pvid"** command to configure the 802.1 PVID TLV attachenable status. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to restore the pvid to default value.

Switch# **configure terminal**
Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)# **lldp tlv-select pvid (disable|enable)**

Switch(config-if)# **no lldp tlv-select pvid**

Syntax	**Lldp tlv-select pvid (disable|enable)** **no lldp tlv-select pvid**
Parameter	**Disable** Disable LLDP 802.1 PVID TLV attach state **Enable** Enable LLDP 802.1 PVID TLV attach state
Mode	Port Configuration
Example	This example sets port gi1 PVID TLV attaches status to disable and port gi2 to enable. Switch# **configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **lldp tlv-select pvid disable** Switch(config-if)# **interface** gi2 Switch(config-if)# **lldp tlv-select pvid enable** Switch# **show lldp interfaces** gi1,gi2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# interface gil
Switch(config-if)# lldptlv-select pvid disable
Unknown command
Switch(config-if)# lldptlv-select pvid
Unknown command
Switch(config-if)# lldp tlv-select pvid disable
Switch(config-if)#
Switch#
Switch#
Switch#
Switch# configure terminal
Switch(config)# interface gil
Switch(config-if)# lldp tlv-select pvid disable
Switch(config-if)# exit
Switch(config)# interface gi2
Switch(config-if)# lldp tlv-select pvid enable
Switch(config-if)#
Switch#
Switch# show lldp interfaces gil,gi2

 State: Enabled
 Timer: 100 Seconds
 Hold multiplier: 3
 Reinit delay: 5 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Bridging

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
      gil |  RX,TX | PD, SN, SD, SC |192.168.0.1
      gi2 |  RX,TX |                |192.168.0.1

Port ID: gil
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size
802.1 optional TLVs
PVID: Disabled
VLANs: 1

Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
VLANs: 1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.15 LLDP TLV-SELECT VLAN-NAME

Use **"lldp tlv-select vlan-name"** command to add or remove VLAN list for 802.1 VLAN-NAME TLV. The configuration could be shown by **"show lldp"** command.

Switch# **configure terminal**
Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)# **lldp tlv-select vlan-name (add|remove)** *{VLAN-LIST}*

Syntax	**lldp tlv-select vlan-name (add|remove)** *{VLAN-LIST}*
Parameter	**add** *VLAN-LIST* Add VLAN list for LLDP 802.1 VLAN-NAME TLV on the specific interface. The configured ports should be member of all the specified VLANs or the VLAN- LIST is not valid. remove VLAN-LIST Remove VLAN list of LLDP 802.1 VLAN-NAME TLV from interface
Mode	Port Configuration
Example	This example add VLAN 100 to VLAN-NAME TLV for port gi10. Switch# **configure terminal** Switch(config)# **vlan** 100 Switch(config-vlan)# **exit** Switch(config)# **interface** g2 Switch(config-if)# **switchport trunk allowed vlan add 1,100** Switch(config-if)# **lldp tlv-select vlan-name add** 100 Switch(config-if)# **end** Switch# **show lldp interfaces gi1** Switch# **show lldp interfaces g2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)#  interface g2
Switch(config-if)# switchport trunk allowed vlan add 1,100
Switch(config-if)# lldp tlv-select vlan-name add 100
Switch(config-if)#
Switch# show lldp interfaces gi1

 State: Enabled
 Timer: 100 Seconds
 Hold multiplier: 3
 Reinit delay: 5 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Bridging

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
      gi1 |  RX,TX | PD, SN, SD, SC |192.168.0.1

Port ID: gi1
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size
802.1 optional TLVs
PVID: Enabled
VLANs: 1

Switch# show lldp interfaces g2

 State: Enabled
 Timer: 100 Seconds
 Hold multiplier: 3
 Reinit delay: 5 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Bridging

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
      gi2 |  RX,TX |                |192.168.0.1

Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
VLANs: 1,100
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.16 LLDP TX

Use **“lldp tx”** command to enable the LLDP PDU TX ability. The configuration could be shown by **“show lldp”** command. Use the **“no”** form of this command to disable the TX ability.

Switch# **configure terminal**
Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)# **lldp tx**

Switch(config-if)# **no lldp tx**

Syntax	**lldp tx** **no lldp tx**
Mode	Port Configuration
Example	This example sets port gi1 to enable LLDP TX, port gi2 to disable RX but enable TX, port gi3 to enable RX but disable TX, port gi4 to disable RX and TX. Switch# **configure terminal** Switch(config)# **interface** g1 Switch(config-if)# **lldp rx** Switch(config-if)# **lldp tx** Switch(config-if)# **interface** g2 Switch(config-if)# **no lldp rx** Switch(config-if)# **lldp tx** Switch(config-if)# **interface** g3 Switch(config-if)# **lldp rx** Switch(config-if)# **no lldp tx** Switch(config-if)# **interface** g4 Switch(config-if)# **no lldp rx** Switch(config-if)# **no lldp tx** Switch(config-if)# **end** Switch# **show lldp interfaces** g 1-4

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)#  interface g1
Switch(config-if)# lldp rx
Switch(config-if)# lldp tx
Switch(config-if)#  interface g2
Switch(config-if)# no lldp rx
Switch(config-if)# lldp tx
Switch(config-if)#  interface g3
Switch(config-if)# lldp rx
Switch(config-if)# no lldp tx
Switch(config-if)# interface g4
Switch(config-if)#  no lldp rx
Switch(config-if)#  no lldp tx
Switch(config-if)# end
Switch# show lldp interfaces g 1-4

 State: Enabled
 Timer: 100 Seconds
 Hold multiplier: 3
 Reinit delay: 5 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Bridging

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
      gi1 |  RX,TX | PD, SN, SD, SC |192.168.0.1
      gi2 |     TX |                |192.168.0.1
      gi3 |     RX | PD, SN, SD, SC |192.168.0.1
      gi4 |Disable |                |192.168.0.1

Port ID: gi1
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size
802.1 optional TLVs
PVID: Enabled
VLANs: 1

Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
VLANs: 1,100
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.17 LLDP TX-DELAY

Use **"lldp tx-delay"** command to configure the delay in seconds between successive LLDP frame transmissions. The delay starts to count in any case LLDP PDU is sent such as by LLDP PDU advertise routine, LLDP PDU content change, port link up, etc. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to restore the delay to default value.

Switch# **configure terminal**
Switch(config)# **lldp tx-delay** *<1-8192>*

Switch(config)# **no lldp tx-delay**

Syntax	**lldp tx-delay** *<1-8192>* **no lldp tx-delay**
Parameter	*<1-8192>*Specify the LLDP tx delay in unit of seconds.
Default	Default TX delay is 2 seconds
Mode	Global Configuration
Example	This example sets LLDP PDU TX delay to 10 seconds. Switch# **configure terminal** Switch(config)# **lldp tx-delay 1** Switch# **show lldp**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# lldp tx-delay 1
Switch(config)# exit
Switch# show lldp

 State: Enabled
 Timer: 10 Seconds
 Hold multiplier: 3
 Reinit delay: 5 Seconds
 Tx delay: 1 Seconds
 LLDP packet handling: Bridging

 Port     |  State | Optional TLVs   | Address
 -------- + ------ + --------------- + --------
      gi1 |  RX,TX | PD, SN, SD, SC |192.168.100.93
      gi2 |     TX |                 |192.168.100.93
      gi3 |     RX | PD, SN, SD, SC |192.168.100.93
      gi4 |Disable |                 |192.168.100.93
      gi5 |  RX,TX |                 |192.168.100.93
      gi6 |  RX,TX |                 |192.168.100.93
      gi7 |  RX,TX |                 |192.168.100.93
      gi8 |  RX,TX |                 |192.168.100.93
      gi9 |  RX,TX |                 |192.168.100.93
     gi10 |  RX,TX |                 |192.168.100.93
     gi11 |  RX,TX |                 |192.168.100.93
     gi12 |  RX,TX |                 |192.168.100.93
     gi13 |  RX,TX |                 |192.168.100.93
     gi14 |  RX,TX |                 |192.168.100.93
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.18 SHOW LLDP

Use **“show lldp”** and **“show lldp interface”** commands to display LLDP global information including LLDP enable status, LLDP PDU TX interval, hold time multiplier, re-initial delay, TX delay, and LLDP packet handling when LLDP is disabled. Single port information displayed includes port LLDP RX/TX enable status, selected TLV to TX and IP address. The abbreviations in optional TLVs are: port description (PD), system name (SN), system description (SD), and system capability (SC).

Switch# **show lldp**
Switch# **show lldp interface** *{IF_NMLPORTS}*

Syntax	**show lldp** **show lldp interface** *{IF_NMLPORTS}*
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC

Example	This example displays lldp information of port gi1 and gi2
	Switch# **show lldp interfaces gi1,gi2**
	`Switch# show lldp interfaces gi1,gi2`
	`State: Enabled`
	`Timer: 10 Seconds`
	`Hold multiplier: 3`
	`Reinit delay: 5 Seconds`
	`Tx delay: 1 Seconds`
	`LLDP packet handling: Bridging`
	`Port | State | Optional TLVs | Address`
	`gi1 | RX,TX | PD, SN, SD, SC |192.168.100.93`
	`gi2 | TX | |192.168.100.93`
	`Port ID: gi1`
	`802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, management-addr`
	`802.1 optional TLVs`
	`PVID: Disabled`
	`VLANs: 100`
	`Port ID: gi2`
	`802.3 optional TLVs:`
	`802.1 optional TLVs`
	`PVID: Enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.19 SHOW LLDP LOCAL-DEVICE

Use **"show lldp local-device"** command to show the local configuration of LLDP PDU. By the commands, a user can view the contents of LLDP/ LLDP-MED TLVs that would be attached in LLDP PDU.

Switch# **show lldp local-device**
Switch# **show lldp interfaces** *{IF_NMLPORTS}* **local-device**

Syntax	**show lldp local-device** **show lldp interfaces** *{IF_NMLPORTS}* **local-device**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC

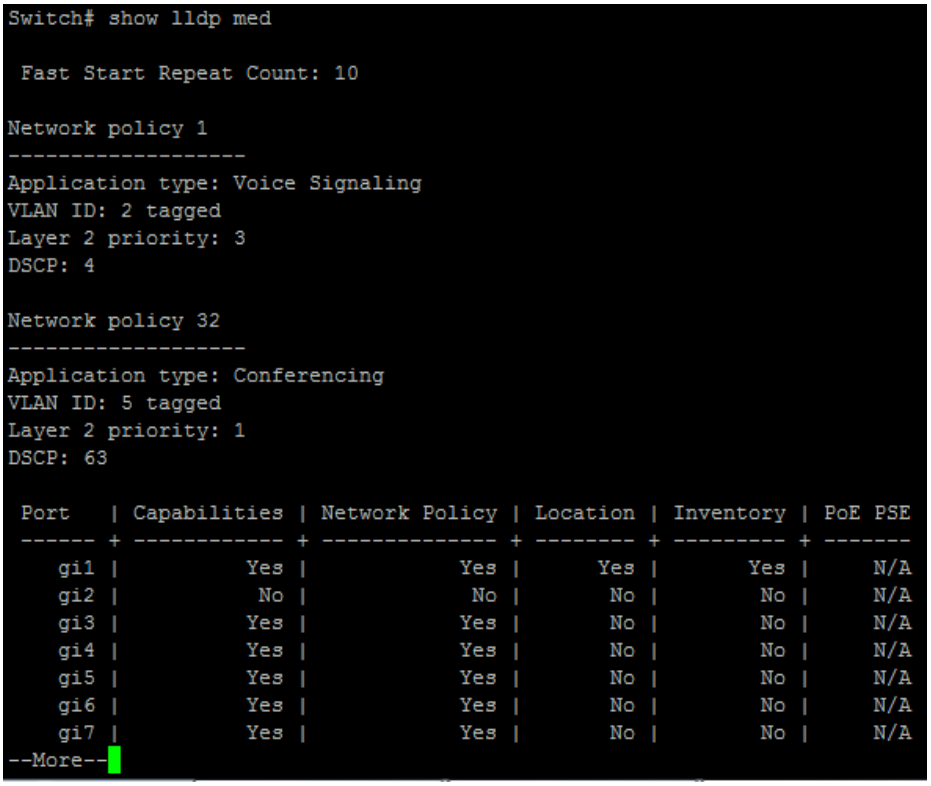
Example	This example displays the local device information.
	Switch# **show lldp local-device**
	`Switch# show lldp local-device`
	
	`LLDP Local Device Information:`
	` Chassis Type : Mac Address`
	` Chassis ID : 8C:02:FA:05:00:04`
	` System Name : Switch`
	` System Description : C3000-24GP+4X`
	` System Capabilities Support : Bridge, Router`
	` System Capabilities Enable : Bridge, Router`
	` Management Address : 0.0.0.0(IPv4)`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.20 SHOW LLDP MED

Use **“show lldp med”** command to display the LLDP MED configuration information.

Switch# **show lldp med**
Switch# **show lldp interfaces** *{IF_NMLPORTS}* **med**

Syntax	**show lldp med** **show lldp interfaces** *{IF_NMLPORTS}* **med**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC
Example	This example displays the LLDP MED information. Switch# **show lldp med** 

```
Switch# show lldp med

 Fast Start Repeat Count: 10

Network policy 1
--------------------
Application type: Voice Signaling
VLAN ID: 2 tagged
Layer 2 priority: 3
DSCP: 4

Network policy 32
--------------------
Application type: Conferencing
VLAN ID: 5 tagged
Layer 2 priority: 1
DSCP: 63

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |          Yes |            Yes |      Yes |       Yes |     N/A
    gi2 |           No |             No |       No |        No |     N/A
    gi3 |          Yes |            Yes |       No |        No |     N/A
    gi4 |          Yes |            Yes |       No |        No |     N/A
    gi5 |          Yes |            Yes |       No |        No |     N/A
    gi6 |          Yes |            Yes |       No |        No |     N/A
    gi7 |          Yes |            Yes |       No |        No |     N/A
--More--
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.21 SHOW LLDP NEIGHBOR

Use **"show lldp neighbor"** command to display the received neighbor LLDP PDU information. When LLDP PDU is received on LLDP RX enable ports, system would store the PDU information in database until time to live of the PDU counts down to zero.

Switch# **show lldp neighbor**
Switch# **show lldp interfaces** *{IF_NMLPORTS}* **neighbor**

Syntax	**show lldp neighbor** **show lldp interfaces** *{IF_NMLPORTS}* **neighbor**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC

Example	This example displays the neighbor information.
	Switch# **show lldp neighbor**
	`Switch# show lldp neighbor`
	`Port | Device ID | Port ID | SysName | Capabilities | TTL`
	`---- + ---------- + ---------- + ---------- + ------------ + -----`
	`gi23 | E0:DB:55:BE:35:5B |E0:DB:55:BE:35:5B | | | 3528`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.22 SHOW LLDP STATISTICS

Use **"show lldp statistics"** command to display the LLDP RX/TX statistics.

Switch# **show lldp statistics**
Switch# **show lldp interfaces** *{IF_NMLPORTS}* **statistics**

Syntax	**show lldp statistics** **show lldp interfaces** *{IF_NMLPORTS}* **statistics**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC
Example	This example display the LLDP statistics. Switch# **show lldp statistics** Switch(config)# **show lldp interfaces gi1 statistics**

```
Switch# show lldp statistics

LLDP Global Statistics:
Insertions : 1
Deletions  : 0
Drops      : 0
Age Outs   : 0

        | TX Frames |          RX Frames          |          RX TLVs          | RX Ageouts
  Port  |   Total   | Total | Discarded | Errors | Discarded | Unrecognized |    Total
--------+-----------+-------+-----------+--------+-----------+--------------+----------
    gi1 |        19 |     0 |         0 |      0 |         0 |            0 |         0
    gi2 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    gi3 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    gi4 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    gi5 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    gi6 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    gi7 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    gi8 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    gi9 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi10 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi11 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi12 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi13 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi14 |        18 |     0 |         0 |      0 |         0 |            0 |         0
   gi15 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi16 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi17 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi18 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi19 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi20 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi21 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi22 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi23 |        39 |     5 |         0 |      0 |         0 |            0 |         0
   gi24 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    te1 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    te2 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    te3 |         0 |     0 |         0 |      0 |         0 |            0 |         0
    te4 |         0 |     0 |         0 |      0 |         0 |            0 |         0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show lldp interfaces gi1 statistics

LLDP Port Statistics:
       | TX Frames |         RX Frames          |          RX TLVs          | RX Ageouts
  Port |   Total   | Total | Discarded | Errors | Discarded | Unrecognized |    Total
-------+-----------+-------+-----------+--------+-----------+--------------+----------
   gi1 |         0 |     0 |         0 |      0 |         0 |            0 |        0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.23 CLEAR LLDP STATISTICS

Use **“clear lldp globle statistics”** command to clear the LLDP RX/TX statistics.

Switch# **clear lldp globle statistics**

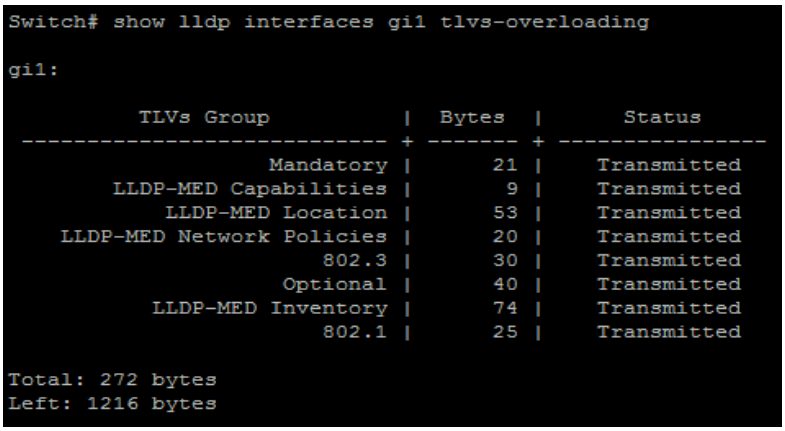
Syntax	**clear lldp globle statistics**
Mode	Privileged EXEC
Example	This example shows how to clear LLDP statistics. Switch# **clear lldp statistics**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

13.24 SHOW LLDP TLV-OVERLOADING

The LLDP PDU is composed by TLVs and selected number TLVs may compose a large PDU that the system cannot handle. The maximum PDU length is to take the smaller number of jumbo frame size minus 30 bytes (30 bytes kept for header) or 1488 bytes. Use **"show lldptlv-overloading"** command to display the length of LLDP TLVs and if the TLVs overload the PDU length. The TLVs with status marked **"overload"** would not be transmitted.

Switch# **show lldp interfaces** *{IF_NMLPORTS}* **tlvs-overloading**

Syntax	**show lldp interfaces** *{IF_NMLPORTS}* **tlvs-overloading**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC
Example	This example display the LLDP TLVs overloading status of port gi1. Switch# **show lldp interfaces gi1 tlvs-overloading** 

```
Switch# show lldp interfaces gi1 tlvs-overloading

gi1:

          TLVs Group          |  Bytes  |      Status
 ---------------------------- + ------- + ----------------
                    Mandatory |      21 |    Transmitted
        LLDP-MED Capabilities |       9 |    Transmitted
            LLDP-MED Location |      53 |    Transmitted
    LLDP-MED Network Policies |      20 |    Transmitted
                        802.3 |      30 |    Transmitted
                     Optional |      40 |    Transmitted
           LLDP-MED Inventory |      74 |    Transmitted
                        802.1 |      25 |    Transmitted

Total: 272 bytes
Left: 1216 bytes
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

14. LOGGING

Almost all information technology systems generate a log, which serves as a record of all the activity that the system conducted in its operation. Such logs are generated by network infrastructure devices (firewalls, switches, domain name service devices, routers, load balancers), computer platforms (servers, appliances, and smartphones), operating systems (Windows, Linux, iOS) and applications (client/server, web applications, cloud-based utilities).

In an application, a network log is typically a file that contains a record of events that occurred in the application. It contains the record of user and process access calls to objects, attempts at authentication, and other activity. Generally, an event is categorized as an error, a warning, or an informational activity. The specific format and data that are in a log are typically determined by the application designer, to meet various application requirements, and then implemented by the application developer.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

14.1 CLEAR LOGGING

To clear the log messages from the internal logging buffer and flash, use command **"clear logging"** in the Privileged EXEC mode.

Switch# **clear logging**

Syntax	**clear logging**
Parameter	**buffered** Clear the log messages stored in the RAM. **file** Clear the log messages stored in the Flash.
Mode	Privileged EXEC
Example	The following example clear the log messages stored in RAM and Flash. Switch# **clear logging buffered** Switch# **clear logging file**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

14.2 LOGGING

To enable logging service on the switch, use the command logging in the Global Configuration mode. Otherwise, use the no form of the command to disable the logging service on the switch. The status of global logging server is available from the command show logging in the Privileged EXEC mode. When the logging service is enabled, logging on and off at each destination rule can be individually configured by the command logging console, logging buffered, logging file, and logging host in the Global Configuration mode. If the logging service is disabled, no messages will be sent to these destinations.

Switch#**configure terminal**
Switch(config)# **logging**

Switch(config)# **no logging**

Syntax	**logging** **no logging**
Default	Logging service is enabled
Mode	Global Configuration
Example	The following example disables and enables the logging service on the switch. Switch#**configure terminal** Switch(config)# **no logging** Switch(config)# **logging** To display loggin information Switch# **show logging**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# sh logging

Logging service is enabled

Aggregation: enabled
Aggregation aging time: 300 sec

Console Logging: level info
Buffer Logging : level info
File Logging   : disabled


Buffer Logging
--------------
*Dec 31 2021 17:13:38: PORT-6-SPEED_DUPLEX: Interface GigabitEthernet14 link speed 100M duplex full, aggregated (3)
*Dec 31 2021 17:13:38: PORT-5-LINK_UP: Interface GigabitEthernet14 link up, aggregated (3)
*Dec 31 2021 17:13:28: PORT-5-LINK_UP: Interface VLAN2 link up, aggregated (3)
*Dec 31 2021 17:13:28: PORT-6-SPEED_DUPLEX: Interface GigabitEthernet1 link speed 100M duplex full, aggregated (3)
*Dec 31 2021 17:13:28: PORT-5-LINK_UP: Interface GigabitEthernet1 link up, aggregated (3)
*Dec 31 2021 17:15:37: PORT-5-LINK_DOWN: Interface GigabitEthernet14 link down
*Dec 31 2021 17:15:37: PORT-5-LINK_DOWN: Interface VLAN2 link down
*Dec 31 2021 17:15:37: PORT-5-LINK_DOWN: Interface GigabitEthernet1 link down
*Dec 31 2021 17:13:38: PORT-6-SPEED_DUPLEX: Interface GigabitEthernet14 link speed 100M duplex full
*Dec 31 2021 17:13:38: PORT-5-LINK_UP: Interface GigabitEthernet14 link up
*Dec 31 2021 17:13:28: PORT-5-LINK_UP: Interface VLAN2 link up
*Dec 31 2021 17:13:28: PORT-6-SPEED_DUPLEX: Interface GigabitEthernet1 link speed 100M duplex full
*Dec 31 2021 17:13:28: PORT-5-LINK_UP: Interface GigabitEthernet1 link up
*Dec 31 2021 17:00:25: AAA-5-CONNECT: New telnet connection for user admin, source 192.168.0.22 ACCEPTED
*Dec 31 2021 17:00:12: LLDP-6-NEIGHBOR_DISCOVER: New neighbor on port GigabitEthernet23: Chassis ID E0:DB:55:BE:35:5B, Port ID E0:DB:55:BE:35:5B
*Dec 31 2021 17:00:12: PORT-5-LINK_UP: Interface VLAN1 link up
*Dec 31 2021 17:00:12: PORT-6-SPEED_DUPLEX: Interface GigabitEthernet23 link speed 1000M duplex full
*Dec 31 2021 17:00:12: PORT-5-LINK_UP: Interface GigabitEthernet23 link up
*Jan 01 2022 00:00:09: SYSTEM-5-COLDSTART: Cold startup
*Jan 01 2022 00:00:09: LOGGING-6-START: Logging is started

Buffer logging current number of log entries:20
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

14.3 LOGGING HOST

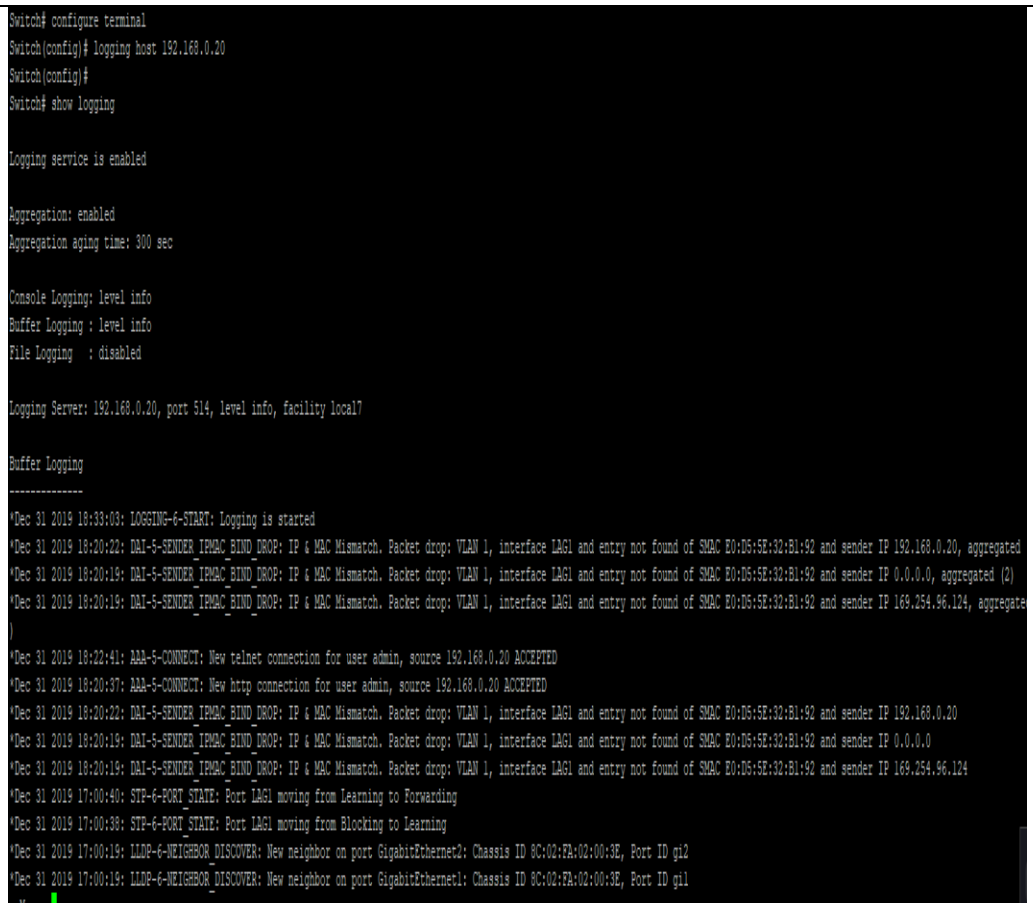
To define the logging server, use the command logging host to add the remote logging server in the Global Configuration mode. Otherwise, use the command no logging host to remove the remote logging rules. For the host name configuration, logging service would try translating the host name to IP address directly. Add the logging host would be failed on the failure of host name translating.

Switch# **configure terminal**
Switch(config)# **logging host (ip-addr|hostname) [facility facility] [port port] [severity sev]**

Switch(config)# **no logging host (ip-addr|hostname)**

Syntax	**logging host (ip-addr|hostname) [facility facility] [port port] [severity sev]** **no logging host (ip-addr|hostname)**
Parameter	**ipv4-addr** IPv4 address of the remote logging server. **hostname** Hostname of the remote logging server. **facility** facility Specify the facility of the logging messages. It can be on of the following value: local0, local1, local2, local3, local4, local5, local6, and local7. The default value of facility is local7. **port** Specify the port number of the remote logging server. The valid range is from 0 to 65535, and the default value is 512. **severity** Specify the minimum severity of the logging messages. The valid range is from 0 to 7, and the number 0 to 7 represents emergency, alert, critical, error, warning, notice, info, and debug individually. The default value of minimum severity level is 5 (emergency, alert, critical, error, warning, notice)
Mode	Global Configuration
Example	The following example adds the remote logging rules by IP and Hostname. Switch# **configure terminal** Switch(config)# **logging host 192.168.0.20**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.



© 2024 COMMANDO Networks Inc., USA. All rights reserved.

14.4 LOGGING SEVERITY

To set the minimum severity for the messages that are logged to RAM, console, or Flash, use the command logging severity in the Global Configuration mode. Use the **"no"** form of the command to remove the mechanism of logging to RAM, console, or Flash individually.

Switch# **configure terminal**
Switch(config)# **logging (buffered|console|file) [severity sev]**

Switch(config)# **no logging (buffered|console|file)**

Syntax	**logging (buffered|console|file) [severity sev]** **no logging (buffered|console|file)**
Parameter	**buffered** Log messages to RAM. **console** Log messages to console buffer. **file** Log messages to Flash. **severity** sev Specify the minimum severity of the logging messages. The valid range is from 0 to 7, and the number 0 to 7 represents emergency, alert, critical, error, warning, notice, info, and debug individually. The default minimum severity of the logging severity configuration is 5 (emerg, alert, crit, error, warning, notice).
Default	Logging to buffered and console is enabled, and the default minimum severity level is 5 (emerg, alert, crit, error, warning, notice).
Mode	Global Configuration
Example	The following example sets the minimum severity level of logging to RAM and Flash as debugging. Switch# **configure terminal** Switch(config)# **logging buffered severity 2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# logging buffered severity 2
Switch(config)#
Switch# show logging

Logging service is enabled

Aggregation: enabled
Aggregation aging time: 300 sec

Console Logging: level info
Buffer Logging : level crit
File Logging   : disabled

Logging Server: 192.168.0.20, port 514, level info, facility local7

Buffer Logging
-------------
*Dec 31 2019 18:41:36: LOGGING-6-BUF_START: Buffer logging is started with minimum severity crit
*Dec 31 2019 18:33:03: LOGGING-6-START: Logging is started
*Dec 31 2019 18:20:22: DAI-5-SENDER_IPMAC_BIND_DROP: IP & MAC Mismatch. Packet drop: VLAN 1, interface LAG1 and entry not found of SMAC E0:D5:5E:32:B1:92 and sender IP 192.168.0.20, aggre
*Dec 31 2019 18:20:19: DAI-5-SENDER_IPMAC_BIND_DROP: IP & MAC Mismatch. Packet drop: VLAN 1, interface LAG1 and entry not found of SMAC E0:D5:5E:32:B1:92 and sender IP 0.0.0.0, aggregated
*Dec 31 2019 18:20:19: DAI-5-SENDER_IPMAC_BIND_DROP: IP & MAC Mismatch. Packet drop: VLAN 1, interface LAG1 and entry not found of SMAC E0:D5:5E:32:B1:92 and sender IP 169.254.96.124, agg
)
*Dec 31 2019 18:22:41: AAA-5-CONNECT: New telnet connection for user admin, source 192.168.0.20 ACCEPTED
*Dec 31 2019 18:20:37: AAA-5-CONNECT: New http connection for user admin, source 192.168.0.20 ACCEPTED
*Dec 31 2019 18:20:22: DAI-5-SENDER_IPMAC_BIND_DROP: IP & MAC Mismatch. Packet drop: VLAN 1, interface LAG1 and entry not found of SMAC E0:D5:5E:32:B1:92 and sender IP 192.168.0.20
*Dec 31 2019 18:20:19: DAI-5-SENDER_IPMAC_BIND_DROP: IP & MAC Mismatch. Packet drop: VLAN 1, interface LAG1 and entry not found of SMAC E0:D5:5E:32:B1:92 and sender IP 0.0.0.0
*Dec 31 2019 18:20:19: DAI-5-SENDER_IPMAC_BIND_DROP: IP & MAC Mismatch. Packet drop: VLAN 1, interface LAG1 and entry not found of SMAC E0:D5:5E:32:B1:92 and sender IP 169.254.96.124
*Dec 31 2019 17:00:40: STP-6-PORT_STATE: Port LAG1 moving from Learning to Forwarding
*Dec 31 2019 17:00:38: STP-6-PORT_STATE: Port LAG1 moving from Blocking to Learning
*Dec 31 2019 17:00:19: LLDP-6-NEIGHBOR_DISCOVER: New neighbor on port GigabitEthernet2: Chassis ID 8C:02:FA:02:00:3E, Port ID gi2
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

14.5 SHOW LOGGING

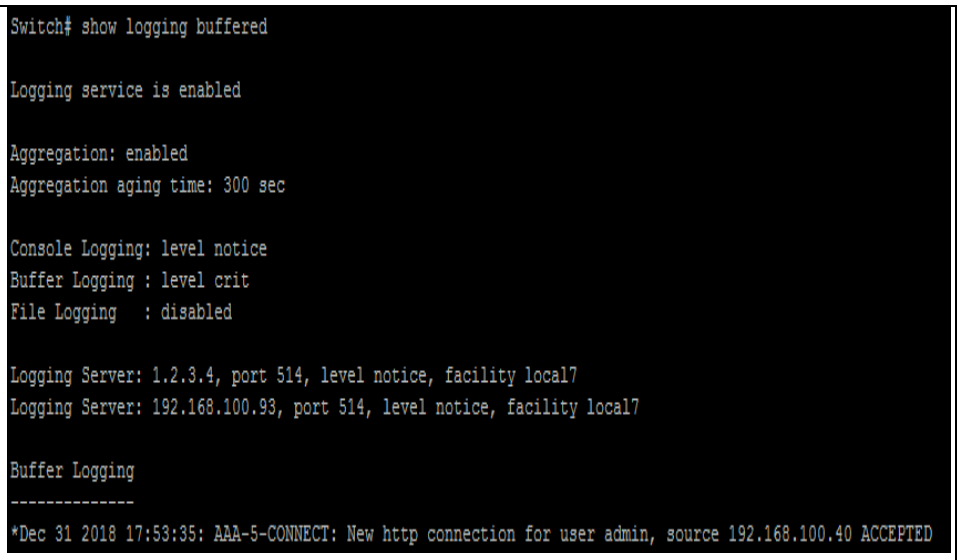
To display the global logging configuration, and the logging messages stored in the RAM and Flash, use the command show logging in the Privileged EXEC mode.

Switch# **show logging [buffered|file]**

Syntax	**show logging [buffered|file]**
Parameter	Buffered Display the log messages stored in the RAM. File Display the log messages stored in the Flash.
Mode	Privileged EXEC

Example	The following example shows the global logging configuration.
	
	Switch# **show logging**
	`Switch# show logging`
	
	`Logging service is enabled`
	
	`Aggregation: enabled`
	`Aggregation aging time: 300 sec`
	
	`Console Logging: level notice`
	`Buffer Logging : level crit`
	`File Logging : disabled`
	
	`Logging Server: 1.2.3.4, port 514, level notice, facility local7`
	`Logging Server: 192.168.100.93, port 514, level notice, facility local7`
	
	`Buffer Logging`
	`--------------`
	`*Dec 31 2018 17:53:35: AAA-5-CONNECT: New http connection for user admin, source 192.168.100.40 ACCEPTED`
	Switch# **show logging buffered**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

15. 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. Now let's break this down a little bit to understand how the MAC address table is built and used by an Ethernet switch to help traffic move along the path to its destination.

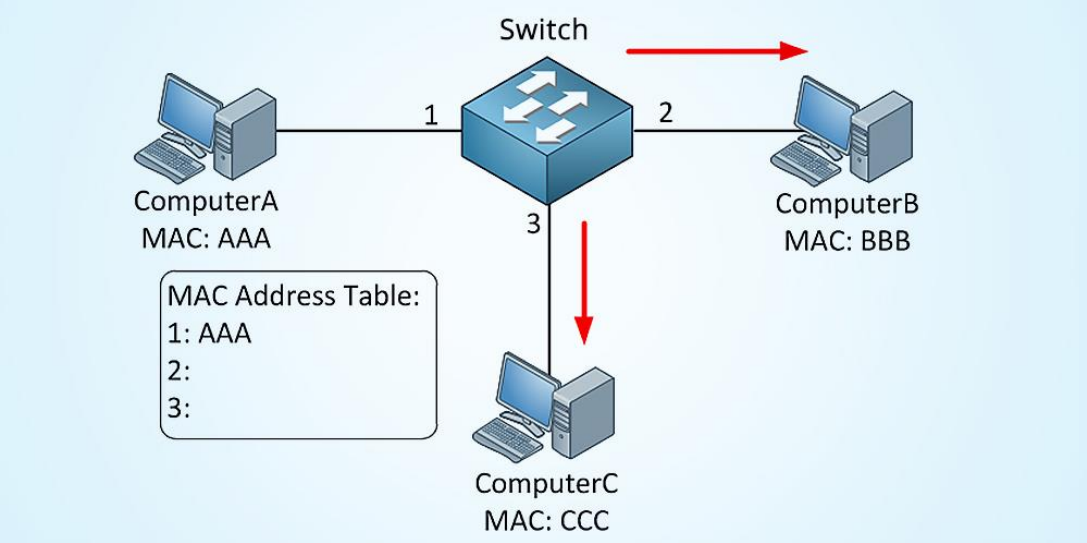


Fig 15.1 MAC Address Table

Normally your switch will automatically learn MAC addresses and fill its MAC address table (CAM table) by looking at the source MAC address of incoming frames and flooding frames if it doesn't know where to forward the frame.

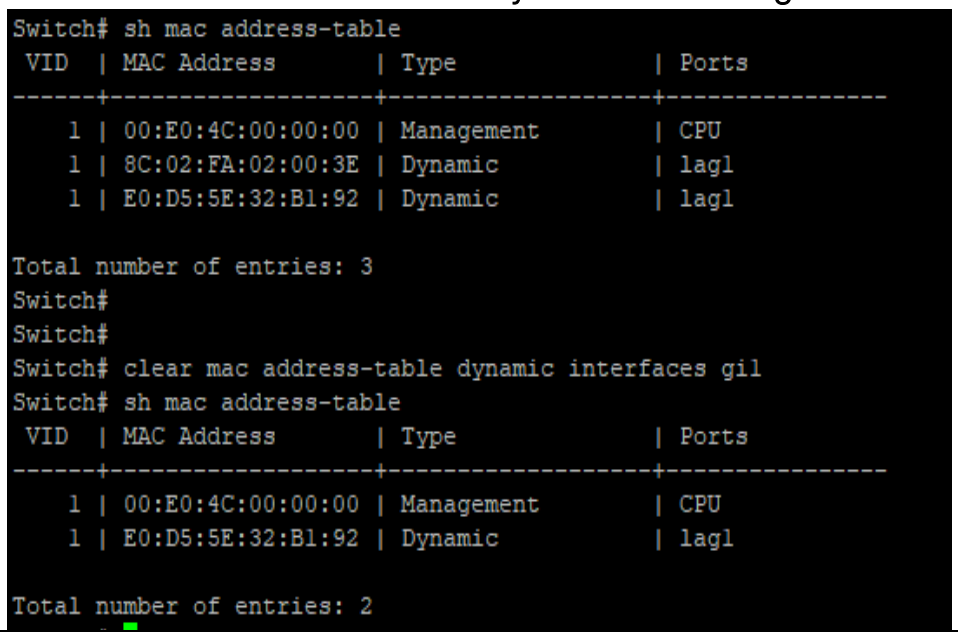
```
Switch# sh mac address-table
 VID   | MAC Address       | Type              | Ports
-------+-------------------+-------------------+---------------
    1  | 00:E0:4C:00:00:00 | Management        | CPU
    1  | 8C:02:FA:02:00:3E | Dynamic           | lag1
    1  | E0:D5:5E:32:B1:92 | Dynamic           | lag1

Total number of entries: 3
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

15.1 CLEAR MAC ADDRESS-TABLE

To clear the dynamic (learned) MAC entries from the MAC address table, the specific interface, or the specific VLAN, use the command clear mac address-table in the Privileged EXEC mode.

Switch# **clear mac address-table dynamic [interfaces** *IF_PORTS*| **vlan vlan-id]**

Syntax	**clear mac address-table dynamic [interfaces** *IF_PORTS*|**vlan vlan-id]**
Parameter	**Interfaces** IF_PORTS Delete all dynamic addresses learned on the specific interface. **vlan** vlan-id Delete all source addresses learned on the specific VLAN
Mode	Privileged EXEC
Example	The following example clears the learned MAC addresses on the interface gi1. Switch# **clear mac address-table dynamic interfaces gi1** 

```
Switch# sh mac address-table
 VID  | MAC Address       | Type              | Ports
------+-------------------+-------------------+---------------
    1 | 00:E0:4C:00:00:00 | Management        | CPU
    1 | 8C:02:FA:02:00:3E | Dynamic           | lag1
    1 | E0:D5:5E:32:B1:92 | Dynamic           | lag1

Total number of entries: 3
Switch#
Switch#
Switch# clear mac address-table dynamic interfaces gi1
Switch# sh mac address-table
 VID  | MAC Address       | Type              | Ports
------+-------------------+-------------------+---------------
    1 | 00:E0:4C:00:00:00 | Management        | CPU
    1 | E0:D5:5E:32:B1:92 | Dynamic           | lag1

Total number of entries: 2
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

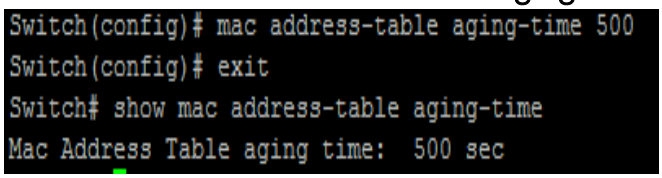
15.2 MAC ADDRESS-TABLE AGING-TIME

To set the aging time of the MAC address table, use the command macAddress-table aging-time in the Global Configuration mode.

Switch# **configure terminal**

Switch(config)# **mac accress-table aging-time** {seconds}

Syntax	**mac accress-table aging-time seconds**
Parameter	Seconds The time in seconds that an entry remains in the MAC address table. Its valid range is from 10 to 630 seconds, and the default value is 300 seconds.
Default	The default aging time is 300 seconds.
Mode	Global Configuration

Example	The following example set the agimg time to 500 seconds.
	Switch# **configure terminal**
	Switch(config)# **mac address-table aging-time** 500
	Switch# **show mac address-table aging-time**
	 
	`Switch(config)# mac address-table aging-time 500`
	`Switch(config)# exit`
	`Switch# show mac address-table aging-time`
	`Mac Address Table aging time:  500 sec`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

15.3 MAC ADDRESS-TABLE STATIC

To add a static address to the MAC address table, use the command mac address-table static in the Global Configuration mode. For the unicast MAC address filtering, use the command mac address-table static with parameter drop to drop the packets with the specified source or destination unicast MAC address. To delete the static entry from the MAC address table, use the **"no"** form of the command.

Switch# **configure terminal**

Switch(config)# **mac address-table static mac-addr vlan vlan-id interfaces** *{IF_PORTS}*
Switch(config)# **mac address-table static mac-addr vlan vlan-id drop**

Switch(config)# **no mac address-table static mac-addr vlan vlan-id**

Syntax	**mac address-table static mac-addr vlan** {vlan-id} **interfaces** *{IF_PORTS}* **mac address-table static mac-addr vlan** {vlan-id} **drop** **no mac address-table static mac-addr vlan vlan-id**
Parameter	**mac-addr** MAC address. **vlan** vlan-id Specify the VLAN ID for the interface. **Interface** IF_PORTS Specify the interface ID or a list of interface IDs. **drop**Drop the packets with the specified source or destination unicast MAC address.
Mode	Global Configuration
Example	The following example adds a static address into MAC address table. Switch#**configure terminal** Switch(config)# **mac address-table static** 00:11:22:33:44:55 **vlan** 1 **interfaces** gi5 Switch(config)# **mac address-table static** 00:11:22:33:44:55 **vlan** 1 **drop**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch#
Switch# configure terminal
Switch(config)# mac address-table static 00:11:22:33:44:55 vlan 1 interfaces gi5
Switch(config)#  mac address-table static 00:11:22:33:44:55 vlan 1 drop
Mac entry exist in static table
Switch(config)#
Switch# sh mac address-table static vlan 1
 VID  | MAC Address       | Type              | Ports
------+-------------------+-------------------+---------------
    1 | 00:11:22:33:44:55 | Static            | gi5

Total number of entries: 1
Switch#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

15.4 SHOW MAC ADDRESS-TABLE

To show the entry in the MAC address table, use the command show mac address-table in the Privileged EXEC mode.

Switch# **show mac address-table [dynamic|static] [interface** *IF_PORTS*] **[vlan vlan- id]**
Switch# **show mac address-table** [mac-addr] [vlan vlan-id]

Syntax	**show mac address-table [dynamic|static] [interface** *IF_PORTS*] **[vlan vlan- id]** **show mac address-table [mac-addr] [vlan vlan-id]**
Parameter	**dynamic** Display only dynamic MAC addresses **static** Display only static MAC addresses **Interface** *IF_PORTS* Display the MAC addresses entries for a specifc interface. **vlan** vlan-id Display the MAC address entries for a specific VLAN. **mac-addr** Display entries for a specific MAC address
Mode	Privileged EXEC
Example	The following example displays the entire MAC address table. Switch# **show mac address-table**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show mac address-table
 VID  | MAC Address       | Type              | Ports
------+-------------------+-------------------+----------------
    1 | 00:E0:4C:00:00:00 | Management        | CPU
    1 | 00:00:00:00:00:00 | Dynamic           | gi21
    1 | 00:11:22:33:44:55 | Static            | gi1
    1 | 00:15:FA:42:22:A1 | Dynamic           | gi21
    1 | 00:21:6B:E1:61:9E | Dynamic           | gi21
    1 | 1C:1B:0D:D6:E7:F0 | Dynamic           | gi21
    1 | 24:79:F3:B6:18:BF | Dynamic           | gi21
    1 | 3C:F7:A4:17:8B:DD | Dynamic           | gi21
    1 | 40:8D:5C:20:BC:1E | Dynamic           | gi21
    1 | 40:B0:76:72:4E:82 | Dynamic           | gi21
    1 | 44:94:FC:6E:29:66 | Dynamic           | gi21
    1 | 44:D1:FA:16:BC:A8 | Dynamic           | gi21
    1 | 44:D1:FA:25:CD:91 | Dynamic           | gi21
    1 | 44:D1:FA:25:D1:0F | Dynamic           | gi21
    1 | 44:D1:FA:25:D1:12 | Dynamic           | gi21
    1 | 44:D1:FA:25:D1:BD | Dynamic           | gi21
    1 | 48:88:CA:68:D8:79 | Dynamic           | gi21
    1 | 58:00:E3:5D:DB:45 | Dynamic           | gi21
    1 | 70:14:A6:81:05:BE | Dynamic           | gi21
    1 | 88:51:FB:55:6F:2E | Dynamic           | gi21
    1 | 90:2B:34:E2:AA:98 | Dynamic           | gi21
    1 | 98:09:CF:79:29:A1 | Dynamic           | gi21
--More--
```

Switch# **show mac address-table static interfaces gi1**

```
Switch# show mac address-table static interfaces gi1
 VID  | MAC Address       | Type              | Ports
------+-------------------+-------------------+----------------
    1 | 00:11:22:33:44:55 | Static            | gi1

Total number of entries: 1
```

Switch# **show mac address-table 00:11:22:33:44:55 vlan 100**

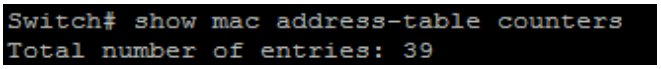
```
Switch# show mac address-table 00:11:22:33:44:55 vlan 100
 VID  | MAC Address       | Type              | Ports
------+-------------------+-------------------+----------------

Total number of entries: 0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

15.5 SHOW MAC ADDRESS-TABLE COUNTERS

To display the total entries in the MAC address table, use the command show mac address-table counters in the Privileged EXEC mode.

Switch# **show mac address-table counters**

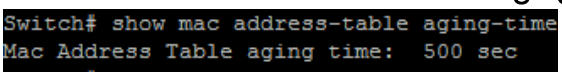
Syntax	**show mac address-table counters**
Mode	Privileged EXEC
Example	The following example display numbers of addresses in the address table. Switch# **show mac address-table counters** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

15.6 SHOW MAC ADDRESS-TABLE AGING-TIME

To show MAC address aging time, use the command show mac address-table aging-time in the Privileged EXEC mode.

Switch# **show mac address-table aging-time**

Syntax	**show mac address-table aging-time**
Mode	Privileged EXEC
Example	The following example displays aging time for the MAC address table. Switch# **show mac address-table aging-time** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

16. 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. The MAC based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet. You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. The MAC-based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet. You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table.

The MAC-based VLAN feature assigns hosts to a VLAN based on their MAC addresses. This feature is usually used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

16.1 VLAN MAC-VLAN GROUP (GLOBAL)

Use the vlan mac-vlan group command to create MAC address group. Use the **"no"** form of this command to delete specify group.

Switch#**configure terminal**
Switch(config)# **vlan mac-vlan group** *<1- 2147483647>* **mac-address mask** *<9-48>*

Switch(config)# **no vlan mac-vlan group mac-address mask** *<9-48>*

Syntax	**vlan mac-vlan group** *<1- 2147483647>* **mac-address mask** *<9-48>* **no vlan mac-vlan group mac-address mask** *<9-48>*
Parameter	*<1-2147483647>*Specify the group ID **mac-address**Specify the MAC address to be mapped. *<9-48>*Specify the mask length of MAC address.
Mode	Global Configuration

Example	The following example shows how to create a MAC group with group ID 3.
	Switch#**configure terminal**
	Switch(config)# **vlan mac-vlan group 333 22:33:44:55:66:77 mask 48**
	
	Switch# **show vlan mac-vlan groups**
	
	`Switch#`
	`Switch# configure terminal`
	`Switch(config)#  vlan mac-vlan group 333 22:33:44:55:66:77 mask 48`
	`Switch(config)#`
	`Switch# show vlan mac-vlan groups`
	
	`  Mac Address    Mask   Group Id`
	`---------------- ---- ------------`
	`22:33:44:55:66:77   48         333`
	
	`Total 1 Entry`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

16.2 VLAN MAC-VLAN GROUP (INTERFACE)

Use the **"vlan mac-vlan group"** to create mapping of group and VLAN ID of an interface. Use the **"no"** form of this command to delete mapping.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **vlan mac-vlan group** *<1- 2147483647>* **vlan** *<1-4094>*

Switch(config-if)# **no vlan mac-vlan** [**group** *<1- 2147483647>*]

Syntax	**vlan mac-vlan group** *<1- 2147483647>* **vlan <1-4094>** **no vlan mac-vlan** [**group** *<1- 2147483647>*]
Parameter	*<1-2147483647>* Specify the group ID. (optional in no form) Delete all mapping group if not specify. *<1-4094>* Specify the VLAN ID to give to match packet
Mode	Interface Configuration
Example	The following example shows how to mapping group id 333 to VLAN 100 on interface GigabitEthernet 1. Switch# Switch# **configure terminal** Switch(config)# **interface GigabitEthernet** 3 Switch(config-if)# **switchport mode hybrid** Switch(config-if)# **vlan mac-vlan group** 333 **vlan** 2 Switch(config-if)# Switch# **show vlan mac-vlan groups**

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 3
Switch(config-if)# switchport mode hybrid
Switch(config-if)# vlan mac-vlan group 333 vlan 2
Switch(config-if)#
Switch#  show vlan mac-vlan groups

   Mac Address    Mask   Group Id
----------------- ---- ------------
22:33:44:55:66:77   48         333

Total 1 Entry
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

16.3 SHOW VLAN MAC-VLAN GROUPS

Use the show vlan mac-vlan groups command to display mac groups configuration.

Switch# **show vlan mac-vlan groups**

Syntax	**show vlan mac-vlan groups**
Mode	Privileged EXEC

Example	This following example shows how to display mac group.
	
	Switch# **show vlan mac-vlan groups**
	`Switch# show vlan mac-vlan groups`
	
	`Mac Address Mask Group Id`
	`----------------- ---- ------------`
	`22:33:44:55:66:77 48 333`
	
	`Total 1 Entry`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

16.4 SHOW VLAN MAC-VLAN INTERFACES

Use the show vlan mac-vlan interface command in EXEC mode to display the mac-vlan interfaces setting.

Switch# **show vlan mac-vlan [interfaces** *IF_PORTS*]

Syntax	**show vlan mac-vlan [interfaces** *IF_PORTS*]
Parameter	*IF_PORTS* (Optional) Specify interfaces mac vlan to display. Display all ports if not specif.
Mode	Privileged EXEC

Example	The following example shows how to display the MAC-Based VLAN interfaces setting
	Switch# **show vlan mac-vlan interfaces GigabitEthernet 1**
	`Switch# show vlan mac-vlan interfaces GigabitEthernet 1`
	
	`Interface gi1 Mac based VLANs:`
	`  Group ID    Vlan ID`
	`------------  -------`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

17. MANAGEMENT ACL

An Access Control List (ACL) is a set of rules that is usually used to filter network traffic. ACLs can be configured on network devices with packet filtering capabilities, such as L2/L3 Switches, routers, and firewalls.

ACLs contain a list of conditions that categorize packets and help you determine when to allow or deny network traffic. They are applied on the interface basis to packets leaving or entering an interface

Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attack. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network. Access control lists (ACLs) classify traffic with the same characteristics. The ACL can have multiple access control entries (ACEs), which are commands that match fields against the contents of the packet. ACLs can filter packets received on interface by many fields such as ip address, mac address and deny or permit the packets.

Access control entry (ACE): Each ACE includes an action element (permit or deny) and a series of filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.

MAC ACL: MAC ACL can filter packet by mac-sa and mac-da, and the mac-address can be masked, or configured as host id, or configured as any to filter all MAC addresses. MAC ACL can also filter other L2 fields such as COS, VLAN-ID, INNER-COS, INNER-VLAN-ID, L2 type, L3 type.

IPv4 ACL: IPv4 ACL can filter packet by ip-sa and ip-da, and ip-address can be masked, or configured as host id, or configured as any to filter all IPv4 address. IPv4 ACL can also filter other L3 fields such as DSCP, L4 protocol and L4 fields such as TCP port, UDP port, and so on.

Time Range: Time range can define a period of time only between which the ACE can be valid if the ACE is associated to the time range.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

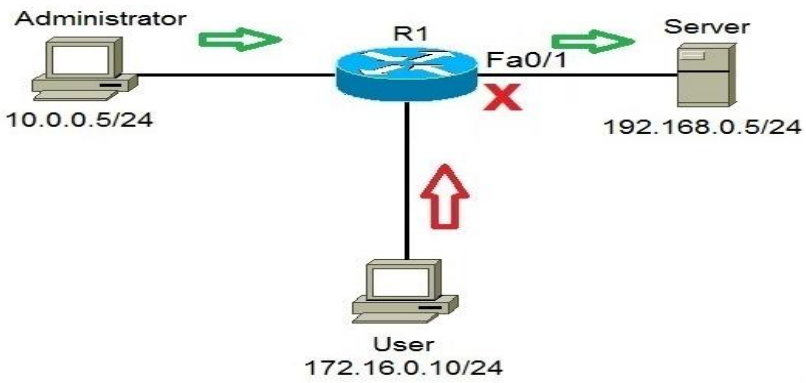


Fig 17.1 ACL Feature

Advantages of ACL

- Improve network performance.
- Provides security as administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of network.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

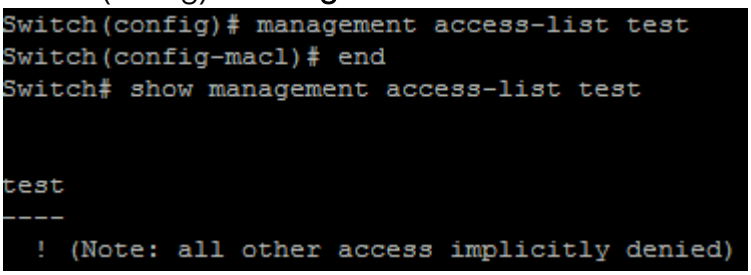
17.1 MANAGEMENT ACCESS-LIST

Use the management access-list command to create a management access list and to enter management access-list configuration mode. The name of ACL must be unique that cannot have same name with other management ACL. Use the **"no"** form of this command to delete.

Switch#**configure terminal**
Switch(config)# **management access-list** *[NAME]*

Switch(config)#**no management access-list** *[NAME]*

Syntax	**management access-list NAME** **no management access-list NAME**
Parameter	NAME The name of management ACL
Mode	Global Configuration

Example	The following example shows how to add a management ACL with name **"test"**
	Switch#**configure terminal**
	Switch(config)# **management access-list** test
	 
	`Switch(config)# management access-list test`
	`Switch(config-macl)# end`
	`Switch# show management access-list test`
	
	`test`
	`----`
	`  ! (Note: all other access implicitly denied)`

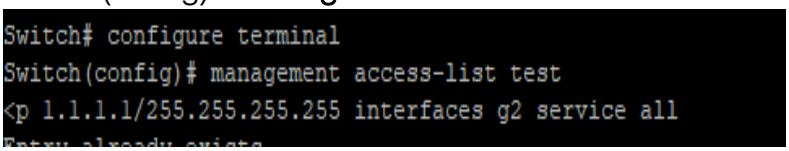
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

17.2 MANAGEMENT ACCESS-CLASS

Use the management access-class command to activate a management ACL. Use the **"no"** form of this command to delete.

Switch#**configure terminal**
Switch(config)# **management access-class** *[NAME]*

Switch(config)# **no management access-class**

Syntax	**management access-class** *[NAME]* **no management access-class**
Parameter	NAME The name of management ACL to be used
Mode	Global Configuration
Example	The following example shows how to add a management ACL with name **"test"** Switch#**configure terminal** Switch(config)# **management access-class** test 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

17.3 DENY

Use the deny command to add deny rules that drop those packets hit the rule.

Switch#**configure terminal**
Switch(config)# **management access-list** *[NAME]*
Switch(config-macl)# **sequence** *<1-65535>*] **deny interfaces** *{IF_PORTS}***service (all|http|https|snmp|ssh|telnet)**

Switch(config-macl)# [**sequence** *<1-65535>*] **deny ip** A.B.C.D/A.B.C.D **interfaces** *{IF_PORTS}***service (all|http|https|snmp|ssh|telnet)**

Switch(config-macl)# [**sequence** *<1-65535>*] **deny ipv6** *X:X::X:X/<0-128>* **interfaces** *{IF_PORTS}***service (all|http|https|snmp|ssh|telnet)**

Syntax	[sequence *<1-65535>*] deny interfaces *{IF_PORTS}*service (all|http|https|snmp|ssh|telnet) [sequence *<1-65535>*] deny ip A.B.C.D/A.B.C.D interfaces *{IF_PORTS}* service (all|http|https|snmp|ssh|telnet) [sequence *<1-65535>*] deny ipv6 *X:X::X:X/<0-128>* interfaces *{IF_PORTS}* service (all|http|https|snmp|ssh|telnet)
Parameter	*<1-65535>* (Optional) Specify sequence index of ACL entry, the sequence index represent the priority of an entry in ACL. If not specified, the switch assigns a number from 1 in ascending order. **interfaces** IF_PORTS Specify the interface ID or a list of interface IDs. **ip**A.B.C.D/A.B.C.DSpecify the source IP address and mask of packet. **ipv6** X:X::X:X/<0-128> Specify the source IPv6 address and prefix length of packet. **(all|http|https|snmp|ssh|telnet)** Specify the type of services
Mode	Management Access-List Configuration
Example	The following example shows how to add a deny rule to drop all types of services packets that source ip is 1.1.1.1 from interface gi2. Switch#**configure terminal** Switch(config)# **management access-list** commando Switch(config-macl)#**sequence 1 deny ip 10.10.10.10/255.255.255.255 interfaces gi2 service all**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch# configure terminal Switch(config)# management access-list commando Switch(config-macl)# sequence 1 deny ip 10.10.10.10/255.255.255.255 interfaces gi2 service all Switch# **show management access-list** commando Switch# sh management access-list commando commando -------- sequence 1 deny ip 10.10.10.10/255.255.255.255 interfaces gi2 service all ! (Note: all other access implicitly denied)

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

17.4 PERMIT

Use the permit command to add permit rules that bypass those packets hit the rule.

Switch#**configure terminal**
Switch(config)# **management access-list** *[NAME]*
Switch(config-macl)# **sequence** *<1-65535>*] **permit interfaces** *{IF_PORTS}* **service(all|http|https|snmp|ssh|telnet)**

Switch(config-macl)# [**sequence** *<1-65535>*] **permit ip** A.B.C.D/A.B.C.D **interfaces** *{IF_PORTS}***service (all|http|https|snmp|ssh|telnet)**

Switch(config-macl)# [**sequence** *<1-65535>*] **permit ipv6** *X:X::X:X/<0-128>* **interfaces** *{IF_PORTS}***service (all|http|https|snmp|ssh|telnet)**

Syntax	[sequence *<1-65535>*] permit interfaces *{IF_PORTS}* service (all|http|https|snmp|ssh|telnet) [sequence *<1-65535>*] permit ip A.B.C.D/A.B.C.D interfaces *{IF_PORTS}*service (all|http|https|snmp|ssh|telnet) [sequence *<1-65535>*] permit ipv6 *X:X::X:X/<0-128>* interfaces *{IF_PORTS}*service (all|http|https|snmp|ssh|telnet)
Parameter	*<1-65535>* (Optional) Specify sequence index of ACL entry, the sequence index represent the priority of an entry in ACL. If not specified, the switch assigns a number from 1 in ascending order. **interfaces***IF_PORTS* Specify the interface ID or a list of interface IDs. **ip** A.B.C.D/A.B.C.D Specify the source IP address and mask of packet. **ipv6***X:X::X:X/<0-128>*Specify the source IPv6 address and prefix length of packet. **(all|http|https|snmp|ssh|telnet)** Specify the type of services
Mode	Management Access-List Configuration
Example	The following example shows how to add a permit rule to bypass http service packets that source ip is 2.2.2.2 from interface gi2. Switch#**configure terminal** Switch(config)# **management access-list test** Switch(config-macl)# **sequence 2 permit ip 2.2.2.2/255.255.255.255 interfaces gi2 service http**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# management access-list test
Switch(config-macl)# sequence 2 permit ip 2.2.2.2/255.255.255.255 interfaces gi2 service http
```

Switch#Show management access-list test

```
Switch# sh management access-list test


test
----
  sequence 1 deny ip 1.1.1.1/255.255.255.255 interfaces gi2 service all
  sequence 2 permit ip 2.2.2.2/255.255.255.255 interfaces gi2 service http
```

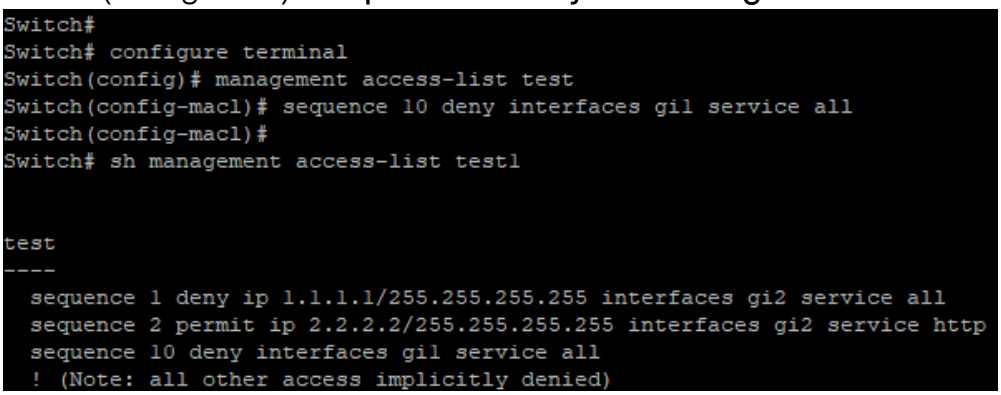
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

17.5 NO SEQUENCE

Use the **"no"** sequence command to delete an entry in management ACL.

Switch#**configure terminal**
Switch(config)# **management access-list** *[NAME]*

Switch(config-macl)# **no sequence** *<1-65535>*

Syntax	**no sequence** *<1-65535>*
Parameter	*<1-65535>*Specify sequence index of ACL entry to delete.
Mode	Management Access-List Configuration
Example	The following example shows how to delete an entry. Switch#**configure terminal** Switch(config)# **management access-list** test Switch(config-macl)# **sequence 10 deny interfaces gi1 service all** 

```
Switch#
Switch# configure terminal
Switch(config)# management access-list test
Switch(config-macl)# sequence 10 deny interfaces gi1 service all
Switch(config-macl)#
Switch# sh management access-list testl


test
----
  sequence 1 deny ip 1.1.1.1/255.255.255.255 interfaces gi2 service all
  sequence 2 permit ip 2.2.2.2/255.255.255.255 interfaces gi2 service http
  sequence 10 deny interfaces gi1 service all
  ! (Note: all other access implicitly denied)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

17.6 SHOW MANAGEMENT ACCESS-CLASS

Use the show management access-class command to show the active management access-list.

Switch# **show management access-class**

Syntax	**show management access-class**
Mode	Privileged EXEC

Example	The example shows how to show management access-class
	Switch# **show management access-class**
	`Switch(config)#`
	`Switch# show management access-class`
	`Management access-class is enabled, using access-list test`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

17.7 SHOW MANAGEMENT ACCESS-LIST

Use the show management access-list command to show management ACL.

Switch# **show management access-list** *[NAME]*

Syntax	**show management access-list** *[NAME]*
Parameter	*NAME* Specify the name of management ACL to displayed
Mode	Privileged EXEC

Example	The example shows how to show management access-list
	
	Switch# **show management access-list 1**
	`Switch# show management access-list test`
	
	`test`
	`----`
	`  sequence 2 permit ip 2.2.2.2/255.255.255.255 interfaces gi2 service http`
	`  sequence 10 deny interfaces gi1 service all`
	`  ! (Note: all other access implicitly denied)`
	`List does not exist`
	`Switch#`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

18. MIRROR

You can analyze network traffic passing through ports by using Switched Port Analyzer (SPAN). This sends a copy of the traffic to another port on the switch that has been connected to a Switch Probe device, another Remote Monitoring (RMON) probe or security device. SPAN mirrors receive or transmit (or both) traffic on one or more source ports to a destination port for analysis.
Remote SPAN (RSPAN) extends SPAN by enabling RMON of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources is copied onto the RSPAN VLAN through a reflector port and then forwarded over trunk ports carrying the RSPAN VLAN to any RSPAN destination session monitoring the RSPAN VLAN.
SPAN and RSPAN do not affect the switching of network traffic on source ports. A copy of the packets received or sent by the source interfaces are sent to the destination interface. Except for traffic that is required for the SPAN or RSPAN session, reflector ports and destination ports do not receive or forward traffic.

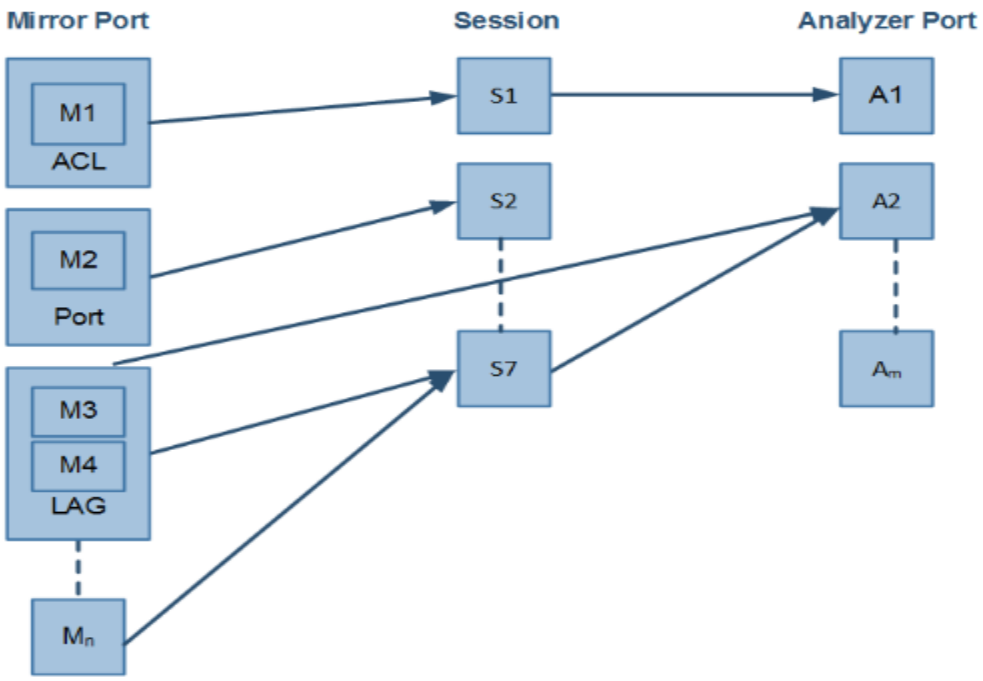


Fig 18.1 Mirror and Analyzer Port

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

18.1 MIRROR SESSION DESTINATION INTERFACE

Use the **"mirror session destination interface"** command to start a destination interface of a port mirror session. Use the **"no"** form of this command to stop a destination interface of a port mirroring session. Use the **"no mirror session"** command to disable all mirror sessions or specific mirror session.

Switch#**configure terminal**

Switch(config)# **mirror session** *<1-4>* **destination interface** IF_NMLPORT [allow-ingress]

Switch(config)# **no mirror session** *<1-4>***destination interface** IF_NMLPORT
Switch(config)# **no mirror session** (*<1-4>*| **all**)

Syntax	**mirror session** *<1-4>* **destination interface** IF_NMLPORT [allow-ingress] **no mirror session** *<1-4>***destination interface** IF_NMLPORT **no mirror session** (*<1-4>*| **all**)
Parameter	*<1-4>* Specify the mirror session to configure IF_NMLPORT Specify the SPAN destination. A destination must be aphysical port allow-ingress Enable ingress traffic forwarding.
Default	No monitor sessions are configured.
Mode	Global Configuration

Example	The following example shows how to create a local session 1 to monitor both sent and received traffic on source port GigabitEthernet2.
	
	Switch#**configure terminal**
	Switch(config)#**mirror session** 1 **destination interface GigabitEthernet** 11 **allow-ingress**
	`Switch# configure terminal`
	`Switch(config)# mirror session 1 destination interface GigabitEthernet 11 allow-ingress`
	
	Switch#**show mirror session 1**
	`Switch#  show mirror session 1`
	
	`Session 1 Configuration`
	`Mirrored source   : Not Config`
	`Destination port  : gill`
	`Ingress State: enabled`
	
	To disable Mirror session

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch#configure terminal Switch(config)#no mirror session 1 destination interface GigabitEthernet 11 Switch(config)# no mirror session all

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

18.2 MIRROR SESSION SOURCE INTERFACE

Use the **"mirror session source interface"** command to start a port mirror session. Use the **"no"** form of this command to stop a port mirroring session. Use the **"no mirror session"** command to disable all mirror sessions or specific mirror session.

Switch#**configure terminal**

Switch(config)# **mirror session** *<1-4>* **source interfaces IF_PORTS (both | rx | tx)**

Switch(config)# **no mirror session** *<1-4>***source interfaces IF_PORTS (both | rx | tx)**
Switch(config)# **no mirror session (***<1-4>***| all)**

Syntax	**mirror session** *<1-4>* **source interfaces IF_PORTS (both | rx | tx)** **no mirror session** *<1-4>***source interfaces IF_PORTS (both | rx | tx)** **no mirror session (***<1-4>***| all)**
Parameter	*<1-4>* Specify the mirror session to configure **IF_PORTS** Specify the source interface, Valid interfaces include physical ports and port channels. both Mirror tx and rx direction rx Mirror rx direction only tx Mirror tx direction only
Mode	Global Configuration

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Example	The following example shows how to create a local SPAN session 1 to monitor both sent and received rate on source port gi3-5.
	
	Switch#**configure terminal**
	Switch(config)# **mirrorsession** 1 **sourceinterfaces** GigabitEthernet 3-5 **both**
	Switch(config)# **mirror session** 1 **destination interface** GigabitEthernet 2
	Switch# **show mirror session**1
	`Switch(config)# mirror session 1 source interface GigabitEthernet 3-5 both`
	`Switch(config)# mirror session 1 destination interface GigabitEthernet 2`
	`Switch(config)# exit`
	`Switch# show mirror session 1`
	
	`Session 1 Configuration`
	`Source RX Port : gi3-5`
	`Source TX Port : gi3-5`
	`Destination port : gi2`
	`Ingress State: disabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

18.3 SHOW MIRROR

Use the show mirror command to display mirror session configuration.

Switch#**show mirror** [**session** *<1-4>*]

Syntax	**show mirror** [**session** *<1-4>*]
Parameter	*<1-4>*Specify the mirror session to display
Mode	Privileged EXEC

Example	This following example shows how to display mirror session configuration
	
	Switch# **show mirror**
	`Switch# show mirror`
	
	`Session 1 Configuration`
	`Source RX Port : gi3-5`
	`Source TX Port : gi3-5`
	`Destination port : gi2`
	`Ingress State: disabled`
	
	`Session 2 Configuration`
	`Mirrored source : Not Config`
	`Destination port : Not Config`
	
	`Session 3 Configuration`
	`Mirrored source : Not Config`
	`Destination port : Not Config`
	
	`Session 4 Configuration`
	`Mirrored source : Not Config`
	`Destination port : Not Config`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19. MLD SNOOPING

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes configured to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2, and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a sub protocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

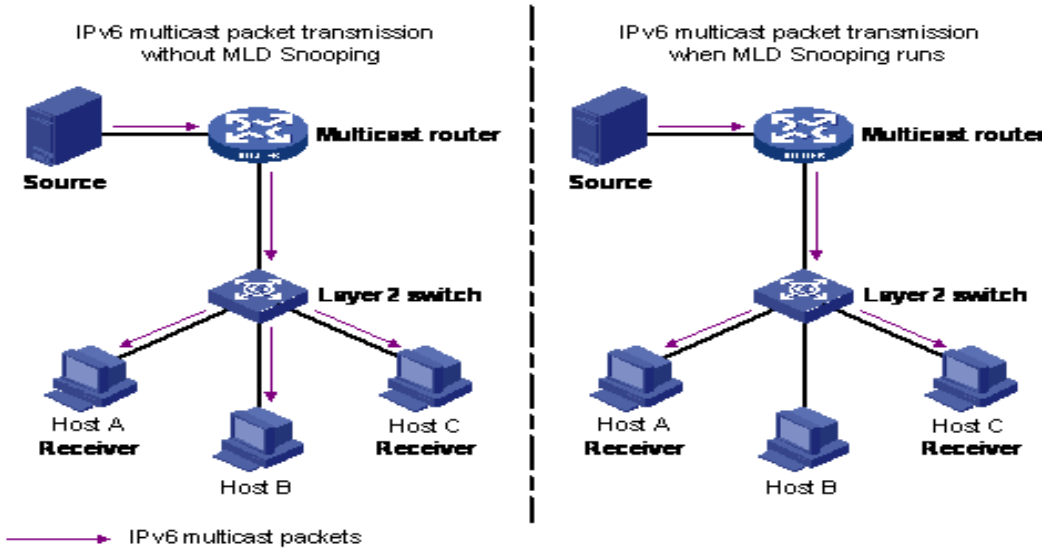


Fig 19.1 MLD snooping concept

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.1 IPV6 MLD SNOOPING

Generally, Layer 2 switches can use MLD snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated with IPv6 multicast devices. As the name implies, MLD snooping requires the LAN switch to snoop on the MLD transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an MLD report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry, when it receives an MLD Leave Group message from a host, it removes the host port from the table entry. It also deletes entries per entry if it does not receive MLD membership reports from the multicast clients. The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send report and are added to the forwarding table entry. The switch forwards only one report per IPv6 multicast group to the multicast router. It creates one entry per VLAN in the Layer 2 forwarding table for each MAC group from which it receives an MLD report.

Layer 2 multicast groups learned through MLD snooping are dynamic. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by MLD snooping. Multicast group membership lists can consist of both user-defined and MLD snooping-learned settings.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

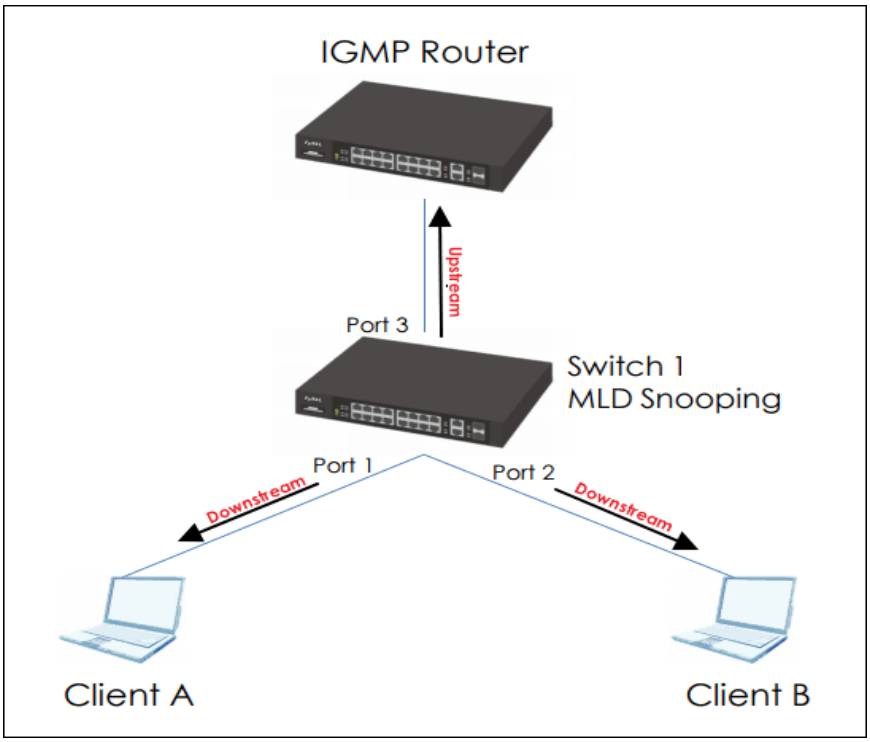


Fig 19.2 ipv6 mld snooping

Switch#**configure terminal**
Switch(config)# **ipv6 mld snooping**

Switch(config)# **no ipv6 mld snooping**

Syntax	**ipv6 mld snooping** **no ipv6 mld snooping**
Default	Default is disabled
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld snooping**
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping`
	
	Switch(config)#**no ipv6 mld snooping**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.2 IPV6 MLD SNOOPING REPORT-SUPPRESSION

Use the ipv6 mld snooping report-suppression command to enable MLD snooping report-suppression function. Use the **"no"** form of this command to disable. Disable report-suppression will forward all received reports to the vlan router ports. You can verify settings by the show ipv6 mld snooping command.

Switch#**configure terminal**
Switch(config)# **ipv6 mld snooping report-suppression**

Switch(config)# **no ipv6 mld snooping report-suppression**

Syntax	**ipv6 mld snooping report-suppression** **no ipv6 mld snooping report-suppression**
Parameter	None
Default	Default is enabled
Mode	Global Configuration
Example	The following example specifies that disable ipv6 mld snooping report-suppression test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping report-suppression** Switch# configure terminal Switch(config)# ipv6 mld snooping report-suppression Switch(config)# **no ipv6 mld snooping report-suppression**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.3 IPV6 MLD SNOOPING VERSION

Use the ipv6 mld snooping version command to change MLD support version. Version 2 packet won't be processed if choose version 1. You can verify settings by the show ip igmp snooping command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping version (1|2)**

Syntax	**ipv6 mld snooping version (1|2)**
Parameter	**(1|2)** Ipv6 mld snooping running version 1 or 2
Default	Default is version 1
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping version 2.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld snooping version 2**
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping version 2`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.4 IPV6 MLD SNOOPING UNKNOWN-MULTICAST ACTION

When igmp and mld snooping disabled, it can't set action router-port. When disable igmp snooping & mld snooping, it set unknown multicast action flood. When action is router-port to flood or drop, it will delete the unknown multicast group entry. Use the ipv6 mld snooping unknown-multicast action command to change action. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping command.

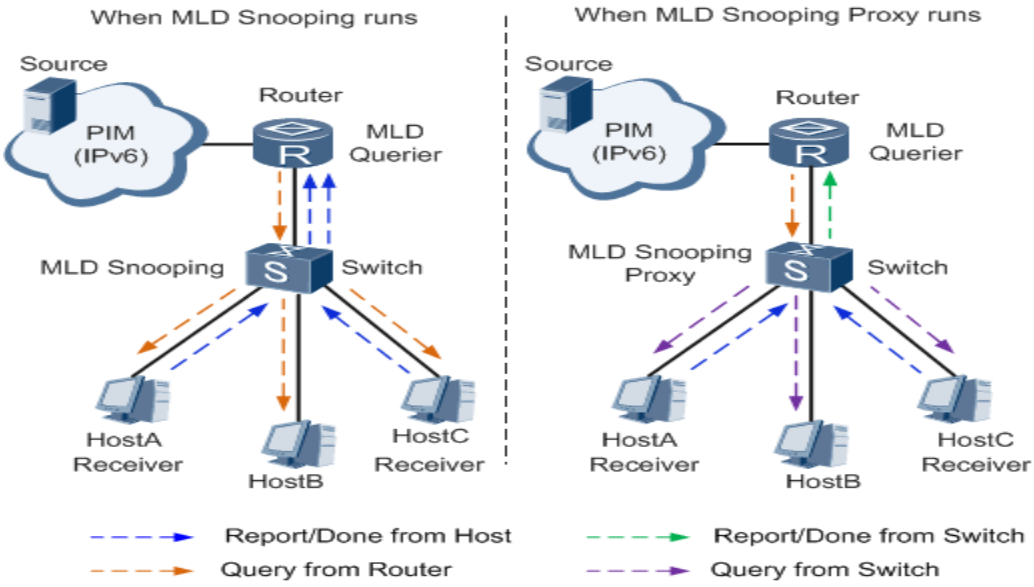


Fig 19.3 MLD SNOOPING action

Switch#**configure terminal**

Switch(config)# **ipv6 mld snooping unknown-multicast action (drop | flood |router-port)**

Switch(config)# **no ipv6 mld snooping unknown-multicast action**

Syntax	**ipv6 mld snooping unknown-multicast action (drop | flood |router-port)** **no ipv6 mld snooping unknown-multicast action**
Parameter	**(drop | flood | router- port)**Dropflood in vlan or forward to router port of unknown multicast packet
Default	Default is flood

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Mode	Global Configuration
Example	The following example specifies that set ipv6 mld unknown multicast action router-port test. Switch#configure terminal Switch(config)# ipv6 mld snooping unknown-multicast action router-port Switch# configure terminal Switch(config)# ipv6 mld snooping unknown-multicast action router-port

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.5 IPV6 MLD SNOOPING VLAN

Disable will clear all ipv6 mld snooping dynamic group and dynamic router port and make all static ip igmp group invalid of this vlan. It will not learn dynamic group and router port by igmp message anymore. Use the ipv6 mld snooping vlan command to enable MLD on VLAN. Use the **"no"** form of this command to disable. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**
Switch(config)# **ipv6 mld snooping vlan** *<VLAN-LIST>*

Switch(config)# **no ipv6 mld snooping vlan** *<VLAN-LIST>*

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **no ipv6 mld snooping vlan** *<VLAN-LIST>*
Parameter	*VLAN-LIST* specifies VLAN ID list to set
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping vlan test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld snooping vlan** 2
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping vlan 2`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.6 IPV6 MLD SNOOPING VLAN PARAMETERS

MLD (on a multicast router) or, locally, the MLD snooping querier, sends out periodic general MLD queries that the switch forwards through all ports in the VLAN. No ipv6 mld snooping vlan 1 (last-member-query-count | last-member-query- interval | query-interval | response-time | robustness-variable)' will set the vlan parameters to default. The cli setting will change the ipv6 mld vlan parameters admin settings.

Switch#configure terminal
Switch(config)# ipv6 mld snooping vlan *<VLAN-LIST>*last-member-query-count *<1-7>*
Switch(config)# no ipv6 mld snooping vlan *<VLAN-LIST>*last-member-query-count
Switch(config)# ipv6 mld snooping vlan *<VLAN-LIST>*last-member-query-interval *<1-60>*
Switch(config)# no ipv6 mld snooping vlan *<VLAN-LIST>*last-member-query-interval[no]
Switch(config)# ipv6 mld snooping vlan *<VLAN-LIST>*router learn pim-dvmrp[no]
Switch(config)# ipv6 mld snooping vlan *<VLAN-LIST>*fastleave
Switch(config)# ipv6 mld snooping vlan *<VLAN-LIST>*query-interval *<30-18000>*
Switch(config)# no ipv6 mld snooping vlan *<VLAN-LIST>*query-interval
Switch(config)# ipv6 mld snooping vlan *<VLAN-LIST>*response-time *<5-20>*
Switch(config)# no ipv6 mld snooping vlan *<VLAN-LIST>*response-time
Switch(config)# ipv6 mld snooping vlan *<VLAN-LIST>*robustness-variable *<1-7>*
Switch(config)# no ipv6 mld snooping vlan *<VLAN-LIST>*robustness-variable

Syntax	ipv6 mld snooping vlan *<VLAN-LIST>*last-member-query-count *<1-7>* no ipv6 mld snooping vlan *<VLAN-LIST>*last-member-query-count ipv6 mld snooping vlan *<VLAN-LIST>*last-member-query-interval *<1- 60>* no ipv6 mld snooping vlan *<VLAN-LIST>*last-member-query-interval[no] ipv6 mld snooping vlan *<VLAN-LIST>*router learn pim-dvmrp[no] ipv6 mld snooping vlan *<VLAN-LIST>*fastleave ipv6 mld snooping vlan *<VLAN-LIST>*query-interval *<30-18000>* no ipv6 mld snooping vlan *<VLAN-LIST>*query-interval ipv6 mld snooping vlan *<VLAN-LIST>*response-time *<5-20>*

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	no ipv6 mld snooping vlan *<VLAN-LIST>***response-time** **ipv6 mld snooping vlan** *<VLAN-LIST>***robustness-variable** *<1-7>* **no ipv6 mld snooping vlan** *<VLAN-LIST>***robustness-variable**
Parameter	*VLAN-LIST* specifies VLAN ID list to set **last-member-query-count***<1-7>* **last-member-query-interval***<1-60>* **query-interval***<30-18000>* **response-time***<5-20>* **robustness-variable** specifies a robustness value to set, default is 2 *<1-7>*
Default	no ipv6 mld snooping vlan 1-4094 last-member-query-count no ipv6 mld snooping vlan 1-4094 last-member-query-interval ipv6 mld snooping vlan 1-4094 router learn pim-dvmrp no ipv6 mld snooping vlan 1-4094 fastleave no ipv6 mld snooping vlan 1-4094 query-interval no ipv6 mld snooping vlan 1-4094 response-time no ipv6 mld snooping vlan 1-4094 robustness-variable
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan parameters test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 1 **fastleave** Switch(config)# **ipv6 mld snooping vlan** 1 **last-member-query-count** 5 Switch(config)# **ipv6 mld snooping vlan** 1 **last-member-query-interval** 3 Switch(config)**# ipv6 mld snooping vlan** 1 **query-interval** 100 Switch(config)# **ipv6 mld snooping vlan** 1 **response-time** 12 Switch(config)**# ipv6 mld snooping vlan** 1 **robustness-variable** 4 Switch# **show ipv6 mld snooping vlan** 1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show ipv6 mld snooping vlan 1

MLD Snooping is globaly enabled
MLD Snooping VLAN 1 admin : disabled
MLD Snooping oper mode : disabled
MLD Snooping robustness: admin 4 oper 2
MLD Snooping query interval: admin 100 sec oper 125 sec
MLD Snooping query max response : admin 12 sec oper  10 sec
MLD Snooping last member query counter: admin 5  oper 2
MLD Snooping last member query interval: admin 3 sec  oper 1 sec
MLD Snooping immediate leave: enabled
MLD Snooping automatic learning of multicast router ports: enabled
```

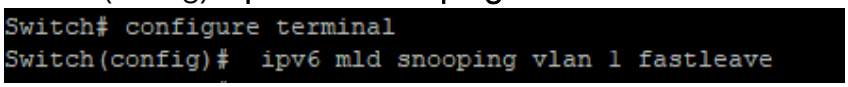
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.7 IPV6 MLD SNOOPING VLAN FASTLEAVE

Use the ipv6 mld snooping vlan fastleave command to enable fastleave function. Group will remove port immediately when receive leave packet. Use the **"no"** form of this command to disable. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**
Switch(config)# **ipv6 mld snooping vlan** *<VLAN-LIST>***fastleave**

Switch(config)# **no ipv6 mld snooping vlan** *<VLAN-LIST>***fastleave**

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>***fastleave** **no ipv6 mld snooping vlan** *<VLAN-LIST>***fastleave**
Parameter	*VLAN-LIST* specifies VLAN ID list to set
Default	Default is disabled
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan fastleave test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 1 **fastleave**  Switch(config)# **no ipv6 mld snoopingvlan** 1 **fastleave**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.8 IPV6 MLD SNOOPING VLAN LAST-MEMBER-QUERY-COUNT

Use the ipv6 mld snooping vlan last-member-query-count command to change how many query packets will send. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping vlan command

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **last-member-query-count** *<1-7>*

Switch(config)#**no ipv6 mld snooping vlan** *<VLAN-LIST>* **last-member-query-count**

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **last-member-query-count** *<1-7>* **no ipv6 mld snooping vlan** *<VLAN-LIST>* **last-member-query-count**
Parameter	VLAN-LIST last-member-query-count *<1-7>* specifies VLAN ID list to set. Specifies last member query count to set
Default	Default is 2
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan last-member-query-count test. Switch#**configure terminal** Switch(config)**# ipv6 mld snooping vlan** 1 **last-member-query-count** 5 Switch# configure terminal Switch(config)# ipv6 mld snooping vlan 1 last-member-query-count 5 Switch(config)# **no ipv6 mld snooping vlan** 1 **last-member-query-count** 5

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.9 IPV6 MLD SNOOPING VLAN LAST-MEMBER-QUERY-INTERVAL

Use the ipv6 mld snooping vlan last-member-query-interval command to set interval between each query packet. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **last-member-query-interval** *<1-60>*

Switch(config)# **no ipv6 mld snooping vlan** *<VLAN-LIST>* **last-member-query-interval**

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **last-member-query-interval** *<1- 60>* **no ipv6 mld snooping vlan** *<VLAN-LIST>* **last-member-query-interval**
Parameter	VLAN-LIST last-member-query-interval *<1-60>* specifies VLAN ID list to set.specifies last member query interval to set
Default	Default is 1
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping vlan last-member-query-interval test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld snooping vlan** 1 **last-member-query-interval** 3
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping vlan 1 last-member-query-interval 3`
	
	Switch(config)#**no ipv6 mld snooping vlan** 1 **last-member-query-interval** 3

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.10 IPV6 MLD SNOOPING VLAN QUERY-INTERVAL

Use the ipv6 mld snooping vlan query-interval command to set interval between each query. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **query-interval** *<30-18000>*

Switch(config)# **no ipv6 mld snooping vlan** *<VLAN-LIST>* **query-interval**

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **query-interval** *<30-18000>* **no ipv6 mld snooping vlan** *<VLAN-LIST>* **query-interval**
Parameter	VLAN-LIST query-interval *<30-18000>* specifies VLAN ID list to set specifies query interval to set
Default	Default is 125
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping vlan query-interval test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld snooping vlan** 1 **query-interval** 100
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping vlan 1 query-interval 100`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.11 IPV6 MLD SNOOPING VLAN RESPONSE-TIME

Use the ipv6 mld snooping vlan response-time command to set response time. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **response-time** *<5-20>*

Switch(config)# **no ipv6 mld snooping vlan** *<VLAN-LIST>* **response-time**

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **response-time** *<5-20>* **no ipv6 mld snooping vlan** *<VLAN-LIST>* **response-time**
Parameter	VLAN-LIST specifies VLAN ID list to set response-time *<5-20>* specifies VLAN ID list to set
Default	Default is 10
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping vlan response- time test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld snooping vlan** 1 **response-time** 12
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping vlan 1 response-time 12`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.12 IPV6 MLD SNOOPING VLAN ROBUSTNESS-VARIABLE

Use the ipv6 mld snooping vlan robustness-variable command to times to retry. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **robustness-variable** *<1-7>*

Switch(config)# **no ipv6 mld snooping vlan** *<VLAN-LIST>* **robustness-variable**

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **robustness-variable** *<1-7>* **no ipv6 mld snooping vlan** *<VLAN-LIST>* **robustness-variable**
Parameter	VLAN-LIST robustness-variable*<1-7>*specifies VLAN ID list to set.specifies a robustness value to set
Default	Default is 2
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping vlan parameters test.
	Switch#**configure terminal**
	Switch(config)# **ip igmp snooping vlan** 1 **robustness-variable** 5
	`Switch# configure terminal`
	`Switch(config)# ip igmp snooping vlan 1 robustness-variable 5`
	
	Switch(config)# **no ip igmp snooping vlan** 1 **robustness-variable**

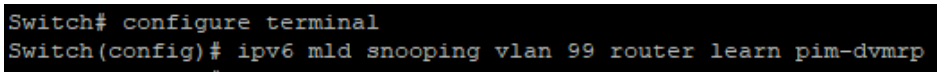
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.13 IPV6 MLD SNOOPING VLAN ROUTER

Use the ipv6 mld snooping vlan router command to enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF. Use the **"no"** form of this command to disable. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **router learn pim-dvmrp**

Switch(config)# **no ipv6 mld snooping vlan** *<VLAN-LIST>* **router learn pim-dvmrp**

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **router learn pim-dvmrp** **no ipv6 mld snooping vlan** *<VLAN-LIST>* **router learn pim-dvmrp**
Parameter	VLAN-LIST specifies VLAN ID list to set
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan router test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 99 **router learn pim-dvmrp**  Switch(config)# **no ipv6 mld snooping vlan** 99 **router learn pim-dvmrp**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.14 IPV6 MLD SNOOPING VLAN STATIC-PORT

Use the ipv6 mld snooping vlan static-port command to add static forwarding port, all known vlan 1 ipv6 group will add the static ports. Use the **"no"** form of this command to delete static port. You can verify settings by the show ipv6 mld snooping forward-all command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **static-port** *{IF_PORTS}*

Switch(config)# **no ipv6 mld snooping vlan** *<VLAN-LIST>* **static-port** *{IF_PORTS}*

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **static-port** *{IF_PORTS}* **no ipv6 mld snooping vlan** *<VLAN-LIST>* **static-port** *{IF_PORTS}*
Parameter	VLAN-LIST specifies VLAN ID list to set *{IF_PORTS}* specifies a port list to set or remove
Default	No static port by default
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping static port test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld snooping vlan** 1 **static-port** gi3-5
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping vlan 1 static-port gi3-5`
	Switch(config)# **no ipv6 mld snooping vlan** 1 **static-port** gi3-5

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.15 IPV6 MLD SNOOPING VLAN FORBIDDEN-ROUTER-PORT

Use the ipv6 mld snooping vlan forbidden-router-port command to add static forbidden router port. This will also remove port from static router port. The forbidden router port will not forward received query packet. Use the **"no"** form of this command to delete forbidden router port. You can verify settings by the show ipv6 mld snooping router command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **forbidden-router-port** *{IF_PORTS}*

Switch(config)#**no ipv6 mld snooping vlan** *<VLAN-LIST>* **forbidden-router-port** *{IF_PORTS}*

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **forbidden-router-port** *{IF_PORTS}* **no ipv6 mld snooping vlan** *<VLAN-LIST>* **forbidden-router-port** *{IF_PORTS}*
Parameter	VLAN-LIST specifies VLAN ID list to set *{IF_PORTS}* specifies a port list to set or remove
Default	No forbidden router ports by default
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping forbidden test.
	Switch#**configure terminal**
	Switch(config)**# ipv6 mld snooping vlan** 1 **forbidden-router-port** gi2
	`Switch# configure terminal`
	`Switch(config)#  ipv6 mld snooping vlan 1 forbidden-router-port gi2`
	Switch(config)# **no ipv6 mld snooping vlan** 1 **forbidden-router-port** gi2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.16 IPV6 MLD SNOOPING VLAN FORBIDDEN-ROUTER-PORT

Use the ipv6 mld snooping vlan forbidden-router-port command to add static forbidden router port. This will also remove port from static router port. The forbidden router port will not forward received query packet. Use the **"no"** form of this command to delete forbidden router port. You can verify settings by the show ipv6 mld snooping router command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **forbidden-router-port** *{IF_PORTS}*
Switch(config)#**no ipv6 mld snooping vlan** *<VLAN-LIST>***forbidden-router-port** *{IF_PORTS}*

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **forbidden-router-port** *{IF_PORTS}* **no ipv6 mld snooping vlan** *<VLAN-LIST>***forbidden-router-port** *{IF_PORTS}*
Parameter	VLAN-LIST specifies VLAN ID list to set *{IF_PORTS}* specifies a port list to set or remove
Default	No forbidden router ports by default
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping forbidden test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld snooping vlan** 1 **forbidden-router-port** gi2
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping vlan 1 forbidden-router-port gi2`
	Switch(config)# **no ipv6 mld snooping vlan** 1 **forbidden-router-port** gi2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.17 IPV6 MLD SNOOPING VLAN STATIC ROUTER PORT

Use the ipv6 mld snooping vlan static-router-port command to add static router port. All query packets will forward to this port. Use the **"no"** form of this command to delete static router port. You can verify settings by the show ipv6 mld snooping router command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **static-router-port** *{IF_PORTS}*

Switch(config)#**no ipv6 mld snooping vlan** *<VLAN-LIST>* **static-router-port** *{IF_PORTS}*

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **static-router-port** *{IF_PORTS}* **no ipv6 mld snooping vlan** *<VLAN-LIST>* **static-router-port** *{IF_PORTS}*
Parameter	VLAN-LIST specifies VLAN ID list to set *{IF_PORTS}* specifies a port list to set or remove
Default	Non static router ports by default
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping static test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld snooping vlan** 1 **static-router-port** gi1-2
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping vlan 1 static-router-port gi1-2`
	Switch(config)# **no ipv6 mld snooping vlan** 1 **static-router-port** gi1-2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.18 IPV6 MLD SNOOPING VLAN STATIC-GROUP

Use the ipv6 mld snooping vlan static-group command to add a static group. The static group will not learn other dynamic ports. If the dynamic group exists, then the static group will overlap the dynamic group. The static group set to valid unless igmp snooping global and vlan enable. Use the **"no"** form of this command to delete a port in static group. If remove the last member of static group, the static group will be deleted. You can verify settings by the show ipv6 mld snooping group command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld snooping vlan** *<VLAN-LIST>* **static-group** [*<ipv6-addr>*] **interfaces** *{IF_PORTS}*

Switch(config)#**no ipv6 mld snooping vlan** *<VLAN-LIST>* **static-group** *<ipv6-addr>* **interfaces** *{IF_PORTS}*

Syntax	**ipv6 mld snooping vlan** *<VLAN-LIST>* **static-group** [*<ipv6-addr>*] **interfaces** *{IF_PORTS}* **no ipv6 mld snooping vlan** *<VLAN-LIST>* **static-group** *<ipv6-addr>* **interfaces** *{IF_PORTS}*
Parameter	*<VLAN-LIST>* specifies VLAN ID list to set *<Ipv6-addr>* specifies multicast group ipv4 address *{IF_PORTS}* specifies port list to set or remove
Default	No static group by default
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping static group test.
	Switch#**configure terminal**
	Switch(config)**#ipv6 mld snooping vlan** 1 **static-group** ff13::1 **interfaces** gi1-2
	`Switch# configure terminal`
	`Switch(config)# ipv6 mld snooping vlan 1 static-group ff13::1 interfaces gi1-2`
	
	Switch(config)# **no ipv6 mld snooping vlan** 1 **static-group** ff13::1 **interfaces** gi1-2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.19 PROFILE RANGE

Use the profile command to generate MLD profile. You can verify settings by the show ipv6 mld profile command.

Switch#**configure terminal**
Switch(config)# **ipv6 mld profile** {Profile-No}
Switch(config-mld-profile)#**profile range ipv6** *<ipv6-addr>* **[ipv6-addr] action (permit | deny)**

Syntax	**profile range ipv6** *<ipv6-addr>* **[ipv6-addr] action (permit | deny)**
Parameter	*<ipv6-addr>* Start ipv6 multicast address [ipv6-addr] End ipv6 multicast address (permit | deny) **permit**: allow Multicast address range ip address learning **deny**: do not allow Multicast address range ip address learning
Mode	mld profile configuration mode

Example	The following example specifies that set ipv6 mld profile test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld profile** 1
	Switch(config-mld-profile)# **profile range ipv6** ff13::1 ff13::10 **action permit**
	`Switch(config)# ipv6 mld profile 1`
	`Switch(config-mld-profile)# profile range ipv6 ff13::1 ff13::10 action permit`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.20 IPV6 MLD PROFILE

Use the ipv6 mld profile command to enter profile configuration Use the **"no"** form of this command to delete profile. You can verify settings by the show ipv6 mld profile command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld profile** *<1-128>*

Switch(config)# **no ipv6 mld profile** *<1-128>*

Syntax	**ipv6 mld profile** *<1-128>* **no ipv6 mld profile** *<1-128>*
Parameter	*<1-128>*specifies profile ID
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld profile test.
	Switch#**configure terminal**
	Switch(config)# **ipv6 mld profile** 1
	`Switch(config)# ipv6 mld profile 1`
	`Switch(config-mld-profile)# profile range ipv6 ff13::1 ff13::10 action permit`
	Switch(config)# **no ipv6 mld profile** 1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.21 IPV6 MLD FILTER

Use the ipv6 mld filter command to bind a profile for port. When the port binds a profile, then the port learning group will update. If the group is not matching the profile rule, it will remove the port from the group. Static group is excluded. Use the **"no"** form of this command to delete profile. You can verify settings by the show ipv6 mld filter command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld filter** *<1-128>*

Switch(config)# **no ipv6 mld filter**

Syntax	**ipv6 mld filter** *<1-128>* **no ipv6 mld filter**
Parameter	*<1-128>* specifies profile ID [interfaces IF_PORTS] Specifies interfaces to display
Mode	Port Configuration

Example	The following example specifies that set ipv6 mld filter test.
	Switch#**configure terminal**
	Switch(config)# **interface** gi1
	Switch(config-if)# **ipv6 mld filter** 1
	`Switch# configure terminal`
	`Switch(config)# interface gil`
	`Switch(config-if)#  ipv6 mld filter 1`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.22 IPV6 MLD MAX-GROUPS

Use the ipv6 mld max-groups command to limit port learning max group number. When the port has reach limitation, new group will not add this port. Static group is excluded. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld max-groups command.

Switch#**configure terminal**
Switch(config)#**ipv6 mld max-groups** *<0-1024>*

Switch(config)# **no ipv6 mld max-groups**

Syntax	**ipv6 mld max-groups** *<0-1024>* **no ipv6 mld max-groups**
Parameter	*<0-1024>*specifies profile ID
Default	Default is 1024
Mode	Port Configuration

Example	The following example specifies that set ipv6 mld max-groups test.
	Switch#**configure terminal**
	Switch(config)# **interface** gi1
	Switch(config-if)# **ipv6 mld max-groups** 10
	`Switch# configure terminal`
	`Switch(config)# interface gi1`
	`Switch(config-if)# ipv6 mld max-groups 10`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.23 IP IGMP MAX-GROUPS ACTION

Use the ipv6 mld max-groups action command to set the action when the numbers of groups reach the limitation. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld max-groups command.

Switch#**configure terminal**
Switch(config)# **interface** {INTERFACE-ID}

Switch(config-if)#**ipv6 mld max-groups action (deny | replace)**

Syntax	**ipv6 mld max-groups action (deny | replace)**
Parameter	(deny | replace) Deny: current port igmp group arrived max-groups, don't add group. Replace: current port igmp group arrived max-groups, remove port for rand group, and add port to new group.
Default	Default action is deny
Mode	Interface mode

Example	The following example specifies that set action replace test.
	Switch#**configure terminal**
	Switch(config)# **interface** gi1
	Switch(config-if)#**ipv6 mld max-groups action replace**
	`Switch# configure terminal`
	`Switch(config)# interface gi1`
	`Switch(config-if)# ipv6 mld max-groups action replace`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.24 CLEAR IPV6 MLD SNOOPING GROUPS

This command will clear the ipv6 mld groups for dynamic or static or all of type. You can verify settings by the show ipv6 mld snooping groups command.

Switch#clear ipv6 mld snooping groups [(dynamic | static)]

Syntax	clear ipv6 mld snooping groups [(dynamic | static)]
Parameter	None Clear ipv6 mld groups include dynamic and static (dynamic | static) ipv6 mld group type is dynamic or static
Mode	Privileged EXEC
Example	The following example specifies that clear ipv6 mld snooping groups test. Switch# clear ipv6 mld snooping groups static

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.25 CLEAR IPV6 MLD SNOOPING STATISTICS

This command will clear the igmp statistics. You can verify settings by the show ipv6 mld snooping command.

Switch#clear ipv6 mld snooping statistics

Syntax	clear ipv6 mld snooping statistics
Mode	Privileged EXEC
Example	The following example specifies that clear ipv6 mld snooping statistics test. Switch# clear ipv6 mld snooping statistics

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.26 SHOW IPV6 MLD SNOOPING GROUPS COUNTERS

This command will display the ipv6 mld group counter include static group.

Switch#**show ipv6 mld snooping groups counters**

Syntax	**show ipv6 mld snooping groups counters**
Mode	Privileged EXEC

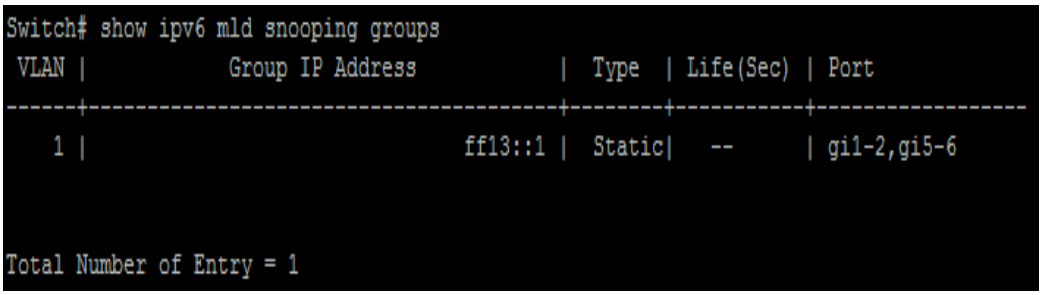
Example	The following example specifies that display ipv6 mld snooping group counter test.
	Switch# **show ipv6 mld snooping group counters**
	Total ipv6 mld snooping group number: 1
	`Switch# show ipv6 mld snooping group counters`
	`Total ipv6 mld snooping group number: 1`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.27 SHOW IPV6 MLD SNOOPING GROUPS

This command will display the ipv6 mld groups for dynamic or static or all of type.

Switch#**show ipv6 mld snooping groups [(dynamic | static)]**

Syntax	**show ipv6 mld snooping groups [(dynamic | static)]**
Parameter	**none** Show ipv6 mld groups include dynamic and static (dynamic | static) Display ipv6 mld group type is dynamic or static
Default	display all ipv6 mld groups
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld snooping groups test. Switch# **show ipv6 mld snooping groups** 

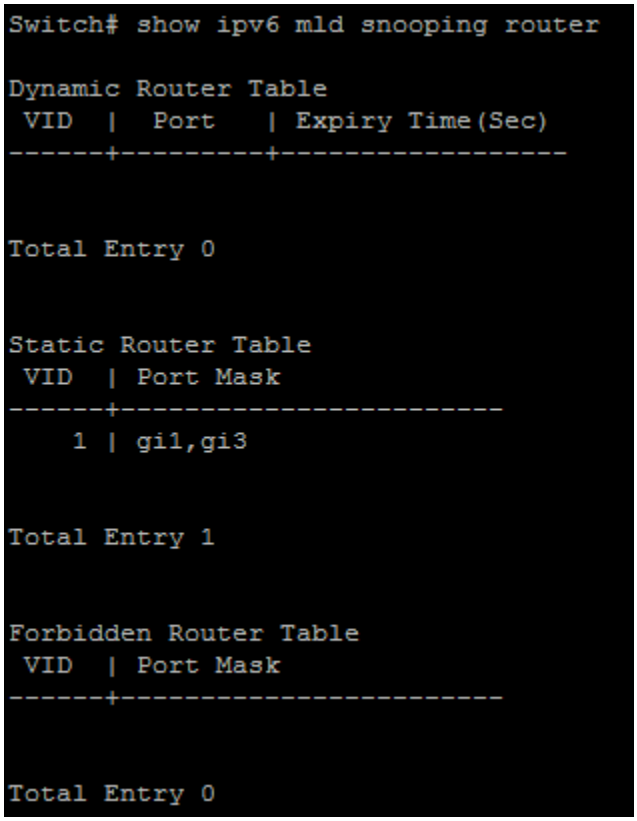
```
Switch# show ipv6 mld snooping groups
 VLAN |           Group IP Address           |  Type  | Life(Sec) | Port
------+---------------------------------------+--------+-----------+-----------------
    1 |                              ff13::1 |  Static|   --      | gi1-2,gi5-6


Total Number of Entry = 1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.28 SHOW IPV6 MLD SNOOPING ROUTER

This command will display the ipv6 mld router info.

Switch#**show ipv6 mld snooping router [(dynamic | forbidden |static)]**

Syntax	**show ipv6 mld snooping router [(dynamic | forbidden |static)]**
Parameter	none Show ipv6 mld router include dynamic and static and forbidden (dynamic |forbidden | static)Display ipv6 mld router info for different type
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld snooping router test. Switch# **show ipv6 mld snooping router** 

```
Switch# show ipv6 mld snooping router

Dynamic Router Table
 VID  |  Port   | Expiry Time(Sec)
------+---------+------------------


Total Entry 0


Static Router Table
 VID  | Port Mask
------+-------------------------
    1 | gi1,gi3


Total Entry 1


Forbidden Router Table
 VID  | Port Mask
------+-------------------------


Total Entry 0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.29 SHOW IPV6 MLD SNOOPING

This command will display ipv6 mld snooping global info.

Switch#**show ipv6 mld snooping**

Syntax	**show ipv6 mld snooping**
Mode	Privileged EXEC

Example	The following example specifies that show ipv6 mld snooping test.
	Switch# **show ipv6 mld snooping**
	
	`Switch# show ipv6 mld snooping`
	
	`MLD Snooping Status`
	`--------------------`
	
	`Snooping : Disabled`
	`Report Suppression : Enabled`
	`Operation Version : v1`
	`Forward Method : mac`
	`Unknown IPv6 Multicast Action : Flood`
	
	`Packet Statistics`
	`Total RX : 0`
	`Valid RX : 0`
	`Invalid RX : 0`
	`Other RX : 0`
	`Leave RX : 0`
	`Report RX : 0`
	`General Query RX : 0`
	`Specail Group Query RX : 0`
	`Specail Group & Source Query RX : 0`
	`Leave TX : 0`
	`Report TX : 0`
	`General Query TX : 0`
	`Specail Group Query TX : 0`
	`Specail Group & Source Query TX : 0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.30 SHOW IPV6 MLD SNOOPING VLAN

This command will display ipv6 mld snooping vlan info.

Switch#**show ipv6 mld snooping vlan** *<VLAN-LIST>*

Syntax	**show ipv6 mld snooping vlan** *<VLAN-LIST>*
Parameter	**none** Show all ipv6 mld snooping vlan info *<VLAN-LIST>*Show specifies vlan ipv6 mld snooping info
Default	Show all ipv6 mld snooping vlan info
Mode	Privileged EXEC

Example	The following example specifies that show ipv6 mld snooping vlan test.
	Switch# **show ipv6 mld snooping vlan** 1
	
	`Switch# show ipv6 mld snooping vlan 1`
	
	`MLD Snooping is globaly disabled`
	`MLD Snooping VLAN 1 admin : disabled`
	`MLD Snooping oper mode : disabled`
	`MLD Snooping robustness: admin 2 oper 2`
	`MLD Snooping query interval: admin 125 sec oper 125 sec`
	`MLD Snooping query max response : admin 10 sec oper 10 sec`
	`MLD Snooping last member query counter: admin 2 oper 2`
	`MLD Snooping last member query interval: admin 1 sec oper 1 sec`
	`MLD Snooping immediate leave: disabled`
	`MLD Snooping automatic learning of multicast router ports: enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.31 SHOW IPV6 MLD SNOOPING FORWARD-ALL

This command will display ipv6 mld snooping forward all info.

Switch#**show ipv6 mld snooping forward-all** [**vlan** *<VLAN-LIST>*]

Syntax	**show ipv6 mld snooping forward-all** [**vlan** *<VLAN-LIST>*]
Parameter	**none** Show all ipv6 mld snooping vlan forward-all info [vlan *<VLAN-LIST>*] Show specifies vlan of ipv6 mld forward info
Default	Show all vlan ipv6 mld forward all info
Mode	Privileged EXEC

Example	The following example specifies that show ipv6 mld snooping forward-all test.
	Switch# **show ipv6 mld snooping forward-all**
	`Switch# show ipv6 mld snooping forward-all`
	
	`MLD Snooping VLAN : 1`
	`MLD Snooping static port : gi3-5`
	`MLD Snooping forbidden port : None`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.32 SHOW IPV6 MLD PROFILE

This command will display ipv6 mld profile info.

Switch#**show ipv6 mld profile**[*<1-128>*]

Syntax	**show ipv6 mld profile**[*<1-128>*]
Parameter	**none** Show all ipv6 mld snooping profile info [<1-128>] Show specifies index profile info
Default	Show all ipv6 mld profile info
Mode	Privileged EXEC

Example	The following example specifies that show ipv6 mld profile test.
	
	Switch#**show ipv6 mld profile**
	`Switch# show ipv6 mld profile`
	`IPv6 mld profile index: 1`
	`IPv6 mld profile action: permit`
	`Range low ip: ff13::1`
	`Range high ip: ff13::10`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.33 SHOW IPV6 MLD FILTER

This command will display ipv6 mld port filter info.

Switch#**show ipv6 mld filter** [**interfaces***{IF_PORTS}*]

Syntax	**show ipv6 mld filter** [**interfaces***{IF_PORTS}*]
Parameter	**none** Show all port filter [interfaces *{IF_PORTS}*] Show specifies ports filter
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld filter test. Switch#**show ipv6 mld filter** `Switch# show ipv6 mld filter` `Port ID	Profile ID` `---------+--------------` `gi1 : 1` `gi2 : None` `gi3 : None` `gi4 : None` `gi5 : None` `gi6 : None` `gi7 : None` `gi8 : None` `gi9 : None` `gi10 : None` `gi11 : None` `gi12 : None` `gi13 : None` `gi14 : None` `gi15 : None` `gi16 : None` `gi17 : None` `gi18 : None` `gi19 : None` `gi20 : None` `gi21 : None` `gi22 : None` `gi23 : None` `gi24 : None` `gi25 : None` `gi26 : None` `gi27 : None` `gi28 : None` `lag1 : None` `lag2 : None` `lag3 : None` `lag4 : None` `lag5 : None` `lag6 : None` `lag7 : None` `lag8 : None`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.34 SHOW IPV6 MLD MAX-GROUP

This command will display ipv6 mld port max-group.

Switch#**show ipv6 mld max-group [interfaces***{IF_PORTS}*]

Syntax	**show ipv6 mld max-group [interfaces***{IF_PORTS}*]
Parameter	**none** Show all port max-group [interfaces *{IF_PORTS}*] Show specifies ports max-group
Mode	Privileged EXEC

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Example	The following example specifies that show ipv6 mld max-group test. Switch# show ipv6 mld max-groups 50

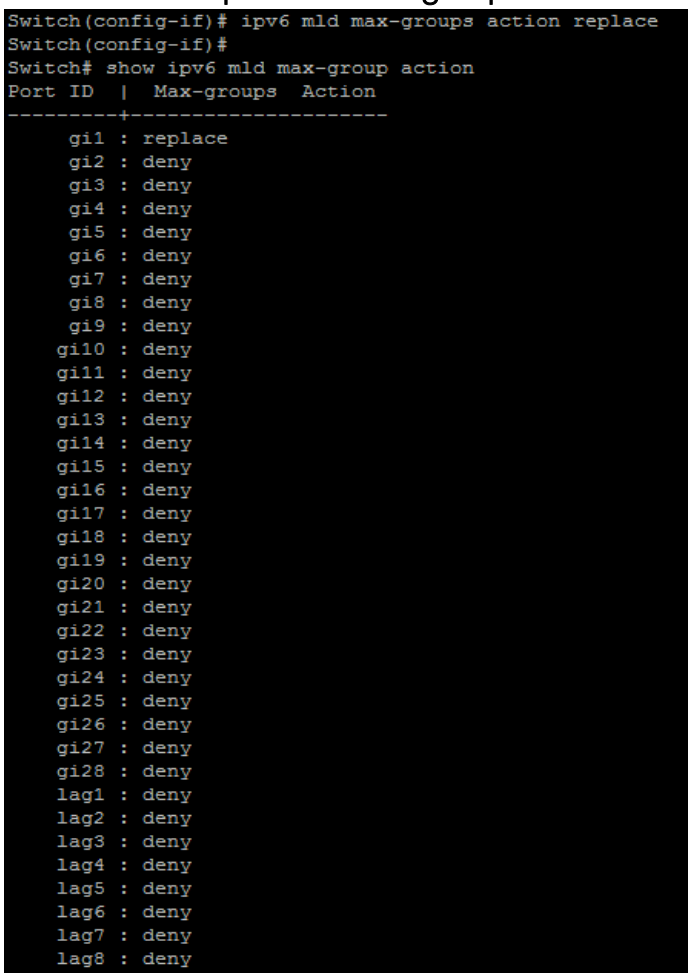
```
Switch(config)# interface gi1
Switch(config-if)# ipv6 mld max-groups 50
Switch(config-if)#
Switch# show ipv6 mld max-group
Port ID   |  Max Group
---------+--------------
     gi1 : 50
     gi2 : 256
     gi3 : 256
     gi4 : 256
     gi5 : 256
     gi6 : 256
     gi7 : 256
     gi8 : 256
     gi9 : 256
    gi10 : 256
    gi11 : 256
    gi12 : 256
    gi13 : 256
    gi14 : 256
    gi15 : 256
    gi16 : 256
    gi17 : 256
    gi18 : 256
    gi19 : 256
    gi20 : 256
    gi21 : 256
    gi22 : 256
    gi23 : 256
    gi24 : 256
    gi25 : 256
    gi26 : 256
    gi27 : 256
    gi28 : 256
    lag1 : 256
    lag2 : 256
    lag3 : 256
    lag4 : 256
    lag5 : 256
    lag6 : 256
    lag7 : 256
    lag8 : 256
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

19.35 SHOW IPV6 MLD PORT MAX-GROUP ACTION

This command will display ipv6 mld port max-group action.

Switch#**show ipv6 mld max-group action [interfaces** *{IF_PORT}*]

Syntax	**show ipv6 mld max-group action [interfaces** *{IF_PORT}*]
Parameter	**none** Show all port max-group action [interfaces *{IF_PORTS}*]Show specifies ports max-group action
Default	Show all ports ipv6 mld max-group action
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld max-group action test. Switch# **show ipv6 mld max-group action** 

```
Switch(config-if)# ipv6 mld max-groups action replace
Switch(config-if)#
Switch# show ipv6 mld max-group action
Port ID  |  Max-groups  Action
---------+--------------------
     gi1 : replace
     gi2 : deny
     gi3 : deny
     gi4 : deny
     gi5 : deny
     gi6 : deny
     gi7 : deny
     gi8 : deny
     gi9 : deny
    gi10 : deny
    gi11 : deny
    gi12 : deny
    gi13 : deny
    gi14 : deny
    gi15 : deny
    gi16 : deny
    gi17 : deny
    gi18 : deny
    gi19 : deny
    gi20 : deny
    gi21 : deny
    gi22 : deny
    gi23 : deny
    gi24 : deny
    gi25 : deny
    gi26 : deny
    gi27 : deny
    gi28 : deny
    lag1 : deny
    lag2 : deny
    lag3 : deny
    lag4 : deny
    lag5 : deny
    lag6 : deny
    lag7 : deny
    lag8 : deny
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20. Multicast VLAN Registration (MVR)

In multicast VLAN networks, subscribers to a multicast group can exist in more than one VLAN. If the VLAN boundary restrictions in a network consist of Layer 2 switches, it might be necessary to replicate the multicast stream to the same group in different subnets, even if they are on the same physical network. Multicast VLAN Registration (MVR) routes packets received in a multicast source VLAN to one or more receive VLANs. Clients are in the receive VLANs and the multicast server is in the source VLAN. Multicast routing has to be disabled when MVR is enabled.

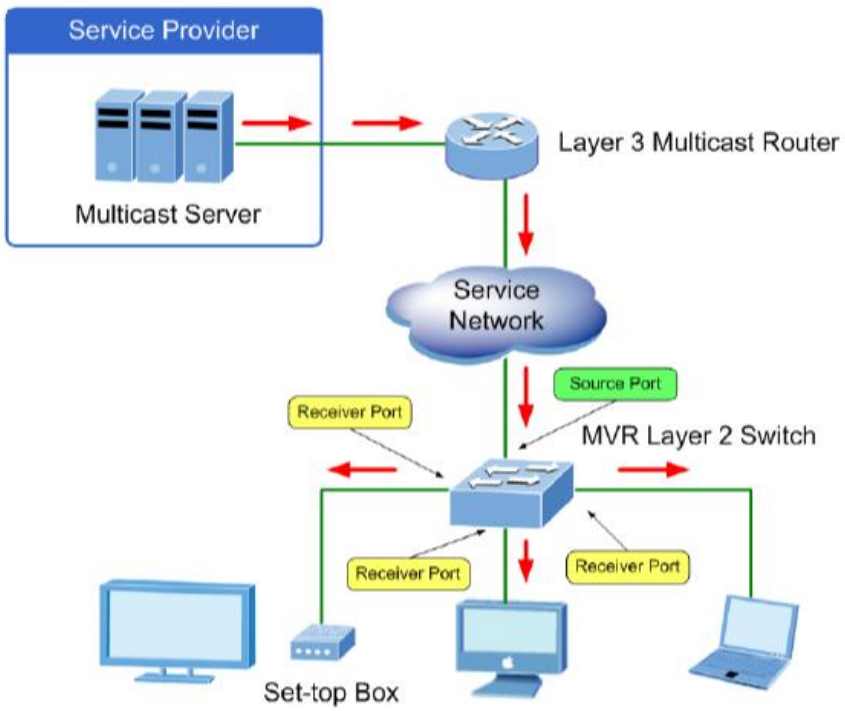


Fig 20.1 MVR concept

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.1 MVR

Use the mvr command to enable MVR function. The command will clear all mvr VLAN ID multicast snooping group. Use the **"no"** form of this command to disable. Disable will clear all mvr group. You can verify settings by the show mvr command.

Switch#**configure terminal**
Switch(config)# **mvr**

Switch(config)# **no mvr**

Syntax	**mvr** **no mvr**
Mode	Global Configuration

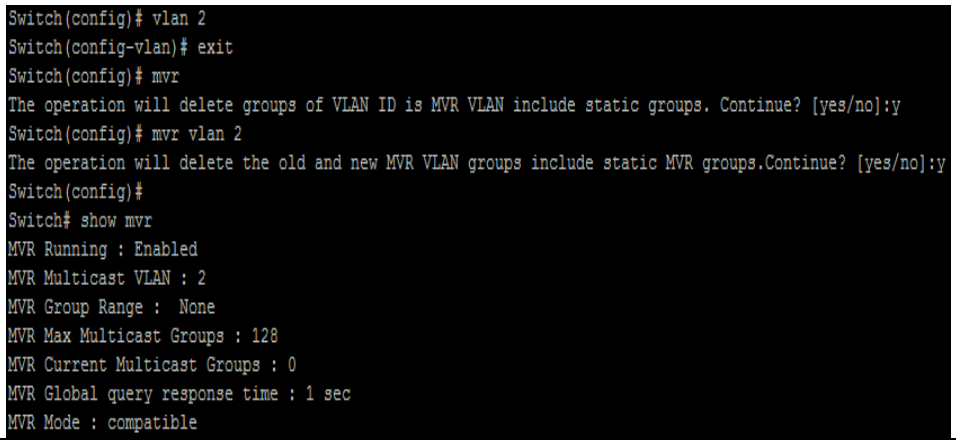
Example	The following example specifies that set mvr test. Switch#**configure terminal**
	Switch(config)# **mvr**
	Switch(config)# **no mvr**
	The operation will make mvr setting is default. Continue? [yes/no]:y
	Switch(config)#
	Switch# **show mvr**
	
	`Switch(config)# mvr`
	`Switch(config)# no mvr`
	`The operation will make mvr setting is default. Continue? [yes/no]:y`
	`Switch(config)#`
	`Switch# show mvr`
	`MVR Running : Disabled`
	`MVR Multicast VLAN : 1`
	`MVR Group Range : None`
	`MVR Max Multicast Groups : 128`
	`MVR Current Multicast Groups : 0`
	`MVR Global query response time : 1 sec`
	`MVR Mode : compatible`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.2 MVR VLAN

Use the mvr vlan command to modify mvr vlan id when the mvr status is enabled. Change mvr vlan id will delete the old mvr vlan and new mvr vlan group. If there have configure source or receiver port, there will check the source must only in the mvr vlan, and receiver port must not in the mvr vlan member. You can verify settings by the show mvr command.

Switch#**configure terminal**
Switch(config)#**mvr vlan** *<VLAN-ID>*

Syntax	**mvr vlan** *<VLAN-ID>*
Parameter	*<VLAN-ID>*The exist static vlan id
Default	Default mvr vlan id is 1
Mode	Global Configuration
Example	The following example specifies that configure mvr vlan 2 test. Switch#**configure terminal** Switch(config)# **vlan** 2 Switch(config-vlan)# **exit** Switch(config)# **mvr** The operation will delete groups of VLAN ID is MVR VLAN include static groups. Continue? [yes/no]:y Switch(config)# **mvr vlan** 2 The operation will delete the old and new MVR VLAN groups include static MVR groups.Continue? [yes/no]:y Switch# **show mvr**  Switch(config)# vlan 2 Switch(config-vlan)# exit Switch(config)# mvr The operation will delete groups of VLAN ID is MVR VLAN include static groups. Continue? [yes/no]:y Switch(config)# mvr vlan 2 The operation will delete the old and new MVR VLAN groups include static MVR groups.Continue? [yes/no]:y Switch(config)# Switch# show mvr MVR Running : Enabled MVR Multicast VLAN : 2 MVR Group Range : None MVR Max Multicast Groups : 128 MVR Current Multicast Groups : 0 MVR Global query response time : 1 sec MVR Mode : compatible

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.3 MVR GROUP

Use the mvr group command to configure mvr group address range when mvr is enabled. The command will delete all mvr vlan ipv4 group entry. You can verify settings by the show mvr command.

Switch#**configure terminal**
Switch(config)#**mvr group** *<ip-address>* [*<1-128>*]

Syntax	**mvr group***<ip-address>*[*<1-128>*]
Parameter	*<ip-address>*Start MVR IP multicast address [*<1-128>*]Contiguous series of IP addresses.
Mode	Global Configuration
Example	The following example specifies that set mvr group range is 224.1.1.1 ~ 224.1.1.8 test. Switch#**configure terminal** Switch(config)# **mvr** Switch(config)# **mvr group** 224.1.1.1 8 The operation will delete the MVR VLAN groups include static MVR groups.Continue? [yes/no]:y Switch# **show mvr** Switch(config)# mvr Switch(config)# mvr group 224.1.1.1 8 The operation will delete the MVR VLAN groups include static MVR groups.Continue? [yes/no]:y Switch(config)# Switch# show mvr MVR Running : Enabled MVR Multicast VLAN : 2 MVR Group Range : 224.1.1.1 ~ 224.1.1.8 MVR Max Multicast Groups : 128 MVR Current Multicast Groups : 0 MVR Global query response time : 1 sec MVR Mode : compatible

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.4 MVR MODE

Use the mvr mode command to change mvr mode when mvr is enabled. You can verify settings by the show mvr command.

Switch#**configure terminal**
Switch(config)#**mvr mode (dynamic | compatible)**

Syntax	**mvr mode (dynamic | compatible)**
Parameter	**(dynamic|compatible)** **dynamic** Allows dynamic MVR membership on source ports **compatible** does not support IGMP dynamic joins on source ports.
Default	Default is compatible
Mode	Global Configuration

Example	The following example specifies that set mvr mode dynamic test.
	Switch(config)#**mvr**
	Switch(config)#**mvr mode dynamic**
	
	Switch# **show mvr**
	`Switch(config)# mvr`
	`Switch(config)# mvr mode dynamic`
	`Switch(config)#`
	`Switch# show mvr`
	`MVR Running : Enabled`
	`MVR Multicast VLAN : 2`
	`MVR Group Range : 224.1.1.1 ~ 224.1.1.8`
	`MVR Max Multicast Groups : 128`
	`MVR Current Multicast Groups : 0`
	`MVR Global query response time : 1 sec`
	`MVR Mode : dynamic`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.5 MVR QUERY-TIME

Use the mvr query-time command to configure when mvr is enabled. Use the **"no"** form of this command to set query-time default value. You can verify settings by the show mvr command.

Switch#**configure terminal**
Switch(config)#**mvr query-time** *<1-10>*

Switch(config)# **no mvr query-time**

Syntax	**mvr query-time** *<1-10>* **no mvr query-time**
Parameter	*<1-10>*specifies query response time is 1~10 sec.
Default	Default is 1 sec
Mode	Global Configuration

Example	The following example specifies that set mvr query-time 10 sec test.
	Switch#**configure terminal**
	Switch(config)#**mvr**
	Switch(config)# **mvr query-time** 10
	Switch# **show mvr**
	`Switch(config)# mvr`
	`Switch(config)# mvr query-time 10`
	`Switch(config)#`
	`Switch# show mvr`
	`MVR Running : Enabled`
	`MVR Multicast VLAN : 2`
	`MVR Group Range : 224.1.1.1 ~ 224.1.1.8`
	`MVR Max Multicast Groups : 128`
	`MVR Current Multicast Groups : 0`
	`MVR Global query response time : 10 sec`
	`MVR Mode : dynamic`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.6 MVR PORT TYPE

Use the mvr type command to configure mvr port type when mvr is enabled. The source port must only belong to mvr vlan. The receiver port must not belong to mvr vlan, and port mode must be access mode. Use the **"no"** form of this command to set mvr type none. You can verify settings by the show mvr interface command.

Switch#**configure terminal**
Switch(config)#**mvr type (source | receiver)**
Switch(config)#**no mvr type**

Syntax	**mvr type (source | receiver)** **no mvr type**
Parameter	**(source | receiver)** **Source** Configure uplink ports that receive and send multicast data as source ports.Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN. **Receiver** Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages.Receiver ports cannot belong to the multicast VLAN.
Mode	Port Configuration

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Example	The following example specifies that set gi1 is source port, gi2 is receiver port test. Switch#**configure terminal** Switch(config)# **vlan** 2 Switch(config-vlan)#**exit** Switch(config)#**mvr** Switch(config)#**mvr vlan** 2 Switch(config)#**mvr group** 224.1.1.1 8 Switch(config)# **interface** gi1 Switch(config-if)# **switchport trunk allowed vlan add** 2 Switch(config-if)# **mvr type source** Switch(config-if)#**exit** Switch(config)# **interface** gi2 Switch(config-if)# **switchport mode access** Switch(config-if)#**mvr type receiver** Switch# **show mvr interface**

```
Switch(config)# vlan 2
Switch(config-vlan)# exit
Switch(config)# mvr
Switch(config)# mvr vlan 2
The operation will delete the old and new MVR VLAN groups include static MVR groups.Continue? [yes/no]:y
Switch(config)# mvr group 224.1.1.1 8
The operation will delete the MVR VLAN groups include static MVR groups.Continue? [yes/no]:y
Switch(config)# interface gi1
Switch(config-if)# switchport trunk allowed vlan add 2
Switch(config-if)# mvr type source
Switch(config-if)# exit
Switch(config)# interface gi2
Switch(config-if)# switchport mode access
Switch(config-if)# mvr type receiver
Switch(config-if)#
Switch# show mvr interface
  Port   |  Type    | Immediate Leave
---------+----------+-----------------
 gi1     |   Source|    Disabled
 gi2     | Receiver|    Disabled
 gi3     |     None|    Disabled
 gi4     |     None|    Disabled
 gi5     |     None|    Disabled
 gi6     |     None|    Disabled
 gi7     |     None|    Disabled
 gi8     |     None|    Disabled
 gi9     |     None|    Disabled
gi10     |     None|    Disabled
gi11     |     None|    Disabled
gi12     |     None|    Disabled
gi13     |     None|    Disabled
gi14     |     None|    Disabled
gi15     |     None|    Disabled
gi16     |     None|    Disabled
gi17     |     None|    Disabled
gi18     |     None|    Disabled
gi19     |     None|    Disabled
gi20     |     None|    Disabled
gi21     |     None|    Disabled
gi22     |     None|    Disabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.7 MVR PORT IMMEDIATE

Use the mvr immediate command to configure mvr support immediate leave when mvr is enabled. Note This command applies to only receiver ports and should only be enabled on receiver ports to which a single receiver device is connected. Use the **"no"** form of this command to disable immediate leave. You can verify settings by the show mvr interface command.

Switch#**configure terminal**
Switch(config)#**mvr immediate**

Switch(config)# **no mvr immediate**

Syntax	**mvr immediate** **no mvr immediate**
Mode	Port Configuration
Example	The following example specifies that set gi2 immediate enable test. The configure should configure mvr receiver port firstly.(eg. mvr port type) Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)#**mvr immediate** Switch(config-if)#**exit** Switch(config)# **exit** Switch# **show mvr interface**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface gi2
Switch(config-if)# mvr immediate
Switch(config-if)# exit
Switch(config)# exit
Switch# show mvr interface
  Port   |  Type    | Immediate Leave
---------+----------+-----------------
 gi1     |   Source|     Disabled
 gi2     | Receiver|      Enabled
 gi3     |     None|     Disabled
 gi4     |     None|     Disabled
 gi5     |     None|     Disabled
 gi6     |     None|     Disabled
 gi7     |     None|     Disabled
 gi8     |     None|     Disabled
 gi9     |     None|     Disabled
gi10     |     None|     Disabled
gi11     |     None|     Disabled
gi12     |     None|     Disabled
gi13     |     None|     Disabled
gi14     |     None|     Disabled
gi15     |     None|     Disabled
gi16     |     None|     Disabled
gi17     |     None|     Disabled
gi18     |     None|     Disabled
gi19     |     None|     Disabled
gi20     |     None|     Disabled
gi21     |     None|     Disabled
gi22     |     None|     Disabled
gi23     |     None|     Disabled
gi24     |     None|     Disabled
gi25     |     None|     Disabled
gi26     |     None|     Disabled
gi27     |     None|     Disabled
gi28     |     None|     Disabled
lag1     |     None|     Disabled
lag2     |     None|     Disabled
lag3     |     None|     Disabled
lag4     |     None|     Disabled
lag5     |     None|     Disabled
lag6     |     None|     Disabled
lag7     |     None|     Disabled
lag8     |     None|     Disabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.8 MVR STATIC GROUP

Use the mvr vlan group command to add a static group or configure static group member ports when mvr is enabled. This command applies to only receiver ports. In compatible mode, this command applies to only receiver ports. In dynamic mode, it applies to receiver ports and source ports. When remove static mvr group all ports, the static group will be deleted. Or can use **"no"** ip igmp vlan VLAN-ID group to delete the mvr static group. Static group can't learn dynamic port by igmp message. Use the **"no"** form of this command to delete a port in static group. If remove the last member of static group, the static group will be deleted. You can verify settings by the show mvr members command.

Switch#**configure terminal**
Switch(config)#**mvr vlan** *<VLAN-ID>* **group** *<ip-addr>* **interfaces** *{IF_PORTS}*

Switch(config)#**no mvr vlan** *< VLAN-ID>* **group** *<ip-addr>* **interfaces** *{IF_PORTS}*

Syntax	**mvr vlan** *<VLAN-ID>* **group** *<ip-addr>* **interfaces** *{IF_PORTS}* **no mvr vlan** *< VLAN-ID>* **group** *<ip-addr>* **interfaces** *{IF_PORTS}*
Parameter	*VLAN-ID* specifies MVR VLAN ID for static group *ip-addr* Specifies multicast MVR group address *IF_PORT S* specifies port list to set or remove
Mode	Global Configuration

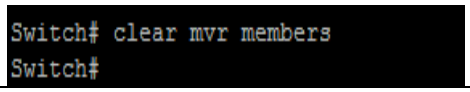
Example	The following example specifies that set mvr static group test.
	The configure must configure mvr receiver port firstly.(eg. mvr port type)
	Switch(config)# **mvr vlan** 2 **group** 224.1.1.1 **interfaces** gi2
	Switch# **show mvr members**
	`Switch(config)# mvr vlan 2 group 224.1.1.1 interfaces gi2`
	`Switch(config)#`
	`Switch# show mvr members`
	`Gourp IP Address | Type | Life(Sec) | Port`
	`------------------+--------+-----------+------------------`
	`224.1.1.1 | Static| -- | gi2`
	
	`Total Number of Entry = 1`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.9 CLEAR MVR MEMBERS

This command will clear the mvr groups for selected type.

Switch#clear mvr members [dynamic|static]

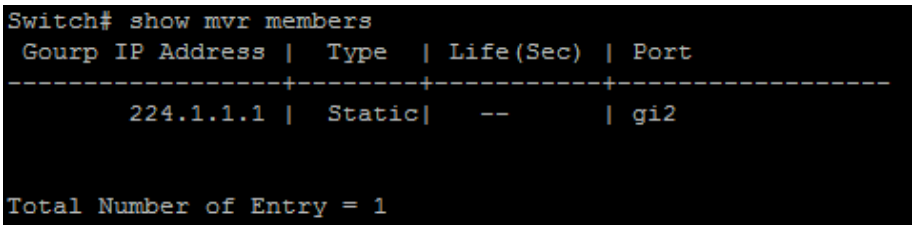
Syntax	clear mvr members [dynamic|static]
Parameter	**dynamic** specifies MVR dynamic group **static** specifies MVR static group
Default	Clear all of mvr group
Mode	Privileged EXEC
Example	The following example specifies that clear all mvr groups test. Switch# clear mvr members 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.10 SHOW MVR MEMBERS

This command will display the mvr groups for all of type.

Switch#**show mvr members**

Syntax	**show mvr members**
Mode	Privileged EXEC
Example	The following example specifies that show mvr groups test. Switch# **show mvr members** 

```
Switch# show mvr members
 Gourp IP Address |  Type  | Life(Sec) | Port
------------------+--------+-----------+------------------
        224.1.1.1 |  Static|   --      | gi2


Total Number of Entry = 1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.11 SHOW MVR INTERFACE

This command will display mvr port type and port immediate status.

Switch#**show mvr interface** *{IF_PORTS}*

Syntax	**show mvr interface** *{IF_PORTS}*
Parameter	*IF_PORTS* Show specifies port list configuration
Mode	Privileged EXEC
Example	The following example specifies that show mvr interface test. Switch# **show mvr interface** Switch# show mvr interface Port | Type | Immediate Leave --------+---------+----------------- gi1 | Source| Disabled gi2 | Receiver| Enabled gi3 | None| Disabled gi4 | None| Disabled gi5 | None| Disabled gi6 | None| Disabled gi7 | None| Disabled gi8 | None| Disabled gi9 | None| Disabled gi10 | None| Disabled gi11 | None| Disabled gi12 | None| Disabled gi13 | None| Disabled gi14 | None| Disabled gi15 | None| Disabled gi16 | None| Disabled gi17 | None| Disabled gi18 | None| Disabled gi19 | None| Disabled gi20 | None| Disabled gi21 | None| Disabled gi22 | None| Disabled gi23 | None| Disabled gi24 | None| Disabled gi25 | None| Disabled gi26 | None| Disabled gi27 | None| Disabled gi28 | None| Disabled lag1 | None| Disabled lag2 | None| Disabled lag3 | None| Disabled lag4 | None| Disabled lag5 | None| Disabled lag6 | None| Disabled lag7 | None| Disabled lag8 | None| Disabled

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

20.12 SHOW MVR

This command will display mvr global information.

Switch#**show mvr**

Syntax	**show mvr**
Mode	Privileged EXEC

Example	The following example specifies that show mvr test.
	Switch# **show mvr**
	
	`Switch# show mvr`
	`MVR Running : Enabled`
	`MVR Multicast VLAN : 2`
	`MVR Group Range : 224.1.1.1 ~ 224.1.1.8`
	`MVR Max Multicast Groups : 128`
	`MVR Current Multicast Groups : 0`
	`MVR Global query response time : 1 sec`
	`MVR Mode : compatible`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21. PORT

The switch comes with default port settings that should allow you to connect to the ethernet ports without any necessary configuration. There should be a need to change the name of the ports, port state, negotiation settings or flow control settings etc., as per desired configuration. Switch interfaces are used to exchange data. Physical interfaces (excluding management interfaces) used to transmit frames. Basically, interfaces are classified into physical interfaces, and logical interfaces. Physical interfaces are also called ports. The port is where you plug in the physical cable connector. The interface is what you configure in the switch, therefore is the software representation of the physical port.

Physical interfaces

Physical interfaces exist on interface cards and transmit service data. Physical interfaces are classified into the following types:

LAN Interface: They are 10/100/1000 Mbps ports to exchange data with network devices on LANs. Following are common LAN interfaces used worldwide.

1. Fast Ethernet interface

A FE interface works at the data link layer, provides a maximum transmission rate of 100 Mbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

2. Gigabit Ethernet interface

A GE interface works at the data link layer, provides a maximum transmission rate of 1000 Mbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

3. 10 Gigabit Ethernet interface

A 10GE interface works at the data link layer, provides a maximum transmission rate of 10 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

4. MultiGE interface

It is an Ethernet electrical interface that can work at the rate of 1000 Mbps, 2500 Mbps, 5000 Mbps, or 10000 Mbps.

5. 40 Gigabit Ethernet interface

A 40GE interface works at the data link layer, provides a maximum transmission rate of 40 Gbps, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

Management interface: Management interfaces are used to log in to switches for configuration and management purposes.

USB interface: It is a generally data transmission interface. You can perform USB based deployment on a switch through this interface.

Mini USB interface: It is a data transmission interface as well as management interface. You can perform basic configuration and management on a switch through this interface.

Monitoring Interface: Monitoring interfaces are used to monitor a switch's components, including the cabinet door, power supply, and backup power supply.

Console interface: The console interface is connected to the COM serial interface of a configuration terminal to set up an on-site configuration environment. This interface can be connected to a network interface of a configuration terminal or network management workstation to set up an onsite or remote configuration environment.

Out of band Eth interface: This interface can be connected to a network interface with RJ45 cable of a configuration terminal or network management workstation to set up an onsite or remote configuration environment.

Optical Interfaces: In a fiber optic communications link, a point at which an optical signal is passed from one equipment or medium to another without conversion to an electrical signal. Depending on transmission rates, optical modules are classified into 100G, 40G, 10G, and 1G optical modules.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Logical interfaces

Logical interfaces do not physically exist. They are manually configured and can be used to exchange data and transmit service data.

Trunk Interface: A Trunk has Layer 2 and Layer 3 features and is formed by binding multiple Ethernet interfaces to provide more bandwidth and higher transmission reliability.

Tunnel interface: A tunnel interface has Layer 3 features, transmits packets, & identifies and processes packets transmitted over a tunnel.

VLAN interface: A VLAN interface has Layer 3 features and enables VLANs to have gateway IP.

Ethernet Sub interface: An Ethernet sub interface is configured on a main interface to allow the local L3 device to communicate with multiple L2 devices.

Loopback interface: A loopback interface is always UP and can be configured with a 32-bit subnet mask.

NULL interface: A null interface is used to filter routes because any data packets received by the null interface are discarded

NVE interface: An NVE interface is the logical interface to establish VXLAN tunnels with other NVE devices.

VBD interface: A VBD interface is the virtual interface based on a BD to support Layer 3 features and implement communication between different BDs, between BD and non-BD networks, and between BDs and Layer 3 networks.

Virtual Ethernet (VE) interface: A VE interface is used when other data link layer protocols need to be carried by the Ethernet protocol. A VE sub interface can be created to allow an L2VPN to access to an L3VPN.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Layer 2 Interface: A L2 interface can act a switchport decides how to forward data based on the MAC address. They can only forward the received packets in Layer 2 switching mode or join VLANs to forward the packets in Layer 3 routing mode through VLAN interfaces.

Layer 3 Interface: Layer 3 interfaces forward packets to another device using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing and inter VLAN routing of Layer 2 traffic. IP addresses can be configured for these interfaces. They can forward the received packets in Layer 3 routing mode. That is, they can send and receive the packets whose source and destination IP addresses are in different segments.

Port settings for ports can be carried out with help of following commands

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.1 BACK-PRESSURE

In backpressure flow control mechanism in which switch causes a transmitting device to hold off on sending data packets until the switch s bottleneck has been solved. To create backpressure, the switch either broadcasts false collision detection signals or sends packets back to the originating device if the buffer is full. Use "**back-pressure**" command to make port to enable back pressure feature. Use **"no"** form of this command to disable back pressure feature. The only way to show this configuration is using "**show running-config**" command.

Switch#**configure terminal**
Switch(config-if)# **back-pressure**

Switch(config-if)# **no back-pressure**

Syntax	**back-pressure** **no back-pressure**
Default	Default back pressure state is enabled.
Mode	Interface Configuration

Example	This example shows how to configure port gi1 and gi2 to be protected port.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 1
	Switch(config-if)# **back-pressure**
	`Switch# configure terminal`
	`Switch(config)#  interface GigabitEthernet 1`
	`Switch(config-if)# back-pressure`
	Switch(config-if)# **no back-pressure**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.2 CLEAR INTERFACE

Use "**clear interface**" command to clear statistic counters on specific ports.

Switch#**configure terminal**
Switch(config)# **clear interfaces** *{IF_PORTS}* **counters**

Syntax	**clear interfaces** *{IF_PORTS}* **counters**
Parameter	*IF_PORTS* Specify port to clear counters
Default	No default value for this command.
Mode	Privileged EXEC

Example	This example shows how to clear counters on port gi1.
	Switch# **clear interfaces** gi1 **counters**
	
	This example shows how to show current counters
	
	Switch# **show interfaces** gi1
	
	`Switch# show interfaces gi1`
	`GigabitEthernet1 is down`
	`  Hardware is Gigabit Ethernet`
	`  Auto-duplex, Auto-speed, media type is Copper`
	`  flow-control is off`
	`  back-pressure is disabled`
	`     0 packets input, 0 bytes, 0 throttles`
	`     Received 0 broadcasts (0 multicasts)`
	`     0 runts, 0 giants, 0 throttles`
	`     0 input errors, 0 CRC, 0 frame`
	`     0 multicast, 0 pause input`
	`     0 input packets with dribble condition detected`
	`     0 packets output, 0 bytes, 0 underrun`
	`     0 output errors, 0 collisions`
	`     0 babbles, 0 late collision, 0 deferred`
	`     0 PAUSE output`
	`Switch#`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.3 DESCRIPTION

Use "**description**" command to give the port a name to identify it easily. If description includes space character, please use double quoted to wrap it. Use **"no"** form to restore description to empty string.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)#**description** WORD*<1-32>*

Switch(config-if)#**no description**

Syntax	**description** WORD*<1-32>* **no description**
Parameter	WORD*<1-32>* Specify port description string.
Mode	Interface Configuration

Example	This example shows how to modify port descriptions.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 1
	Switch(config-if)# **description userport**
	`Switch# configure terminal`
	`Switch(config)#  interface GigabitEthernet 1`
	`Switch(config-if)# description userport`
	
	Switch#**show interface g1 status**
	`Switch#  show interfaces gil st`
	`Port  Name  Status  Vlan  Duplex  Speed  Type`
	`gil  userport  connected  1  a-full  a-1000M  Copper`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.4 DUPLEX

Use "**duplex**" command to change port duplex configuration.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)#**duplex (auto | full | half)**

Syntax	**duplex (auto | full | half)**
Parameter	**auto** Specify port duplex to auto negotiation. **full** Specify port duplex to force full duplex. **half** Specify port duplex to force half duplex.
Default	Default port duplex is auto
Mode	Interface Configuration

Example	This example shows how to modify port duplex configuration.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 1
	Switch(config-if)# **duplex full**
	Switch(config-if)# **exit**
	This example shows how to show current interface link speed
	Switch# **show interfaces status**
	`Switch# config t`
	`Switch(config)# int gl`
	`Switch(config-if)# duplex full`
	`Switch(config-if)#`
	`Switch#  show interfaces gil status`
	`Port  Name  Status  Vlan  Duplex  Speed  Type`
	`gil  userport  connected  1  full  a-1000M  Copper`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

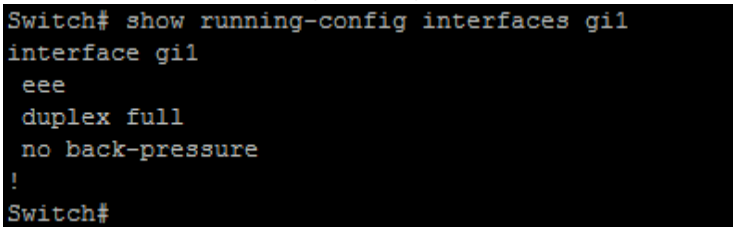
21.5 EEE

Use "**eee**" command to make port to enable the energy efficient Ethernet Feature. Use **"no"** form of this command to disable eee. IEEE 802.3az Energy Efficient Ethernet (EEE) is a standard that allows physical layer transmitters to consume less power during periods of low data activity. The only way to show this configuration is using "**show running-config**" command.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)# **eee**

Switch(config-if)#**no eee**

Syntax	**eee** **no eee**
Parameter	None
Default	Default eee state is disabled
Mode	Interface Configuration

Example	This example shows how to configure port gi1 and gi2 to be protected port.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 1
	Switch(config-if)# **eee**
	
	This example shows how to show current jumbo-frmae size
	Switch# **show running-config** interface gi1
	 
	`Switch# show running-config interfaces gi1`
	`interface gi1`
	` eee`
	` duplex full`
	` no back-pressure`
	`!`
	`Switch#`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.6 FLOWCONTROL

Use "**flowcontrol**" command to change port flow control configuration. Use **"no"** form to restore flow control to default (off) configuration.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)#**flowcontrol (auto | off | on)**

Switch(config-if)#**no flowcontrol**

Syntax	**flowcontrol (auto | off | on)** **no flowcontrol**
Parameter	**auto** Automatically enables or disables flow control on the interface. **off** Disable port flow control. **on** Enable port flow control.
Default	Default port flow control is off
Mode	Interface Configuration
Example	This example shows how to modify port duplex configuration. Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **flowcontrol on** This example shows how to show current flow control configuration Switch# **show interfaces**GigabitEthernet 1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show interfaces GigabitEthernet 1
GigabitEthernet1 is down
  Hardware is Gigabit Ethernet
  Full-duplex, Auto-speed, media type is Copper
  flow-control is on
  back-pressure is disabled
     0 packets input, 0 bytes, 0 throttles
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame
     0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underrun
     0 output errors, 0 collisions
     0 babbles, 0 late collision, 0 deferred
     0 PAUSE output
Switch#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.7 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. Use "**jumbo-frame**" command to modify maximum frame size. The only way to show this configuration is using **"show running-config"** command.

Switch#**configure terminal**
Switch(config)#**jumbo-frame** *<1518-10000>*

Syntax	**jumbo-frame** *<1518-10000>*
Parameter	*<1518-10000>*Specify the maximum frame size.
Default	Default maximum frame size is 1522.
Mode	Global Configuration

Example	This example shows how to modify maximum frame size on gi1 to 10000 bytes.
	Switch#**configure terminal**
	Switch(config)# **jumbo-frame** 9216
	`Switch# config t`
	`Switch(config)# jumbo-frame`
	`  <1518-10000>  Maximum frame size`
	This example shows how to show current jumbo-frame size
	
	Switch# **show running-config**
	`Switch#  show running-config`
	`SYSTEM CONFIG FILE ::= BEGIN`
	`! System Description: KT-NOS C3000-24GP+4X Switch`
	`! System Version: vSoldierOS.3K.v1.10`
	`! System Name: Switch`
	`! System Up Time: 0 days, 0 hours, 23 mins, 24 secs`
	`!`
	`!`
	`jumbo-frame 9216`
	`system location ""`
	`system contact ""`
	`system manufacturer "COMMANDO Networks"`
	`system support "support@commandonetworks.com"`
	`system telephone ""`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.8 PROTECTED

Use "**protected**" command 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. Use **"no"** form to make port unprotected.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)# **protected**

Switch(config-if)#**no protected**

Syntax	**protected** **no protected**
Default	Default protected state is no protected.
Mode	Interface Configuration
Example	This example shows how to configure port gi1 and gi2 to be protected port. Switch#**configure terminal** Switch(config)# **interface range** gi11-12 Switch(config-if-range)# **protected** This example shows how to show current protected port state. Switch# **show interfaces** GigabitEthernet 11-12 **protected** `Switch# configure terminal` `Switch(config)# interface range gi11-12` `Switch(config-if-range)#  protected` `Switch(config-if-range)#` `Switch# show interfaces GigabitEthernet 11-12 protected` ` Port	Protected State` `--------+----------------` ` gi11 |enabled` ` gi12 |enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.9 SHOW INTERFACE

Use "**show interface**" command to show detail port counters, parameters, and status. Use "**show interface status**" command to show brief port status. Use "**show interface protected**" command to show protected status.

Switch# **show interfaces** *{IF_PORTS}*
Switch# **show interfaces** *{IF_PORTS}* **status**
Switch# **show interfaces** *{IF_PORTS}* **protected**

Syntax	**show interfaces** *{IF_PORTS}* **show interfaces** *{IF_PORTS}* **status** **show interfaces** *{IF_PORTS}* **protected**
Parameter	*{IF_PORTS}* Specify port to show.
Mode	Privileged EXEC

Example	This example shows how to show current counters
	Switch# **show interfaces** GigabitEthernet 1
	`Switch# show interfaces GigabitEthernet 1`
	`GigabitEthernet1 is down`
	`  Hardware is Gigabit Ethernet`
	`  Full-duplex, Auto-speed, media type is Copper`
	`  flow-control is on`
	`  back-pressure is disabled`
	`     0 packets input, 0 bytes, 0 throttles`
	`     Received 0 broadcasts (0 multicasts)`
	`     0 runts, 0 giants, 0 throttles`
	`     0 input errors, 0 CRC, 0 frame`
	`     0 multicast, 0 pause input`
	`     0 input packets with dribble condition detected`
	`     0 packets output, 0 bytes, 0 underrun`
	`     0 output errors, 0 collisions`
	`     0 babbles, 0 late collision, 0 deferred`
	`     0 PAUSE output`
	`Switch#`
	
	This example shows how to show current protected port state.
	
	Switch# **show interfaces** GigabitEthernet 1-2 **protected**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show interfaces GigabitEthernet 1-2 protected
 Port    | Protected State
---------+----------------
    gi1 |enabled
    gi2 |enabled
Switch#
```

This example shows how to show current port status

Switch# show interfaces GigabitEthernet 1-2 status

```
Switch# show interfaces GigabitEthernet 1-2 status
Port  Name               Status      Vlan  Duplex  Speed    Type
gi1                      notconnect  1     full    auto     Copper
gi2   uplink port        notconnect  1     half    auto     Copper
Switch#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.10 SPEED

Use "**speed**" command to change port speed configuration. The speed is only able to configure to the physical maximum speed. For example, in fast Ethernet port, speed 1000 is not available. You cannot configure the speed on the SFP module ports, but you can configure the speed to not negotiate (nonegotiate) if it is connected to a device that does not support autonegotiation.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)# **speed (10 | 100 | 1000|auto)**

Syntax	**speed (10 | 100 | 1000|auto)**
Parameter	**10** Force 10 Mbps operation **100** Force 100 Mbps operation **1000** Force 1000 Mbps operation **auto** Enable AUTO speed configuration
Default	Default port speed is auto with all available abilities.
Mode	Interface Configuration

Example	This example shows how to modify port speed configuration.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 1
	Switch(config-if)# **speed 100**
	Switch# **show running-config interfaces** GigabitEthernet 1
	`Switch# show running-config interfaces GigabitEthernet 1`
	`interface gil`
	` lag 1 mode static`
	` speed 100`
	` duplex full`
	` description "userport"`
	` ipv6 mld max-groups 10`
	` ipv6 mld max-groups action replace`
	` ipv6 mld filter 1`
	` lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size`
	` lldp tlv-select vlan-name add 1`
	` lldp med tlv-select network-policy location inventory`
	` lldp med network-policy add 1`

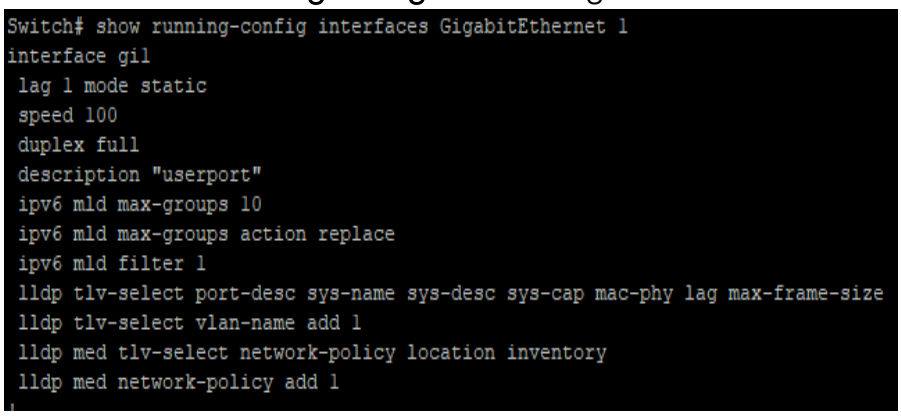
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

21.11 SHUTDOWN

Use "**shutdown**" command to disable port and use "**no shutdown**" to enable port. If port is error disabled by some reason, use "**no shutdown**" command can also recovery the port manually.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)# **shutdown**

Switch(config-if)#**no shutdown**

Syntax	**shutdown** **no shutdown**
Default	Default port admin state is no shutdown.
Mode	Interface Configuration
Example	This example shows how to modify port duplex configuration. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **shutdown** This example shows how to show current admin state configuration Switch# **show running-config interfaces** gi1 

```
Switch# show running-config interfaces GigabitEthernet 1
interface gi1
 lag 1 mode static
 speed 100
 duplex full
 description "userport"
 ipv6 mld max-groups 10
 ipv6 mld max-groups action replace
 ipv6 mld filter 1
 lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size
 lldp tlv-select vlan-name add 1
 lldp med tlv-select network-policy location inventory
 lldp med network-policy add 1
!
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

22. PORT ERROR DISABLE

When a port is in error-disabled state, it is effectively shut down and no traffic is sent or received on that port. The ErrDisable feature is implemented to handle critical situations where the switch detected excessive or late collisions on a port, port duplex misconfiguration, Ether Channel misconfiguration, Bridge Protocol Data Unit (BPDU) port-guard violation, UniDirectional Link Detection (UDLD), and other causes.

The error-disable function let the switch to shut down a port when it encounters physical, driver or configuration problems. A port being error-disabled is not by itself a cause for alarm, but for a reason of a problem that must be resolved. When a port is in error-disabled state, it will shut down and no traffic is sent or received on that port.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

22.1 ERRDISABLE RECOVERY CAUSE

Ports would be disabled because of the invalid actions detected by protocols. To enable the port error disable recovery from the specific cause, use the command errdisable recovery cause in the Global Configuration mode.

Switch#**configure terminal**

Switch(config)#**errdisable recovery cause(all|acl|arp-inspection |bpduguard| broadcast-flood|dhcp-rate-limit|psecure-violation|selfloop|unicast-flood|unknown-multicastflood)**

Switch(config)#**no errdisable recovery cause(all| acl| arpinspection |bpduguard|broadcast-flood|dhcp-rate-limit|psecure-violation| selfloop| unicast-flood|unknown- multicastflood)**

Syntax	**errdisable recovery cause(all| acl| arp-inspection| bpduguard| broadcast- flood| dhcp-rate-limit| psecure-violation| selfloop| unicast-flood| unknown-multicastflood)** **no errdisable recovery cause(all| acl| arp inspection| bpduguard| broadcast- flood| dhcp-rate-limit| psecure-violation| selfloop| unicast-flood| unknown- multicastflood)**
Parameter	**all** Enable the auto recovery for port error disabled from all causes. **acl** Enable the auto recovery for port error disabled from the ACL cause. **arp-inspection** Enable the auto recovery for port error disabled from the ARP inspection cause. **bpduguard** Enable the auto recovery for port error disabled from the STP BPDU Guard cause. **broadcast-flood** Enable the auto recovery for port error disabled from the broadcast flooding cause.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	dhcp-rate-limit Enable the auto recovery for port error disabled from the DHCP rate limit cause. **psecure-violation** Enable the auto recovery for port error disabled from the port security cause. **selfloop** Enable the auto recovery for port error disabled from the STP self-loop cause. **unicast-flood** Enable the auto recovery for port error disabled from the unicast flooding cause. **unknown-multicastflood** Enable the auto recovery for port error disabled from the unknown multicast flooding cause.
Default	Error disable recovery is disabled for all cause
Mode	Global Configuration

Example	The following example enables the port error disable recovery for the STP BPDU Guard and self-loog cause.
	Switch#**configure terminal**
	Switch(config)# **errdisable recovery cause bpduguard**
	Switch(config)# **errdisable recovery cause selfloop**
	
	`Switch# configure terminal`
	`Switch(config)#  errdisable recovery cause bpduguard`
	`Switch(config)# errdisable recovery cause selfloop`
	
	The following example To remove the port error disable recovery from the specific cause.
	Switch#**configure terminal**
	Switch(config)# **no errdisable recovery cause bpduguard**
	Switch(config)# **no errdisable recovery cause selfloop**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

22.2 ERRDISABLE RECOVERY INTERVAL

To set the recovery time of the error disabled ports, use the command ErrDisable recovery interval in the Global Configuration mode.

Switch#**configure terminal**

Switch(config)# **errdisable recovery interval** (seconds)

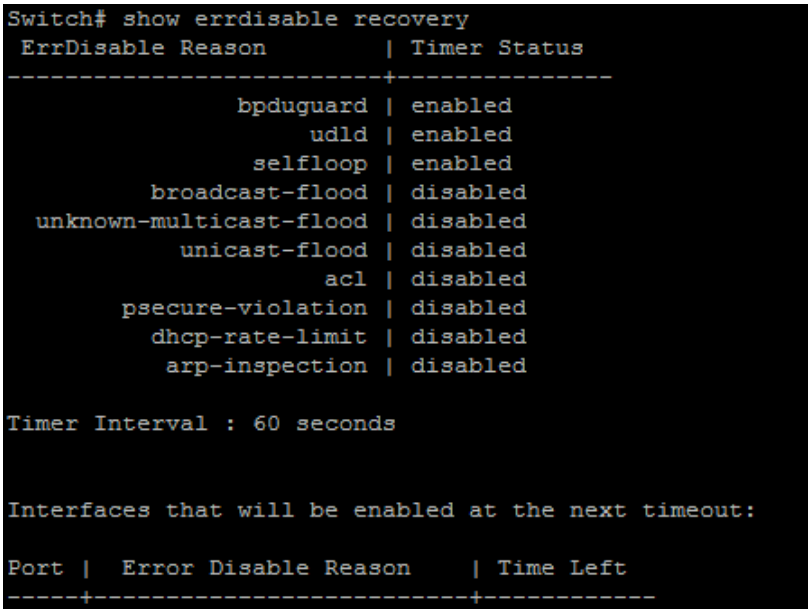
Syntax	**errdisable recovery interval** seconds
Parameter	**seconds** The time in seconds to recover from a specific error- disable state. The valid range is 0 to 86400 seconds, and the default value is 300 seconds.
Default	The default recovery time is 300 seconds
Mode	Global Configuration
Example	The following example set the agimg time to 500 seconds. Switch#**configure terminal** Switch(config)# **errdisable recovery interval** 60

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

22.3 SHOW ERRDISABLE RECOVERY

To show the error disable configuration and the interfaces in the error disabled state, use the command show ErrDisable recovery in the Privileged EXEC mode.

Switch# **show errdisable recovery**

Syntax	**show errdisable recovery**
Mode	Privileged EXEC
Example	The following example shows the error disable configuration, and the interfaces in the error disabled state. Switch# **show errdisable recovery** 

```
Switch# show errdisable recovery
 ErrDisable Reason        | Timer Status
--------------------------+---------------
               bpduguard | enabled
                    udld | enabled
                selfloop | enabled
          broadcast-flood | disabled
  unknown-multicast-flood | disabled
            unicast-flood | disabled
                      acl | disabled
        psecure-violation | disabled
          dhcp-rate-limit | disabled
           arp-inspection | disabled

Timer Interval : 60 seconds


Interfaces that will be enabled at the next timeout:

Port |  Error Disable Reason    | Time Left
-----+--------------------------+-----------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

23. PORT SECURITY

Port Security helps secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits:

You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.

You can enable port security on a per port basis. Port security implements two traffic filtering methods, dynamic locking, and static locking. These methods can be used concurrently.

Dynamic locking

You can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is given in the datasheet. After the limit is reached, additional MAC addresses are not learned. Only frames with allowable source MAC addresses are forwarded. Dynamically locked addresses can be converted to statically locked addresses. Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. You can set the time out value. Dynamically locked MAC addresses are eligible to be learned by another port. Static MAC addresses are not eligible for aging.

Static locking

you can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses. By using port security, a network administrator can associate specific MAC addresses with the interface, which can prevent an attacker to connect his device. This way you can restrict access to an interface so that only the authorized devices can use it. If an unauthorized device is connected, you can decide what action the switch will take, for example discarding the traffic and shutting down the port.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

23.1 PORT-SECURITY (GLOBAL)

By using port security, users can limit the number of MAC addresses that can be learned to a port, set static MAC addresses, and set penalties for that port if it is used by an unauthorized user.it provides the ability to limit what addresses will be allowed to send traffic on individual switchports within the switched network. The "**port-security**" command enables the port security functionality globally. Use the **"no"** form of this command to disable. You can verify settings by the show port-security command.

Switch#**configure terminal**
Switch(config)# **port-security**

Switch(config)# **no port-security**

Syntax	**port-security** **no port-security**
Default	Default is disabled
Mode	Global Configuration

Example	The following example shows how to enable port security
	Switch#**configure terminal**
	Switch(config)# **port-security**
	Switch# **show port-security**
	
	`Switch# configure terminal`
	`Switch(config)#  port-security`
	`Switch(config)#`
	`Switch# show port-security`
	`Port Security: Enabled`
	`Rate Limit: 100 pps`
	
	`Port  MaxAddr  TotalAddr  ConfigAddr  Violation  Action`
	`----- -------- ---------- ---------- ---------- ---------`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

23.2 PORT-SECURITY (INTERFACE)

The "**port-security**" command enables the port security functionality on this port. Use the **"no"** form of this command to disable. You can verify settings by the show port-security interface command.

Switch#**configure terminal**
Switch(config)# **port-security**

Switch(config)# **no port-security**

Syntax	**port-security** **no port-security**
Mode	Port Configuration

Example	The following example shows how to enable port security on interface GigabitEthernet 1
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 1
	Switch(config-if)# **port-security**
	Switch# **show port-security interfaces** GigabitEthernet 1
	
	`Switch# configure terminal`
	`Switch(config)# interface GigabitEthernet 1`
	`Switch(config-if)# port-security`
	`Switch(config-if)#`
	`Switch# show port-security interfaces GigabitEthernet 1`
	`Port Status MaxAddr TotalAddr ConfigAddr Violation Action`
	`----- ----------- -------- ----------- ----------- ------------ ---------`
	`gil SecureUp 1 0 0 0 Protect`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

23.3 PORT-SECURITY ADDRESS-LIMIT

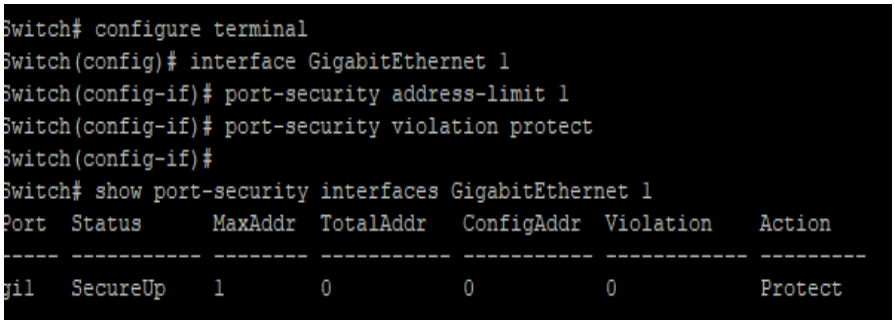
Use the "**port-security address-limit**" command to set the learning-limit number and the violation action. Use the **"no"** form of this command to restore the default settings. You can verify settings by the show port-security interface command.

Switch#**configure terminal**
Switch(config)#**port-security address-limit** *<1-256>* **action (forward |discard |shutdown)**

Switch(config)#**no port-security address-limit**

Syntax	**port-security address-limit** *<1-256>***action (forward| discard| shutdown)** **no port-security address-limit**
Parameter	*<1-256>*The learning-limit number. It specifies how many MAC addresses this port can learn. **forward** Forward this packet whose SMAC is new to system and exceed the learning-limit number. **discard** Discard this packet whose SMAC is new to system and exceed the learning-limit number. **shutdown** Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number.
Default	The address-limit default is 1 and action is "drop".
Mode	Port Configuration
Example	The following example shows how to enable port security on port 1 and set the learning limit number to 10. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **port-security address-limit** 1 Switch(config-if)# **port-security violation protect** Switch# **show port-security interfaces** GigabitEthernet 1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# port-security address-limit 1
Switch(config-if)# port-security violation protect
Switch(config-if)#
Switch# show port-security interfaces GigabitEthernet 1
Port  Status      MaxAddr  TotalAddr   ConfigAddr  Violation    Action
----- ----------- -------- ----------- ----------- ------------ ---------
gi1   SecureUp    1        0           0           0            Protect
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

23.4 SHOW PORT-SECURITY

Use "**show port-security**" command to show port-security global information.

Switch# **show port-security**

Syntax	**show port-security**
Mode	Privileged EXEC

Example	This example shows how to show port-security configurations.
	Switch# **show port-security**
	`Switch# show port-security`
	`Port Security: Enabled`
	`Rate Limit: 100 pps`
	
	`Port  MaxAddr  TotalAddr  ConfigAddr  Violation  Action`
	`----- -------- ----------- ----------- ---------- ----------`
	`gil   1        0           0           0          Protect`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

23.5 SHOW PORT-SECURITY INTERFACE

Use "**show port-security interfaces**" command to show port-security information of the specified port.

Switch# **show port-security interface** *{IF_PORTS}*

Syntax	**show port-security interface***{IF_PORTS}*
Parameter	*{IF_PORTS}* Select port to show port-security configurations
Default	No default value for this command.
Mode	Privileged EXEC
Example	This example shows how to show port-security configurations on interface GigabitEthernet 1. Switch# **show port-security interfaces** GigabitEthernet 1 Switch# Switch# show port-security interfaces GigabitEthernet 1 Port Status MaxAddr TotalAddr ConfigAddr Violation Action ----- ----------- -------- ----------- ----------- ------------ --------- gi1 Down 1 0 0 0 Protect Switch#

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

24. PROTOCOL VLAN

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, switch assigns untagged packets to VLAN 1. You can override this default behavior by defining port-based VLANs, protocol-based VLANs, or both. Switch always processes tagged packets according to the 802.1q standard and does not forward them to protocol based VLANs. If you assign a port to a protocol-based VLAN for a specific protocol, switch assigns the protocol-based VLAN ID to untagged frames that it receives on the port for that protocol. For other protocols, switch assigns the port VLAN ID to untagged frames that it receives on the port, either the default PVID1 or a PVID that you assigned to the port.

You define a protocol based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple ports. When you create a group, you must specify a name. The smart switch assigns a group ID automatically.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

24.1 VLAN PROTOCOL-VLAN GROUP (GLOBAL)

Use the vlan protocol-vlan group Global Configuration mode command to add protocol vlan group with specific protocol type and value. Use the **"no"** form of this command to remove protocol vlan group setting. You can verify your setting by entering the show vlan protocol-vlan Privileged EXEC command.

Switch# **configure terminal**
Switch(config)# **vlan protocol-vlan group***<1-8>* **frame-type (ethernet_ii |llc_other |snap_1042) protocol-value** VALUE

Switch(config)# **no vlan protocol-vlan group***<1-8>*

Syntax	**vlan protocol-vlan group***<1-8>***frame-type (ethernet_ii|llc_other|snap_1042)protocol-value** VALUE **no vlan protocol-vlan group***<1-8>*
Parameter	*<1-8>* Specify protocol vlan group to configure **(ethernet_ii|llc_other|snap_1042)** Specify protocol based frame type VALUE Specify protocol value to configure
Mode	Global Configuration
Example	The following example show how to configure protocol vlan group: Switch# **configure terminal** Switch(config)# **vlan protocol-vlan group** 1 **frame-type ethernet_ii protocol-value** 0x806 Switch(config)# **vlan protocol-vlan group** 2 **frame-type llc_other protocol-value** 0x800 Switch# **show vlan protocol-vlan**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# vlan protocol-vlan group 1 frame-type ethernet_ii protocol-value 0x806
Switch(config)# vlan protocol-vlan group 2 frame-type llc_other protocol-value 0x800
Switch(config)#
Switch# show vlan protocol-vlan

  Group ID    |     Status    |      Type      |        value
--------------+---------------+----------------+-----------------
     1        |  Enabled      |    Ethernet    |       0x0806
     2        |  Enabled      |   LLC other    |       0x0800
     3        |  Disabled     |       --       |         --
     4        |  Disabled     |       --       |         --
     5        |  Disabled     |       --       |         --
     6        |  Disabled     |       --       |         --
     7        |  Disabled     |       --       |         --
     8        |  Disabled     |       --       |         --
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

24.2 VLAN PROTOCOL-VLAN GROUP (INTERFACE)

Use the vlan protocol-vlan binding Interface Configuration mode command to binding protocol VLAN Group on specified interfaces. Use the **"no"** form of this command to cancel protocol VLAN Group Binding. You can verify your setting by entering the show vlan protocol-vlan interfaces IF_PORTS Privileged EXEC command

Switch# **configure terminal**
Switch(config-if)# **vlan protocol-vlan group** *<1-8>* **vlan** *<1-4094>*

Switch(config-if)# **no vlan protocol-vlan group** *<1-8>*

Syntax	**vlan protocol-vlan group** *<1-8>***vlan** *<1-4094>* **no vlan protocol-vlan group** *<1-8>*
Parameter	*<1-8>* Specify protocol vlan group to binding *<1-4094>* Specifies the Proto VLAN ID to configure.
Mode	Interface configuration
Example	The following example how to configure Protocol VLAN function on specified interfaces. Switch# **configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **vlan protocol-vlan group** 1 **vlan** 2 Switch# **show vlan protocol-vlan interfaces** GigabitEthernet 1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# vlan protocol-vlan group 1 vlan 2
Switch(config-if)#
Switch#  show vlan protocol-vlan interfaces GigabitEthernet 1

Port gil :
  Group 1
    Status      : Enabled
    VLAN ID     : 2
  Group 2
    Status      : Disabled
  Group 3
    Status      : Disabled
  Group 4
    Status      : Disabled
  Group 5
    Status      : Disabled
  Group 6
    Status      : Disabled
  Group 7
    Status      : Disabled
  Group 8
    Status      : Disabled
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

24.3 SHOW VLAN PROTOCOL-VLAN

Use the show vlan proto-vlan command in EXEC mode to display Proto VLAN group configuration.

Switch# **show vlan protocol-vlan** [**group***<1-8>*]

Syntax	**show vlan protocol-vlan**[**group***<1-8>*]
Parameter	*<1-8>*Specify protocol vlan group to display
Mode	Privileged EXEC

Example	The following example how to display Proto VLAN group configuration
	Switch# **show vlan protocol-vlan**
	`Switch# show vlan protocol-vlan`
	
	`Group ID | Status | Type | value`
	`1 | Enabled | Ethernet | 0x0806`
	`2 | Enabled | LLC other | 0x0800`
	`3 | Disabled | -- | --`
	`4 | Disabled | -- | --`
	`5 | Disabled | -- | --`
	`6 | Disabled | -- | --`
	`7 | Disabled | -- | --`
	`8 | Disabled | -- | --`
	
	`Switch#`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

24.4 SHOW VLAN PROTOCOL-VLAN INTERFACES

Use the show vlan protocol-vlan interface command in EXEC mode to display the Protocol VLAN interfaces setting.

Switch# **show vlan protocol-vlan interfaces***{IF_PORTS}*

Syntax	**show vlan protocol-vlan interfaces***{IF_PORTS}*
Parameter	*{IF_PORTS}* Specify interfaces protocol vlan to display
Mode	Privileged EXEC

Example	The following example shows how to display the Protocol VLAN interfaces setting
	Switch# **show vlan protocol-vlan interfaces** GigabitEthernet 1
	`Switch# show vlan protocol-vlan interfaces GigabitEthernet 1`
	
	`Port gi1 :`
	`  Group 1`
	`    Status      : Enabled`
	`    VLAN ID     : 2`
	`  Group 2`
	`    Status      : Enabled`
	`    VLAN ID     : 3`
	`  Group 3`
	`    Status      : Disabled`
	`  Group 4`
	`    Status      : Disabled`
	`  Group 5`
	`    Status      : Disabled`
	`  Group 6`
	`    Status      : Disabled`
	`  Group 7`
	`    Status      : Disabled`
	`  Group 8`
	`    Status      : Disabled`
	
	`Switch#`

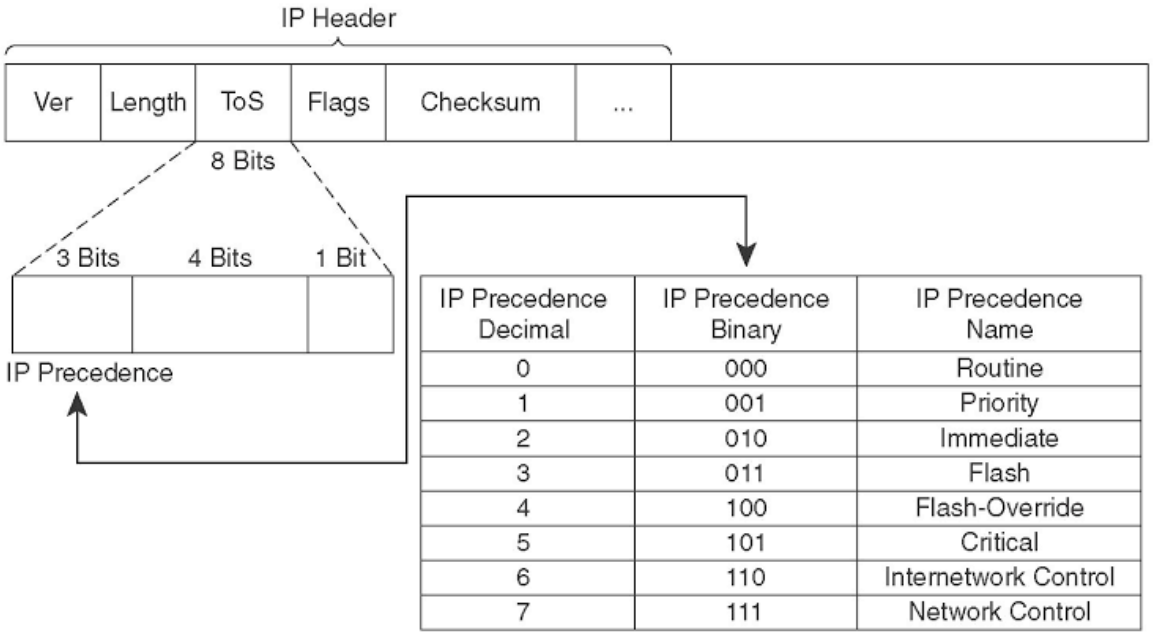
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25. QOS

A communications network forms the backbone of any successful organization. These networks transport a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. The bandwidth-intensive applications stretch network capabilities and resources, but also complement, add value, and enhance every business process. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required Quality of Service (QoS) by managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution. Thus, QoS is the set of techniques to manage network resources.

IP Precedence and DSCP Compared

The IP header is defined in RFC 791, including a 1-byte field called the Type of Service (ToS) byte. The ToS byte was intended to be used as a field to mark a packet for treatment with QoS tools. The ToS byte itself was further subdivided, with the high-order 3 bits defined as the IP Precedence (IPP) field. The complete list of values from the ToS byte's original IPP 3-bit field, and the corresponding names, is provided in Figure.



IP Precedence Decimal	IP Precedence Binary	IP Precedence Name
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash-Override
5	101	Critical
6	110	Internetwork Control
7	111	Network Control

Fig 25.1 QoS in IP header with IP Precedence

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Ethernet LAN Class of Service

Ethernet supports a 3-bit QoS marking field, but the field only exists when the Ethernet header includes either an 802.1Q or ISL trunking header. IEEE 802.1Q defines its QoS field as the 3 most significant bits of the 2-byte Tag Control field, calling the field the user-priority bits. ISL defines the 3 least-significant bits from the 1-byte User field, calling this field the Class of Service (CoS).

LAN CoS Fields

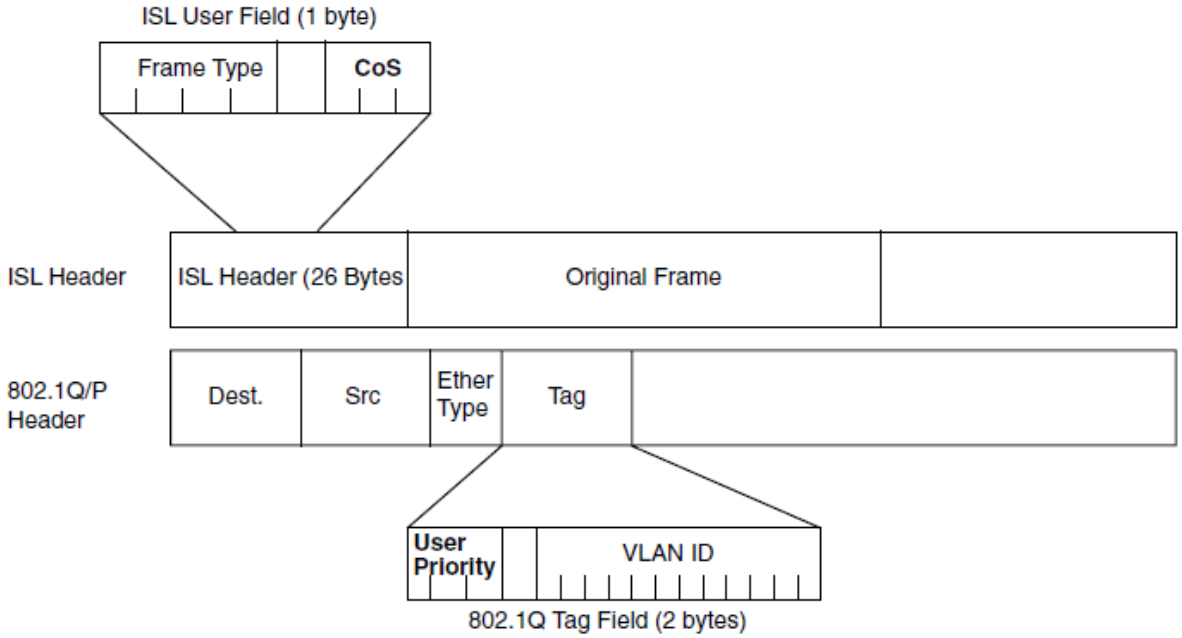


Fig 25.2 QoS in IP header with LAN CoS Feilds

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.1 QOS

Use **“qos”** command to enable quality of service which according to basic trust type to assign queue for packets, and packets with higher priority are able to send first. Use **“no”** form of this command to disable quality of service.

Switch#**configure terminal**
Switch(config)#**qos {map | queue | trust }**

Switch(config)# **no qos**

Syntax	**qos {map | queue | trust }** **no qos**
Mode	Global Configuration

Example	**map** Configure the QoS maps.
	queue Queue configuration
	trust Configure the global trust mode . Use the no form to return untrusted state.
	
	This example shows how to change qos to basic mode.
	Switch#**configure terminal**
	Switch(config)# **qos**
	This example shows how to check current qos mode.
	
	Switch# **show qos**
	`Switch# configure terminal`
	`Switch(config)# qos`
	`Switch(config)#`
	`Switch# sh qos`
	`QoS Mode: basic`
	`Basic trust: cos`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.2 QOS COS

Sometimes, there is no qos information in the packets, such as CoS, DSCP, IP Precedence. But we still can give the priority for packets by configuring the interface default cos value. If there is no qos information in the packets, the device will use this default cos value and find the cos-queue map to get the final destination queue. Use **"qos cos"** command to assign port default cos value.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)#**qos cos** *<0-7>*

Syntax	**Qos cos** *<0-7>*
Parameter	cos *<0-7>* Specify the CoS value for the interface.
Default	Default CoS value for interface is 0.
Mode	Interface Configuration
Example	This example shows how to configure default cos value 7 on interface gi1. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **qos cos** 7 Switch(config-if)# **end** Switch# **show qos interface** GigabitEthernet 1 Switch(config)# interface GigabitEthernet 1 Switch(config-if)# qos cos 7 Switch(config-if)# end Switch# show qos interface GigabitEthernet 1 Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec gi1 | 7 | enabled | disabled | disabled | disabled | Switch#

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.3 QOS MAP

According to different trust type, packets will be assigned to different queue based on the specific qos map. For example, if the trust type is trust cos, the device will get the cos value in packet and reference the cos-queue mapping to assign the correct queue.

The queue to cos, dscp or precedence maps are used by remarking function. If the port remarking feature is enabled, the remarking function will reference these 3 tables to remark packets.

Switch#**configure terminal**
Switch(config)#**qos map (cos-queue | dscp-queue | precedence-queue) SEQUENCE to** *<1-8>*
Switch(config)#**qos map (queue-cos | queue-precedence) SEQUENCE to** *<0-7>*
Switch(config)#**qos map queue-dscp SEQUENCE to** *<0-63>*

Syntax	**qos map (cos-queue | dscp-queue | precedence-queue) SEQUENCE to** *<1-8>* **qos map (queue-cos | queue-precedence) SEQUENCE to** *<0-7>* **qos map queue-dscp SEQUENCE to** *<0-63>*
Parameter	**cos-queue** Configure or show CoS to queue map **dscp-queue** Configure or show DSCP to queue map **precedence-queue** Configure or show IP Precedence to queue map. **queue-cos** Configure or show queue to CoS map **queue-dscp** Configure or show queue to DSCP map **queue-precedence** Configure or show queue to IP Precedence map **SEQUENCE** Specify the cos, dscp, precedence or queue with one or multiple values. *<1-8>*Specify the queue id *<0-7>*Specify the cos or precedence values *<0-63>*Specify the dscp values
Default	The default values of cos-queue are showing in the following table.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

CoS	Queue ID
0	2
1	1
2	3
3	4
4	5
5	6
6	7
7	8

The default values of dscp-queue are showing in the following table.

DSCP	Queue ID
0~7	1
8~15	2
16~23	3
24~31	4
32~39	5
40~47	6
48~55	7
56~63	8

The default values of ip precedence are showing in the following table

IP Precedence	Queue ID
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

The default values of queue-cos are showing in the following table.

Queue ID	CoS
1	1
2	0
3	2
4	3
5	4
6	5

The default values of queue-dscp are showing in the following table.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	<table><tr><th>Queue ID</th><th>DSCP</th></tr><tr><td>1</td><td>0</td></tr><tr><td>2</td><td>8</td></tr><tr><td>3</td><td>16</td></tr><tr><td>4</td><td>24</td></tr><tr><td>5</td><td>32</td></tr><tr><td>6</td><td>40</td></tr><tr><td>7</td><td>48</td></tr><tr><td>8</td><td>56</td></tr></table> The default values of queue-precedence are showing in the following table. <table><tr><th>Queue ID</th><th>IP Precedence</th></tr><tr><td>1</td><td>0</td></tr><tr><td>2</td><td>1</td></tr><tr><td>3</td><td>2</td></tr><tr><td>4</td><td>3</td></tr><tr><td>5</td><td>4</td></tr><tr><td>6</td><td>5</td></tr><tr><td>7</td><td>6</td></tr><tr><td>8</td><td>7</td></tr></table>
Mode	Global Configuration

Example	This example shows how to map cos 6 and 7 to queue 1.
	Switch#**configure terminal**
	Switch(config)# **qos map cos-queue** 6 7 **to** 1
	Switch# **show qos map cos-queue**
	`Switch# configure terminal`
	`Switch(config)# qos map cos-queue 6 7 to 1`
	`Switch(config)#`
	`Switch# show qos map cos-queue`
	
	`CoS to Queue mappings`
	`COS 0 1 2 3 4 5 6 7`
	`--------------------------------`
	`Queue 2 1 3 4 5 6 1 1`
	
	This example shows how to map queue 4 and 5 to cos 7.
	Switch#**configure terminal**
	Switch(config)# **qos map queue-cos** 4 5 **to** 7

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch# **show qos map queue-cos**
	
	`Switch# configure terminal`
	`Switch(config)# qos map queue-cos 4 5 to 7`
	`Switch(config)#`
	`Switch# show qos map cos-queue`
	
	`CoS to Queue mappings`
	`COS 0 1 2 3 4 5 6 7`
	`--------------------------------`
	`Queue 2 1 3 4 5 6 1 1`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.4 QOS QUEUE

The device support total 8 queues for QoS queuing. It can set the queue to be strict priority queue or weighted queue to prevent starvation. The queue with higher id value has higher priority. First, you need to decide how many strict priority queue you need. The strict priority queue will always occupy the higher priority queue. For example, if you specify the strict priority number to be 2, then the queue 7 and 8 will be the strict priority queues and the others are weighted queues. After you setup the number of strict priority queue, you need to setup the weight for the weighted queues by using **"qos queue weight"** command. And the bandwidth will be shared by the weight you configured between these weighted queues.

Switch#**configure terminal**
Switch(config)#**qos queue strict-priority-num <0-8>**
Switch(config)#**qos queue weight SEQUENCE**

Switch#**show qos queueing**

Syntax	**qos queue strict-priority-num** *<0-8>* **qos queue weight SEQUENCE** **show qos queueing**
Parameter	strict-priority-num *<0-8>* Specify the strict priority queue number weight SEQUENCE Specify the non-strict priority queue weight value. The valid queue weight value is from 1 to 127.
Default	Default strict priority queue number is 8, it means all queues are strict priority queue. The default queue weight for each queue is shown in following table.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	<table><tr><th>Queue ID</th><th>Queue Weight</th></tr><tr><td>1</td><td>1</td></tr><tr><td>2</td><td>2</td></tr><tr><td>3</td><td>3</td></tr><tr><td>4</td><td>4</td></tr><tr><td>5</td><td>5</td></tr><tr><td>6</td><td>9</td></tr><tr><td>7</td><td>13</td></tr><tr><td>8</td><td>15</td></tr></table>
Mode	Global Configuration

Example	This example shows how to setup device with 3 strict priority queues and give other weighted queues with weight 5, 10, 15, 20, 25.
	Switch#**configure terminal**
	Switch(config)# **qos queue strict-priority-num** 3
	Switch(config)# **qos queue weight** 5 10 15 20 25
	Switch# **show qos queueing**
	
	`Switch# configure terminal`
	`Switch(config)# qos queue strict-priority-num 3`
	`Switch(config)# qos queue weight 5 10 15 20 25`
	`Switch(config)#`
	`Switch# show qos queueing`
	`qid-weights  Ef - Priority`
	`1 -  5  dis- N/A`
	`2 -  10  dis- N/A`
	`3 -  15  dis- N/A`
	`4 -  20  dis- N/A`
	`5 -  25  dis- N/A`
	`6 - N/A  ena- 6`
	`7 - N/A  ena- 7`
	`8 - N/A  ena- 8`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.5 QOS REMARK

QoS remarking feature allow you to change priority information in packets based on egress queue. For example, you want all packets egress from interface queue 1 to remark the cos value to be 5 for next tier of device, you can enable the cos remarking feature on interface and configure the queue-cos map for queue 1 map to cos 5.

Use **"qos remark"** command to enable remarking feature on specific type. And use **"no qow remark"** command to disable it.

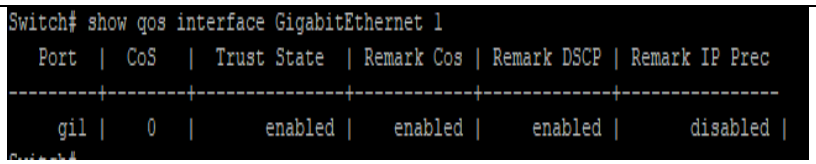
Switch#**configure terminal**
Switch(config)#**qos remark (cos | dscp | precedence)**

Switch(config)# **no qos remark (cos | dscp | precedence)**

Syntax	**qos remark (cos | dscp | precedence)** **no qos remark (cos | dscp | precedence)**
Parameter	cos Enable/Disable cos remarking. dscp Enable/Disable dscp remarking. precedence Enable/Disable precedence remarking
Default	Default CoS remarking is disabled. Default DSCP remarking is disabled. Default IP Precedence remarking is disabled.
Mode	Interface Configuration

Example	This example shows how to enable remarking features on interface gi1.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 1
	Switch(config-if)# **qos remark cos**
	Switch(config-if)# **qos remark dscp**
	Switch(config-if)# **qos remark precedence**
	`Switch# config t`
	`Switch(config)# interface GigabitEthernet 1`
	`Switch(config-if)# qos remark cos`
	`Switch(config-if)# qos remark dscp`
	`Switch(config-if)#  qos remark precedence`
	
	Switch# **show qos interface** GigabitEthernet 1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.6 QOS TRUST

In QoS basic mode, there are 4 trust types for device to judge the appropriate queue of the packets. This command is able to switch between these trust types.

CoS

IEEE 802.1p defined 3bits priority value in vlan tag. Trust this value in packets and assign queue according to cos-queue map.

DSCP

IETF RFC2474 defined 6bits priority value in IP packet (highest 6bits in ToS field). Trust this value in packets and assign queue according to dscp-queue map.

IP Precedence

The highest 3bits priority value in IP packet ToS field. Trust this value in packets and assign queue according to precedence-queue map.

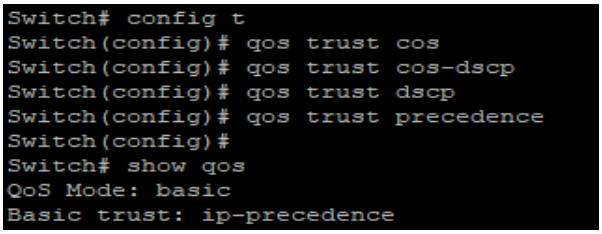
CoS-DSCP

Trust DSCP for IP packets and assign queue according to dscp-queue map. Trust CoS for non-IP packets and assign queue according to cos-queue map.

Switch#**configure terminal**
Switch(config)#**qos trust (cos | cos-dscp | dscp | precedence)**

Syntax	**qos trust (cos | cos-dscp | dscp | precedence)**
Parameter	**cos** Specify the device to trust CoS **cos-dscp** Specify the device to trust DSCP for IP packets, and trust CoS for non-IP packets. **dscp** Specify the device to trust DSCP **precedence** Specify the device to trust IP Precedence
Default	Default QoS trust type is cos.
Mode	Global Configuration
Example	This example shows how to change qos basic mode trust types.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch#configure terminal Switch(config)# qos trust cos Switch(config)# qos trust cos-dscp Switch(config)# qos trust dscp Switch(config)# qos trust precedence This example shows how to check current qos trust type. Switch# show qos 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.7 QOS TRUST (INTERFACE)

Interface Configuration After QoS function is enabled in basic mode, the device also supports per interface enable/disable the qos function. If the trust state on interface is enabled, all ingress packets of this interface will remap according to the trust type and the qos maps. Otherwise, all ingress packets will assign to queue 1.

Use **"qos trust"** to enable trust state on interface and use **"no qos trust"** to disable trust state on interface.

Switch#**configure terminal**
Switch(config)#**qos trust**

Switch(config)# **no qos trust**

Syntax	**qos trust** **no qos trust**
Default	Default interface qos trust state is enabled.
Mode	Interface Configuration
Example	This example shows how to disable qos trust state on interface gi1. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)#**qos trust** Switch# **show qos interface** GigabitEthernet 1 Switch# config t Switch(config)# interface GigabitEthernet 1 Switch(config-if)# qos trust Switch(config-if)# Switch# show qos interface GigabitEthernet 1 Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec gi1 | 0 | enabled | enabled | enabled | disabled |

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.8 SHOW QOS

Use **“show qos”** command to show qos state and trust type.

Switch#**show qos**

Syntax	**show qos**
Mode	Privileged EXEC

Example	This example shows how to check current qos mode.
	Switch# **show qos**
	
	`Switch# show qos`
	`QoS Mode: basic`
	`Basic trust: ip-precedence`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.9 SHOW QOS INTERFACE

Use **"show qos interfaces"** command to show port default cos, remarking state and remarking type state information.

Switch#**show qos interface** *{IF_PORTS}*

Syntax	**show qos interface** *{IF_PORTS}*
Parameter	*{IF_PORTS}*Select port to show qos configurations
Mode	Privileged EXEC
Example	This example shows how to show qos configurations on interface gi1. Switch# **show qos interface**GigabitEthernet 1 Switch# Switch# show qos interface GigabitEthernet 1 Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec ---------+--------+---------------+------------+-------------+--------------- gi1 | 7 | disabled | enabled | enabled | disabled | Switch#

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.10 SHOW QOS MAP

Use **“show qos map”** command to show all kinds of mapping for qos remapping and remarking features.

Switch#**show qos map [(cos-queue | dscp-queue | precedence-queue | queue-cos | queue-dscp | queue-precedence)]**

Syntax	**show qos map [(cos-queue | dscp-queue | precedence-queue | queue-cos |queue-dscp | queue-precedence)]**
Parameter	**cos-queue** Show CoS to queue map. **dscp-queue** Show DSCP to queue map. precedence-queue Show IP Precedence to queue map. queue-cos Show queue to CoS map. **queue-dscp** Show queue to DSCP map. **queue-precedence** Show queue to IP Precedence map.
Mode	Privileged EXEC
Example	This example shows how to show all qos maps. Switch# **show qos map**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show qos map

CoS to Queue mappings
   COS   0  1  2  3  4  5  6  7
--------------------------------
 Queue   1  2  3  4  5  6  1  1

DSCP to Queue mappings
d1: d2  0  1  2  3  4  5  6  7  8  9
---------------------------------------
 0:     1  1  1  1  1  1  1  1  2  2
 1:     2  2  2  2  2  2  3  3  3  3
 2:     3  3  3  3  4  4  4  4  4  4
 3:     4  4  5  5  5  5  5  5  5  5
 4:     6  6  6  6  6  6  6  6  7  7
 5:     7  7  7  7  7  7  8  8  8  8
 6:     8  8  8  8

IP Precedence to Queue mappings
 IP Precedence   0  1  2  3  4  5  6  7
---------------------------------------
        Queue   1  2  3  4  5  6  7  8

Queue to CoS mappings
 Queue   1  2  3  4  5  6  7  8
--------------------------------
   CoS   0  1  2  7  7  5  6  7

Queue to DSCP mappings
 Queue   1  2  3  4  5  6  7  8
--------------------------------
  DSCP   0  8 16 24 32 40 48 56

Queue to IP Precedence mappings
 Queue   1  2  3  4  5  6  7  8
--------------------------------
ipprec   0  1  2  3  4  5  6  7
Switch#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

25.11 SHOW QOS QUEUEING

Use "**show qos queueing**" command to show qos queueing information.

Switch#**show qos queueing**

Syntax	**show qos queueing**
Mode	Privileged EXEC

Example	This example shows how to check current qos queueing information.
	Switch# **show qos queueing**
	`Switch# show qos queueing`
	`qid-weights    Ef - Priority`
	`1 -    5         dis- N/A`
	`2 -   10         dis- N/A`
	`3 -   15         dis- N/A`
	`4 -   20         dis- N/A`
	`5 -   25         dis- N/A`
	`6 - N/A         ena- 6`
	`7 - N/A         ena- 7`
	`8 - N/A         ena- 8`
	`Switch#`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

26. RATE LIMIT

Rate-limiting for all traffic operates on a per-port basis to allow only the specified bandwidth to be used for inbound or outbound traffic. When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port and is a tool for enforcing maximum service level commitments granted to network users. This feature operates on a per-port level and is not configurable on port trunks. Rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.

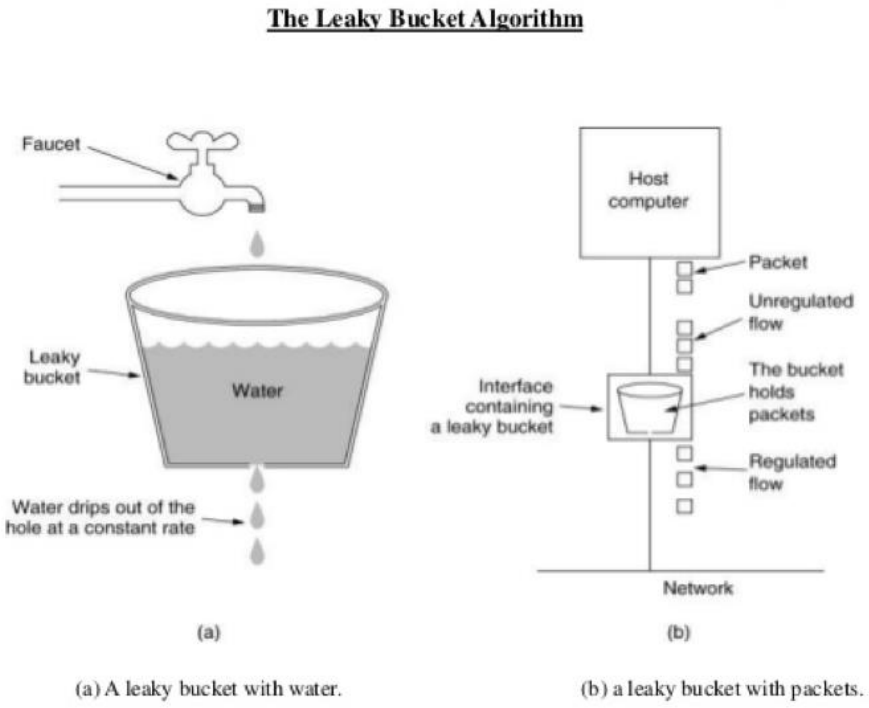


Fig 26.1 Leaky bucket Model

All traffic rate-limiting, Rate-limiting for all traffic operates on a per-port basis to allow only the specified bandwidth to be used for inbound or outbound traffic. When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port and is a tool for enforcing maximum service level commitments granted to

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

network users. This feature operates on a per-port level and is not configurable on port trunks. Rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.

Uses:

1) Rate-limiting can be applied by a RADIUS server during an authentication client session. Applying rate-limiting to desirable traffic is not recommended.
2) The switches also support ICMP rate-limiting to mitigate the effects of certain ICMP-based attacks. ICMP traffic is necessary for network routing functions. For this reason, blocking all ICMP traffic is not recommended.

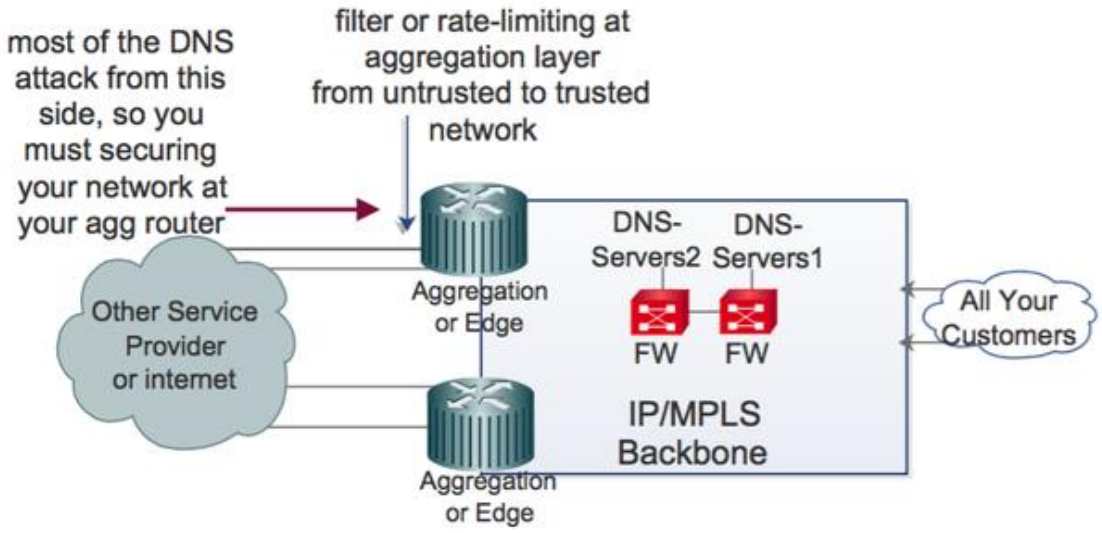


Fig 26.2 Rate limiting on Aggregation Layer

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

26.1 RATE LIMIT EGRESS

Use the "**rate-limit egress**" command to configure the egress port shaper. Use the **"no"** form of this command to disable the shaper. You can verify your setting by entering the show running-config interfaces command.

Switch# **configure terminal**
Switch(config)# **interface** { Interface-ID}

Switch(config-if)#**rate-limit egress <16-1000000>**

Switch(config-if)#**no rate-limit egress**

Syntax	**rate-limit egress <16-1000000>** **no rate-limit egress**
Parameter	<16-1000000> Specify the committed information rate.
Default	Default rate limit is disabled.
Mode	Interface configuration

Example	The following example shows how to configure ingress port rate limit and egress port shaper.
	Switch# **configure terminal**
	Switch(config)# **interface** gi1
	Switch(config-if)# **rate-limit egress** 2048
	Switch# **show running-config interfaces** gi1
	`Switch# config t`
	`Switch(config)# interface gi1`
	`Switch(config-if)# rate-limit egress 2048`
	`Switch(config-if)#`
	`Switch# show running-config interfaces gi1`
	`interface gi1`
	` lag 1 mode static`
	` switchport mode hybrid`
	` vlan protocol-vlan group 1 vlan 2`
	` rate-limit egress 2048`
	` speed 100`
	` duplex full`
	` description "userport"`
	` port-security`
	` qos remark cos`
	` qos remark dscp`
	` ipv6 mld max-groups 10`
	` ipv6 mld max-groups action replace`
	` ipv6 mld filter 1`
	` lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size`
	` lldp tlv-select vlan-name add 1`
	` lldp med tlv-select network-policy location inventory`
	` lldp med network-policy add 1`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

26.2 RATE LIMIT EGRESS QUEUE

Use the "**rate-limit egress queue**" command to configure the egress queue shaper. Use the **"no"** form of this command to disable the queue shaper. You can verify your setting by entering the show running-config interface command.

Switch# **configure terminal**
Switch(config)# **interface** { Interface-ID}

Switch(config-if)#**rate-limit egress queue**<1-8><16-1000000>

Switch(config-if)#**no rate-limit egress queue**<1-8>

Syntax	**rate-limit egress queue**<1-8><16-1000000> **no rate-limit egress queue**<1-8>
Parameter	<1-8>Specify the egress shaper queue number <16-1000000>Specify the queue rate
Default	Default queue rate limit is disabled.
Mode	Interface configuration
Example	The following example show how to configure ingress port rate limit and egress port shaper. Switch# **configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **rate-limit egress queue** 3 2048 Switch# **show running-config interfaces** gi1

```
Switch# config t
Switch(config)# interface gi1
Switch(config-if)#  rate-limit egress queue 3 2048
Switch(config-if)#
Switch# show running-config interfaces gi1
interface gi1
 lag 1 mode static
 switchport mode hybrid
 vlan protocol-vlan group 1 vlan 2
 rate-limit egress 2048
 rate-limit egress queue 3 1996531984
 speed 100
 duplex full
 description "userport"
 port-security
 qos remark cos
 qos remark dscp
 ipv6 mld max-groups 10
 ipv6 mld max-groups action replace
 ipv6 mld filter 1
 lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size
 lldp tlv-select vlan-name add 1
 lldp med tlv-select network-policy location inventory
 lldp med network-policy add 1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

26.3 RATE LIMIT INGRESS

Use the "**rate-limit ingress**" command to limit the incoming traffic rate on a port. Use the **"no"** form of this command to disable the rate limit. You can verify your setting by entering the show running-config interfaces command.

Switch# **configure terminal**
Switch(config)# **interface** { Interface-ID}

Switch(config-if)#**rate-limit ingress**<16-1000000>

Switch(config-if)#**no rate-limit ingress**

Syntax	**rate-limit ingress**<16-1000000> **no rate-limit ingress**
Parameter	<16-1000000>Specify the ingress limit rate <1-8>Specify the egress shaper queue number
Default	Rate limiting is disabled.
Mode	Interface configuration
Example	The following example shows how to configure ingress port rate limit. Switch# **configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **rate-limit ingress** 128 Switch# **show running-config interfaces** gi1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# configure terminal
Switch(config)# interface gil
Switch(config-if)# rate-limit ingress 128
Switch(config-if)#
Switch# show running-config interfaces gil
interface gil
 lag 1 mode static
 switchport mode hybrid
 vlan protocol-vlan group 1 vlan 2
 rate-limit ingress 128
 rate-limit egress 2048
 rate-limit egress queue 3 1996531984
 speed 100
 duplex full
 description "userport"
 port-security
 qos remark cos
 qos remark dscp
 ipv6 mld max-groups 10
 ipv6 mld max-groups action replace
 ipv6 mld filter 1
 lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size
 lldp tlv-select vlan-name add 1
 lldp med tlv-select network-policy location inventory
 lldp med network-policy add 1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

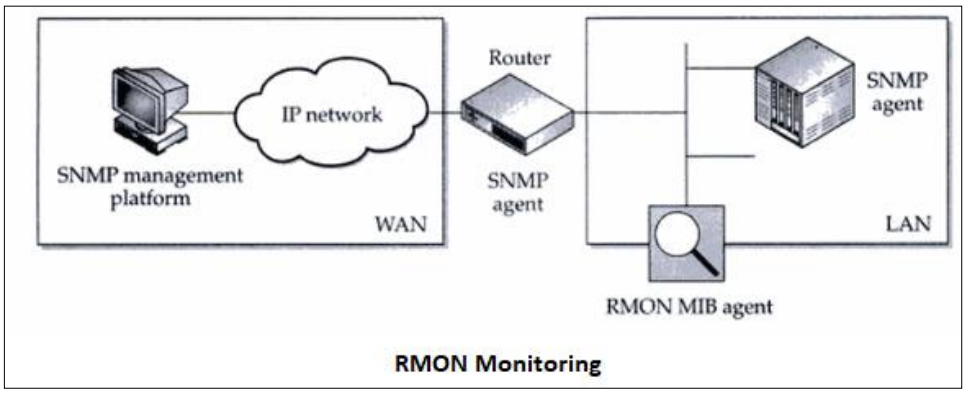
27. RMON

Remote Monitoring (RMON) is a standard specification that facilitates the monitoring of network operational activities using remote devices known as monitors or probes. It assists network administrators (NA) with efficient network infrastructure control and management. It was initially developed to address the issue of remote site and local area network (LAN) segment management from a centralized location. The RMON standard specifies a group of functions and statistics that may be exchanged between RMON compatible network probes and console managers. It performs extensive network-fault detection and provides performance-tuning data to NAs. It collects nine information types, including bytes sent, packets sent, packets dropped and statistics by host. NAs use RMON to determine network user traffic or bandwidth levels and website access information. Additionally, issue alerts may be preconfigured.

RMON uses certain network devices, such as servers, and contains network management applications that serve as clients. It controls the network by using its servers and applications simultaneously. When a network packet is transmitted, RMON facilitates packet status viewing and provides further information, if a packet is blocked, terminated or lost. It is divided into two classes: alarms and events. An event is a numbered, user-configured threshold for a particular SNMP object. You configure events to track, for example, CPU utilization or errors on a particular interface, or anything else you can do with an SNMP object. You set the rising and falling thresholds for these events, and then tell RMON which RMON alarm to trigger when those rising or falling thresholds are crossed. For example, you might want to have the router watch CPU utilization and trigger an SNMP trap or log an event when the CPU utilization rises faster than, say, 20 percent per minute. Or you may configure it to trigger an alarm when the CPU utilization rises to some absolute level, such as 80 percent. Both types of thresholds (relative, or “delta,” and absolute) are supported. Then, you can configure a different alarm notification as the CPU utilization falls, again at some delta or to an absolute level you specify.

The alarm that corresponds to each event is also configurable in terms of what it does (logs the event or sends a trap). If you configure an RMON alarm to send a trap, you also need to supply the SNMP community string for the SNMP server. Event and alarm numbering are locally significant. Alarm numbering provides a pointer to the corresponding event. That is, the configured events each point to specific alarm numbers, which you must also define.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.



Flg 27.1 RMON Monitoring

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.1 RMON

Use the rmon event command to add or modify a RMON event entry. Use the **"no"** form of this command to delete. You can verify settings by the show rmon event command.

Switch#**configure terminal**
Switch(config)#**rmon event**<1-65535>[**log**] [**trap COMMUNITY**] [**description** DESCRIPTION] [**owner** NAME]

Switch(config) #**no rmon event***<1-65535>*

Syntax	**rmon event***<1-65535>***[log] [trap** COMMUNITY] [**description** DESCRIPTION] [**owner** NAME] **no rmon event**<1-65535>
Parameter	*<1-65535>*Specify event index to create or modify. [log](Optional) Specify to show syslog. [trap COMMUNITY] (Optional) Specify SNMP community to show SNMP trap. [description DESCRIPTION] (Optional) Specify description of event [owner NAME] (Optional) Specify owner of event.
Mode	Global Configuration
Example	The example shows how to add RMON event entry with log and trap action and then modify it action to log only. Switch#**configure terminal** Switch(config)# **rmon event** 1 **log trap** public **description** test **owner** admin Switch# **show rmon event** 1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch#
Switch# configure terminal
Switch(config)# rmon event 1 log trap public description test owner admin
Switch(config)#
Switch# show rmon event 1
Rmon Event Index       : 1
Rmon Event Type        : Log and Trap
Rmon Event Community   : public
Rmon Event Description : test
Rmon Event Last Sent   :  (0) 0:00:00.00
Rmon Event Owner       : admin
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.2 RMON ALARM

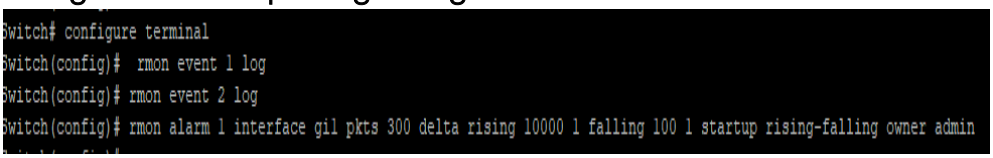
Use the rmon alarm command to add or modify a RMON alarm entry. Before add alarm entry, at least one event entry must be added. Use the **"no"** form of this command to delete. You can verify settings by the show rmon alarm command.

Switch#**configure terminal**
Switch(config) #**rmon alarm** *<1-65535>* **interface** *{IF_PORT}* (drop-events| octets| pkts| broadcast-pkts| multicast-pkts| crc-align-errors| undersize-pkts| oversize-pkts| fragments| jabbers| collisions| pkts64octets| pkts65to127octets| pkts128to255octets| pkts256to511octets | pkts512to1023octets | pkts1024to1518octets) *<1-2147483647>* (absolute| delta) rising *<0-2147483647><0-65535>* falling *<0-2147483647><0-65535>*startup (rising| rising-falling| falling) [owner NAME]

Switch(config) #**no rmon alarm** *<1-65535>*

Syntax	**rmon alarm** *<1-65535>* **interface** *{IF_PORT}* (**drop-events|octets|pkts| broadcast-pkts| multicast-pkts|crc-align-errors|undersize-pkts|oversize-pkts|fragments|jabbers|collisions|pkts64octets|pkts65to127octets |pkts128to255octets|pkts256to511octets|pkts512to1023octets |pkts1024to1518octets**) *<1-2147483647>* (**absolute|delta**) **rising** *<0-2147483647><0-65535>* **falling** *<0-2147483647><0-65535>***startup** (**rising|rising-falling|falling**) [**owner** NAME] **no rmon alarm** *<1-65535>*
Parameter	*<1-65535>* Specify alarm index to create or modify *{IF_PORT}* Specify the interface to sample (variable) Specify a mib object to sample *<1-2147483647>* Specify the time in seconds that the alarm monitors the MIB variable. (absolute|delta) Specify absolute to compare sample counter absolutely. Specify delta to compare delta counter between samples *<0-2147483647>* Specify a number which the alarm trigger rising event *<0-65535>* Specify event index when the rising threshold exceeds.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	<0-2147483647> Specify a number which the alarm trigger falling event *<0-65535>* Specify event index when the falling threshold exceeds. (rising|rising- falling|falling)Specify only to how rising or falling startup event. Or show either rising or falling startup event. [owner NAME] (Optional) Specify owner of alarm.
Mode	Global Configuration
Example	The example shows how to add RMON alarm entry that sample interface fa1 packets delta count every 300 seconds. Trigger event index 1 if over than rising threshold 10000, trigger event index 2 if lower than falling threshold. Switch#**configure terminal** Switch(config)# **rmon event** 1 **log** Switch(config)# **rmon event** 2 **log** Switch(config)# **rmon alarm** 1 **interface** gi1 **pkts** 300 **delta rising** 10000 1 **falling** 100 1 **startup rising-falling owner** admin 

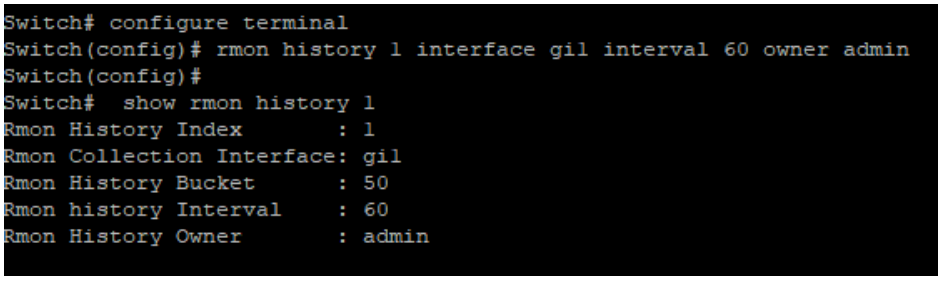
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.3 RMON HISTORY

Use the rmon history command to add or modify a RMON history entry. Use the **"no"** form of this command to delete. You can verify settings by the show rmon history command.

Switch#**configure terminal**
Switch(config)#**rmon history** *<1-65535>* **interface** *{IF_PORT}* [buckets *<1-65535>*] [**interval** *<1-3600>*/[**owner** NAME]

Switch(config) #**no rmon history** *<1-65535>*

Syntax	**rmon history** *<1-65535>***interface** *{IF_PORT}* [buckets *<1-65535>*][**interval** *<1-3600>*/[**owner** NAME]
Parameter	*<1-65535>*Specify history index to create or modify. *{IF_PORT}* Specify the interface to sample [bucket *<1-65535>*] (Optional) Specify the maximum number of buckets. [interval *<1-3600>*](Optional) Specify time interval for each sample [owner NAME](Optional)Specify owner of history
Mode	Global Configuration
Example	The example shows how to add RMON history entry that monitor interface gi1 every 60 seconds and then modify it to monitor every 30 seconds. Switch#**configure terminal** Switch(config)# **rmon history** 1 interface gi1 interval 60 owner admin Switch# **show rmon history** 1 

```
Switch# configure terminal
Switch(config)# rmon history 1 interface gi1 interval 60 owner admin
Switch(config)#
Switch#  show rmon history 1
Rmon History Index       : 1
Rmon Collection Interface: gi1
Rmon History Bucket      : 50
Rmon history Interval    : 60
Rmon History Owner       : admin
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.4 CLEAR RMON INTERFACES STATISTICS

Use the clear rmon interfaces statistics command to clear RMON etherStat statistics those are recorded on interface. You can verify results by the show rmon interface statistics command.

Switch #**clear rmon interfaces** *{IF_PORTS}* **statistics**

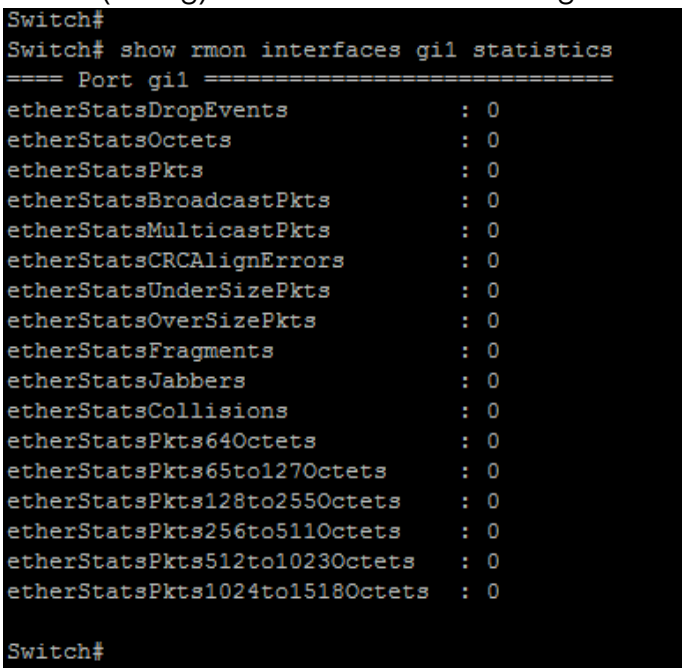
Syntax	**clear rmon interfaces** {*IF_PORTS*} **statistics**
Parameter	*{IF_PORTS}* specifies ports to clear
Mode	Privileged EXEC
Example	The example shows how to clear RMON etherStat statistics on interface gi1. switch# **clear rmon interfaces** gi1 **statistics** switch# **show rmon interfaces** gi1 **statistics** Switch# clear rmon interfaces gi1 statistics Switch# show rmon interfaces gi1 statistics ==== Port gi1 ========== etherStatsDropEvents : 0 etherStatsOctets : 0 etherStatsPkts : 0 etherStatsBroadcastPkts : 0 etherStatsMulticastPkts : 0 etherStatsCRCAlignErrors : 0 etherStatsUnderSizePkts : 0 etherStatsOverSizePkts : 0 etherStatsFragments : 0 etherStatsJabbers : 0 etherStatsCollisions : 0 etherStatsPkts64Octets : 0 etherStatsPkts65to127Octets : 0 etherStatsPkts128to255Octets : 0 etherStatsPkts256to511Octets : 0 etherStatsPkts512to1023Octets : 0 etherStatsPkts1024to1518Octets : 0 Switch#

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.5 SHOW RMON INTERFACES STATISTICS

Use the show rmon interfaces statistics command to show RMON etherStat Statistics of interface.

Switch #**show rmon interfaces** *{IF_PORTS}***statistics**

Syntax	**show rmon interfaces** *{IF_PORTS}***statistics**
Parameter	*{IF_PORTS}*specifies ports to show
Mode	Privileged EXEC
Example	The example shows how to show RMON etherStat statistics of interface gi1. Switch(config)# **show rmon interfaces** gi1 **statistics** 

```
Switch#
Switch# show rmon interfaces gi1 statistics
==== Port gi1 ==============================
etherStatsDropEvents            : 0
etherStatsOctets                : 0
etherStatsPkts                  : 0
etherStatsBroadcastPkts         : 0
etherStatsMulticastPkts         : 0
etherStatsCRCAlignErrors        : 0
etherStatsUnderSizePkts         : 0
etherStatsOverSizePkts          : 0
etherStatsFragments             : 0
etherStatsJabbers               : 0
etherStatsCollisions            : 0
etherStatsPkts64Octets          : 0
etherStatsPkts65to127Octets     : 0
etherStatsPkts128to255Octets    : 0
etherStatsPkts256to511Octets    : 0
etherStatsPkts512to1023Octets   : 0
etherStatsPkts1024to1518Octets  : 0

Switch#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.6 SHOW RMON EVENT

Use the show rmon event command to show existed RMON event entry.

Switch #**show rmon event** (*<1-65535>*| **all**)

Syntax	**show rmon event** (*<1-65535>*| **all**)
Parameter	*<1-65535>*specifies event index to show all Show all existed event
Mode	Privileged EXEC

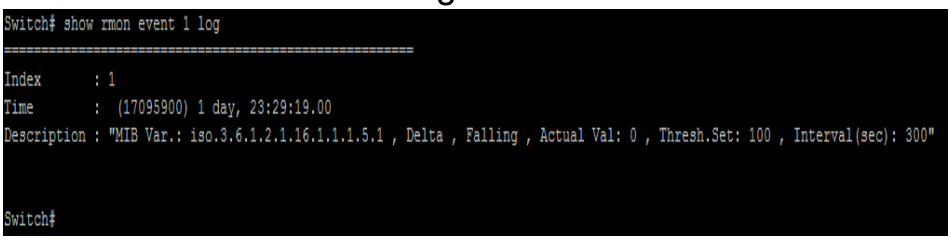
Example	The example shows how to show rmon event entry.
	Switch#**configure terminal**
	Switch(config)# **rmon event** 1 **log trap public description** test **owner** admin
	switch# **show rmon event** 1
	`Switch# config t`
	`Switch(config)# rmon event 1 log trap public description test owner admin`
	`Switch(config)#`
	`Switch# show rmon event 1`
	`Rmon Event Index : 1`
	`Rmon Event Type : Log and Trap`
	`Rmon Event Community : public`
	`Rmon Event Description : test`
	`Rmon Event Last Sent : (0) 0:00:00.00`
	`Rmon Event Owner : admin`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.7 SHOW RMON EVENT LOG

Use the show rmon event log command to show log triggered by RMONalarm.

Switch #**show rmon event** *<1-65535>* **log**

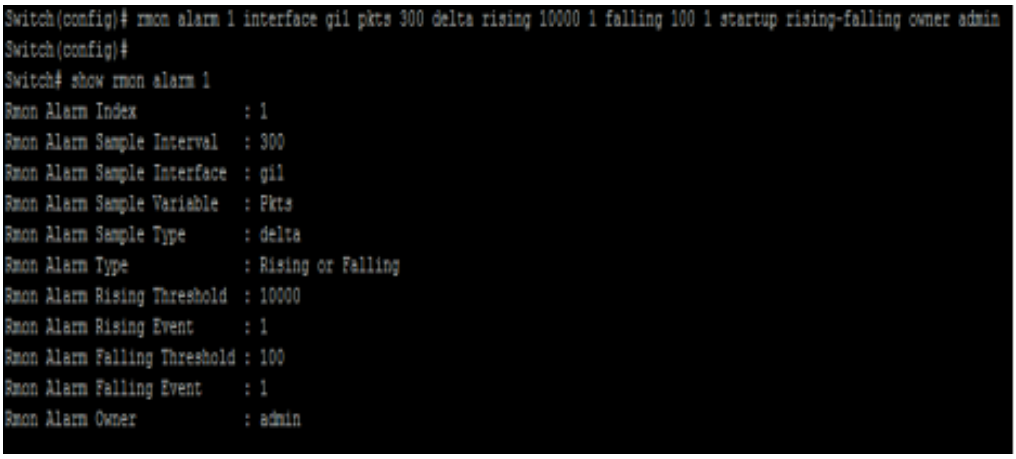
Syntax	**show rmon event** *<1-65535>* **log**
Parameter	*<1-65535>*specifies event index to show event log
Default	No entry and log is exist
Mode	Privileged EXEC
Example	The example shows how to show rmon event log. Switch# **show rmon event** 1 **log**  Switch# show rmon event 1 log ========== Index : 1 Time : (17095900) 1 day, 23:29:19.00 Description : "MIB Var.: iso.3.6.1.2.1.16.1.1.1.5.1 , Delta , Falling , Actual Val: 0 , Thresh.Set: 100 , Interval(sec): 300" Switch#

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.8 SHOW RMON ALARM

Use the show rmon alarm command to show existed RMON alarm entry.

Switch #**show rmon alarm** (*<1-65535>*| **all**)

Syntax	**show rmon alarm** (*<1-65535>*| all)
Parameter	*<1-65535>*specifies alarm index to show all Show all existed alarm
Mode	Privileged EXEC
Example	The example shows how to show rmon alarm entry. Switch#**configure terminal** Switch(config)**# rmon alarm** 1 **interface** gi1 **pkts** 300 **delta rising** 10000 1 **falling** 100 1 **startup rising-falling owner** admin Switch#**show rmon alarm** 1  Switch(config)# rmon alarm 1 interface gi1 pkts 300 delta rising 10000 1 falling 100 1 startup rising-falling owner admin Switch(config)# Switch# show rmon alarm 1 Rmon Alarm Index : 1 Rmon Alarm Sample Interval : 300 Rmon Alarm Sample Interface : gi1 Rmon Alarm Sample Variable : Pkts Rmon Alarm Sample Type : delta Rmon Alarm Type : Rising or Falling Rmon Alarm Rising Threshold : 10000 Rmon Alarm Rising Event : 1 Rmon Alarm Falling Threshold : 100 Rmon Alarm Falling Event : 1 Rmon Alarm Owner : admin

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.9 SHOW RMON HISTORY

Use the show rmon history command to show existed RMON history entry.

Switch #**show rmon history** (*<1-65535>*| **all**)

Syntax	**show rmon history** (*<1-65535>*| **all**)
Parameter	*<1-65535>* specifies history index to show all Show all existed history
Mode	Privileged EXEC
Example	The example shows how to show RMON history entry. switch(config)# rmon history 1 interface gi1 interval 30 owner admin switch# **show rmon history** 1 Switch(config)# rmon history 1 interface gi1 interval 30 owner admin Switch(config)# Switch# show rmon history 1 Rmon History Index : 1 Rmon Collection Interface: gi1 Rmon History Bucket : 50 Rmon history Interval : 30 Rmon History Owner : admin

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

27.10 SHOW RMON HISTORY STATISTIC

Use the show rmon history statistic command to show statistics that are recorded by RMON history.

Switch #**show rmon history** *<1-65535>***statistic**

Syntax	show rmon history *<1-65535>*statistic
Parameter	*<1-65535>*specifies history index to show history statistic
Mode	Privileged EXEC
Example	The example shows how to show RMON history statistics switch# **show rmon history** 1 **statistics** `Switch# show rmon history 1 statistic`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28. 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. It has been defined with four major functional areas to support the core function of allowing managers to manage agents:

Data:

The syntax conventions for how to define the data to an agent or manager. These specifications are called the Structure of Management Information (SMI).

MIBs:

Over 100 Internet standards define different MIBs, each for a different technology area, with countless vendor proprietary MIBs as well. The MIB definitions conform to the appropriate SMI version.

Protocols:

The messages used by agents and managers to exchange management data.

Security and Administration:

Definitions for how to secure the exchange of data between agents and managers.

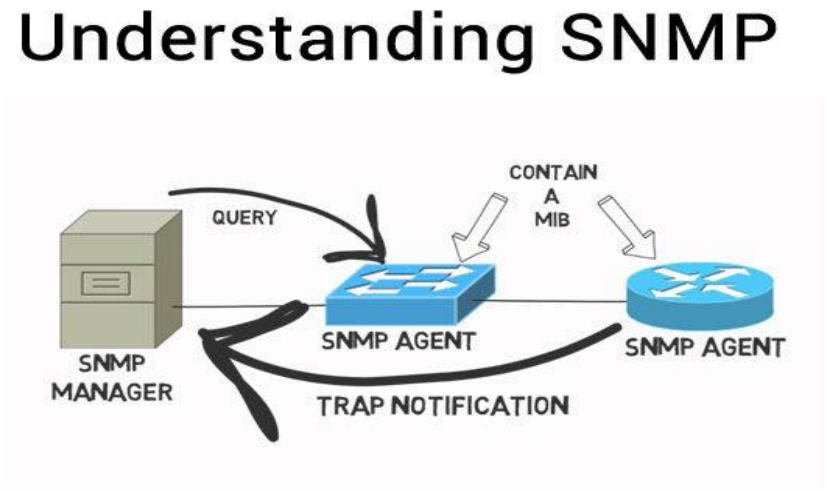


Fig 28.1 SNMP concept

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

SNMP Versions

v1, -simple authentication with communities, but used MIB-I originally.

v2 Uses SMIv2, removed requirement for communities, added Get Bulk and Inform messages, but began with MIB-II originally. 2c Pseudo-release (RFC 1905) that allowed SNMPv1-style communities with SNMPv2; otherwise, equivalent to SNMPv2.

v3 Mostly identical to SNMPv2, but adds significantly better security, although it supports communities for backward compatibility. Uses MIB-II.

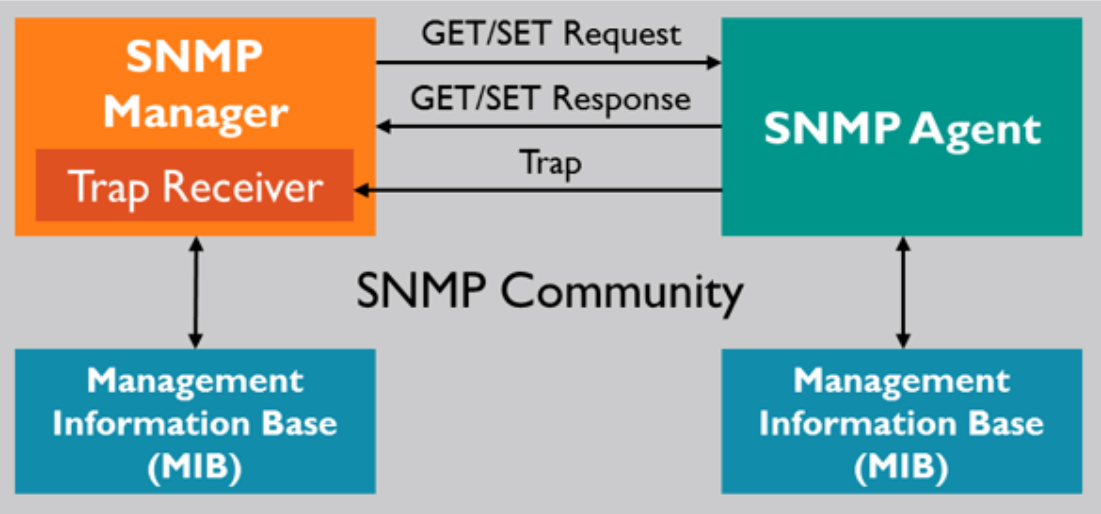


Fig 28.2 SNMP Community concept

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.1 SHOW SNMP

To show the status of Simple Network Management Protocol (SNMP), use the command show snmp in the Privileged EXEC mode.

Switch# **show snmp**

Syntax	**show snmp**
Mode	Privileged EXEC

Example	The following example shows the SNMP status.
	Switch# **show snmp**
	`Switch# show snmp`
	`SNMP is enabled.`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.2 SHOW SNMP COMMUNITY

To show the configuration of snmp communities, use the command show snmp community in the Privileged EXEC mode.

Switch# **show snmp community**

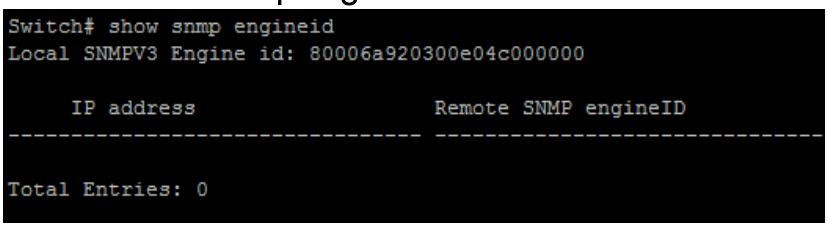
Syntax	**show snmp community**
Mode	Privileged EXEC

Example	The following example shows the SNMP communities configuration.
	Switch# **show snmp community**
	`Switch# show snmp community`
	`Commnunity Name  Group Name  View  Access`
	`public  all  ro`
	`Total Entries: 1`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.3 SHOW SNMP ENGINEID

To show the SNMPv3 engine IDs defined on the switch, use the command show snmp engine id in the Privileged EXEC mode.

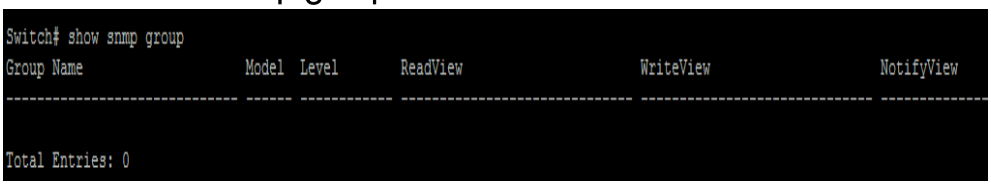
Syntax	show snmp engine id
Mode	Privileged EXEC
Example	The following example shows the SNMP engine id information. Switch# show snmp engineid 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.4 SHOW SNMP GROUP

To show the SNMP group configuration on the switch, use the command show snmp group in the Privileged EXEC mode.

Switch# **show snmp group**

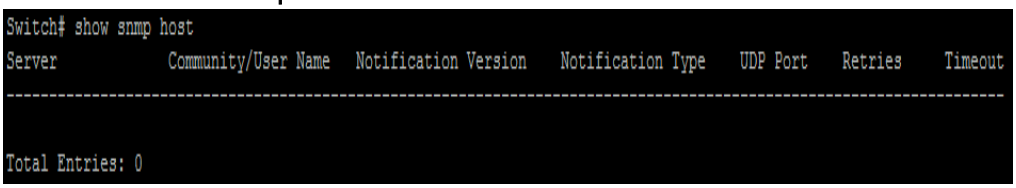
Syntax	**show snmp group**
Mode	Privileged EXEC
Example	The following example shows the SNMP group configuration. Switch# **show snmp group** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.5 SHOW SNMP HOST

To show the SNMP trap notification recipients defined on the switch, use the command show snmp host in the Privileged EXEC mode.

Switch# **show snmp host**

Syntax	**show snmp host**
Mode	Privileged EXEC
Example	The following example shows the configuration of SNMP notification recipients on the switch. Switch# **show snmp host** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.6 SHOW SNMP TRAP

To show the status of SNMP traps on the switch, use the command show snmp trap in the Privileged EXEC mode.
Switch#**show snmp trap**

Syntax	**show snmp trap**
Mode	Privileged EXEC

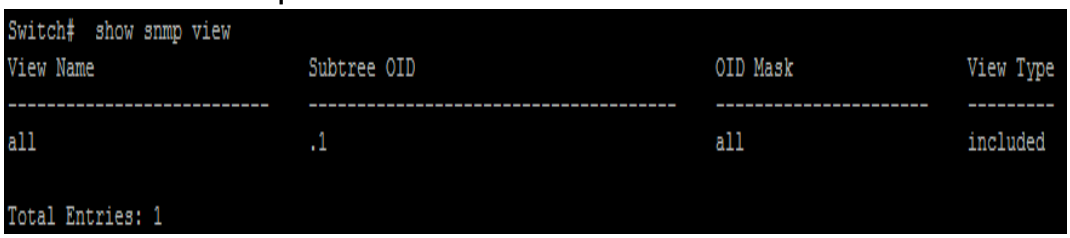
Example	The following example shows the status of SNMP traps.
	Switch# **show snmp trap**
	`Switch# show snmp trap`
	`SNMP auth failed trap  : Enable`
	`SNMP linkUpDown trap   : Enable`
	`SNMP cold-start trap   : Enable`
	`SNMP warm-start trap   : Enable`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.7 SHOW SNMP VIEW

To show the SNMP view defined on the switch, use the command show snmp view in the Privileged EXEC mode.

Switch# **show snmp view**

Syntax	**show snmp view**
Mode	Privileged EXEC
Example	The following example shows the configuration of SNMP view. Switch# **show snmp view** 

```
Switch#  show snmp view
View Name                Subtree OID                        OID Mask              View Type
-----------------------  ---------------------------------  --------------------  ---------
all                      .1                                 all                   included

Total Entries: 1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.8 SHOW SNMP USER

To show the SNMP users defined on the switch, use the command show snmp user in the Privileged EXEC mode.
Switch# **show snmp user**

Syntax	**show snmp user**
Mode	Privileged EXEC

Example	The following example shows the configuration of SNMP user.
	Switch# **show snmp user**
	`Switch# show snmp user`
	
	`Total Entries: 0`

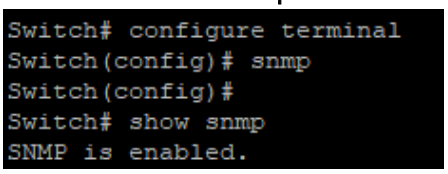
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.9 SNMP

To enable the SNMP on the switch, use the command snmp in the Global Configuration mode. Otherwise, use the **"no"** form of the command to disable to SNMP.

Switch# **configure terminal**
Switch(config)# **snmp**

Syntax	**snmp**
Default	SNMP is disabled by default
Mode	Global Configuration

Example	The following example enables the SNMP.
	Switch# **configure terminal**
	Switch(config)# **snmp**
	Switch# **show snmp**
	 
	`Switch# configure terminal`
	`Switch(config)# snmp`
	`Switch(config)#`
	`Switch# show snmp`
	`SNMP is enabled.`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.10 SNMP COMMUNITY

To define the SNMP community that permit access for SNMP v1 and v2, use the command snmp community in the Global Configuration mode.

Switch# **configure terminal**
Switch(config)#**snmp community community-name [view view-name] (ro|rw)**
Switch(config)#**snmp community community-name group group-name**

Switch(config)#**no snmp community community-name**

Syntax	**snmp community community-name [view view-name] (ro|rw)** **snmp community community-name group group-name** **no snmp community community-name**
Parameter	**community-name** The SNMP community name. Its maximum length is 20 characters. **view** view-name Specify the SNMP view configured by the command snmp view to define the object available to the community. **ro** Read only access (default) **rw** Writable access **group** group-name Specify the SNMP group configured by the command **snmp** group to define the object available to the community.
Mode	Global Configuration

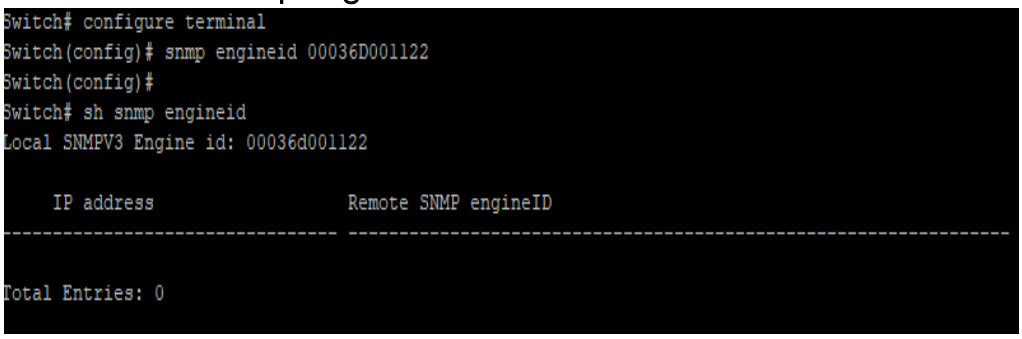
Example	The following example defines the SNMP community named private with the default view all, and the access right is read-only.
	Switch# **configure terminal**
	Switch(config)# **snmp community private ro**
	`Switch# configure terminal`
	`Switch(config)# snmp community private ro`
	`Switch(config)#`
	`Switch# show snmp community`
	`Commnunity Name  Group Name  View  Access`
	`private  all  ro`
	`public  all  ro`
	`Total Entries: 2`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.11 SNMP ENGINEID

To define the SNMP engine on the switch, use the command snmp engineid in the Global Configuration mode.

Switch# **configure terminal**
Switch(config)# **snmp engineid 00036D001122**

Syntax	**Snmp engineid (default|ENGINEID)**
Parameter	**Default** Default engine ID generated on the basis of the switch MAC address. **ENGINEID** Specify SNMP engine ID. The engine ID is the 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.
Default	The default SNMP engine ID on the switch is based on switch MAC address.
Mode	Global Configuration
Example	The following example configure the switch SNMP engine ID Switch# **configure terminal** Switch(config)# **snmp engineid 00036D001122** Switch# **show snmp engineid** 

```
Switch# configure terminal
Switch(config)# snmp engineid 00036D001122
Switch(config)#
Switch# sh snmp engineid
Local SNMPV3 Engine id: 00036d001122

    IP address                  Remote SNMP engineID
------------------------------ ------------------------------------------------------------------

Total Entries: 0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.12 SNMP ENGINEID RMOTE

To define the remote host for SNMP engine, use the command snmp engineid remote in the Global Configuration mode and use the **"no"** form of the command to delete the remote host from the SNMP engine.

Switch# **configure terminal**
Switch(config)# **snmp engineid remote (ip-addr|ipv6-addr)** *[ENGINEID]*

Switch(config)# **no snmp engineid remote (ip-addr|ipv6-addr)**

Syntax	**snmp engineid remote (ip-addr|ipv6-addr)** ENGINEID **no snmpengineid remote (ip-addr|ipv6-addr)**
Parameter	***ENGINEID*** Specify SNMP engine ID. The engine ID is a 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2. **ip-addr** IP address of the remote host **ipv6-addr** IPv6 address of the remote host
Mode	Global Configuration

Example	The following example adds the remote 192.168.1.11 into SNMP engine
	Switch# **configure terminal**
	Switch(config)# **snmp engineid remote** 192.168.1.1 100036D10000A
	`Switch(config)# snmp engineid remote 192.168.1.11 00036D10000A`
	`Switch(config)# exit`
	`Switch# show snmp engineid`
	`Local SNMPV3 Engine id: 00036d001122`
	
	`IP address Remote SNMP engineID`
	`192.168.1.11 00036D10000A`
	
	`Total Entries: 1`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.13 SNMP GROUP

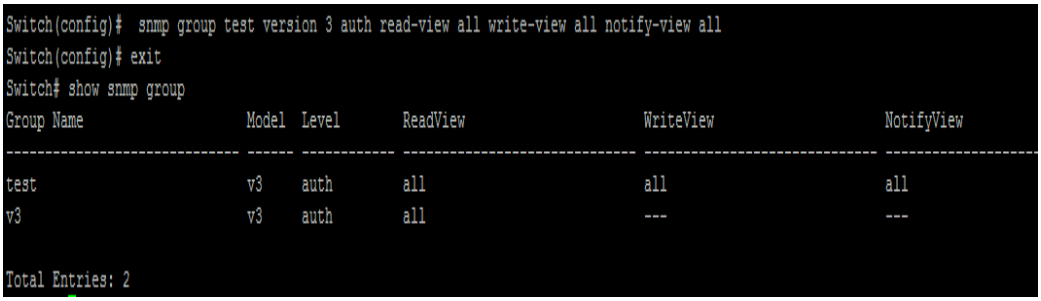
To define the SNMP group, use the command snmp group in the Global Configuration mode, and use the **"no"** form of the command to delete the configuration. SNMP group configuration is used in the command snmp use to map SNMP users to the SNMP group. These users would be automatically mapped to the SNMP views defined in this command. The security level for SNMP v1 or v2 is always noauth.

Switch# **configure terminal**
Switch(config)# **snmp group group-name (1|2c|3) (noauth|auth|priv) read-view read-view write-view write-view [notify-view notify-view]**

Switch(config)# **no snmp group group-name security-mode version (1|2c|3)**

Syntax	**snmp group group-name (1|2c|3) (noauth|auth|priv) read-view read-view** **write-view write-view [notify-view notify-view]** **no snmp group group-name security-mode version (1|2c|3)**
Parameter	group-name Specify SNMP group name, and the maximum length is 30 characters. (1|2c|3) Specify the SNMP version. **noauth** Specify that no packet authentication is performed. **auth** Specify that no packet authentication without entryption is performed. It is applicable only to the SNMPv3 security mode. **priv** Specify that no packet authentication with entryption is performed. It is applicable only to the SNMPv3 security mode. **read-view** read- view Set the view name that enables configuring the agent, and its maximum length is 30 characters. **write-view** write- view Set the view name that enables viewing only, and its maximum length is 30 characters. **notify-view** notify- view Sets the view name that sends only traps with

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	contents that is included in SNMP view selected for notification. The maximum length is 30 characters.
Mode	Global Configuration
Example	The following example adds SNMPv3 group Switch# **configure terminal** Switch(config)# **snmp group v3 version 3 auth read-view all write-view all notify-view all** 

```
Switch(config)#  snmp group test version 3 auth read-view all write-view all notify-view all
Switch(config)# exit
Switch# show snmp group
Group Name                  Model  Level       ReadView                    WriteView                   NotifyView
--------------------------- ------ ----------- --------------------------- --------------------------- ------------------
test                        v3     auth        all                         all                         all
v3                          v3     auth        all                         ---                         ---

Total Entries: 2
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.14 SNMP HOST

To configure the hosts to receive SNMP notifications, use the command snmp host in the Global Configuration mode and use the **"no"** form of the command to delete the configuration.

Switch# **configure terminal**
Switch(config)# **snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version (1|2c)] community-name [udp-port udp-port] [timeout timeout] [retries retries]**
Switch(config)# **snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] version 3 [(auth|noauth|priv)] community-name [udp-port udp-port] [timeout timeout] [retries retries]**

Switch(config)# **no snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version (1|2c|3)]**

Syntax	**snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version (1|2c)] community-name [udp-port udp-port] [timeout timeout] [retries retries]** **snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] version 3 [(auth|noauth|priv)] community-name [udp-port udp-port] [timeout timeout] [retries retries]** **no snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version (1|2c|3)]**
Parameter	**ip-addr** The IP adderss of recipet. **ipv6-addr** The IPv6 adderss of recipet. **hostname** The host name of recipet. **traps** Send SNMP traps to the host. It is the default action. **informs** Send SNMP informs to the host. **version (1|2c|3)** Specify the SNMP version. **noauth** Specify that no packet authentication is performed. It is applicable only to the SNMPv3 security mode. **auth** Specify that no packet authentication without encryption is performed. It is applicable only to the SNMPv3 security mode. **priv** Specify that no packet authentication with encryption is performed.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	It is applicable only to the SNMPv3 security mode. **community-name** The SNMP community sent with the notification. **udp-port** udp-port Specify the UDP port number. **timeout** timeout Specify the SNMP informs timeout **retries** retries Specify the retry counter of the SNMP informs.
Default	The default SNMP version for the command is SNMPv1.
Mode	Global Configuration

Example	The following example adds the receipt 192.168.1.11 for the SNMP traps notification.
	Switch# **configure terminal**
	Switch(config)# **snmp host 192.168.1.11 private**
	`Switch# configure terminal`
	`Switch(config)# snmp host 192.168.1.11 private`
	`Switch(config)#`
	`Switch# sh snmp host`
	`Server Community/User Name Notification Version Notification Type UDP Port Retries Timeout`
	`192.168.1.11 private v1 trap 162 -- --`
	`Total Entries: 1`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.15 SNMP TRAP

To send the SNMP traps, use the command snmp trap in the Global Configuration mode and use the **"no"** form of the command to disable the SNMP traps.

Switch# **configure terminal**
Switch(config)# **snmp trap (auth|cold-start|linkUpDown|port-security|warm-start)**

Switch(config)# **no snmp trap (auth|cold-start|linkUpDown|port-security |warm-start)**

Syntax	**snmp trap (auth|cold-start|linkUpDown|port-security|warm-start)** **no snmp trap (auth|cold-start|linkUpDown|port-security |warm-start)**
Parameter	**auth** Enable the SNMP authentication failure trap. **cold-start** Enable the SNMP cold start-up failure trap. **linkUpDown** Enable the SNMP link up and down failure trap. **port-security** Enable the SNMP port security trap. **warm-start** Enable the SNMP warm start-up failure trap.
Default	All the SNMP traps are enabled
Mode	Global Configuration

Example	The following example disables and enables the SNMP link up and down traps individually.
	Switch# **configure terminal**
	Switch(config)# **snmp trap linkUpDown**
	`Switch# configure terminal`
	`Switch(config)#  snmp trap linkUpDown`
	`Switch(config)#`
	`Switch# sh snmp trap`
	`SNMP auth failed trap  : Enable`
	`SNMP linkUpDown trap  : Enable`
	`SNMP cold-start trap  : Enable`
	`SNMP warm-start trap  : Enable`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.16 SNMP USER

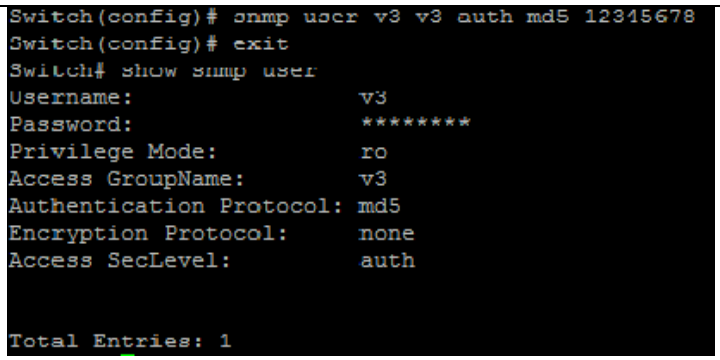
To define a SNMP user, use the command snmp user in the Global Configuration mode and use the **"no"** form to delete the SNMP user.

Switch# **configure terminal**
Switch(config)# **snmp user username group-name [auth (md5|sha) AUTHPASSWD] snmp user username group-name auth (md5|sha) AUTHPASSWD priv PRIVPASSWD**

Switch(config)# **no snmp user username**

Syntax	**snmp user username group-name [auth (md5|sha) AUTHPASSWD] snmp user username group-name auth (md5|sha) AUTHPASSWD priv PRIVPASSWD** **no snmp user username**
Parameter	**username** Specify the SNMP username on the host that connects to the SNMP agent. The max character is 30 characters. For the SNMP v1 or v2c, the username must match the community name by the command snmp host. **group-name** Specify the SNMP group to which the SNMP user belongs. The SNMP group should be SNMPv3 and configured by the command snmp group. **auth (md5|)** Specify the HMAC-MD5-96 authentication protocol as the user authentication. **auth (sha|)** Specify the HMAC-SHA-96 authentication protocol as the user authentication. AUTHPASSWD The password for authentication and the range of length is from 8 to 32 characters. **Priv** PRIVPASSWD The private password for the privacy key, and the range of length is from 8 to 64 characters
Mode	Global Configuration
Example	The following example adds SNMP user v3 into the group v3 by the MD5 authentication. Switch# **configure terminal** Switch(config)# **snmp user v3 v3 auth md5 12345678**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

28.17 SNMP VIEW

To configure the SNMP view, use the command snmp view in the Global Configuration mode and use the **"no"** form of the command to delete the SNMP view. The default SNMP view cannot be deleted and modified by users. By default, the maximum numbers of SNMP view is limited to 16.

Switch# **configure terminal**
Switch(config)# **snmp view view-name subtreeoid-tree oid-mask (all|oid-mask) viewtype(included|excluded)**

Switch(config)# **no snmp view view-name subtree (all|oid-tree)**

Syntax	**snmp view view-name subtreeoid-tree oid-mask (all|oid-mask) viewtype(included|excluded)** **no snmp view view-name subtree (all|oid-tree)**
Parameter	**view-name** The SNMP view name. Its maximum length is 30 characters. **subtreeoid-tree** Specify the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP view. **oid-mask (all|oid- mask)** Specify the OID family mask. It is used to define a family of view subtrees. For example, OID mask FA.80 is 11111010.10000000. The length of the OID mask must be less than the length of subtreeOID.Viewtype **(included|excluded)**Include or exclude the selected MIBs in the view.
Mode	Global Configuration
Example	The following example defines the SNMP view. Switch# **configure terminal** Switch(config)# **snmp view private subtree** 1.3.3.1 **oid-mask all viewtype included**

```
Switch# configure terminal
Switch(config)# snmp view private subtree 1.3.3.1 oid-mask all viewtype included
Switch(config)#
Switch# sh snmp view
View Name                Subtree OID                        OID Mask             View Type
-----------------------  ---------------------------------  -------------------  ---------
all                      .1                                 all                  included
private                  .1.3.3.1                           all                  included

Total Entries: 2
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29. SPANNING TREE

SPANNING TREE

STP uses messaging between switches to stabilize the network into a logical, loop-free topology. To do so, STP causes some interfaces (popularly called *ports* to simply not forward or receive traffic in other words, the ports are in a *blocking* state. The remaining ports, in an STP forwarding state, together provide a loop-free path to every Ethernet segment in the network.

Three Major 802.1d STP Process Steps

1) **Elect the root switch:** The switch with the lowest bridge ID wins; the standard bridge ID is 2-byte priority followed by a MAC address unique to that switch.

2) **Determine each switch's Root Port:** The one port on each switch with the least cost path back to the root.

3) **Determine the Designated Port for each segment:** When multiple switches connect to the same segment, this is the switch that forwards the least cost Hello onto a segment.

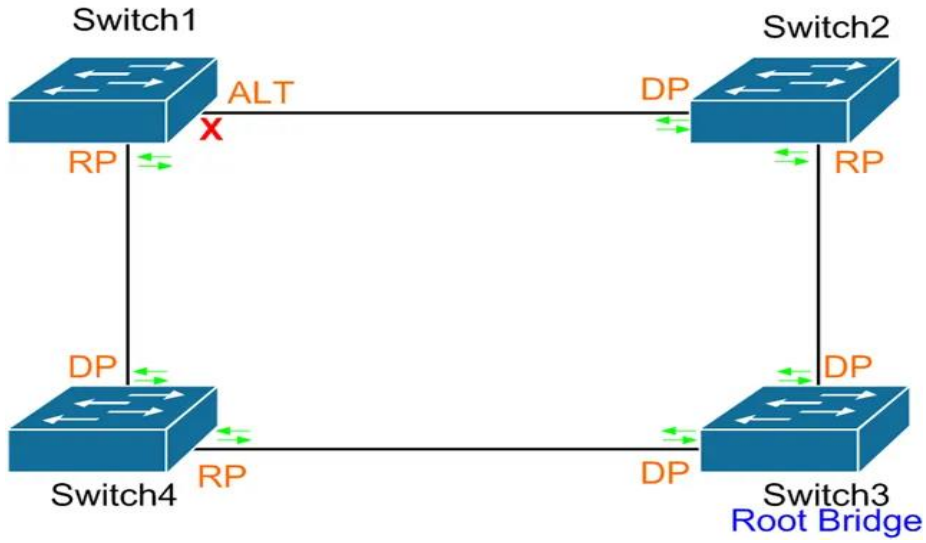


Fig 29.1 Spanning tree concept

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Electing a Root Switch

Only one switch can be the root of the spanning tree to select the root, the switches hold an election. Each switch begins its STP logic by creating and sending an STP Hello bridge protocol data unit (BPDU) message, claiming to be the root switch. If a switch hears a superior Hello means a Hello with a lower bridge ID, it stops claiming to be root by ceasing to originate and send Hellos. Instead, the switch starts forwarding the superior Hellos received from the superior candidate. Eventually, all switches except the switch with the best bridge ID cease to originate Hellos; that one switch wins the election and becomes the root switch.

The original IEEE 802.1d bridge ID held two fields:

■ The 2-byte Priority field, which was designed to be configured on the various switches to affect the results of the STP election process.

■ A 6-byte MAC Address field, which was included as a tiebreaker, because each switch's bridge ID includes a MAC address value that should be unique to each switch. As a result, some switch must win the root election.

IEEE 802.1d STP Bridge ID Formats

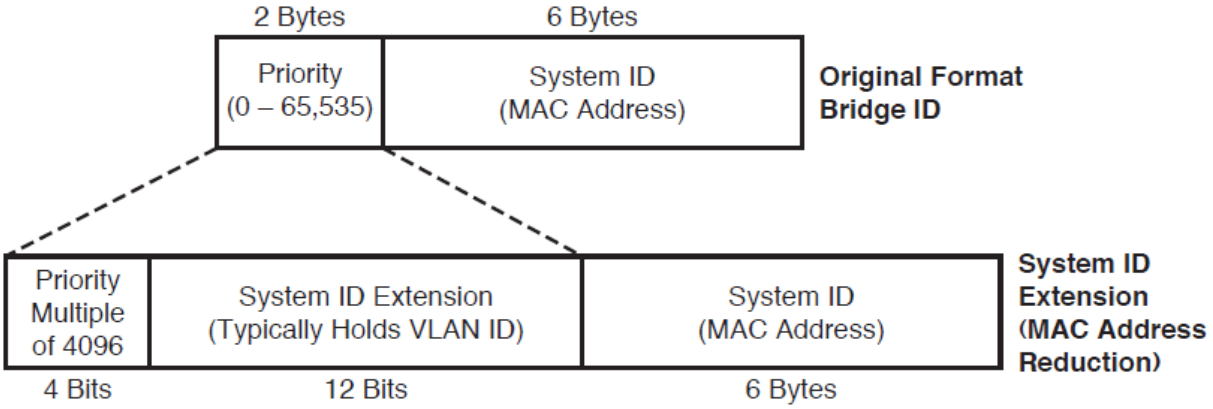


Fig 29.2 IEEE 802.1d STP Bridge ID

The format was changed mainly due to the advent of multiple spanning trees as supported by Per VLAN Spanning Tree Plus (PVST+) and IEEE 802.1s Multiple Spanning Trees (MST). With the old-style bridge ID format, a switch's bridge ID for

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

each STP instance (possibly one per VLAN) was identical if the switch used a single MAC address when building the bridge ID.

The System ID Extension allows a network to use multiple instances of STP, even one per VLAN, but without the need to consume a separate BIA on each switch for each STP instance. The System ID Extension field allows the VLAN ID to be placed into what was formerly the last 12 bits of the Priority field. A switch can use a single MAC address to build bridge IDs, and with the VLAN number in the System ID Extension field still have a unique bridge ID in each VLAN. The use of the System ID Extension field is also called MAC address reduction, because of the need for many fewer reserved MAC addresses on each switch.

Determining the Root Port with old costs

Link Speed(Bandwidth)	Port Cost
10 mbps	100
100 bmps	19
1 gbps	4
10 gbps	2

Fig 29.3 Port with IEEE old costs

Bandwidth	STP cost	RSTP cost
4 Mbps	250	5000000
10 Mbps	100	2000000
16 Mbps	62	1250000
100 Mbps	19	200000
1 Gbps	4	20000
2 Gbps	3	10000
10 Gbps	2	2000
100 Gbps	-	200
1 Tbps	-	20

Fig 29.4 Port with IEEE New costs

Once the root is elected, the rest of the switches now need to determine their Root Port (RP). The process proceeds as described in the following list:

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

1. The root creates and sends a Hello every Hello timer (2 seconds default).
2. Each switch that receives a Hello forwards the Hello after updating the following fields in the Hello the cost, the forwarding switch's bridge ID, forwarder's port priority, and forwarder's port number.
3. Switches do not forward Hellos out ports that stabilize into a blocking state.
4. Of all the ports in which a switch receives Hellos, the port with the least calculated cost to the root is the RP. A switch must examine the cost value in each Hello, plus the switch's STP port costs, to determine its least cost path to reach the root. To do so, the switch adds the cost listed in the Hello message to the switch's port cost of the port on which the Hello was received.

When a switch receives multiple Hellos with equal calculated cost, it uses the following tie breakers:

1. Pick the lowest value of the forwarding switch's bridge ID.
2. Use the lowest port priority of the neighboring switch. The neighboring switch added its own port priority to the Hello before forwarding it.
3. Use the lowest internal port number (of the forwarding switch) as listed inside the received Hellos.

Note that if the first tiebreaker in this list fails to produce an RP, this switch must have multiple links to the same neighboring switch. The last two tiebreakers simply help decide which of the multiple parallel links to use.

IEEE 802.1d Spanning Tree Interface States

802.1D State	802.1w State	Default Port Operational Status	Port in Active Topology?	Port Learning MAC Addresses?
Disabled	Discarding	Enabled	No	No
Blocking	Discarding	Enabled	No	No
Listening	Discarding	Enabled	Yes	No
Learning	Learning	Enabled	Yes	Yes
Forwarding	Forwarding	Enabled	Yes	Yes

Fig 29.5 Spanning Tree Interface States

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.1 INSTANCE (MST)

802.1Q, along with 802.1s Multiple instance Spanning Tree (MST), allows 802.1Q trunks for support multiple STP instances.

Multiple Spanning Trees: IEEE 802.1s

IEEE 802.1s Multiple Spanning Trees (MST), sometimes referred to as Multiple Instance STP (MISTP) or Multiple STP (MSTP), defines a way to use multiple instances of STP in a network that uses 802.1Q trunking. The following are some of the main benefits of 802.1s:

■ Like PVST+, it allows the tuning of STP parameters so that while some ports block for one VLAN, the same port can forward in another VLAN.

■ Always uses 802.1w RSTP, for faster convergence.

■ Does not require an STP instance for each VLAN rather, the best designs use one STP instance per redundant path.

One of the key benefits of MST versus PVST+ is that it requires only one MST instance for a group of VLANs. If this MST region had hundreds of VLANs, and used PVST+, hundreds of sets of STP messages would be used. With MST, only one set of STP messages is needed for each MST instance.

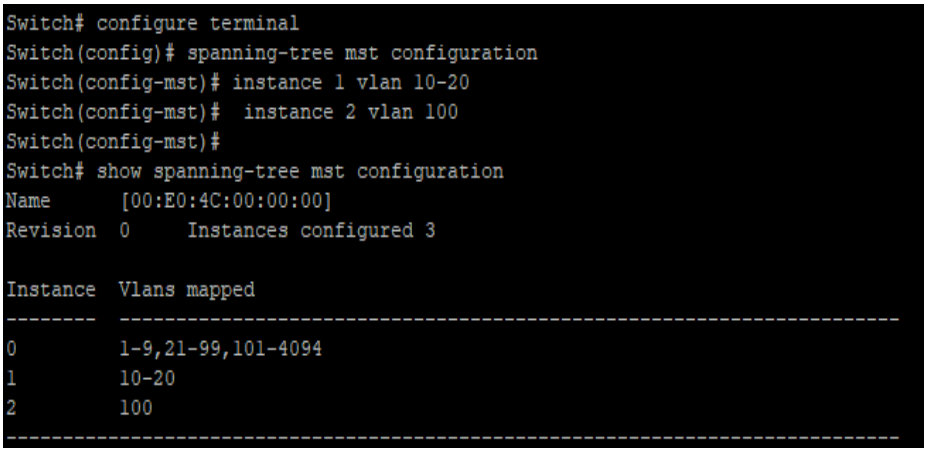
When connecting an MST region to a non-MST region or to a different MST region, MST makes the entire MST region appear to be a single switch to map the VLAN to the Multiple Spanning Tree (MSTP) instances, use the command instance in the MST Configuration mode; and use the no form of the command to restore its default configuration. All VLANs that are not explicitly configured to an MSTP instance are mapped to the CIST instance (instance 0). For two or more switches in the same MSTP region, their VLAN mapping, name and revision number configuration, must be the same.

Switch#**configure terminal**
Switch(config)# **spanning-tree mst configuration**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Switch(config-mst)# **instance instance-id vlan** *[vlan-list]*

Switch(config-mst)# **no instance instance-id vlan** *[vlan-list]*

Syntax	**instance instance-**id **vlan** *[vlan-list]* **no instance instance-**id **vlan** *[vlan-list]*
Parameter	**instance-id** The MSTP instance ID from 0 to 15. **vlan** vlan-list Add the VLAN list to the MSTP instance.
Default	All VLANs are mapped to the Common and Internal Spanning Tree (CIST)instance (instance 0).
Mode	MST Configuration
Example	The following example maps the vlan 10-20 to the MSTP instance 1, and VLAN 100 to instance 2. Switch#**configure terminal** Switch(config)# **spanning-tree mst configuration** Switch(config-mst)# **instance 1 vlan 10-20** Switch(config-mst)# **instance 2 vlan 100** Switch# **show spanning-tree mst configuration** 

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)#  instance 2 vlan 100
Switch(config-mst)#
Switch# show spanning-tree mst configuration
Name      [00:E0:4C:00:00:00]
Revision  0     Instances configured 3

Instance  Vlans mapped
--------  ------------------------------------------------------------------
0         1-9,21-99,101-4094
1         10-20
2         100
------------------------------------------------------------------------------
```

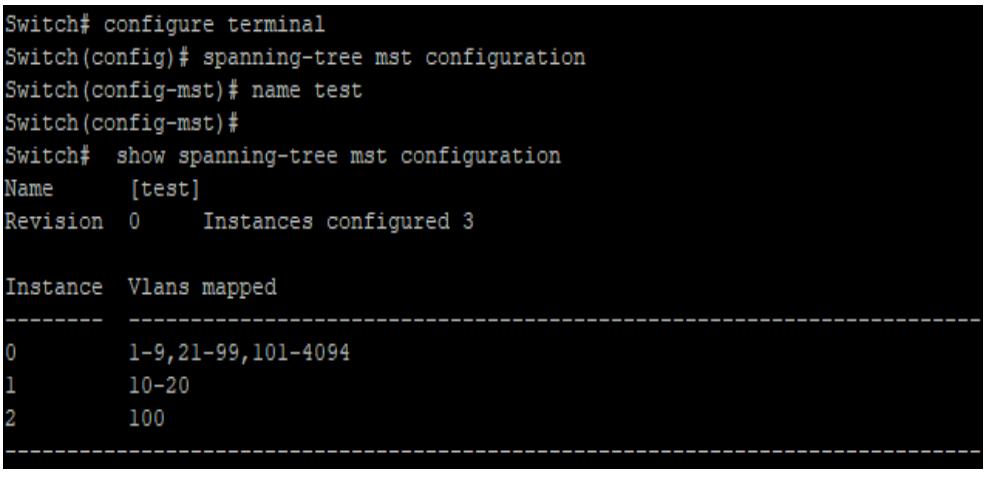
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.2 NAME (MST)

To define the name for MSTP instance, use the command name in the MST Configuration mode and use the **"no"** form to restore the default name configuration.

Switch#**configure terminal**
Switch(config)# **spanning-tree mst configuration**
Switch(config-mst)# **name name-str**

Switch(config-mst)# **no name**

Syntax	**name name-str** **no name**
Parameter	**name-str** The MSTP instance name. Its maximum length is 32 characters
Default	The default MSTP name is the switch MAC address
Mode	MST Configuration
Example	The following example configures the name of MST instance to test, Switch#**configure terminal** Switch(config)# **spanning-tree mst configuration** Switch(config-mst)# **name test** Switch# **show spanning-tree mst configuration** 

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name test
Switch(config-mst)#
Switch#  show spanning-tree mst configuration
Name      [test]
Revision  0     Instances configured 3

Instance  Vlans mapped
--------  ------------------------------------------------------------------------
0         1-9,21-99,101-4094
1         10-20
2         100
--------  ------------------------------------------------------------------------
```

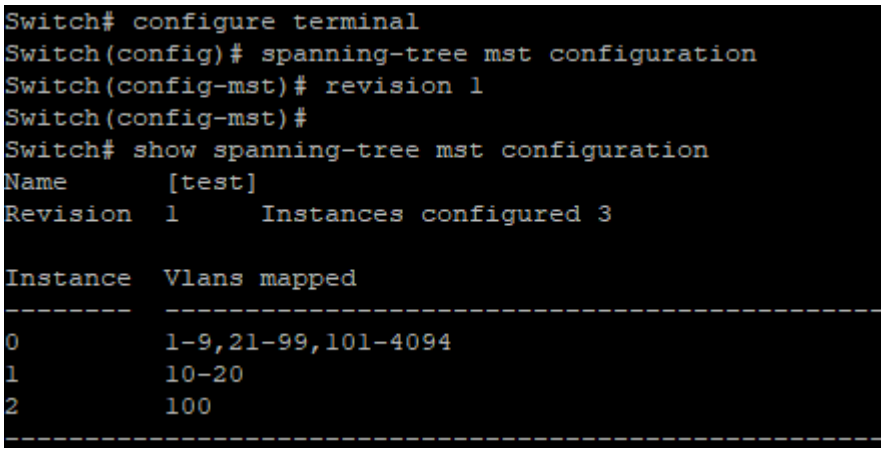
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.3 REVISION (MST)

To define the revision for the MSTP configuration, use the command revision in the MST Configuration mode and use the **"no"** form of the command to restore it default configuration.

Switch#**configure terminal**
Switch(config)# **spanning-tree mst configuration**
Switch(config-mst)# **revision rev**

Switch(config-mst)# **no revision**

Syntax	**revision rev** **no revision**
Parameter	**rev** The MSTP revision number. Its valid rage is from 0 to 65535
Default	The default revision number is 0.
Mode	MST Configuration
Example	The following example defines the revision MSTP configuration to 1. Switch#**configure terminal** Switch(config)# **spanning-tree mst configuration** Switch(config-mst)# **revision 1** Switch# **show spanning-tree mst configuration** 

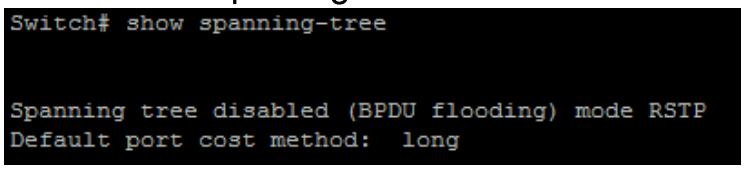
```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# revision 1
Switch(config-mst)#
Switch# show spanning-tree mst configuration
Name      [test]
Revision  1     Instances configured 3

Instance  Vlans mapped
--------  ---------------------------------------------
0         1-9,21-99,101-4094
1         10-20
2         100
-------------------------------------------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.4 SHOW SPANNING-TREE

To display the spanning tree configuration, use the command spanning-tree in the Privileged EXEC mode.

Switch# **show spanning-tree**

Syntax	**show spanning-tree**
Mode	Privileged EXEC
Example	The following example shows the spanning tree configuration. Switch# **show spanning-tree** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.5 SHOW SPANNING-TREE INTERFACE

To show the STP configuration and statistics for an interface, use the command show spanning-tree interface in the Privileged EXEC mode.

Switch# **show spanning-tree interfaces gi1**

Syntax	**show spanning-tree interface** *{IF_PORTS}* [**statistic**]
Parameter	**interface** *IF_PORTS* An interface ID or the list of interface IDs. **statistic** Display the STP statistic for an interface.
Mode	Privileged EXEC

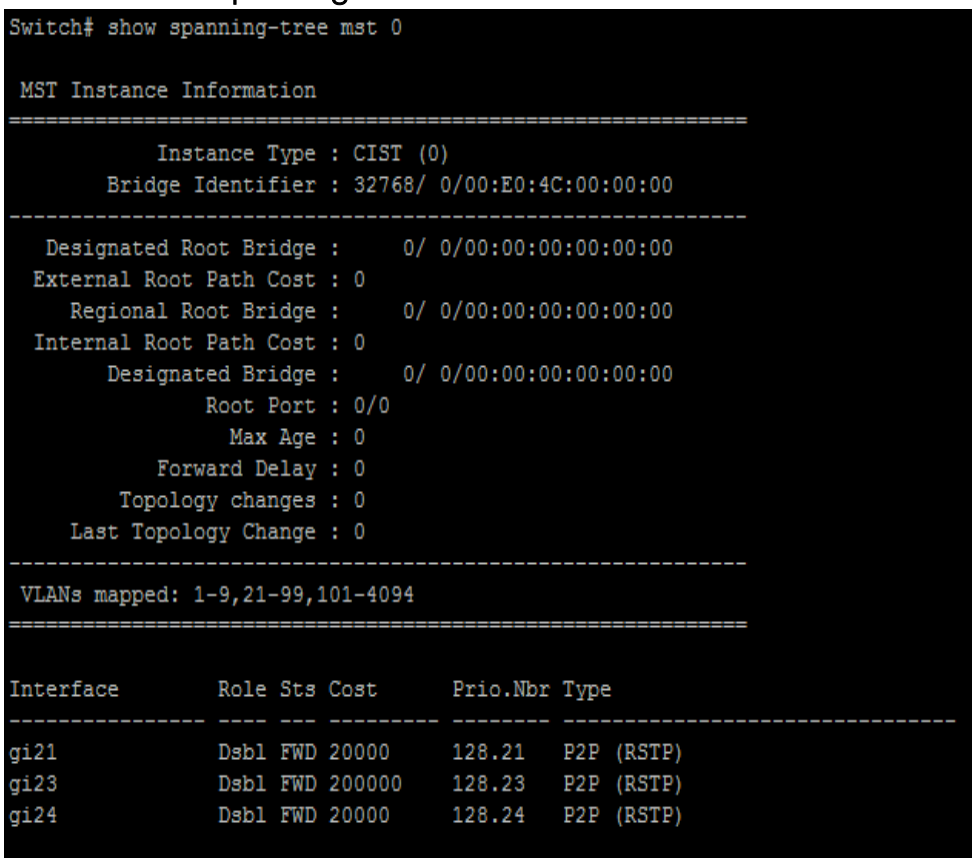
Example	The following example shows the STP configuration for the interface gi23.
	Switch# **show spanning-tree interfaces gi1**
	`Switch# show spanning-tree interfaces gi1`
	`Spanning tree disabled`
	`Switch#`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.6 SHOW SPANNING-TREE MST

To show the information for a specific MSTP instance, use the command show spanning-tree mst in the Privileged EXEC mode.

Switch# **show spanning-tree mst 0**

Syntax	**show spanning-tree mst instance-id**
Parameter	instance-id The MSTP instance ID. Its valid range is from 0 to 15.
Mode	Privileged EXEC
Example	The following example displays the information for the MSTP instance 0 and 1 individually. Switch# **show spanning-tree mst 0** 

```
Switch# show spanning-tree mst 0

 MST Instance Information
============================================================
           Instance Type : CIST (0)
       Bridge Identifier : 32768/ 0/00:E0:4C:00:00:00
------------------------------------------------------------
   Designated Root Bridge :     0/ 0/00:00:00:00:00:00
  External Root Path Cost : 0
     Regional Root Bridge :     0/ 0/00:00:00:00:00:00
  Internal Root Path Cost : 0
       Designated Bridge :     0/ 0/00:00:00:00:00:00
                Root Port : 0/0
                  Max Age : 0
            Forward Delay : 0
         Topology changes : 0
     Last Topology Change : 0
------------------------------------------------------------
 VLANs mapped: 1-9,21-99,101-4094
============================================================

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
gi21             Dsbl FWD 20000     128.21   P2P (RSTP)
gi23             Dsbl FWD 200000    128.23   P2P (RSTP)
gi24             Dsbl FWD 20000     128.24   P2P (RSTP)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.7 SHOW SPANNING-TREE MST CONFIGURATION

To show the global MST configuration, use the command show spanning-tree mst configuration in the Privileged EXEC mode.

Switch# **show spanning-tree mst configuration**

Syntax	**show spanning-tree mst configuration**
Mode	Privileged EXEC

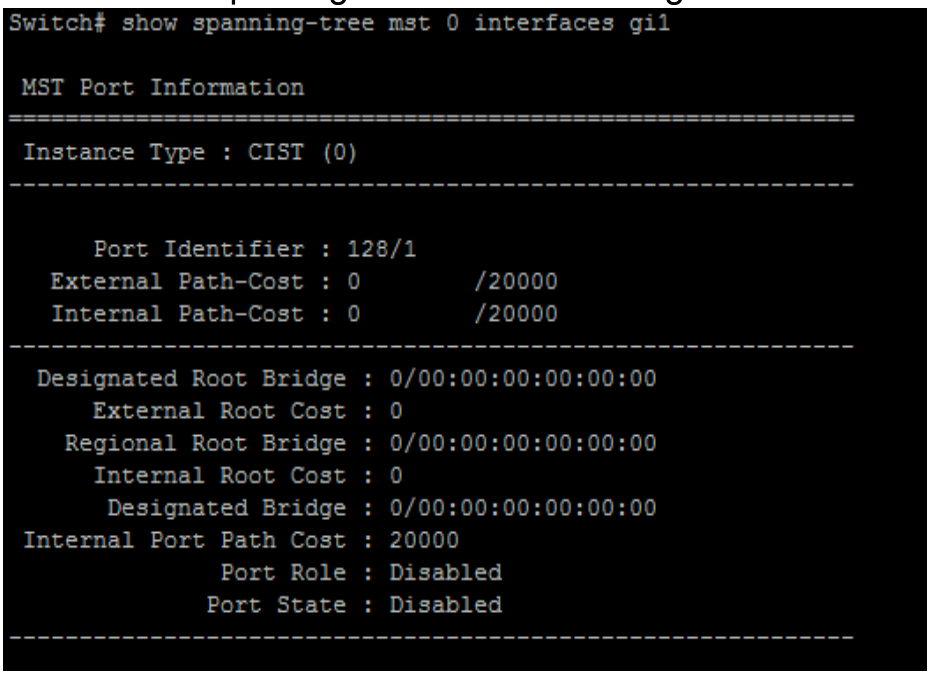
Example	The following example shows the global MST configuration.
	Switch# **show spanning-tree mst configuration**
	`Switch# show spanning-tree mst configuration`
	`Name [test]`
	`Revision 2 Instances configured 3`
	
	`Instance Vlans mapped`
	`-------- ---------------------------------------------`
	`0 1-9,21-99,101-4094`
	`1 10-20`
	`2 100`
	`-------------------------------------------------------`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.8 SHOW SPANNING-TREE MST INTERFACE

To show the MSTP instance information on the specific interface, use the command show spanning-tree mst interface in the Privileged EXEC mode.

Switch# **show spanning-tree mst instance-id interface** *{IF_PORTS}*

Syntax	**show spanning-tree mst instance-id interface** *{IF_PORTS}*
Parameter	**instance-id** The MSTP instance ID. Its valid range is from 0 to 15. **Interface** *IF_PORTS* An interface ID or the list of interface IDs.
Mode	Privileged EXEC
Example	The following example shows the MSTP 0 and 1 information individually on the interface gi1. Switch# **show spanning-tree mst 0 interfaces gi1** 

```
Switch# show spanning-tree mst 0 interfaces gi1

 MST Port Information
============================================================
 Instance Type : CIST (0)
------------------------------------------------------------

     Port Identifier : 128/1
   External Path-Cost : 0        /20000
   Internal Path-Cost : 0        /20000
------------------------------------------------------------
  Designated Root Bridge : 0/00:00:00:00:00:00
      External Root Cost : 0
    Regional Root Bridge : 0/00:00:00:00:00:00
      Internal Root Cost : 0
       Designated Bridge : 0/00:00:00:00:00:00
 Internal Port Path Cost : 20000
               Port Role : Disabled
              Port State : Disabled
------------------------------------------------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.9 SPANNING-TREE

To enable the spanning tree, use the command spanning-tree in the Global Configuration mode and use the **"no"** form of the command to disable the spanning tree on the switch.

Switch#**configure terminal**
Switch(config)# **spanning-tree**

Switch(config)# **no spanning-tree**

Syntax	**spanning-tree** **no spanning-tree**
Default	Spanning-Tree is enabled by default.
Mode	Global Configuration

Example	The following example disables and enables the spanning tree individually.
	Switch#**configure terminal**
	Switch(config)# **spanning-tree**
	Switch# **sh spanning-tree**
	
	`Switch# configure terminal`
	`Switch(config)# spanning-tree`
	`Switch(config)#`
	`Switch# sh spanning-tree`
	
	`Spanning tree enabled mode RSTP`
	`Default port cost method: long`
	
	`Root ID Priority 32768`
	`Address 00:e0:4c:00:00:00`
	`This switch is the root`
	`Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec`
	
	`Number of topology changes 2 last change occurred 04:52:17 ago`
	`Times: hold 0, topology change 0, notification 0`
	`hello 2, max age 20, forward delay 15`
	
	`Interfaces`
	`Name State Prio.Nbr Cost Sts Role EdgePort Type`
	`lag1 enabled 128.29 20000 Frw Desg No P2P (RSTP)`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

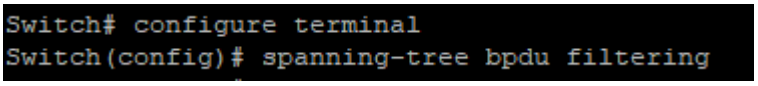
29.10 SPANNING-TREE BPDU

BPDUs are data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities, and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in an network topology. The loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

To configure the action of Bridge Protocol Data Unit (BPDU) handling when STP is disabled, use the command spanning-tree bpdu in the Global Configuration mode. To restore the configuration to the default action, use the no form of the command.

Switch#**configure terminal**
Switch(config)# **spanning-tree bpdu (filtering|flooding)**

Switch(config)# **no spanning-tree bpdu**

Syntax	**spanning-tree bpdu (filtering|flooding)** **no spanning-tree bpdu**
Parameter	**filtering** Filter the BPDU when STP is diabled. **flooding** Flood the BPDU when the STP is disabled.
Default	The default configuration is flooding.
Mode	Global Configuration
Example	The following example configures the action of BPDU handling to fliter when the STP is disabled. Switch#**configure terminal** Switch(config)# **spanning-tree bpdu filtering** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.11 SPANNING-TREE BPDU-FILTER

To enable the BPDU filter, use the command spanning-tree bpdu-filter in the Interface Configuration mode; and use **"no"** form of the command to disable the BPDU filter.

Switch#**configure terminal**
Switch(config)# **interface** {Interfac-ID}
Switch(config-if)# **spanning-tree bpdu-filter**

Switch(config-if)# **no spanning-tree bpdu-filter**

Syntax	**spanning-tree bpdu-filter** **no spanning-tree bpdu-filter**
Default	BPDU filter is disabled.
Mode	Interface Configuration

Example	The following example enables the BPDU filter for interface GigabitEthernet 1.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 1
	Switch(config-if)# **spanning-tree bpdu-filter**
	`Switch# configure terminal`
	`Switch(config)# int gl`
	`Switch(config-if)# spanning-tree bpdu-filter`

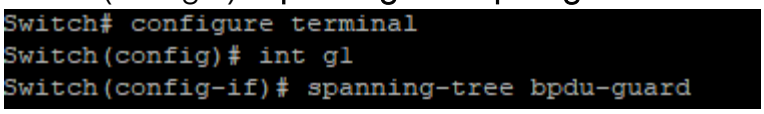
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.12 SPANNING-TREE BPDU-GUARD

To enable the BPDU filter, use the command spanning-tree bpdu-guard in the Interface Configuration mode and use no form of the command to disable the BPDU filter.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **spanning-tree bpdu-guard**

Switch(config-if)# **no spanning-tree bpdu-guard**

Syntax	**spanning-tree bpdu-guard** **no spanning-tree bpdu-guard**
Default	BPDU guard is disabled
Mode	Interface Configuration
Example	The following example enables the BPDU guard for interface gi1. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **spanning-tree bpdu-guard** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.13 SPANNING-TREE COST

To configure the STP path cost for an interface, use the command spanning-tree cost in the Interface Configuration mode and use the no form of the command to restore it to the default configuration.

Default setting are as follows:

Interface Speed	STP Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

Fig 29.6 STP costs

Switch#**configure terminal**
Switch(config)# **interface** {Interfac-ID}
Switch(config-if)# **spanning-tree cost** *{cost}*

Switch(config-if)# **no spanning-tree cost***{cost}*

Syntax	**spanning-tree cost** *{cost}* **no spanning-tree cost***{cost}*
Parameter	***Cost*** The port path cost. For the long path cost method, its valid range is from 0 to 200000000 and the valid range is from 0 to 65535 for the short path cost method. The value 0 indicates AUTO, which the port path cost is determined by the port speed and the path cost method.
Default	The default port path cost is 0, and it is determined by the port speed and the path cost method (long or short). Interface Long Short Gigabit Ethernet (1000Mbps) 20000 4 Fast Ethernet (100Mbps) 200000 19 Ethernet (10Mbps) 2000000 100

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Mode	Interface Configuration
Example	The following example configures port path cost to 30000 for interface gi2. Switch#configure terminal Switch(config)# interface gi1 Switch(config-if)# spanning-tree cost 30000 Switch# configure terminal Switch(config)# int gl Switch(config-if)# spanning-tree cost 30000

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.14 SPANNING-TREE FORWARD-DELAY

To configure the STP bridge forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state, use the command spanning-tree forward-time in the Global Configuration mode. To restore it to the default configuration, use the **"no" form** of the command.

When the forward delay time is configured, the following relationship should be maintained:

2 * (forward-time - 1) >= Max-Age

Timer	Default Value	Description
Hello	2 Seconds	How often will a BPDU be sent.
Max Age	20 Seconds (10 x *Hello* Time)	How long will a port remain in Blocking state after a topology change.
Forward Delay	15 Seconds	How long will a port remain in Listening/Learning states, before transitioning to Forwarding state. (15secs each by default, 30secs total)

Fig 29.7 Spanning Tree Default Timer

Switch#**configure terminal**
Switch(config)# **spanning-tree forward-delay** *{seconds}*

Switch(config)# **no spanning-tree forward-time***{seconds}*

Syntax	**spanning-tree forward-delay***{seconds}* **no spanning-tree forward-delay** *{seconds}*
Parameter	*seconds* STP forward delay time. Its valid range is from 4 to 10 seconds.
Default	The default forward delay time is 15 seconds.
Mode	Global Configuration
Example	The following example configures STP forward delay time to 25.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch#configure terminal
	Switch(config)# spanning-tree forward-delay 25
	Switch# show spanning-tree mst 0
	
	``
	Switch# configure terminal
	Switch(config)# spanning-tree forward-delay 25
	Switch(config)#
	Switch# show spanning-tree mst 0
	
	 MST Instance Information
	==
	           Instance Type : CIST (0)
	       Bridge Identifier : 32768/ 0/00:E0:4C:00:00:00
	-- 	
	   Designated Root Bridge : 32768/ 0/00:E0:4C:00:00:00
	  External Root Path Cost : 0
	    Regional Root Bridge : 32768/ 0/00:E0:4C:00:00:00
	  Internal Root Path Cost : 0
	       Designated Bridge : 32768/ 0/00:E0:4C:00:00:00
	               Root Port : 0/0
	                 Max Age : 20
	           Forward Delay : 25
	        Topology changes : 2
	    Last Topology Change : 18025
	-- 	
	 VLANs mapped: 1-9,21-99,101-4094
	==
	
	Interface Role Sts Cost Prio.Nbr Type
	---------------- ---- --- --------- -------- ------------
	lag1 Desg FWD 20000 128.29 P2P (RSTP)
	``

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.15 SPANNING-TREE HELLO-TIME

STP hello time is the time interval to broadcast its hello message to other bridges. To configure the STP hello time, use the command spanning-tree hello-time in the Global Configuration mode; and use the **"no"** form of the command to restore the hello time to default configuration.

When the hello time is configured, the following relationship should be maintained: Max-Age >= 2 * (hello-time + 1)

Switch#**configure terminal**
Switch(config)# **spanning-tree hello-time seconds**

Switch(config)# **no spanning-tree hello-time**

Syntax	**spanning-tree hello-time seconds** **no spanning-tree hello-time**
Parameter	**seconds** STP hello time in second. Its valid range is from 1 to 10seconds
Default	The default STP hello time is 2 seconds.
Mode	Global Configuration

Example	The following example configures BPDU hello time to 4.
	Switch#**configure terminal**
	Switch(config)# **spanning-tree hello-time 4**
	`Switch# config t`
	`Switch(config)# spanning-tree hello-time 4`

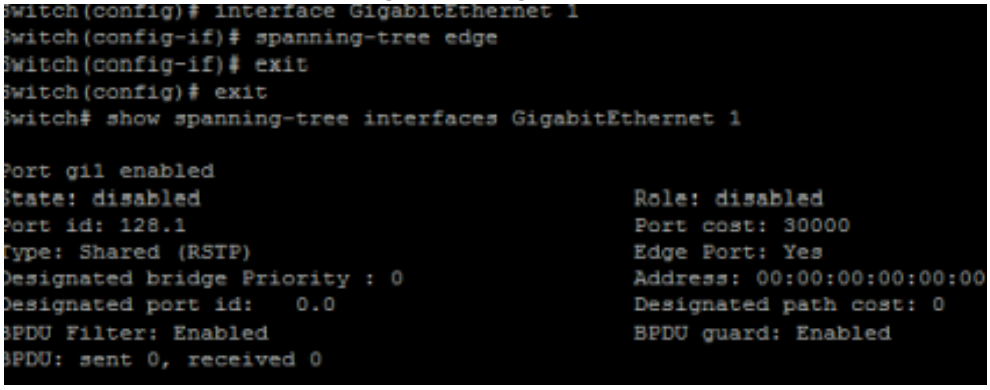
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.16 SPANNING-TREE EDGE

To enable the edge mode for an interface, use the command spanning-tree edge in the Interface Configuration mode; and use the **"no"** form of the command to restore it to the default configuration. In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **spanning-tree edge**

Switch(config-if)# **no spanning-tree edge**

Syntax	**spanning-tree edge** **no spanning-tree edge**
Default	The default configuration is disabled.
Mode	Interface Configuration
Example	The following example enables the edge mode for the interface gi1. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **spanning-tree edge** 

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# spanning-tree edge
Switch(config-if)# exit
Switch(config)# exit
Switch# show spanning-tree interfaces GigabitEthernet 1

Port gi1 enabled
State: disabled                                 Role: disabled
Port id: 128.1                                  Port cost: 30000
Type: Shared (RSTP)                             Edge Port: Yes
Designated bridge Priority : 0                  Address: 00:00:00:00:00:00
Designated port id:   0.0                       Designated path cost: 0
BPDU Filter: Enabled                            BPDU guard: Enabled
BPDU: sent 0, received 0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.17 SPANNING-TREE LINK-TYPE

To set the RSTP link-type for an interface, use the command spanning-tree link in the Interface Configuration mode. For the default configuration, use the **"no"** form of the command.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **spanning-tree link-type (point-to-point|shared)**

Switch(config-if)# **no spanning-tree link-type(point-to-point|shared)**

Syntax	**spanning-tree link-type (point-to-point|shared)** **no spanning-tree link-type(point-to-point|shared)**
Parameter	**point-to-point** Specify the port link type is point to point. **shared** Specify the port link type is shared.
Default	The default configuration link type is point-to-point for the ports with full duplex configuration, and shared for the ports with half duplex settings.
Mode	Interface Configuration
Example	The following example configures the link-type to point-to-point for the interface GigabitEthernet 1. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **spanning-tree link-type point-to-point** Switch(config)# interface GigabitEthernet 1 Switch(config-if)# spanning-tree link-type point-to-point Switch(config-if)# end Switch# show spanning-tree interfaces GigabitEthernet 1 Port gi1 enabled State: disabled Role: disabled Port id: 128.1 Port cost: 30000 Type: P2P (RSTP) Edge Port: Yes Designated bridge Priority : 0 Address: 00:00:00:00:00:00 Designated port id: 0.0 Designated path cost: 0 BPDU Filter: Enabled BPDU guard: Enabled BPDU: sent 0, received 0

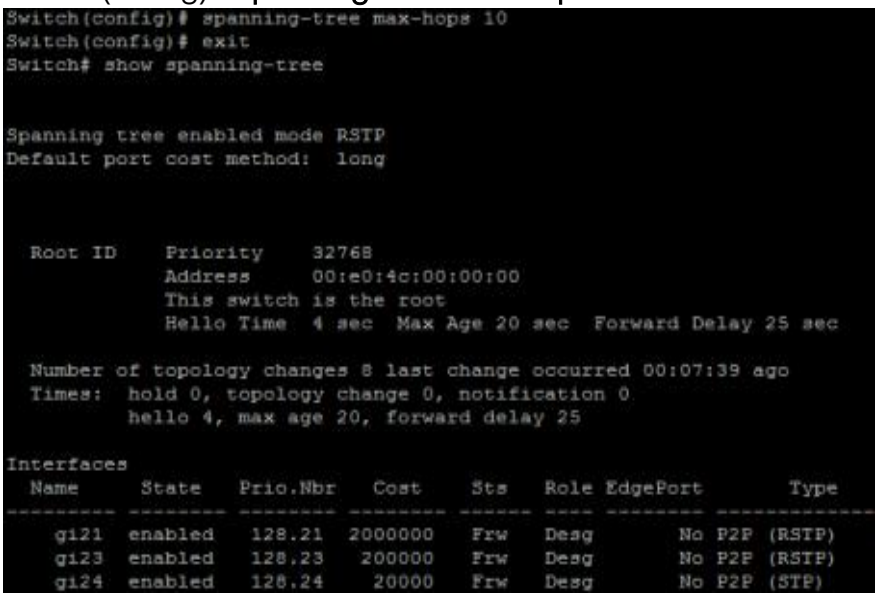
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.18 SPANNING-TREE MAX-HOPS

To specify the number of hops for a BPDU to be forwarded in the MSTP region, use the command spanning-tree max-hops in the Global Configuration mode and restore the setting to default configuration by the **"no"** form of the command.

Switch#**configure terminal**
Switch(config)# **spanning-tree max-hops** *{counts}*

Switch(config)# **no spanning-tree max-hops***{counts}*

Syntax	**spanning-tree max-hops** *{counts}* **no spanning-tree max-hops***{counts}*
Parameter	*counts* Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.
Default	The default max-hops configuration is 20
Mode	Global Configuration
Example	The following example specifies the max hops for BPDU to 10. Switch#**configure terminal** Switch(config)# **spanning-tree max-hops 10** 

```
Switch(config)# spanning-tree max-hops 10
Switch(config)# exit
Switch# show spanning-tree


Spanning tree enabled mode RSTP
Default port cost method:  long



  Root ID     Priority    32768
              Address     00:e0:4c:00:00:00
              This switch is the root
              Hello Time  4 sec  Max Age 20 sec  Forward Delay 25 sec

  Number of topology changes 8 last change occurred 00:07:39 ago
  Times:  hold 0, topology change 0, notification 0
          hello 4, max age 20, forward delay 25

Interfaces
  Name      State    Prio.Nbr    Cost     Sts    Role EdgePort       Type
---------- -------- -------- -------- ------ ---- -------- --------------
    gi21   enabled    128.21  2000000   Frw    Desg       No P2P (RSTP)
    gi23   enabled    128.23   200000   Frw    Desg       No P2P (RSTP)
    gi24   enabled    128.24    20000   Frw    Desg       No P2P (STP)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.19 SPANNING-TREE MAXIMUM-AGE

To set the interval in seconds that the switch can wait without receiving the configuration messages, before attempting to redefine its own configuration, use the command spanning-tree maximum-age in the Global Configuration mode. For the default configuration, use the **"no"** form of the commands.

When the maximum age is configured, the following relationship should be maintained:

2 * (forward-time - 1)>= Max-Age >= 2 * (hello-time + 1)

Switch#**configure terminal**
Switch(config)# **spanning-tree maximum-age** *{seconds}*

Switch(config)# **no spanning-tree maximum-age**

Syntax	**spanning-tree maximum-age** *{seconds}* **no spanning-tree maximum-age**
Parameter	**seconds** The interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.
Default	The default maximum age is 20 seconds.
Mode	Global Configuration
Example	The following example configures STP maximum age to 10. Switch#**configure terminal** Switch(config)# **spanning-tree maximum-age 10**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

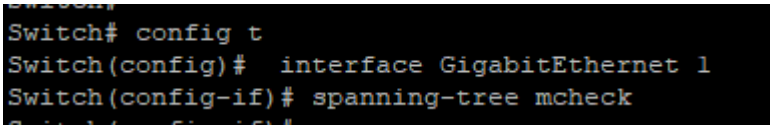
```
Switch# config t
Switch(config)# spanning-tree maximum-age 10
Switch(config)#
Switch# show spanning-tree


Spanning tree enabled mode RSTP
Default port cost method:  long



  Root ID    Priority    32768
             Address     00:e0:4c:00:00:00
             This switch is the root
             Hello Time  4 sec  Max Age 10 sec  Forward Delay 25 sec

  Number of topology changes 2 last change occurred 05:05:51 ago
  Times:  hold 0, topology change 0, notification 0
          hello 4, max age 10, forward delay 25

Interfaces
  Name     State   Prio.Nbr   Cost    Sts   Role EdgePort       Type
--------- -------- -------- -------- ------ ---- -------- ----------
    lag1  enabled   128.29    20000   Frw   Desg       No P2P (RSTP)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.20 SPANNING-TREE MCHECK

To restart the Spanning Tree Protocol (STP) migration process (re-negotiate forcibly with its neighborhood) on the specific interface, use the command spanning-tree mcheck in the Interface Configuration mode.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **spanning-tree mcheck**

Syntax	**spanning-tree mechek**
Mode	Interface Configuration
Example	The following example restarts the STP negotiation on the interface gi1. Switch#**configure terminal** Switch(config)# **interface GigabitEthernet 1** Switch(config-if)# **spanning-tree mcheck** 

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.21 SPANNING-TREE MODE

To specify the spanning tree operation mode, use the command of spanning-tree mode in the Global Configuration mode. For the default configuration, use the command **"no"** spanning-tree force-version in the Global Configuration mode.

When the switch is configured as MSTP mode, it can use STP and RSTP for the backward compatibility with switches working in STP and RSTP mode individually. For the RSTP configuration, the switch can also use STP for the switches working in the STP operation.

Switch#**configure terminal**
Switch(config)# **spanning-tree mode (mstp|rstp|stp)**

Switch(config)# **no spanning-tree force-version**

Syntax	**spanning-tree mode (mstp|rstp|stp)** **no spanning-tree force-version**
Parameter	**mstp** Enable the Multiple Spanning Tree (MSTP) operation. **rstp** Enable the Rapid Spanning Tree (RSTP) operation. **stp** Enable the Spanning Tree (STP) operation.
Default	The default mode is rstp.
Mode	Global Configuration
Example	The following example sets the STP operation to MSTP. Switch#**configure terminal** Switch(config)# **spanning-tree mode mstp**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

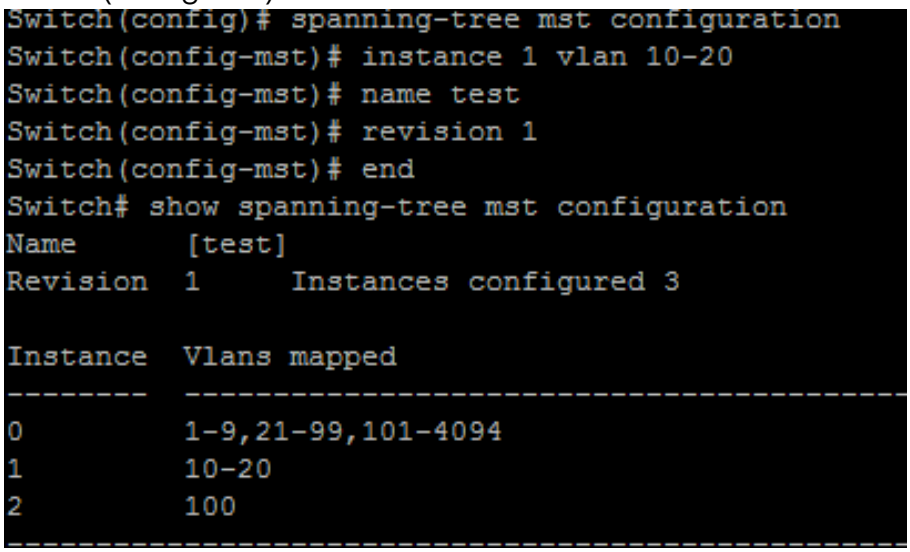
```
Switch# configure terminal
Switch(config)# spanning-tree mode mstp
Switch(config)#
Switch# show spanning-tree


Spanning tree enabled mode MSTP
Default port cost method:  long



Gathering information ..........
###### MST 0 Vlans Mapped: 1-9,21-99,101-4094
CST Root ID    Priority    32768
               Address     00:e0:4c:00:00:00
               This switch is root for CST and IST master
               Hello Time  4 sec  Max Age 10 sec  Forward Delay 25 sec
               Max hops    20
  Name     State   Prio.Nbr   Cost    Sts   Role EdgePort       Type
--------- -------- -------- -------- ------ ---- -------- --------------
lagl      enabled  128.29   20000    Frw    Desg No       P2P Intr
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.22 SPANNING-TREE MST CONFIGURATION

To enter the MST configuration mode for the MSTP configuration modification, use the command spanning-tree mst configuration in the Global Configuration mode.

Switch#**configure terminal**
Switch(config)# **spanning-tree mst configuration**

Syntax	**spanning-tree mst configuration**
Mode	Global Configuration
Example	The following example modifies the MSTP configuration in the MST Configuration mode. Switch#configure terminal Switch(config)# **spanning-tree mst configuration** Switch(config-mst)# **instance 1 vlan 10-20** Switch(config-mst)# **name test** Switch(config-mst)# **revision 1** 

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name test
Switch(config-mst)# revision 1
Switch(config-mst)# end
Switch# show spanning-tree mst configuration
Name      [test]
Revision  1     Instances configured 3

Instance  Vlans mapped
--------  ----------------------------------------
0         1-9,21-99,101-4094
1         10-20
2         100
-------------------------------------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.23 SPANNING-TREE MST COST

To configure the path cost for MSTP calculations, use the command spanning-tree mst cost in the Interface Configuration mode. If the loop occurs, the MSTP considers the path cost when selecting the interface into the Forwarding state. For the default configuration, use the **"no"** form of the command. When configuring the path cost on the CIST (instance 0), it is equal to the command spanning-tree cost in the Interface Configuration mode.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **spanning-tree mst instance-id cost** *{cost}*

Switch(config-if)# **no spanning-tree mst instance-id cost** *{cost}*

Syntax	**spanning-tree mst instance-id cost** *{cost}* **no spanning-tree mst instance-id cost** *{cost}*
Parameter	**instance-id** Specify the instance ID. The valid range is from 0 to 15. **cost** Specify the path cost for the interfaces on the specific MSTP instance. For the long path cost method, its valid range is from 0 to 200000000 and the valid range is from 0 to 65535 for the short path cost method. The value 0 indicates AUTO, which the port path cost is determined by the port speed and the path cost method.
Default	The default port path cost is 0, and it is determined by the port speed and the path cost method (long or short). Interface — Long — Short Gigabit Ethernet (1000Mbps) — 20000 — 4 Fast Ethernet (100Mbps) — 200000 — 19 Ethernet (10Mbps) — 2000000 — 100
Mode	Interface Configuration
Example	The following example configures the path cost of interface fa1 on the instance 1 to 30000 Switch#**configure terminal** Switch(config)# **interface** gi1

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	Switch(config-if)# spanning-tree mst 1 cost 30000 Switch(config)# interface gi1 Switch(config-if)# spanning-tree mst 1 cost 30000 Switch(config-if)# end Switch# show spanning-tree mst 1 MST Instance Information Instance Type : MSTI (1) Bridge Identifier : 32768/ 1/00:E0:4C:00:00:00 Regional Root Bridge : 32768/ 1/00:E0:4C:00:00:00 Internal Root Path Cost : 0 Remaining Hops : 10 Topology changes : 13 Last Topology Change : 263 VLANs mapped: 10-20 Interface Role Sts Cost Prio.Nbr Type gi21 Desg FWD 2000000 128.21 P2P Intr gi23 Desg FWD 200000 128.23 P2P Intr gi24 Desg FWD 20000 128.24 P2P Bound (STP)

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.24 SPANNING-TREE MST PORT-PRIORITY

To configure the interface priority on the specific instances, use the command spanning-tree mst port-priority in the Interface Configuration mode. For the default configuration, use the **"no"** form of the command.

The priority value must be the multiple of 16. When the port priority on the CIST (instance 0) is configured, it is equal to the command spanning-tree port-priority in the Interface Configuration mode.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **spanning-tree mst instance-id port-priority** *{priority}*

Switch(config-if)# **no spanning-tree mst instance-id** *{port-priority}*

Syntax	**spanning-tree mst instance-id port-priority** *{priority}* **no spanning-tree mst instance-id** *{port-priority}*
Parameter	**instance-id** Specify the instance ID. The valid range is from 0 to 15. *priority* Specify the interface priority on the specific instance.
Default	The default port priority on each instance is 128
Mode	Interface Configuration
Example	The following example sets the port priority of gi1 on the instance 1 to 144 and set the port priority of gi1 on the CIST (instance 0) to 96 Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **spanning-tree mst** 0 **port-priority** 96

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# spanning-tree mst 0 port-priority 96
Switch(config-if)# end
Switch# show spanning-tree mst 0

 MST Instance Information
============================================================
           Instance Type : CIST (0)
       Bridge Identifier : 32768/ 0/00:E0:4C:00:00:00
------------------------------------------------------------
   Designated Root Bridge : 32768/ 0/00:E0:4C:00:00:00
  External Root Path Cost : 0
     Regional Root Bridge : 32768/ 0/00:E0:4C:00:00:00
  Internal Root Path Cost : 0
       Designated Bridge : 32768/ 0/00:E0:4C:00:00:00
                Root Port : 0/0
                  Max Age : 10
            Forward Delay : 25
         Topology changes : 13
     Last Topology Change : 549
------------------------------------------------------------
 VLANs mapped: 1-9,21-99,101-4094
============================================================

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
gi21             Desg FWD 2000000   128.21   P2P Intr
gi23             Desg FWD 200000    128.23   P2P Intr
gi24             Desg FWD 20000     128.24   P2P Bound (STP)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.25 SPANNING-TREE MST PRIORITY

To configure the bridge priority on the specific instance, use the command spanning-tree mst priority in the Global Configuration mode. To restore the default configuration, use the **"no"** form of the command. The value of bridge priority must be the multiple of 4096. A switch with the lowest priority is the root of the STP topology. For the configuration of bridge priority on the CIST (instance 0), it is equal to the command spanning-tree priority in the Global Configuration mode.

Switch#**configure terminal**
Switch(config)# **spanning-tree mst instance instance-id priority** *{priority}*

Switch(config)# **no spanning-tree mst instance instance-id** *{priority}*

Syntax	**spanning-tree mst instance instance-id priority** *{priority}* **no spanning-tree mst instance instance-id** *{priority}*
Parameter	**instance-id** Specify the instance ID. The valid range is from 0 to 15. ***priority*** Specify the bridge priority on the specific instance. The valid range is from 0 to 61440. It ensures the probability that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge.
Default	The default priority on each instance is 32768.
Mode	Global Configuration
Example	The following example modifies the bridge priority to 4096 on instance 0 and instance 1 individually. Switch#**configure terminal** Switch(config)# **spanning-tree mst 0 priority 4096**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

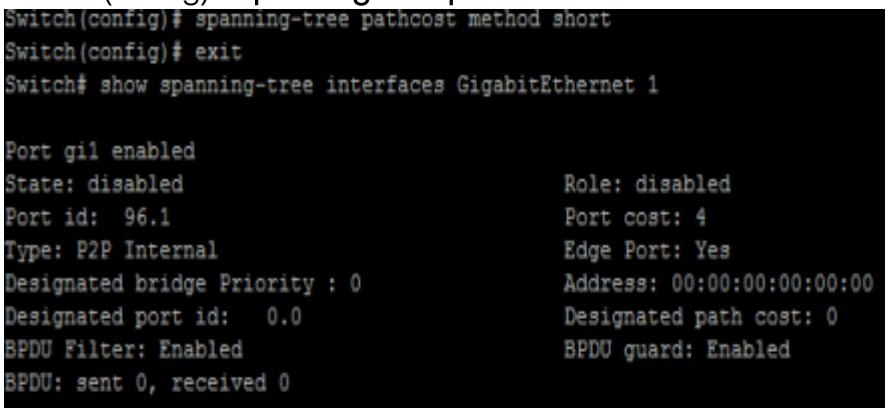
```
Switch(config)# spanning-tree mst 0 priority 4096
Switch(config)# exit
Switch# show spanning-tree mst 0

 MST Instance Information
============================================================
           Instance Type : CIST (0)
       Bridge Identifier :  4096/ 0/00:E0:4C:00:00:00
------------------------------------------------------------
   Designated Root Bridge :  4096/ 0/00:E0:4C:00:00:00
  External Root Path Cost : 0
     Regional Root Bridge :  4096/ 0/00:E0:4C:00:00:00
  Internal Root Path Cost : 0
       Designated Bridge :  4096/ 0/00:E0:4C:00:00:00
               Root Port : 0/0
                 Max Age : 10
           Forward Delay : 25
         Topology changes : 13
     Last Topology Change : 722
------------------------------------------------------------
 VLANs mapped: 1-9,21-99,101-4094
============================================================

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
gi21             Desg FWD 2000000   128.21   P2P Intr
gi23             Desg FWD 200000    128.23   P2P Intr
gi24             Desg FWD 20000     128.24   P2P Bound (STP)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.26 SPANNING-TREE PATHCOST METHOD

To set the spanning tree path cost method, use the command spanning-tree pathcost method in the Global Configuration mode. If the short method is specified, the switch calculates the path cost in the range 1 to 65535 otherwise, It calculates the path cost in the range 1 to 200000000.

Switch#**configure terminal**
Switch(config)# **spanning-tree pathcost method (long|short)**

Syntax	**spanning-tree pathcost method (long|short)**
Parameter	**long** The range for the path cost is from 1 to 200000000. **short** The range for the path cost is from 1 to 65535
Default	The default path cost method is long.
Mode	Global Configuration
Example	The following example modifies path cost method to short. Switch#**configure terminal** Switch(config)# **spanning-tree pathcost method short** 

```
Switch(config)# spanning-tree pathcost method short
Switch(config)# exit
Switch# show spanning-tree interfaces GigabitEthernet 1

Port gi1 enabled
State: disabled                          Role: disabled
Port id:  96.1                           Port cost: 4
Type: P2P Internal                       Edge Port: Yes
Designated bridge Priority : 0           Address: 00:00:00:00:00:00
Designated port id:   0.0                Designated path cost: 0
BPDU Filter: Enabled                     BPDU guard: Enabled
BPDU: sent 0, received 0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.27 SPANNING-TREE PORT-PRIORITY

To configure the STP priority for an interface, use the command spanning- tree port-priority in the Interface Configuration mode. For the default configuration, use the **"no"** form of the command. The priority value must be the multiple of 16.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **spanning-tree port-priority** *{priority}*

Switch(config-if)# **no spanning-tree port-priority** *{priority}*

Syntax	**spanning-tree port-priority** *{priority}* **no spanning-tree port-priority** *{priority}*
Parameter	*priority* Specify the priority for an interface. The valid range is from 0 to 240.
Default	The default priority for each interface is 128.
Mode	Interface Configuration

Example	The following example modifies the port priority to 96 for the interface gi2 .
	Switch#**configure terminal**
	Switch(config)# **interface** gi2
	Switch(config-if)# **spanning-tree port-priority 96**
	`Switch(config)# interface gi2`
	`Switch(config-if)# spanning-tree port-priority 96`
	`Switch(config-if)# end`
	`Switch# show spanning-tree interfaces GigabitEthernet 2`
	
	`Port gi2 enabled`
	`State: disabled  Role: disabled`
	`Port id:  96.2  Port cost: 4`
	`Type: Shared Internal  Edge Port: No`
	`Designated bridge Priority : 0  Address: 00:00:00:00:00:0`
	`Designated port id:  0.0  Designated path cost: 0`
	`BPDU Filter: Disabled  BPDU guard: Disabled`
	`BPDU: sent 0, received 0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.28 SPANNING-TREE PRIORITY

To configure the bridge priority, use the command spanning-tree mst priority in the Global Configuration mode. To restore the default configuration, use the no form of the command. The value of bridge priority must be the multiple of 4096. A switch with the lowest priority is the root of the STP topology. When switches with the same priority configuration in the environment, the switch with lowest MAC address would be selected as the root bridge.

Switch#**configure terminal**
Switch(config)# **spanning-tree priority** *{priority}*

Switch(config)# **no spanning-tree** *{priority}*

Syntax	**spanning-tree priority** *{priority}* **no spanning-tree** *{priority}*
Parameter	**instance**-id Specify the instance ID. The valid range is from 0 to 15. ***priority*** Specify the bridge STP priority. The valid range is from 0 to 61440. It ensures the probability that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge of the STP topology.
Default	The default priority for the switch 32768.
Mode	Global Configuration
Example	The following example modifies the bridge priority to 4096. Switch#**configure terminal** Switch(config)# **spanning-tree priority** 4096

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# spanning-tree priority 4096
Switch(config)# exit
Switch# show spanning-tree


Spanning tree enabled mode MSTP
Default port cost method:  short



Gathering information ..........
###### MST 0 Vlans Mapped: 1-9,21-99,101-4094
CST Root ID     Priority    4096
                Address     00:e0:4c:00:00:00
                This switch is root for CST and IST master
                Hello Time  4 sec  Max Age 10 sec  Forward Delay 25 sec
                Max hops    10
  Name      State   Prio.Nbr   Cost    Sts   Role EdgePort       Type
--------- -------- -------- -------- ------ ---- -------- ------------------
gi21      enabled  128.21   100      Frw    Desg No       P2P Intr
gi23      enabled  128.23   19       Frw    Desg No       P2P Intr
gi24      enabled  128.24   4        Frw    Desg No       P2P Bound (STP)
```

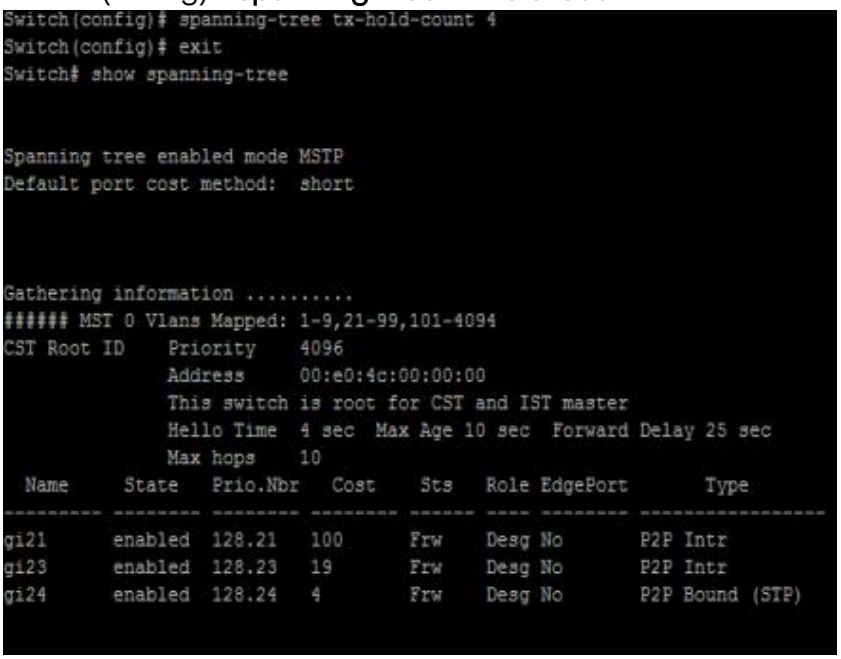
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

29.29 SPANNING-TREE TX-HOLD-COUNT

To limit the maximum numbers of packets transmission per second, use the command spanning-tree tx-hold-count in the global Configuration mode. For the default configuration, use the **"no"** form of the command.

Switch#**configure terminal**
Switch(config)# **spanning-tree tx-hold-count** *{count}*

Switch(config)# **no spanning-tree tx-hold-count***{count}*

Syntax	**spanning-tree tx-hold-count** *{count}* **no spanning-tree tx-hold-count***{count}*
Parameter	***Count*** Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
Default	The default value is 6.
Mode	Global Configuration
Example	The following example sets the tx-hold-count to 4. Switch#**configure terminal** Switch(config)# **spanning-tree tx-hold-count 4** 

```
Switch(config)# spanning-tree tx-hold-count 4
Switch(config)# exit
Switch# show spanning-tree


Spanning tree enabled mode MSTP
Default port cost method:  short



Gathering information .........
###### MST 0 Vlans Mapped: 1-9,21-99,101-4094
CST Root ID    Priority    4096
               Address     00:e0:4c:00:00:00
               This switch is root for CST and IST master
               Hello Time  4 sec  Max Age 10 sec  Forward Delay 25 sec
               Max hops    10
  Name     State   Prio.Nbr   Cost    Sts   Role EdgePort       Type
--------- -------- -------- -------- ------ ---- -------- ----------------
gi21      enabled  128.21   100      Frw    Desg No       P2P Intr
gi23      enabled  128.23   19       Frw    Desg No       P2P Intr
gi24      enabled  128.24   4        Frw    Desg No       P2P Bound (STP)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

30. STORM CONTROL

Switches support rate-limiting traffic at Layer 2 using the storm-control commands. Storm control can be configured to set rising and falling thresholds for each of the three types of port traffic namely unicast, multicast, and broadcast. Each rate limit can be configured on a per-port basis. You can configure storm control to operate on each traffic type based on either packet rate or a percentage of the interface bandwidth. You can also specify rising and falling thresholds for each traffic type. If you don't specify a falling threshold, or if the falling threshold is the same as the rising threshold, the switch port will forward all traffic up to the configured limit and will not wait for that traffic to pass a specified falling threshold before forwarding it again.

When any of the configured thresholds is passed, the switch can take any of three additional actions, also on a per-port basis. The first, and the default, is that the switch can rate-limit by discarding excess traffic according to the configured commands & take no further action. The other two actions include performing the rate-limiting function and either shutting down the port or sending an SNMP trap.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

30.1 SHOW STORM-CONTROL

Use **"show storm-control"** command to show all storm control related configurations including global configuration and per port configurations. Use **"show storm-control interface"** command to show selected port storm control configurations.

Switch# **show storm-control**
Switch# **show storm-control interface** *{IF_PORTS}*

Syntax	**show storm-control** **show storm-control interface** *{IF_PORTS}*
Parameter	*IF_PORTS* Specify port to show.
Mode	Privileged EXEC
Example	This example shows how to show storm control global configuration. Switch# **show storm-control**

```
Switch# show storm-control
  Storm control preamble and IFG: Excluded
  Storm control unit: bps

  Port    | State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast |   Action
          |       |     kbps    |        kbps        |      kbps       |
----------+-------+-------------+--------------------+-----------------|-----------
  gi1       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi2      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi3      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi4      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi5      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi6      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi7      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi8      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi9      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi10     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi11     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi12     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi13     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi14     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi15     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi16     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi17     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi18     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi19     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi20     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi21     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi22     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi23     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi24     disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  te1      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  te2      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  te3      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  te4      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

30.2 STORM-CONTROL

Storm control function is able to enable/disable on each single port. Use the **"storm control"** command to enable storm control feature on the selected ports. And use **"no storm control"** command to disable storm control feature. Not only port is able to enable/disable on the port. Each storm control type is also able to enable/disable on each single port. Use the **"storm-control (broadcast |unknown-unicast |unknown-multicast)"** command to enable the storm control type you need and use **"no"** form to disable it.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **storm-control**

Switch(config-if)# **no storm-control**

Switch(config-if)# **storm-control (broadcast | unknown-unicast | unknown-multicast)**
no storm-control (broadcast | unknown-unicast | unknown-multicast)

Syntax	**storm-control** **no storm-control** **storm-control (broadcast | unknown-unicast | unknown-multicast) no storm-control (broadcast | unknown-unicast | unknown-multicast)**
Parameter	**broadcast** Select broadcast storm control type **unknown-unicast** Select unknown unicast storm control type **unknown- multicast**Select unknown multicast storm control type
Mode	Interface Configuration
Example	This example shows how to enable storm control on interface gi1. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **storm-control** This example shows how to enable broadcast storm control and configure broadcast storm control rate to 200.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# config t
Switch(config)# int range gl-24
Switch(config-if-range-gl-24)# storm-control
Switch(config-if-range-gl-24)#
Switch# show storm-control
  Storm control preamble and IFG: Excluded
  Storm control unit: bps

  Port    | State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast |   Action
          |       |     kbps    |        kbps        |      kbps       |
----------+-------+-------------+--------------------+-----------------|-----------
  gi1       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi2       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi3       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi4       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi5       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi6       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi7       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi8       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi9       enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi10      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi11      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi12      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi13      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi14      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi15      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi16      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi17      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi18      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi19      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi20      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi21      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi22      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi23      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi24      enable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  te1      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  te2      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  te3      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  te4      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
```

Switch#configure terminal
Switch(config)# interface gi1
Switch(config-if)# storm-control broadcast
This example shows how to show current storm control configuration on interface gi1
Switch# show storm-control interfaces gi1

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# storm-control broadcast
Switch(config-if)# end
Switch# show storm-control interfaces gi1

  Port    | State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast |   Action
          |       |     kbps    |        kbps        |      kbps       |
----------+-------+-------------+--------------------+-----------------|-----------
  gi1       enable      10000     Off(  10000)         Off(  10000)          Drop
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

30.3 STORM-CONTROL ACTION

Use **"storm-control action"** command to set the action when the received storm control packets exceed the maximum rate on an interface. Use **"no"** form to restore to default action.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **storm-control action (drop | shutdown)**

Switch(config-if)# **no storm-control action**

Syntax	**storm-control action (drop | shutdown)** **no storm-control action**
Parameter	drop shutdown Storm control rate calculates by octet-based
Default	Default storm control action is drop.
Mode	Interface Configuration

Example	This example shows how to configure storm control action to shutdown port on interface gi1.
	Switch#**configure terminal**
	Switch(config)# **interface gi1**
	Switch(config-if)# **storm-control action shutdown**
	This example shows how to show storm control action on interface gi1.
	Switch# **show storm-control interfaces gi1**
	`Switch(config)# interface gi1`
	`Switch(config-if)# storm-control action shutdown`
	`Switch(config-if)# end`
	`Switch# show storm-control interfaces gi1`
	`Port | State | Broadcast | Unkown-Multicast | Unknown-Unicast | Action`
	`| | kbps | kbps | kbps |`
	`gi1 enable 10000 Off( 10000) Off( 10000) Shutdown`

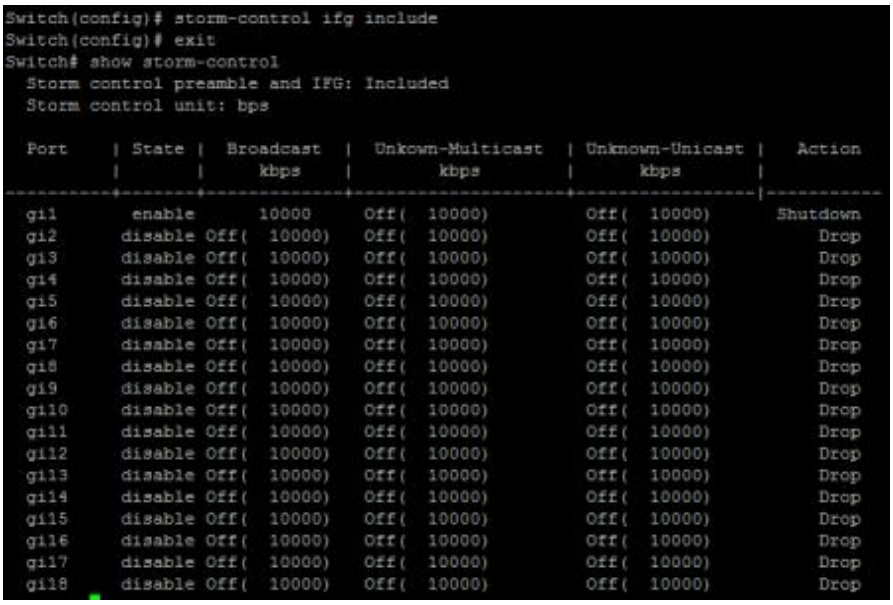
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

30.4 STORM-CONTROL IFG

Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action. Use storm-control ifg command to include/exclude the preamble and inter frame gap into the calculating.

Switch#**configure terminal**

Switch(config)# **storm-control ifg (include | exclude)**

Syntax	**storm-control ifg (include | exclude)**
Parameter	**Include** Include preamble & IFG (20 bytes) when count ingress storm control rate. **Exclude** Exclude preamble & IFG (20 bytes) when count ingress storm control rate
Default	Default storm control inter frame gap is excluded.
Mode	Global Configuration
Example	This example shows how to configure storm inter frame gap to include. Switch#**configure terminal** Switch(config)# **storm-control ifg include** This example shows how to show storm control global configuration. Switch# **show storm-control** 

```
Switch(config)# storm-control ifg include
Switch(config)# exit
Switch# show storm-control
  Storm control preamble and IFG: Included
  Storm control unit: bps

  Port     | State |  Broadcast   |  Unkown-Multicast  | Unknown-Unicast |   Action
           |       |     kbps     |        kbps        |      kbps       |
-----------+-------+--------------+--------------------+-----------------+-----------
  gi1        enable      10000     Off(  10000)         Off(  10000)       Shutdown
  gi2       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi3       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi4       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi5       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi6       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi7       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi8       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi9       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi10      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi11      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi12      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi13      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi14      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi15      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi16      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi17      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi18      disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

30.5 STORM-CONTROL LEVEL

Each control type is allowed to have different storm control rate. Use **"storm-control (broadcast |unknown-unicast| unknown-multicast) level"** command to configure it. Use **"no"** form to restore to default rate.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **storm-control (broadcast | unknown-unicast | unknown-multicast) level** *<1-1000000>*

Switch(config-if)# **no storm-control (broadcast | unknown-unicast | unknown-multicast) level**

Syntax	**storm-control (broadcast | unknown-unicast | unknown-multicast) level***<1-1000000>* **no storm-control (broadcast | unknown-unicast | unknown-multicast)level**
Parameter	**broadcast** Select broadcast storm control type **unknown-unicast** Select unknown unicast storm control type **unknown- multicast** Select unknown multicast storm control type **Level** *<1-1000000>*Specify the storm control rate for selected type. For bps, range is 16-1000000 For pps, range is 1-262143
Default	Default broadcast storm control rate is 10000. Default unknown multicast storm control rate is 10000. Default unknown unicast storm control rate is 10000.
Mode	Interface Configuration
Example	This example shows how to enable broadcast storm control and configure broadcast storm control rate to 200. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **storm-control broadcast** Switch(config-if)# **storm-control broadcast level 200** This example shows how to show current storm control configuration on

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	interface gi1 Switch# show storm-control interfaces gi1 Switch(config)# interface gi1 Switch(config-if)# storm-control broadcast Switch(config-if)# storm-control broadcast level 200 Switch(config-if)# end Switch# show storm-control interfaces gi1 Port | State | Broadcast | Unkown-Multicast | Unknown-Unicast | Action | | kbps | kbps | kbps | ----------+-------+-------------+--------------------+------------------+----------- gi1 enable 208 Off(10000) Off(10000) Shutdown

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

30.6 STORM-CONTROL UNIT

Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action. Use storm-control unit command to change the unit of calculating method.

Switch#**configure terminal**
Switch(config)# **storm-control unit (bps | pps)**

Syntax	**storm-control unit (bps | pps)**
Parameter	bps Storm control rate calculates by octet-based pps Storm control rate calculates by packet-based
Default	Default storm control unit is bps
Mode	Global Configuration
Example	This example shows how to configure storm control rate unit as pps. Switch#**configure terminal** Switch(config)# **storm-control unit pps** This example shows how to show storm control global configuration. Switch# **show storm-control**

```
Switch(config)# storm-control unit pps
Switch(config)# exit
Switch# show storm-control
  Storm control preamble and IFG: Included
  Storm control unit: pps

  Port     | State |  Broadcast   |  Unkown-Multicast  | Unknown-Unicast |   Action
           |       |     pps      |        pps         |      pps        |
----------+-------+--------------+--------------------+-----------------+-----------
  gi1        enable       10000      Off(  10000)          Off(  10000)       Shutdown
  gi2       disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi3       disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi4       disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi5       disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi6       disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi7       disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi8       disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi9       disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi10      disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi11      disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi12      disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi13      disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi14      disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi15      disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi16      disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi17      disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
  gi18      disable Off(  10000)     Off(  10000)          Off(  10000)          Drop
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

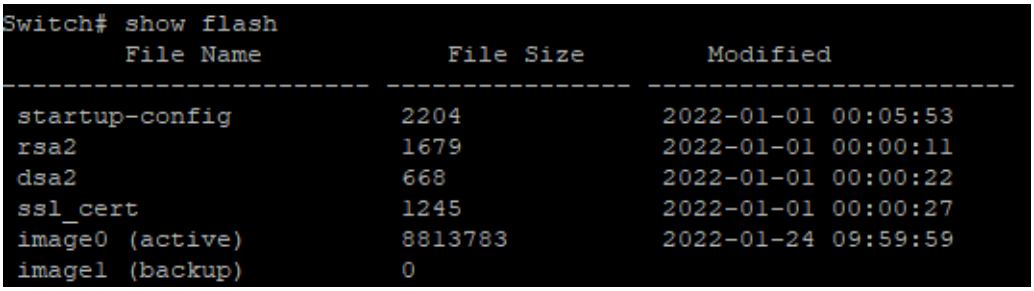
31. SYSTEM FILE

31.1 BOOT SYSTEM

Dual images allow user to have a backup image in the flash partition. Use **"boot system"** command to select the active firmware image. And another firmware image will become a backup one.

Switch#**configure terminal**

Switch(config)# **boot system (image0 | image1)**

Syntax	**boot system (image0 | image1)**
Parameter	image0 Boot from flash image partition 0 image1 Boot from flash image partition 1
Default	Default boot image is image0.
Mode	Global Configuration
Example	This example shows how to select image1 as active image. Switch#**configure terminal** Switch(config)# **boot system image1** Select "image1" Success This example shows how to show active image partition. Switch# **show flash** 

```
Switch# show flash
       File Name             File Size        Modified
----------------------- ---------------- ------------------------
startup-config           2204             2022-01-01 00:05:53
rsa2                     1679             2022-01-01 00:00:11
dsa2                     668              2022-01-01 00:00:22
ssl_cert                 1245             2022-01-01 00:00:27
image0 (active)          8813783          2022-01-24 09:59:59
image1 (backup)          0
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

31.2 COPY

There are many types of files in system. These files are very important for administrator to manage the switch. The most common file operation is copy. By using these copy commands, we can upgrade backup following type of files.

- Firmware Image
- Configuration Files
- Syslog Files
- Language Files
- Security Certificate

Switch# copy (flash:// | tftp://) (flash:// | tftp://)
Switch# copy tftp:// (backup-config | running-config | startup-config) copy (backup-config | running-config | startup-config) tftp://

Switch# copy (backup-config | startup-config) running-config copy (backup-config | running-config) startup-config copy (running-config | startup-config) backup-config

Syntax	copy (flash:// | tftp://) (flash:// | tftp://) copy tftp:// (backup-config | running-config | startup-config) copy (backup-config | running-config | startup-config) tftp:// copy (backup-config | startup-config) running-config copy (backup-config | running-config) startup-config copy (running-config | startup-config) backup-config
Parameter	flash:// Specify the file stored in flash to operation. Available files are: flash://startup-config flash://backup-config flash://rsa1 flash://rsa2 flash://dsa2 flash://image0 flash://image1 flash://ram.log flash://flash.log tftp:// Specify remote tftp server and remote file name. The format is "tftp://192.168.1.111/remote_file_name" running-config Running configuration file startup-config Startup configuration file backup-config Backup configuration file

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Mode	Privileged EXEC

Example	This example shows how to copy running configuration to startup configuration.
	Switch# **copy running-config startup-config**
	
	This example shows how to backup running configuration to remote tftp server 192.168.111 with file name test1.cfg.
	Switch# **copy running-config tftp://**
	`Switch# copy running-config tftp://`
	`Uploading file. Please wait...`
	`Save configuration failed.`
	`Switch#`
	
	Switch# **copy tftp://192.168.1.111/test2.cfg startup-config**
	Switch# **copy flash://dsa2 tftp://192.168.1.111/dsa2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

31.3 DELETE

Use **"delete"** command to delete configuration files or use **"delete system"**command to delete firmware image stored in flash. The **"delete startup-config"** command is using to restore factory default and it is equal to command **"restore-defaults"**.

Switch# **delete (startrup-config | backup-config | flash://)**
Switch# **delete system (image0 | image1)**

Syntax	**delete (startrup-config | backup-config | flash://)** **delete system (image0 | image1)**
Parameter	flash://Specify the configuration file stored in flash to delete. Available files are: flash://startup-config flash://backup-config startup-config Delete startup configuration file backup-config Delete backup configuration file image0 Delete flash image0. image1 Delete flash image1
Mode	Privileged EXEC
Example	This example shows how to delete backup configuration file. Switch# **delete backup-config** This example shows how to delete backup firmware image from flash. Switch# **delete system image1**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

31.4 RESTORE-DEFAULTS

Use **“restore-defaults”** command to restore factory default of all system. The command is equal to **“delete startup-config”.**

Switch# **restore-defaults [interfaces** *{IF_PORTS}***]**

Syntax	**restore-defaults [interfaces** *{IF_PORTS}***]**
Parameter	interfaces *IF_PORTS* Specify port to restore its’ running config
Mode	Privileged EXEC

Example	This example shows how to restore factory defaults.
	Switch# **restore-defaults**
	`Switch# restore-defaults`
	`System: restore factory defaults. Do you want to reboot now? (y/n)y`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

31.5 SAVE

Uses **"save"** command to save running configuration to startup configuration file. This command is equal to **"copy running-config startup-config"**.

Switch# **save**

Syntax	**save**
Mode	Privileged EXEC

Example	This example shows how to save running configuration to startup configuration.
	Switch# **save**
	`Switch# save`
	`Success`
	This example shows how to show r configuration
	Switch# **show startup-config**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show startup-config
Config file startup-config is not existed
Switch# show running-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: KT-NOS C3000-24GP+4X Switch
! System Version: vSoldierOS.3K.v1.10
! System Name: Switch
! System Up Time: 0 days, 1 hours, 6 mins, 33 secs
!
!
!
system location ""
system contact ""
system manufacturer "COMMANDO Networks"
system support "support@commandonetworks.com"
system telephone ""
username "admin" secret encrypted NjI2OWM0ZjcxYTU1YjI0YmFkMGYwMjY3ZDliZTU1MDg=
!
vlan 2
voice-vlan oui-table 00:E0:BB "3COM"
voice-vlan oui-table 00:03:6B "Cisco"
voice-vlan oui-table 00:E0:75 "Veritel"
voice-vlan oui-table 00:D0:1E "Pingtel"
voice-vlan oui-table 00:01:E3 "Siemens"
voice-vlan oui-table 00:60:B9 "NEC/Philips"
voice-vlan oui-table 00:0F:E2 "H3C"
voice-vlan oui-table 00:09:6E "Avaya"
--More--
Switch#
Switch# save
Success
Switch# show startup-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: KT-NOS C3000-24GP+4X Switch
! System Version: vSoldierOS.3K.v1.10
! System Name: Switch
! System Up Time: 0 days, 1 hours, 8 mins, 12 secs
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

31.6 SHOW CONFIG

Our configuration file is text based. Therefore, we can show the configuration on terminal and read it by this command. Use **"show config"** command to show configuration files stored in system. Use **"show config interfaces"** command to show specific port configurations.

Switch#**show (running-config | startrup-config | backup-config)**
Switch#**show running-config interfaces** *{IF_PORTS}*

Syntax	**show (running-config | startrup-config | backup-config)** **show running-config interfaces** *{IF_PORTS}*
Parameter	**running-config** Show running configuration on terminal **startup-config** Show startup configuration on terminal **backup-config** Show backup configuration on terminal **IF_PORTS** Specify port to show its' running config
Mode	Privileged EXEC
Example	This example shows how to show startup configuration Switch# **show startup-config**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show startup-config
Config file startup-config is not existed
Switch# show running-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: KT-NOS C3000-24GP+4X Switch
! System Version: vSoldierOS.3K.v1.10
! System Name: Switch
! System Up Time: 0 days, 1 hours, 6 mins, 33 secs
!
!
!
system location ""
system contact ""
system manufacturer "COMMANDO Networks"
system support "support@commandonetworks.com"
system telephone ""
username "admin" secret encrypted NjI2OWM0ZjcxYTU1YjI0YmFkMGYwMjY3ZDliZTU1MDg=
!
vlan 2
voice-vlan oui-table 00:E0:BB "3COM"
voice-vlan oui-table 00:03:6B "Cisco"
voice-vlan oui-table 00:E0:75 "Veritel"
voice-vlan oui-table 00:D0:1E "Pingtel"
voice-vlan oui-table 00:01:E3 "Siemens"
voice-vlan oui-table 00:60:B9 "NEC/Philips"
voice-vlan oui-table 00:0F:E2 "H3C"
voice-vlan oui-table 00:09:6E "Avaya"
--More--
Switch#
Switch# save
Success
Switch# show startup-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: KT-NOS C3000-24GP+4X Switch
! System Version: vSoldierOS.3K.v1.10
! System Name: Switch
! System Up Time: 0 days, 1 hours, 8 mins, 12 secs
```

This example shows how to show running configuration

Switch# show running-config

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show running-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: KT-NOS C3000-24GP+4X Switch
! System Version: vSoldierOS.3K.v1.10
! System Name: Switch
! System Up Time: 0 days, 1 hours, 16 mins, 25 secs
!
!
!
system location ""
system contact ""
system manufacturer "COMMANDO Networks"
system support "support@commandonetworks.com"
system telephone ""
username "admin" secret encrypted NjI2OWM0ZjcxYTU1YjI0YmFkMGYwMjY3ZDliZTU1MDg=
!
vlan 2
voice-vlan oui-table 00:E0:BB "3COM"
voice-vlan oui-table 00:03:6B "Cisco"
voice-vlan oui-table 00:E0:75 "Veritel"
voice-vlan oui-table 00:D0:1E "Pingtel"
voice-vlan oui-table 00:01:E3 "Siemens"
voice-vlan oui-table 00:60:B9 "NEC/Philips"
voice-vlan oui-table 00:0F:E2 "H3C"
voice-vlan oui-table 00:09:6E "Avaya"
!
!
!
!
!
!
spanning-tree mst configuration
 name "8C:02:FA:05:00:04"
!
!
!
!
!
!
snmp
!
!
```

This example shows how to display running configuration on specific port.

Switch# **show running-config interfaces gi1**

```
Switch# show running-config interfaces gi1
interface gi1
 switchport mode access
 switchport access vlan 2
 storm-control
!
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

31.7 SHOW FLASH

Use **“show flash”** command to show all files status which stored in flash.

Switch# **show flash**

Syntax	**show flash**
Mode	Privileged EXEC

Example	This example shows how to show all files status stored in flash.
	Switch# **show flash**
	`Switch# show flash`
	`File Name  File Size  Modified`
	`startup-config  2204  2022-01-01 01:07:12`
	`image0 (active)  8813783  2022-01-24 09:59:59`
	`image1 (backup)  0`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32. SURVEILLANCE VLAN

Creating a reliable surveillance system can be a challenging task. Adding surveillance to an existing network can be problematic periods of heavy network traffic, such as during mass data transfers or a broadcast storm, can cause your surveillance video feeds to freeze, skip frames, or even drop out completely, surveillance vlan technology that addresses the issue of how to separate data and video in a single network deployment.

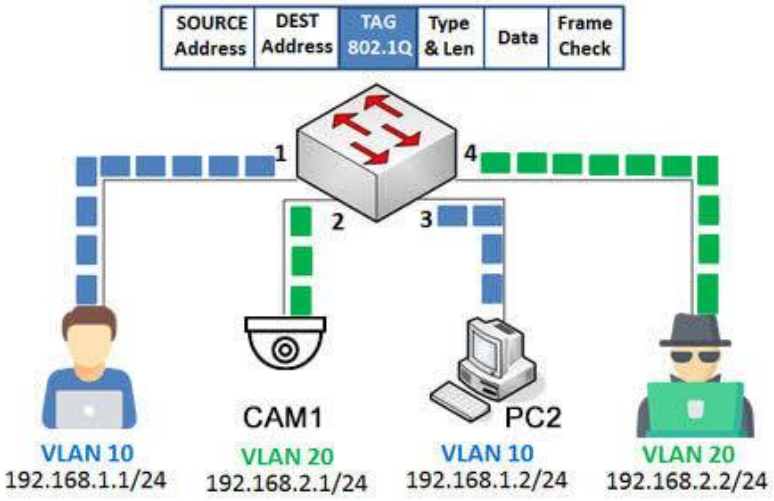


Fig 32.1 Surveillance VLAN concept

Surveillance VLAN allows quick, easy, and automatic creation of a reliable hybrid network that can handle both data and surveillance traffic. By connecting surveillance equipment such as IP cameras and NVRs, VLAN for surveillance traffic and sets quality of Service (QoS) for that traffic to high priority. This allows your surveillance traffic to be secure and ensures that surveillance video continues to stream smoothly and reliably, even during periods of heavy data traffic. Doing this normally requires you to manually configure each setting and add each device to your network one by one.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

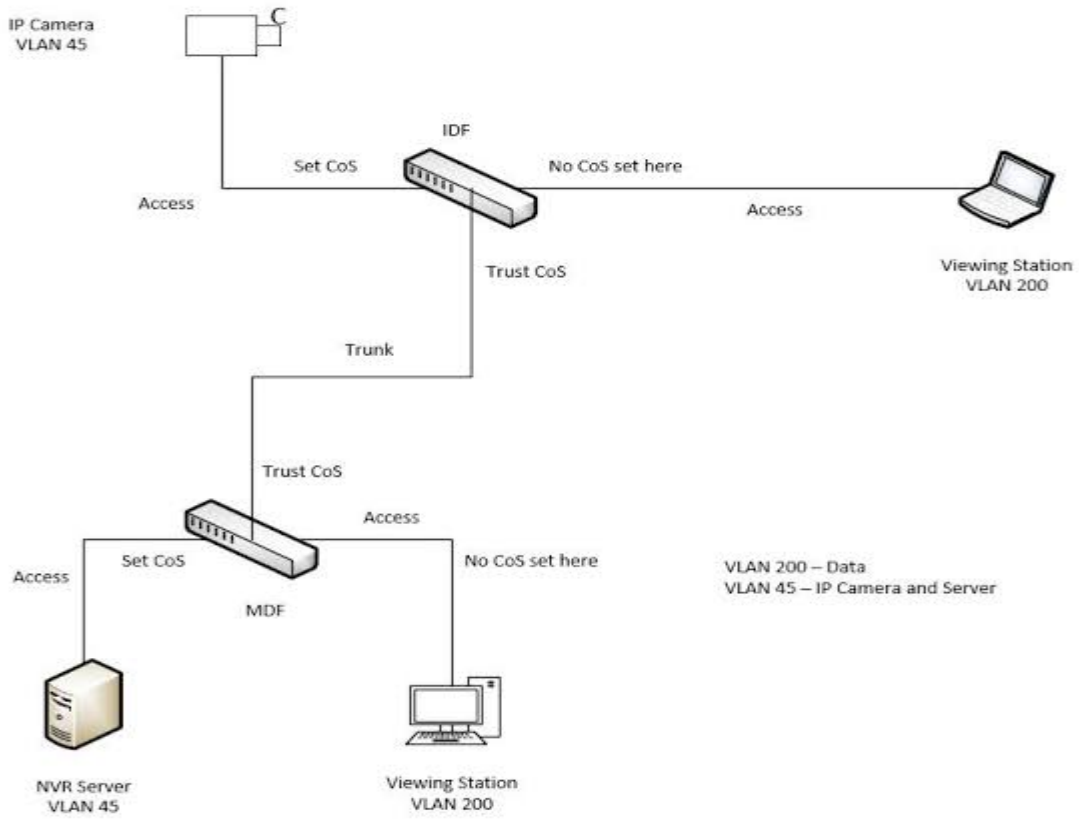


Fig 32.2 Surveillance VLAN with Trust

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32.1 SURVEILLANCE-VLAN

Use the surveillance vlan global configuration command to enable the functional Surveillance VLAN on the device. Use the **"no"** form of this command to disable Surveillance VLAN function. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **surveillance-vlan**

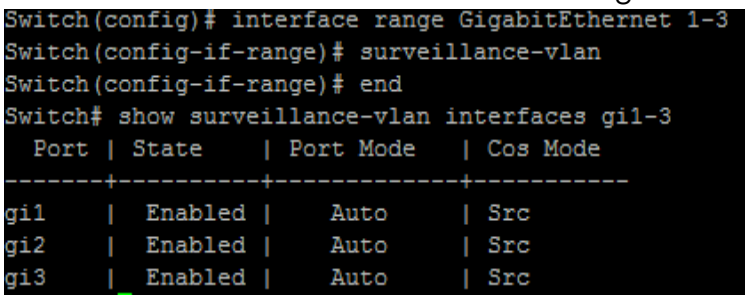
Switch(config)# **no surveillance –vlan**

Syntax	**surveillance-vlan** **no surveillance –vlan**
Mode	Global Configuration
Example	The following example shows how to enable Surveillance VLAN. Switch#**configure terminal** Switch(config)# **surveillance –vlan** Note: For enable Surveillance VLAN you required to create Surveillance VLAN ID. Switch# **show surveillance –vlan** `Switch(config)# surveillance-vlan` `Switch(config)# exit` `Switch# show surveillance-vlan` `Administrate Surveillance VLAN state   : enabled` `Surveillance VLAN ID       : 2` `Surveillance VLAN Aging    : 1440 minutes` `Surveillance VLAN CoS      : 6` `Surveillance VLAN 1p Remark: disabled` `OUI table` ` OUI MAC	Description` `------------+-----------------`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32.2 SURVEILLANCE-VLAN (INTERFACE)

Use the surveillance vlan Interface configuration command to enable OUI surveillance VLAN configuration on an interface. Use the **"no"** form of this command to disable Surveillance VLAN on an interface. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Syntax	**surveillance-vlan** **no surveillance-vlan**
Mode	Interface Configuration
Example	The following example how to enable Surveillance VLAN function in oui mode on an interface Switch#**configure terminal** Switch(config)#**interface range** GigabitEthernet 1-3 Switch(config-if)#**surveillance-vlan** Switch# **show surveillance-vlan interfaces** gi1-3 

```
Switch(config)# interface range GigabitEthernet 1-3
Switch(config-if-range)# surveillance-vlan
Switch(config-if-range)# end
Switch# show surveillance-vlan interfaces gi1-3
  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |    Auto     | Src
gi2    |  Enabled |    Auto     | Src
gi3    |  Enabled |    Auto     | Src
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32.3 SURVEILLANCE-VLAN VLAN

Use the surveillance vlan id global configuration command to configure the VLAN identifier of the surveillance VLAN statically. Use the **"no"** form of this command to restore surveillance VLAN id to default. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)#**surveillance-vlan vlan** *<1-4094>*

Switch(config)#**no surveillance-vlan vlan**

Syntax	**surveillance-vlan vlan** *<1-4094>* **no surveillance-vlan vlan**
Parameter	*<1-4094>*Specify the Surveillance VLAN ID
Default	The default Surveillance VLAN ID is None.
Mode	Global Configuration
Example	The following example shows how to set Surveillance VLAN id. The VLAN id must be created first. Switch#**configure terminal** Switch(config)# **surveillance-vlan vlan** 128 Switch# **show surveillance-vlan** `Switch(config)# surveillance-vlan vlan 2` `Switch(config)# exit` `Switch# show surveillance-vlan` `Administrate Surveillance VLAN state   : enabled` `Surveillance VLAN ID       : 2` `Surveillance VLAN Aging    : 1440 minutes` `Surveillance VLAN CoS      : 6` `Surveillance VLAN 1p Remark: disabled` `OUI table` ` OUI MAC	Description` `------------+-----------------`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32.4 SURVEILLANCE-VLAN OUI-TABLE

Use the surveillance vlan oui-table global configuration command to add OUI mac address to OUI Table. Use the no form of this command to remove all or specified OUI mac address. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **surveillance-vlan oui-table A:B:C [DESCRIPTION]**

Switch(config)# **no surveillance-vlan oui-table [A:B:C]**

Syntax	**surveillance-vlan oui-table A:B:C [DESCRIPTION]** **no surveillance-vlan oui-table [A:B:C]**
Parameter	A:B:C Specify OUI Mac address to add or remove DESCRIPTION Specify description of the specified MAC address to the surveillance VLAN OUI table
Mode	Global Configuration
Example	This following example shows how to add OUI Mac. Switch#**configure terminal** Switch(config)# **surveillance-vlan oui-table** 00:01:02 "Test" Switch# **show surveillance-vlan interfaces** gi1-3

```
Switch(config)# surveillance-vlan oui-table 00:01:03 Test1
Switch(config)# exit
Switch# show surveillance-vlan interfaces gi1-3
  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |    Auto     | Src
gi2    |  Enabled |    Auto     | Src
gi3    |  Enabled |    Auto     | Src
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32.5 SURVEILLANCE-VLAN COS (GLOBAL)

Use the surveillance vlan cos global configurations command to configure the surveillance VLAN cos value and 1p remark function. Use the **"no"** form to restore to default mode. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **surveillance-vlan cos** *<0-7>* **[remark]**

Switch(config)# **no surveillance-vlan cos**

Syntax	**surveillance-vlan cos** *<0-7>* **[remark]** **no surveillance-vlan cos**
Parameter	<0-7> Specify the surveillance VLAN Class of Service value in telephone OUI mode remark Specify that the L2 user priority is remarked with the CoS value
Default	The default cos value is 6, remark is disabled.
Mode	Global Configuration
Example	The following example show how to set cos value and enable 1p remark function Switch#**configure terminal** Switch(config)# **surveillance-vlan cos** 7 **remark** Switch# **show surveillance-vlan** `Switch(config)# surveillance-vlan cos 7 remark` `Switch(config)# exit` `Switch# show surveillance-vlan` `Administrate Surveillance VLAN state   : enabled` `Surveillance VLAN ID       : 2` `Surveillance VLAN Aging    : 1440 minutes` `Surveillance VLAN CoS      : 7` `Surveillance VLAN 1p Remark: enabled` `OUI table` ` OUI MAC	Description` `------------+-----------------` ` 00:01:02	Test` ` 00:01:03	Test1`

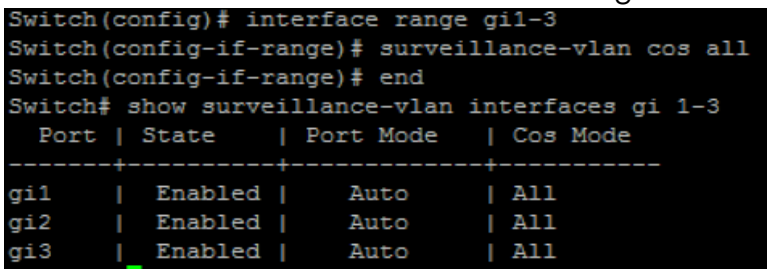
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32.6 SURVEILLANCE-VLAN COS (INTERFACE)

Use the surveillance vlan cos mode Interface configuration command to configure OUI surveillance VLAN cos mode configuration on an interface. Use the **"no"** form to restore to default mode. You can verify your setting by entering the show surveillance-vlan interfaces Privileged EXEC command.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)#**surveillance-vlan cos (src | all)**

Switch(config-if)#**no surveillance-vlan cos**

Syntax	**surveillance-vlan cos (src | all)** **no surveillance-vlan cos**
Parameter	**src** Specify QoS attributes are applied to packets with OUIs in the source MAC address. **All** Specify QoS attributes are applied to packets that are classified to the Surveillance VLAN.
Default	The default all port in Src mode.
Mode	Interface configuration
Example	The following example how to configure surveillance packet QoS attributes on an interface Switch#**configure terminal** Switch(config)#**interface range** gi1-3 Switch(config-if)#**surveillance-vlan cos all** Switch# **show surveillance-vlan interfaces** gi 1-3 

```
Switch(config)# interface range gi1-3
Switch(config-if-range)# surveillance-vlan cos all
Switch(config-if-range)# end
Switch# show surveillance-vlan interfaces gi 1-3
  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |    Auto     | All
gi2    |  Enabled |    Auto     | All
gi3    |  Enabled |    Auto     | All
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32.7 SURVEILLANCE-VLAN MODE

Use the surveillance-vlan mode global configuration command to configure the surveillance VLAN mode for interface. Use the **"no"** form to restore to default mode. You can verify your setting by entering the show surveillance-vlan interfaces Privileged EXEC command.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)#**surveillance-vlan mode (auto|manual)**

Switch(config-if)#**no surveillance-vlan mode**

Syntax	**surveillance-vlan mode (auto|manual)** **no surveillance-vlan mode**
Parameter	**auto** Specifies that the port is identified as a candidate to join the surveillance VLAN. When a packet with a source OUI MAC address that identifies the remote equipment as surveillance equipment is seen on the port, the port joins the surveillance VLAN as a tagged port. **manual** Specifies that the port is manually assigned to the surveillance VLAN.
Default	The default is auto mode.
Mode	Interface Configuration
Example	The following example how to configure surveillance mode to manual Switch#**configure terminal** Switch(config)#**interface range** gi1-3 Switch(config-if)#**surveillance-vlan mode manual** Switch# **show surveillance-vlan interfaces** gi1-3

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface range gi1-3
Switch(config-if-range)# surveillance-vlan mode manual
Switch(config-if-range)# end
Switch# show surveillance-vlan interfaces gi1-3
  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+----------
gi1    |  Enabled |  Manual     | All
gi2    |  Enabled |  Manual     | All
gi3    |  Enabled |  Manual     | All
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32.8 SURVEILLANCE-VLAN AGING-TIME

Use the surveillance vlan aging-time global configuration command to configure the surveillance VLAN aging timeout. Use the **"no"** form to restore to default time. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **surveillance-vlan aging-time** *<30-65536>*

Switch(config)# **no surveillance-vlan aging-time**

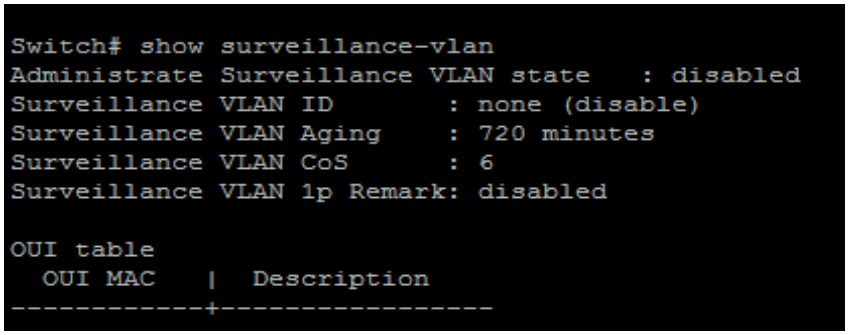
Syntax	**surveillance-vlan aging-time** *<30-65536>* **no surveillance-vlan aging-time**
Parameter	*<30-65536>*Specify the Surveillance VLAN aging timeout interval in minutes
Default	The default aging-timeout value is 1440 minutes
Mode	Global Configuration
Example	The following example shows how to set aging time. Switch#**configure terminal** Switch(config)# **surveillance-vlan aging-time** 720 Switch# **show surveillance-vlan** `Switch(config)# surveillance-vlan aging-time 720` `Switch(config)# exit` `Switch# show surveillance-vlan` `Administrate Surveillance VLAN state   : disabled` `Surveillance VLAN ID       : none (disable)` `Surveillance VLAN Aging    : 720 minutes` `Surveillance VLAN CoS      : 6` `Surveillance VLAN 1p Remark: disabled` `OUI table` ` OUI MAC	Description` `------------+-----------------`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

32.9 SHOW SURVEILLANCE-VLAN

Use the show surveillance vlan command in EXEC mode to display the surveillance VLAN status for all interfaces or for a specific interface if the surveillance VLAN type is OUI.

Switch#**show surveillance-vlan**
Switch#**show surveillance-vlan interfaces [IF_PORTS]**

Syntax	**show surveillance-vlan** **show surveillance-vlan interfaces [IF_PORTS]**
Parameter	*IF_PORTS* Specifies interfaces to display surveillance VLAN settings in OUI mode
Mode	Privileged EXEC
Example	The following example show how to display surveillance vlan OUI mode settings Switch# **show surveillance-vlan** 

```
Switch# show surveillance-vlan
Administrate Surveillance VLAN state   : disabled
Surveillance VLAN ID       : none (disable)
Surveillance VLAN Aging    : 720 minutes
Surveillance VLAN CoS      : 6
Surveillance VLAN 1p Remark: disabled

OUI table
  OUI MAC    |  Description
-------------+-----------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

33. TIME

Switches use NTP client mode, adjusting their clocks based on the time as known by an NTP server. NTP defines the messages that flow between client and server, and the algorithms a client uses to adjust its clock. Switches can also be configured as NTP servers, as well as using NTP symmetric active mode in which the switch mutually synchronizes with another NTP host. NTP servers may reference other NTP servers to obtain a more accurate clock source as defined by the stratum level of the ultimate source clock. You can either set manually time or automatically with sync with PC option or NTP setting.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

33.1 CLOCK SET

Use the clock set command to set static time. The static time won't save to configuration file. You can verify your setting by entering the show clock Privileged EXEC command.

Switch# **clock set HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov |dec)** *<1-31> <2000-2035>*

Syntax	**clock set HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug| sep|oct|nov|dec)***<1-31><2000-2035>*
Parameter	*HH:MM:SS <1-31>* (jan|feb|mar|apr|may|jun|jul|aug| sep|oct|nov|dec) *<2000-2035>* Specify static time of year, month, day, hour, minute, second
Default	No default is defined. The clock set to 2000/01/01 08:00:00 by default at startup.
Mode	Privileged EXEC

Example	The example shows how to set static time of switch.
	Switch# **clock set 10:57:00 feb 12 2022**
	Switch# **show clock**
	`Switch# clock set 10:57:00 feb 12 2022`
	`2022-02-12 10:57:00 UTC-7`
	`Switch# show clock`
	
	`2022-02-12 10:57:11 UTC-7`
	`Time set manually`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

33.2 Clock timezone

Use the clock timezone command to set time zone setting. Use the **"no"** form of this command to restore to default setting. You can verify your setting by entering the show clock detail Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **clock timezone ACRONYM HOUR-OFFSET** [*minutes <0-59>*]

Switch# **no clock timezone**

Syntax	**clock timezone** (ACRONYM HOUR-OFFSET) [*minutes <0-59>*] **no clock timezone**
Parameter	ACRONYM Specify acronym name of time zone HOUR-OFFSET Specify hour offset of time zone Minutes <1-59>Specify minute offset of time zone
Default	Default time zone is UTC+7.
Mode	Global Configuration

Example	The example shows how to set time zone of switch and then restore to default time zone.
	Switch#**configure terminal**
	Switch(config)# **clock timezone** test +5
	Switch# **show clock detail**
	`Switch# show clock detail`
	
	`2022-02-12 23:01:03 test(UTC+5)`
	`Time set manually`
	
	`Time zone:`
	`Acronym is test`
	`Offset is UTC+5`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

33.3 CLOCK SOURCE

Use the clock source command to set the source of time. Use the **"no"** form of this command to restore to default setting. You can verify your setting by entering the show clock detail Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **clock source (local|sntp)**

Syntax	**clock source (local|sntp)**
Parameter	local Specify to use static time sntp Specify to use sntp time
Default	Default is using local time
Mode	Global Configuration

Example	The example shows how to set clock source of switch.
	Switch#**configure terminal**
	Switch(config)# **clock source sntp**
	
	Switch(config)# **show clock detail**
	`Switch# config t`
	`Switch(config)# clock source sntp`
	`Switch(config)#`
	`Switch# show clock detail`
	
	`2022-02-12 23:02:51 test(UTC+5)`
	`Time source is sntp`
	
	`Time zone:`
	`Acronym is test`
	`Offset is UTC+5`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

33.4 CLOCK SUMMER-TIME

Use the clock summer-time command to set daylight saving time for system time. The **"usa"** or **"eu"** means that use the global daylight-saving policy which defined by international organization. In both the **"date"**and **"recurring"**, the first part of the command specifies when summertime begins, and the second part specifies when it ends. All times are relative to the local time zone. The **"recurring"** means that adjust time every year within the month. Use the no form of this command to default setting. You can verify your setting by entering the show clock detail Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **clock summer-time ACRONYM date (jan|feb|mar|apr |may|jun|jul |aug|sep|oct|nov|dec)** *<1-31><2000-2035>*
HH:MM (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) *<1-31><2000-2035> HH:MM [<1-1440>]*
Switch(config)# **clock summer-time ACRONYM recurring (usa|eu)** *[<1-1440>]* **clock summer-time ACRONYM recurring (***<1-5>***|first|last)**
(sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) HH:MM **(***<1-5>***|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug |sep|oct|nov|dec)** HH:MM [*<1-1440>*]

Switch(config)# **no clock summer-time**

Syntax	**clock summer-time ACRONYM date (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)** *<1-31><2000-2037>* **HH:MM (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)** *<1-31><2000-2035> HH:MM [<1-1440>]* **clock summer-time ACRONYM recurring (usa|eu)** *[<1-1440>]* **clock summer-time ACRONYM recurring (***<1-5>***|first|last)** **(sun|mon|tue|wed|thu|fri|sat)** **(jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)** HH:MM **(***<1-5>***|first|last)** **(sun|mon|tue|wed|thu|fri|sat)** **(jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)** HH:MM [*<1-1440>*]

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

	no clock summer-time
Parameter	*ACRONYM<1-31>* Specify acronym name of time zone (jan|feb|mar|apr| may|jun|jul|aug|sep| oct|nov|dec) *<2000-2035>*HH:MM Specify non-recurring daylight saving time duration. *<1-1440>*Specify adjust offset of daylight-saving time **usa** Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November **eu** Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October (*<1-5>*|first|last) (sun|mon| tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun| jul|aug|sep|oct|nov|dec) HH:MM (*<1-5>*|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may| jun|jul|aug|sep |oct|nov|dec) HH:MM Specify ecurring daylight saving time duration.
Mode	Global Configuration

Example	The example shows how to set clock summertime of switch. You can verify settings by the following show show clock command.
	Switch#**configure terminal**
	Switch(config)# **clock summer-time test recurring usa**
	Switch# **show clock detail**
	`Switch(config)# clock summer-time test recurring usa`
	`Switch(config)# exit`
	`Switch# show clock detail`
	
	`01-02-2020 11:20:25 UTC-7`
	`Time source is sntp`
	
	`Time zone:`
	`Acronym is`
	`Offset is UTC-7`
	
	`Summertime:`
	`Acronym is test`
	`Recurring every year.`
	`Begins at 2 0 3 2:0`
	`Ends at 1 0 11 2:0`
	`Offset is 60 minutes.`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

33.5 SHOW CLOCK

Use the show clock command to show clock of switch. The **“detail”** means that show more information of clock such as time zone and daylight-saving time.

Switch# **show clock [detail]**

Syntax	**show clock [detail]**
Parameter	detail Show more detail information of clock
Mode	Privileged EXEC

Example	The example shows how to show clock of switch and detail information.
	Switch#**configure terminal**
	Switch(config)# **clock source sntp**
	Switch(config)# **clock summer-time DLS recurring usa**
	Switch(config)# **sntp host 192.168.1.100**
	Switch# **show clock**
	Switch# **show clock detail**
	`Switch(config)# clock source sntp`
	`Switch(config)# clock summer-time DLS recurring usa`
	`Switch(config)# sntp host 192.168.1.100`
	`Switch(config)# exit`
	`Switch# show clock`
	
	`01-02-2020 11:22:50 UTC-7`
	`Time source is sntp`
	
	`Switch# show clock detail`
	
	`01-02-2020 11:22:58 UTC-7`
	`Time source is sntp`
	
	`Time zone:`
	`Acronym is`
	`Offset is UTC-7`
	
	`Summertime:`
	`Acronym is DLS`
	`Recurring every year.`
	`Begins at 2 0 3 2:0`
	`Ends at 1 0 11 2:0`
	`Offset is 60 minutes.`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

33.6 SNTP

Use the sntp command to set remote SNTP server. Use the no form of this command to default setting. You can verify your setting by entering the show sntp Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **sntp host HOSTNAME** [*port <1-65535>*]

Switch(config)# **no sntp**

Syntax	**sntp host HOSTNAME** [*port <1-65535>*] **no sntp**
Parameter	HOSTNAME Specify ip address or hostname of sntp server sntp Specify server port of sntp server
Default	No default SNTP server defined. Default server port is 123 when server created.
Mode	Global Configuration

Example	The example shows how to set remote SNTP server of switch.
	Switch#**configure terminal**
	Switch(config)# **clock source sntp**
	Switch(config)# **sntp host 192.168.1.100**
	Switch(config)# **show sntp**
	`Switch# configure`
	`Switch(config)# clock source sntp`
	`Switch(config)# sntp host 192.168.1.100`
	`Switch(config)# exit`
	`Switch# show sntp`
	`SNTP is Enabled`
	`SNTP Server address: 192.168.1.100`
	`SNTP Server port: 123`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

33.7 SHOW SNTP

Use the show sntp command to remote SNTP server information.

Switch# **show sntp**

Syntax	**show sntp**
Mode	Privileged EXEC

Example	The example shows how to show remote SNTP server.
	Switch# **show sntp**
	`Switch# show sntp`
	`SNTP is Enabled`
	`SNTP Server address: 192.168.1.100`
	`SNTP Server port: 123`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

34. UDLD

Unidirectional Link Detection (UDLD) is a data link layer protocol from Cisco Systems to monitor the physical configuration of the cables and detect unidirectional links. It complements the Spanning Tree Protocol which is used to eliminate switching loops. It allows two switches to verify if they can both send and receive data on a point-to-point connection. UDLD works with the Layer 1 (L1) mechanisms to determine the physical status of a link. UDLD can be run on both fiber optic and twisted-pair copper links. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it administratively shuts down the affected port and alerts administrator. Unidirectional links can cause a variety of problems, including spanning-tree topology loop, If two devices, A and B, are connected via a pair of optical fibers, one used for sending from A to B and other for sending from B to A, the link is bidirectional (two-way). If one of this fiber is broken, the link has become one-way or unidirectional. The goal of the UDLD protocol is to detect a broken bidirectional link.

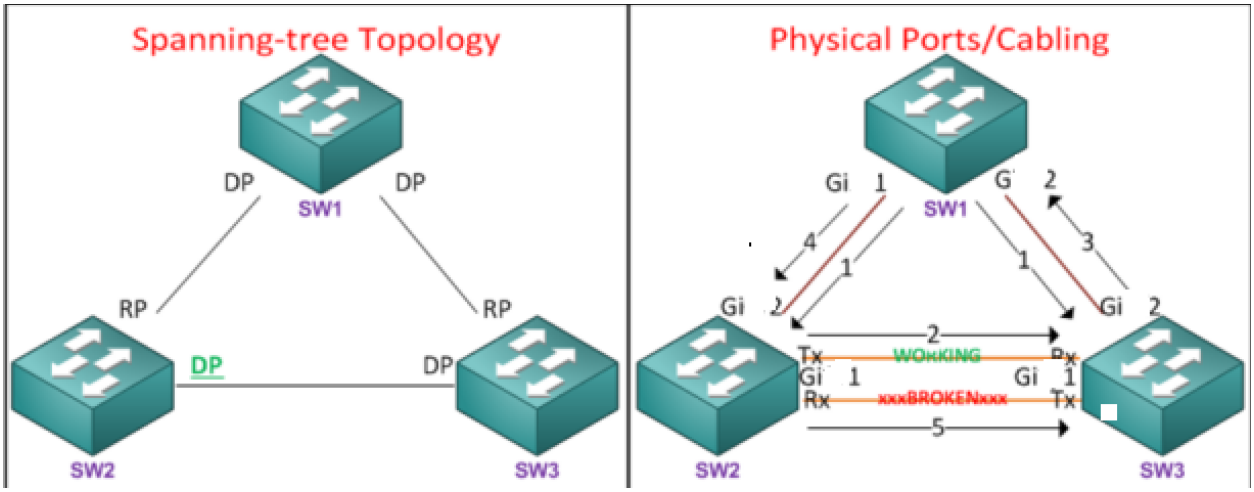


Fig 34.1 Spanning Tree Topology

UDLD supports two modes of operation: Normal (the default) and Aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

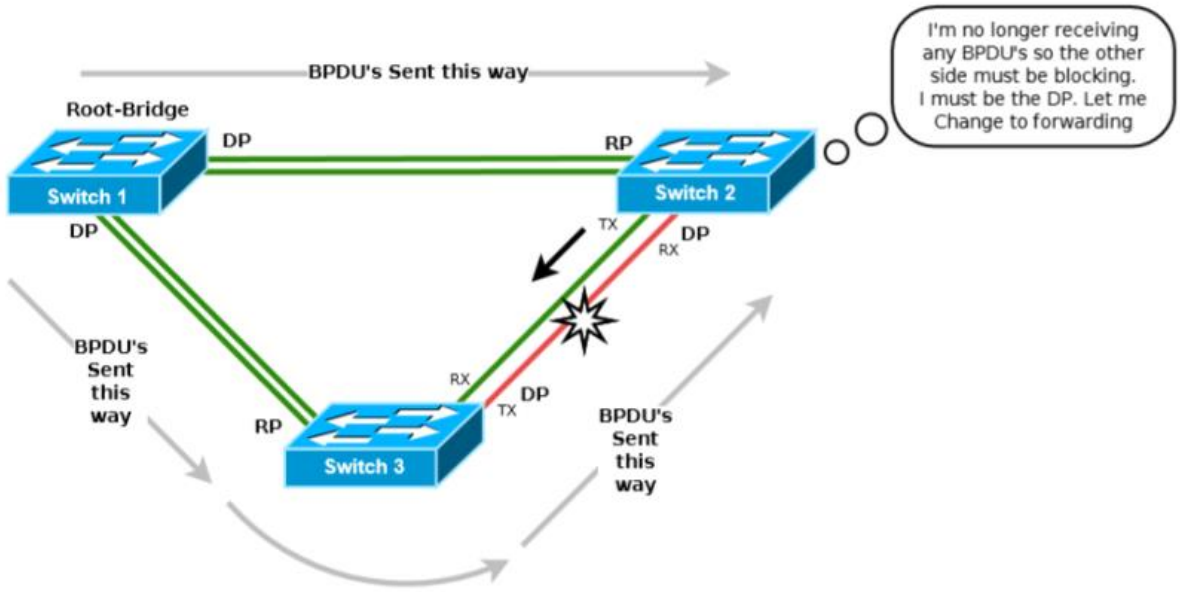


Fig 34.2 BPDU Route

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive.

In normal mode, UDLD can detect unidirectional links due to misconnected interfaces on fiber-optic connections.

In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected interfaces on fiber-optic links. In UDLD aggressive mode, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

34.1 ERRDISABLE RECOVERY CAUSE UDLD

Use the errdisable recovery cause udld to enable auto recovery of UniDirectional Link Detection (UDLD). Use the **"no"** to disable it.

Switch#c**onfigure terminal**
Switch(config)# **errdisable recovery cause udld**

Switch(config)# **no errdisable recovery cause udld**

Syntax	**errdisable recovery cause udld** **no errdisable recovery cause udld**
Default	Error disable auto recovery is disabled by default.
Mode	Global EXEC
Example	The example shows how to enable auto recovery of UniDirectional Link Detection (UDLD). Switch#**configure terminal** Switch(config)# **errdisable recovery cause udld** Switch# **show errdisable recovery**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# errdisable recovery cause udld
Switch(config)# exit
Switch# show errdisable recovery
 ErrDisable Reason        | Timer Status
--------------------------+--------------
               bpduguard | disabled
                    udld | enabled
                selfloop | disabled
         broadcast-flood | disabled
  unknown-multicast-flood | disabled
           unicast-flood | disabled
                     acl | disabled
       psecure-violation | disabled
         dhcp-rate-limit | disabled
          arp-inspection | disabled

Timer Interval : 300 seconds


Interfaces that will be enabled at the next timeout:

Port |  Error Disable Reason    | Time Left
-----+--------------------------+-----------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

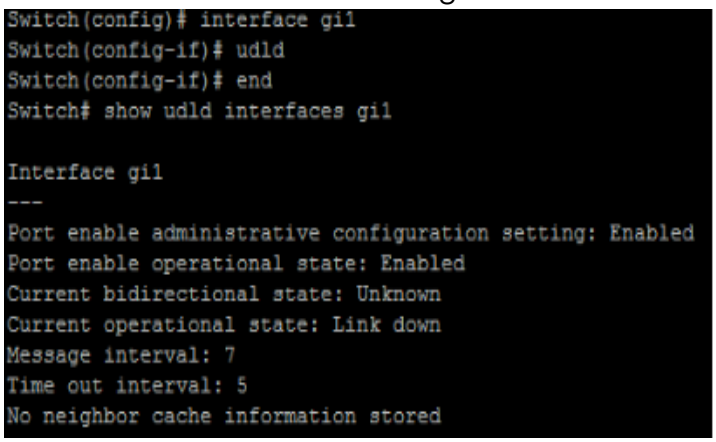
34.2 UDLD

Use the udld command to enable UniDirectional Link Detection (UDLD) normal mode of interface. Use the **"no"** form of this command to restore to default setting. You can verify your setting by entering the show udld interface Privileged EXEC command.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)# **udld**

Switch(config-if)# **no udld**

Syntax	**udld** **no udld**
Mode	Interface Configuration

Example	The example shows how to enable UniDirectional Link Detection (UDLD) normal mode in interface gi1.
	Switch#**configure terminal**
	Switch(config)# **interface** gi1
	Switch(config-if)# **udld**
	Switch# **show udld interfaces** gi1
	 
	`Switch(config)# interface gi1`
	`Switch(config-if)# udld`
	`Switch(config-if)# end`
	`Switch# show udld interfaces gi1`
	
	`Interface gi1`
	`---`
	`Port enable administrative configuration setting: Enabled`
	`Port enable operational state: Enabled`
	`Current bidirectional state: Unknown`
	`Current operational state: Link down`
	`Message interval: 7`
	`Time out interval: 5`
	`No neighbor cache information stored`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

34.3 UDLD AGGRESSIVE

Use the udld aggressive command to enable UniDirectional Link Detection (UDLD) aggressive mode of interface. Use the **"no"** form of this command to restore to default setting. You can verify your setting by entering the show udld interface Privileged EXEC command.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)# **udld aggressive**

Switch(config-if)# **no udld aggressive**

Syntax	**udld aggressive** **no udld aggressive**
Mode	Interface Configuration
Example	The example shows how to enable udld aggressive mode in interface gi1. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **udld aggressive** Switch# **show udld interfaces** gi1

```
Switch(config)# interface gi1
Switch(config-if)# udld aggressive
Switch(config-if)# end
Switch# show udld interfaces gi1

Interface gi1
---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 7
Time out interval: 5
No neighbor cache information stored
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

34.4 UDLD MESSAGE TIME

Use the udld message time to set interval of UniDirectional Link Detection (UDLD) sent message.

Switch#**configure terminal**
Switch(config)# **udld message time message-time-interval**

Syntax	**udld message time message-time-interval**
Parameter	message-time-interval Specify the interval for sending message.Range is 1 -90 seconds.
Default	Default interval is 15 seconds.
Mode	Global Configuration
Example	The example shows how to set interval of UniDirectional Link Detection (UDLD) message. Switch#**configure terminal** Switch(config)# **udld message time 30**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

34.5 UDLD RESET

Use the udld reset command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again. If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

Switch# udld reset

Syntax	udld reset
Mode	Privileged EXEC
Example	The example shows how to reset all interfaces disabled by UDLD Switch# udld reset

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

34.6 SHOW UDLD

Use the show udld command to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

Switch# **show udld**

Switch# **show udld interfaces** {*IF_NMLPORTS}*

Syntax	**show udld** **show udld interfaces** {*IF_NMLPORTS}*
Parameter	*{IF_NMLPORTS}* Specify the normal interfaces to display udld information
Mode	Privileged EXEC

Example	The example shows how to show UniDirectional Link Detection (UDLD) settings and operational status of interface gi1.
	Switch# **show udld interfaces gi1**
	`Switch# show udld interfaces gi1`
	`Interface gi1`
	`---`
	`Port enable administrative configuration setting: Enabled / in aggressive mode`
	`Port enable operational state: Enabled / in aggressive mode`
	`Current bidirectional state: Unknown`
	`Current operational state: Link down`
	`Message interval: 7`
	`Time out interval: 5`
	`No neighbor cache information stored`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35. VLAN

Virtual LANs In an Ethernet LAN, a set of devices that receive a broadcast sent by any one of the devices in the same set is called a broadcast domain. On switches that have no concept of virtual LANs (VLAN), a switch simply forwards all broadcasts out all interfaces, except the interface on which it received the frame. As a result, all the interfaces on an individual switch are in the same broadcast domain. Also, if the switch connects to other switches and hubs, the interfaces on those switches and hubs are also in the same broadcast domain.

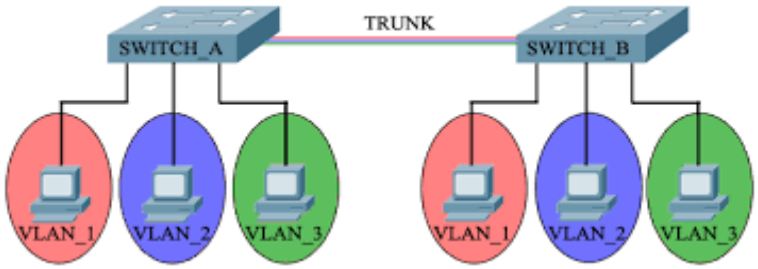


Fig 35.1 VLAN concept

A VLAN is simply an administratively defined subset of switch ports that are in the same broadcast domain. Ports can be grouped into different VLANs on a single switch, and on multiple interconnected switches as well. By creating multiple VLANs, the switches create multiple broadcast domains. By doing so, a broadcast sent by a device in one VLAN is forwarded to the other devices in that same VLAN however, the broadcast is not forwarded to devices in the other VLANs. With VLANs and IP, best practices dictate a one-to-one relationship between VLANs and IP subnets. Simply put, the devices in a single VLAN are typically also in the same single IP subnet. Alternately, it is possible to put multiple subnets in one VLAN and use secondary IP addresses on routers to route between the VLANs and subnets. Also, although not typically done, you can design a network to use one subnet on multiple VLANs and use routers with proxy ARP enabled to forward traffic between hosts in those VLANs.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

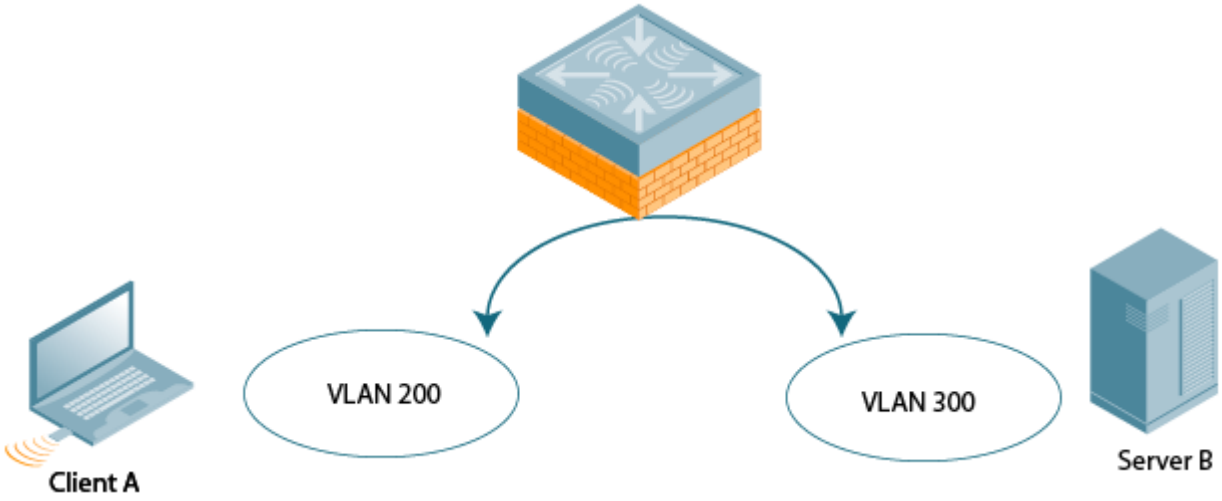


Fig 35.2 Inter VLAN communication

VLAN Configuration

Step 1 Create the VLAN.

Step 2 Associate the correct ports with that VLAN.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.1 VLAN

Use the vlan global configuration command to create VLAN. Use the no form of this command to remove exist VLAN. You can verify your setting by entering the show vlan Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**vlan** {Vlan-ID}

Switch (config)#**no vlan**

Syntax	**vlan** **No vlan**
Default	VLAN 1 created by default
Mode	Global Configuration

Example	The following example creates and removes a VLAN entry (100).
	Switch#**configure terminal**
	Switch (config)# **vlan 2**
	Switch# **show vlan**
	`Switch# show vlan`
	`VID  VLAN Name  Untagged Ports  Tagged Ports  Type`
	`1  default  gi2-24,te1-4,lag1-8  Default`
	`2  VLAN0002  gi1  Static`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.2 NAME (VLAN)

Use the name vlan configuration command to set name of vlan. You can verify your setting by entering the show vlan Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**vlan** {Vlan-No}
Switch(config-vlan)# **name** *{NAME}*

Syntax	**name** *{NAME}*
Parameter	NAME Specify the name of the VLAN (Max. 32 chars).
Default	Default name of new vlan is VLAN xxxx. Xxxx is 4-digit vlan number.
Mode	VLAN Configuration

Example	This example sets the VLAN name of VLAN 100 to be `VLAN- one-hundred`.
	Switch#**configure terminal**
	Switch(config)# **vlan 10**
	Switch(config-vlan)# **name VLAN-COMMANDO1**
	Switch# **show vlan**
	`Switch# show vlan`
	`VID VLAN Name Untagged Ports Tagged Ports Type`
	`1 default gi2-24,te1-4,lag1-8 Default`
	`2 VLAN0002 gi1 Static`
	`10 VLAN-COMMANDO1 Static`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.3 SWITCHPORT MODE

The VLAN mode is used to configure the port for different port role.

Access port: Accepts only untagged frames and join an untagged VLAN.

Hybrid port: Support all functions as defined in IEEE 802.1Q specification.

Trunk port: An untagged member of one VLAN at most and is a tagged member of zero or more VLANs. If it is an uplink port, it can recognize double tagging on this port.

Tunnel port: Port-based Q-in-Q mode.

Use the switch mode port configuration command to set mode of interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport mode (access | hybrid | trunk [uplink] | tunnel)**

Syntax	**switchport mode (access | hybrid | trunk [uplink] | tunnel)**
Parameter	**access** Specify the VLAN mode to Access port. **hybrid** Specify the VLAN mode to Hybrid port. **trunk** Specify the VLAN mode to Trunk port. **uplink** Specify the Uplink property on this Trunk port. **tunnel** Specify the VLAN mode to Dot1Q Tunnel port.
Default	Default is trunk mode of all interfaces
Mode	Port Configuration
Example	This example sets VLAN mode to Access port. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode access** Switch# **show interfaces switchportGigabitEthernet 2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode access
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Access
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : untagged-only
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled:

Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- -----------------
    1               default       Untagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.4 SWITCHPORT HYBRID PVID

Use the switch hybrid pivd port configuration command to set pvid of interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport hybrid pvid** *<1-4094>*

Syntax	**switchport hybrid pvid** *<1-4094>*
Parameter	*<1-4094>*Specify the port-based VLAN ID on the Hybrid port.
Default	Default pivd is 1.
Mode	Port Configuration

Example	This example sets PVID to 100.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 2
	Switch(config-if)# **switchport mode hybrid**
	Switch(config-if)# **switchport hybrid pvid** 100
	Switch# **show interfaces switchport gi2**
	`Switch(config)# interface GigabitEthernet 2`
	`Switch(config-if)# switchport mode hybrid`
	`Switch(config-if)# switchport hybrid pvid 100`
	`Switch(config-if)# end`
	`Switch# show interfaces switchport gi2`
	`Port : gi2`
	`Port Mode : Hybrid`
	`Gvrp Status : disabled`
	`Ingress Filtering : enabled`
	`Acceptable Frame Type : all`
	`Ingress UnTagged VLAN ( NATIVE ) : 100`
	`Trunking VLANs Enabled:`
	`Port is member in:`
	`Vlan Name Egress rule`
	`------- ---------- ----------`
	`1 default Untagged`
	`Forbidden VLANs:`
	`Vlan Name`
	`------- ----------`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.5 SWITCHPORT HYBRID INGRESS-FILTERING

Use the switchport hybrid ingress-filtering port configuration command to enable vlan ingress filter. Use the **"no"** form of this command to disable. You can verify your setting by entering the s show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport hybrid ingress-filtering**

Switch(config-if)# **no switchport hybrid ingress-filtering**

Syntax	**switchport hybrid ingress-filtering** **no switchport hybrid ingress-filtering**
Mode	Port Configuration

Example	This example sets ingress-filtering to disable.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 2
	Switch(config-if)# **switchport mode hybrid**
	Switch(config-if)# **no switchport hybrid ingress-filtering**
	Switch# **show interfaces switchport GigabitEthernet 2**
	`Switch(config)# interface GigabitEthernet 2`
	`Switch(config-if)# switchport mode hybrid`
	`Switch(config-if)# no switchport hybrid ingress-filtering`
	`Switch(config-if)# end`
	`Switch# show interfaces switchport GigabitEthernet 2`
	`Port : gi2`
	`Port Mode : Hybrid`
	`Gvrp Status : disabled`
	`Ingress Filtering : disabled`
	`Acceptable Frame Type : all`
	`Ingress UnTagged VLAN ( NATIVE ) : 100`
	`Trunking VLANs Enabled:`
	`Port is member in:`
	`Vlan Name Egress rule`
	`------- ---------- ----------`
	`1 default Untagged`
	`Forbidden VLANs:`
	`Vlan Name`
	`------- ----------`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.6 SWITCHPORT HYBRID ACCEPTABLE-FRAME-TYPE

Use the switchport hybrid accept-frame-type port configuration command to choose which type of frame can be accepted. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport hybrid acceptable-frame-type (all | tagged-only | untagged- only)**

Syntax	**switchport hybrid acceptable-frame-type (all | tagged-only | untagged-only)**
Parameter	**all** Specify to accept all frames. **tagged-only** Specify to only accept tagged frames. **untagged-only** Specify to only accept untagged frames.
Default	Default is accept all frames
Mode	Port Configuration
Example	This example sets acceptable-frame-type to tagged-only. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode hybrid** Switch(config-if)# **switchport hybrid acceptable-frame-type tagged-only** Switch# **show interfaces switchport GigabitEthernet 2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid acceptable-frame-type tagged-only
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : disabled
Acceptable Frame Type : tagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:

Port is member in:
 Vlan            Name             Egress rule
------- ---------------------- -----------------
    1               default       Untagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.7 SWITCHPORT HYBRID ALLOWED VLAN

Use the switchport hybrid allow vlan add port configuration command to allow vlan on interface. Use the switchport hybrid allows vlan remove port configuration command to remove vlan on interface. You can verify your setting by entering the s show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport hybrid allowed vlan add** *{VLAN-LIST}*
Switch(config-if)#**switchport hybrid allowed vlan remove** *{VLAN-LIST}* **[(tagged|untagged)]**

Syntax	**switchport hybrid allowed vlan add** *{VLAN-LIST}* **switchport hybrid allowed vlan remove** *{ VLAN-LIST}* **[(tagged|untagged)]**
Parameter	*VLAN-LIST* Specifies the VLAN list to be added or remove. **(tagged | untagged)** Specifies the member type is tagged or untagged.
Default	Only vlan 1 is untagged member by default. Default is tagged member when added.
Mode	Port Configuration
Example	This example sets port GigabitEthernet 2 VLAN to join the VLAN 100 as tagged member. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport hybrid allowed vlan add 100-105** Switch(config-if)# **switchport hybrid allowed vlan remove 105** Switch# **show interfaces switchport GigabitEthernet 2**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport hybrid allowed vlan add 100-105
Switch(config-if)# switchport hybrid allowed vlan remove 105
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : disabled
Acceptable Frame Type : tagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:

Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- -----------------
    1               default       Untagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.8 SWITCHPORT ACCESS VLAN

Use the switchport access vlan port configuration command to set native vlan on interface. The vlan will be pvid on interface as well. Use the **"no"** form of this command to restore to default vlan. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport access vlan** *<1-4094>*

Switch(config-if)# **no switchport access vlan**

Syntax	**switchport access vlan** *<1-4094>* **no switchport access vlan**
Parameter	<1-4094>Specifies the access VLAN ID.
Default	Default is vlan 1
Mode	Port Configuration
Example	This example sets Access port gi10 native VLAN ID to 100. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **switchport mode access** Switch(config-if)# **switchport access vlan** 4 Switch# **show interfaces switchport** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface gi2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 4
Switch(config-if)# exit
Switch(config)# exit
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Access
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : untagged-only
Ingress UnTagged VLAN ( NATIVE ) : 4
Trunking VLANs Enabled:

Port is member in:
 Vlan           Name             Egress rule
------- ---------------------- -----------------
    4              VLAN0004       Untagged

Forbidden VLANs:
 Vlan           Name
------- ----------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.9 SWITCHPORT TUNNEL VLAN

Use the switchport tunnel vlan port configuration command to set dot1q tunnel vlan on interface. The vlan will be pvid on interface as well. Use the **"no"** form of this command to remove vlan on interface. The tunnel vlan id will set to reserve vlan 4095. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport tunnel vlan** *<1-4094>*

Switch(config-if)# **no switchport tunnel vlan**

Syntax	**switchport tunnel vlan** *<1-4094>* **no switchport tunnel vlan**
Parameter	*<1-4094>*Specifies the tunnel VLAN ID.
Default	Default is vlan 1
Mode	Port Configuration
Example	This example sets Tunnel port GigabitEthernet 2 native VLAN to 4. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode tunnel** Switch(config-if)# **switchport tunnel vlan** 4 Switch# **show interfaces switchport** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode tunnel
Switch(config-if)# switchport tunnel vlan 4
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Tunnel
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 4
Trunking VLANs Enabled:

Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- -----------------
    4              VLAN0004       Untagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.10 SWITCHPORT TRUNK NATIVE VLAN

Use the switchport trunk native vlan port configuration command to set native vlan on interface. Use the **"no"** form of this command to restore to default vlan. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport trunk native vlan** *<1-4094>*

Switch(config-if)# **no switchport trunk native vlan**

Syntax	**switchport trunk native vlan** *<1-4094>* **no switchport trunk native vlan**
Parameter	*<1-4094>*Specifies the native VLAN ID.
Default	Default is vlan 1
Mode	Default is vlan 1
Example	This example sets Trunk port GigabitEthernet 2 native VLAN to 4. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode trunk** Switch(config-if)# **switchport trunk native vlan** 4 Switch# **show interfaces switchport** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 4
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Trunk
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 4
Trunking VLANs Enabled:

Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- ----------------
    4              VLAN0004       Untagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.11 SWITCHPORT TRUNK ALLOWED VLAN

Use the switchport trunk allow vlan add port configuration command to allow vlan on interface. Use the switchport trunk allows vlan remove port configuration command to remove vlan on interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport trunk allowed vlan (add | remove) (VLAN-LIST | all)**

Syntax	**switchport trunk allowed vlan (add | remove) (VLAN-LIST | all)**
Parameter	**(add | remove)** Specify the action to add or remove the allowed VLAN list. **(VLAN-LIST | all)** Specify the VLAN list or all VLANs to be added or removed.
Mode	Port Configuration
Example	This example sets Trunk port GigabitEthernet 2 to add the allowed VLAN 4. Switch# **configure** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport trunk allowed vlan add** 4 Switch# **show interfaces switchport** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport trunk allowed vlan add 4
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Trunk
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 4
Trunking VLANs Enabled: 4

Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- -----------------
    4              VLAN0004       Untagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.12 SWITCHPORT DEFAULT-VLAN TAGGED

Use the switchport default vlan tagged port configuration command to become default vlan tagged member. Use the **"no"** switchport default vlan tagged port configuration command to restore to default. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport default-vlan tagged**

Switch(config-if)# **no switchport default-vlan tagged**

Syntax	**switchport default-vlan tagged** **no switchport default-vlan tagged**
Default	Default is untagged
Mode	Port Configuration
Example	This example sets Trunk port GigabitEthernet 2 membership with the default VLAN to tag. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport default-vlan tagged** Switch# **show interfaces switchport** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)#  switchport default-vlan tagged
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled: 4

Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- -----------------
    1               default         Tagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.13 SWITCHPORT FORBIDDEN DEFAULT-VLAN

Use the switchport forbidden default-vlan port configuration command to forbid default-vlan on interface. Use the **"no"** switchport forbidden default-vlan port configuration command to restore to default. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport forbidden default-vlan**

Switch(config-if)# **no switchport forbidden default-vlan**

Syntax	**switchport forbidden default-vlan** **no switchport forbidden default-vlan**
Default	Default is allowed
Mode	Port Configuration
Example	This example sets the membership of the default VLAN with port GigabitEthernet 2 to Forbidden. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport forbidden default-vlan** Switch# **show interfaces switchport** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport forbidden default-vlan
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 4095
Trunking VLANs Enabled: 4

Port is member in:
 Vlan           Name             Egress rule
------- ---------------------- ----------------

Forbidden VLANs:
 Vlan           Name
------- ----------------------
    1              default
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.14 SWITCHPORT FORBIDDEN VLAN

Uses the switchport forbidden vlan add port configuration command to forbid vlan on interface. Use the switchport forbidden vlan remove port configuration command to accept vlan on interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport forbidden vlan (add | remove)** *VLAN-LIST*

Syntax	**switchport forbidden vlan (add | remove)** *VLAN-LIST*
Parameter	(add | remove) Add or remove forbidden membership. *VLAN-LIST* Specify the VLAN list.
Mode	Port Configuration
Example	This example sets the membership of the VLAN 4 with port GigabitEthernet 2 to Forbidden. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport forbidden vlan add** 4 Switch# **show interfaces switchport** GigabitEthernet 2

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport forbidden vlan add 4
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Hybrid
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 4095
Trunking VLANs Enabled: 4

Port is member in:
 Vlan           Name             Egress rule
------- ---------------------- ----------------

Forbidden VLANs:
 Vlan           Name
------- ----------------------
    1              default
    4             VLAN0004
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.15 SWITCHPORT VLAN TPID

Use the switchport vlan tpid port configuration command to set TPID on interface. You can verify your setting by entering the show running-config Privileged EXEC command.

Switch#**configure terminal**
Switch (config)#**interface** {Interface-ID}
Switch(config-if)# **switchport vlan tpid (0x8100|0x88a8|0x9100|0x9200)**

Syntax	**switchport vlan tpid (0x8100|0x88a8|0x9100|0x9200)**
Parameter	(0x8100|0x88a8|0x9100|0x9200) Select TPID to set.
Default	Default TPID is 0x8100
Mode	Port Configuration
Example	This example sets the TPID to 0x9100 on interface GigabitEthernet 2. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport vlan tpid 0x9100**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.16 MANAGEMENT-VLAN

Use the management vlan Global Configuration mode command to set management vlan id. Vlan id must be created first. Use the **"no"** form of this command to restore to default setting. You can verify your setting by entering the show management-vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **management-vlan vlan** *<1-4094>*

Switch(config)# **no management-vlan**

Syntax	**management-vlan vlan** *<1-4094>* **no management-vlan**
Parameter	*<1-4094>* Specify the VLAN ID of management-vlan.
Default	Default management vlan is 1.
Mode	Global Configuration
Example	The following example specifies that management vlan 2 is created Switch#**configure terminal** Switch(config)# **vlan** 2 Switch(config)# **management-vlan vlan** 2 The following example specifies that management-vlan is restored to be default VLAN. Switch(config)# **no management-vlan**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.17 SHOW VLAN

Display information about vlan entry.

Switch# **show vlan [(VLAN-LIST|dynamic|static)]**

Syntax	**show vlan [(VLAN-LIST|dynamic|static)]**
Parameter	(VLANLIST|dynamic|static)Specify vlan id to show information or show all static or dynamic vlan entries.
Mode	Privileged EXEC

Example	The following example specifies that show vlan
	Switch# **show vlan**
	`Switch# show vlan`
	
	`VID  VLAN Name  Untagged Ports  Tagged Ports  Type`
	`1  default  gi2-24,te1-4,lag1-8  Default`
	`2  VLAN0002  gi1  Static`
	`10  VLAN-COMMANDO1  Static`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.18 SHOW VLAN INTERFACE MEMBERSHIP

Display information about vlan membership on interfaces.

Switch# **show vlan VLAN-LIST interfaces** *{IF_PORTS}* **membership**

Syntax	**show vlan VLAN-LIST interfaces** *{IF_PORTS}* **membership**
Parameter	*<VLAN-List>* Specify vlan to show *IF_PORTS* Specify interface is to show
Mode	Privileged EXEC
Example	The following example specifies that show vlan interface membership Switch# **show vlan 2 interfaces** GigabitEthernet 2 **membership** `Switch# show vlan 2 interfaces GigabitEthernet 2 membership` `------------------------` ` VLAN ID   : 2` ` VLAN Type : Static` `---------+--------------` ` Port	Membership` `---------+--------------` ` gi2	Excluded` `---------+--------------`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.19 SHOW INTERFACE SWITCHPORT

Display information about default vlan.

Switch# **show interface switchport interfaces** *{IF_*PORTS}

Syntax	**show interface switchport interfaces** *{IF_*PORTS}
Default	*IF_PORTS* Specify interfaces protocol vlan to display
Mode	Privileged EXEC
Example	The following example specifies that show interfacce switchport. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport trunk allowed vlan add** 2 Switch# **show interfaces switchport** GigabitEthernet 2

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport trunk allowed vlan add 2
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Trunk
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled: 2

Port is member in:
 Vlan            Name              Egress rule
------- ---------------------- -----------------
    1               default       Untagged
    2              VLAN0002         Tagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

35.20 SHOW MANAGEMENT-VLAN

Display information about management vlan.

Switch# **show management-vlan**

Syntax	**show management-vlan**
Mode	Privileged EXEC

Example	The following example specifies that show management vlan
	Switch# **show management-vlan**
	`Switch# show management-vlan`
	`    Management VLAN-ID : default(1)`
	`Switch#`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36. VOICE VLAN

The terms Voice VLAN or Auxiliary VLAN typically mean the same thing:
They are a feature which allows an access port which normally only accepts *untagged* traffic for a *single* VLAN to also accept *tagged* traffic for *a second* VLAN.

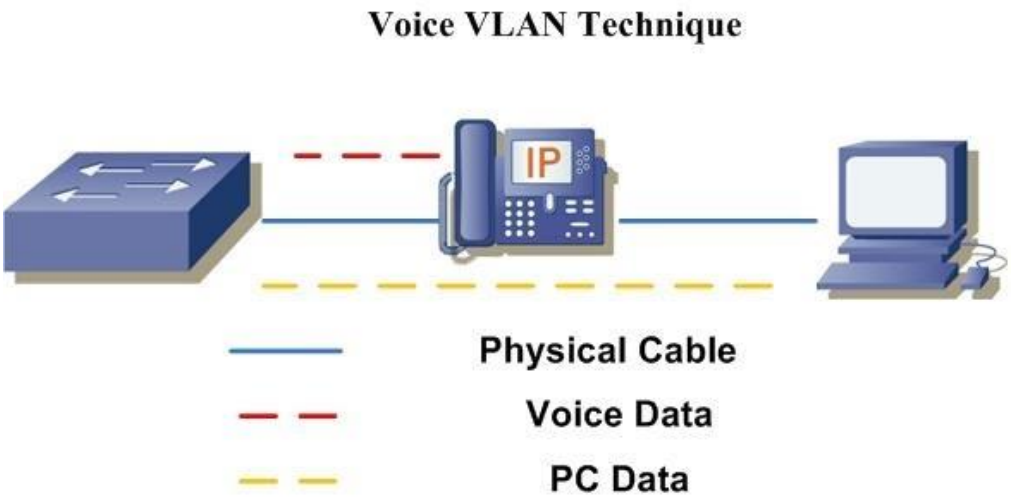


Fig 36.1 Voice VLAN concept

Voice VLAN Functionality

Imagine office cubicles. Imagine each cubicle contains a desk and a computer which an employee uses to connect to your corporate network. A lot of older office build outs, which already only have one LAN drop at each cubicle, simply cannot afford the additional cost or delays to pay another technician to crawl through all the ceilings and walls to run another LAN drop to each cubicle. This means the cubicles are limited to a single LAN drop per employee.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

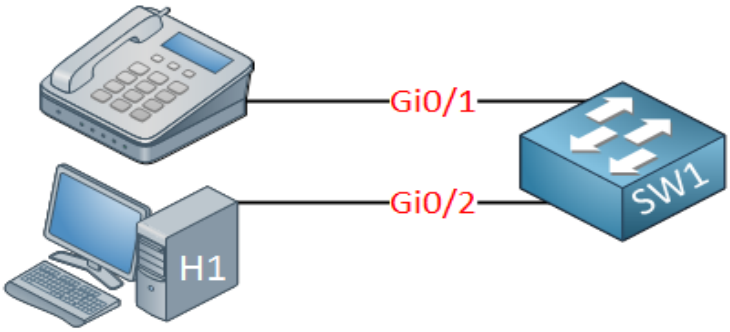


Fig 36.2 IP phone direct connection to switch

VOIP phone manufacturers were able to foresee this problem, and created another solution built right into the VOIP phones themselves. The majority of VOIP phones come with two Ethernet ports: One meant to face the wall jack (and subsequently, the corporate LAN), the other meant to face a PC: Traditionally, if you want to carry traffic for multiple VLANs on a single port, you would configure a Trunk port. This would allow traffic for multiple VLANs to traverse the single link. But typically traffic on trunk ports require tagging to distinguish which bits belong to one VLAN and which bits belong to another VLAN.

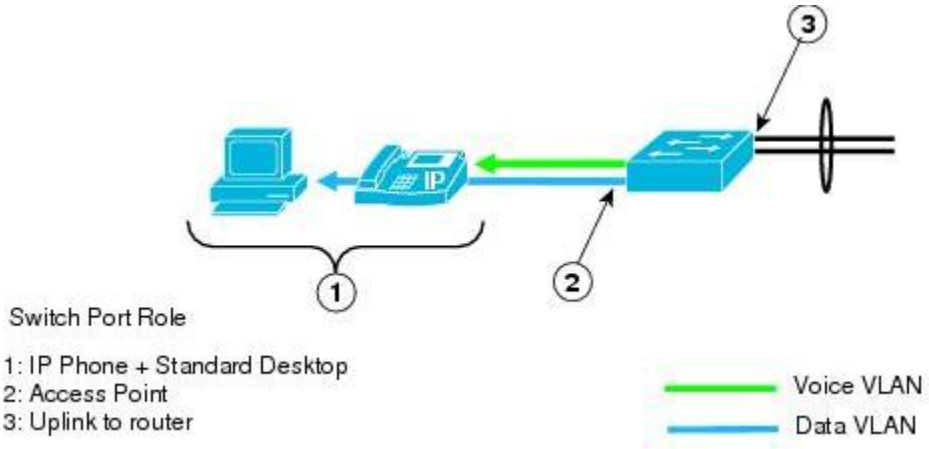


Fig 36.3 Voice and Data VLAN traffic

VOIP phones have the capacity to send and understand 802.1q VLAN tags, and can therefore be configured to send a VLAN tag for all the Voice traffic.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Host only send *untagged* traffic. As such, the switch must have a way to associate the received untagged traffic on the trunk port to a particular VLAN. This is the exact purpose of the Native VLAN.

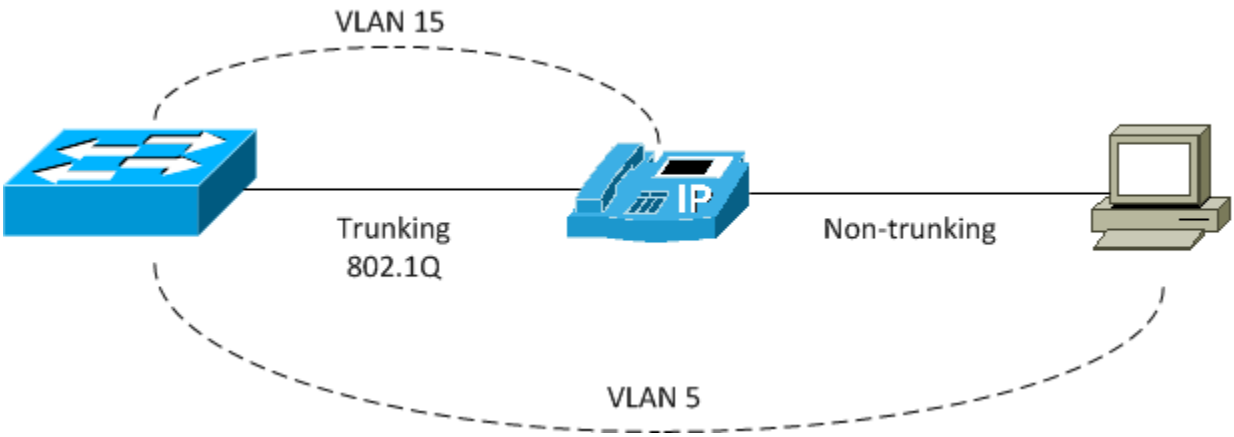


Fig 36.4 Trunking Concept

Therefore, in order to properly configure a single port to accommodate both a Voice and Data VLAN, you must first configure the interface as a Trunk port, then configure the Data VLAN as the Native VLAN:

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36.1 VOICE-VLAN (GLOBAL)

Use the voice vlan global configuration command to enable the functional Voice VLAN on the device. Use the no form of this command to disable voice vlan function. You can verify your setting by entering the show voice vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **voice-vlan**

Switch(config)# **no voice-vlan**

Syntax	**voice-vlan** **no voice-vlan**
Mode	Global Configuration

Example	The following example shows how to enable voice vlan.
	Switch#configure terminal
	Switch(config)# **voice-vlan vlan** {Vlan-ID}
	Switch# **show voice-vlan**
	`Switch(config)# voice-vlan vlan 2`
	`Switch(config)# exit`
	`Switch# show voice-vlan`
	`Administrate Voice VLAN state   : disabled`
	`Voice VLAN ID       : 2`
	`Voice VLAN Aging    : 1440 minutes`
	`Voice VLAN CoS      : 6`
	`Voice VLAN 1p Remark: disabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36.2 VOICE-VLAN (INTERFACE)

Use the voice vlan Interface configuration command to enable OUI voice VLAN configuration on an interface Use the no form of this command to disable voice vlan on an interfaces. You can verify your setting by entering the show voice vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)#**voice-vlan**

Switch(config-if)#**no voice-vlan**

Syntax	**voice-vlan** **no voice-vlan**
Mode	Interface Configuration
Example	The following example how to enable voice VLAN function in oui mode on an interface Switch#**configure terminal** Switch(config)#**interface range** gi3-5 Switch(config-if)#**voice-vlan** Switch# **show voice-vlan interfaces** gi1-8

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface range gi3-5
Switch(config-if-range)# voice-vlan
Switch(config-if-range)# end
Switch# show voice-vlan interfaces gi1-8
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 6
Voice VLAN 1p Remark: disabled

OUI table
   OUI MAC     |   Description
---------------+-----------------
   00:E0:BB    | 3COM
   00:03:6B    | Cisco
   00:E0:75    | Veritel
   00:D0:1E    | Pingtel
   00:01:E3    | Siemens
   00:60:B9    | NEC/Philips
   00:0F:E2    | H3C
   00:09:6E    | Avaya

  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |    Auto     | Src
gi2    | Disabled |    Auto     | Src
gi3    |  Enabled |    Auto     | Src
gi4    |  Enabled |    Auto     | Src
gi5    |  Enabled |    Auto     | Src
gi6    | Disabled |    Auto     | Src
gi7    | Disabled |    Auto     | Src
gi8    | Disabled |    Auto     | Src
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36.3 VOICE-VLAN VLAN

Use the voice vlan id global configuration command to configure the VLAN identifier of the voice VLAN statically. Use the **"no"** form of this command to restore voice vlan id to default. You can verify your setting by entering the show voice vlan Privileged EXEC command. You can verify your setting by entering the show voice vlan Privileged EXEC command identifier of the voice VLAN statically. Use the **"no"** form of this command to restore voice vlan id to default. You can verify your setting by entering the show voice vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **voice-vlan vlan** *<1-4094>*

Switch(config)# **no voice-vlan vlan** {Vlan-ID}

Syntax	**voice-vlan vlan** *<1-4094>* **no voice-vlan vlan**
Parameter	*<1-4094>* Specify the voice VLAN ID
Default	The default Voice VLAN ID is None
Mode	Global Configuration

Example	The following example shows how to set Voice vlan id. The vlan id must be created first.
	Switch#**configure terminal**
	Switch(config)# **voice-vlan vlan** 2
	Switch# **show voice-vlan**
	`Switch(config)# voice-vlan vlan 2`
	`Switch(config)# exit`
	`Switch# show voice-vlan`
	`Administrate Voice VLAN state   : enabled`
	`Voice VLAN ID       : 2`
	`Voice VLAN Aging    : 1440 minutes`
	`Voice VLAN CoS      : 6`
	`Voice VLAN 1p Remark: disabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36.4 VOICE-VLAN OUI-TABLE

Use the voice vlan oui-table global configuration command to add oui mac address to OUI Table. Use the **"no"** form of this command to remove all or specified oui mac address. You can verify your setting by entering the show voice vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **voice-vlan oui-table** A:B:C [DESCRIPTION]

Switch(config)# **no voice-vlan oui-table** [A:B:C]

Syntax	**voice-vlan oui-table** A:B:C [DESCRIPTION] **no voice-vlan oui-table** [A:B:C]
Parameter	A:B:C Specify OUI Mac address to add or remove DESCRIPTION Specify description of the specified MAC address to the voice VLAN OUI table.
Default	The system default has 8 oui addresses
Mode	Global Configuration
Example	This following example shows how to add OUI Mac. Switch#**configure terminal** Switch(config)# **voice-vlan oui-table** 00:01:02 "Test" Switch# **show voice-vlan interfaces all**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# voice-vlan oui-table 00:01:05 test_COMMANDO
Switch(config)# exit
Switch# show voice-vlan interfaces GigabitEthernet 1-8
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 6
Voice VLAN 1p Remark: disabled

OUI table
   OUI MAC    |   Description
--------------+-----------------
   00:E0:BB   | 3COM
   00:03:6B   | Cisco
   00:E0:75   | Veritel
   00:D0:1E   | Pingtel
   00:01:E3   | Siemens
   00:60:B9   | NEC/Philips
   00:0F:E2   | H3C
   00:09:6E   | Avaya
   00:01:02   | "Test"
   00:01:03   | commando
   00:01:04   | COMMANDO@TEST
   00:01:05   | test_COMMANDO

  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |    Auto     | Src
gi2    | Disabled |    Auto     | Src
gi3    |  Enabled |    Auto     | Src
gi4    |  Enabled |    Auto     | Src
gi5    |  Enabled |    Auto     | Src
gi6    | Disabled |    Auto     | Src
gi7    | Disabled |    Auto     | Src
gi8    | Disabled |    Auto     | Src
Switch#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36.5 VOICE-VLAN COS (GLOBAL)

Use the voice vlan cos global configurations command to configure the voice VLAN cos value and 1p remark function. Use the **"no"** form to restore to default mode. You can verify your setting by entering the show voice vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **voice-vlan cos** *<0-7>* **[remark]**

Switch(config)# **no voice-vlan cos**

Syntax	**voice-vlan cos** *<0-7>* **[remark]** **no voice-vlan cos**
Parameter	<0-7> Specify the voice VLAN Class of Service value in telephone oui mode remark Specify that the L2 user priority is remarked with the CoS value
Default	The default cos value is 6, remark is disabled.
Mode	Global Configuration

Example	The following example show how to set cos value and enable 1p remark function
	Switch#**configure terminal**
	Switch(config)# **voice-vlan cos 7 remark**
	Switch# **show voice-vlan**
	`Switch(config)# voice-vlan cos 7 remark`
	`Switch(config)# exit`
	`Switch# show voice-vlan`
	`Administrate Voice VLAN state   : enabled`
	`Voice VLAN ID       : 2`
	`Voice VLAN Aging    : 1440 minutes`
	`Voice VLAN CoS      : 7`
	`Voice VLAN 1p Remark: enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36.6 VOICE-VLAN COS (INTERFACE)

Use the voice vlan cos Interface configuration command to configure OUI voice VLAN cos mode configuration on an interface. Use the **"no"** form to restore to default mode. You can verify your setting by entering the show voice-vlan interfaces Privileged EXEC command.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)#**voice-vlan cos (src | all)**

Switch(config-if)#**no voice-vlan cos**

Syntax	**voice-vlan cos (src | all)** **no voice-vlan cos**
Parameter	**src** Specify QoS attributes are applied to packets with OUIs in the source MAC address. **all** Specify QoS attributes are applied to packets that are classified to the Voice VLAN.
Default	The default all port in Src mode.
Mode	Interface configuration
Example	The following example how to configure voice packet QoS attributes on an interface, Switch#**configure terminal** Switch(config)#**interface range** gi1-3 Switch(config-if)#**voice-vlan cos all** Switch# **show voice-vlan interfaces gi1-8**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# interface range gi1-3
Switch(config-if-range)# voice-vlan cos all
Switch(config-if-range)# end
Switch# show voice-vlan interfaces gi1-8
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 7
Voice VLAN ip Remark: enabled

OUI table
   OUI MAC    |   Description
--------------+-----------------
   00:E0:BB   | 3COM
   00:03:6B   | Cisco
   00:E0:75   | Veritel
   00:D0:1E   | Pingtel
   00:01:E3   | Siemens
   00:60:B9   | NEC/Philips
   00:0F:E2   | H3C
   00:09:6E   | Avaya
   00:01:02   | "Test"
   00:01:03   | commando
   00:01:04   | COMMANDO@TEST
   00:01:05   | test_COMMANDO

  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+----------
gi1    |  Enabled |    Auto     | All
gi2    | Disabled |    Auto     | All
gi3    |  Enabled |    Auto     | All
gi4    |  Enabled |    Auto     | Src
gi5    |  Enabled |    Auto     | Src
gi6    | Disabled |    Auto     | Src
gi7    | Disabled |    Auto     | Src
gi8    | Disabled |    Auto     | Src
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36.7 VOICE-VLAN MODE

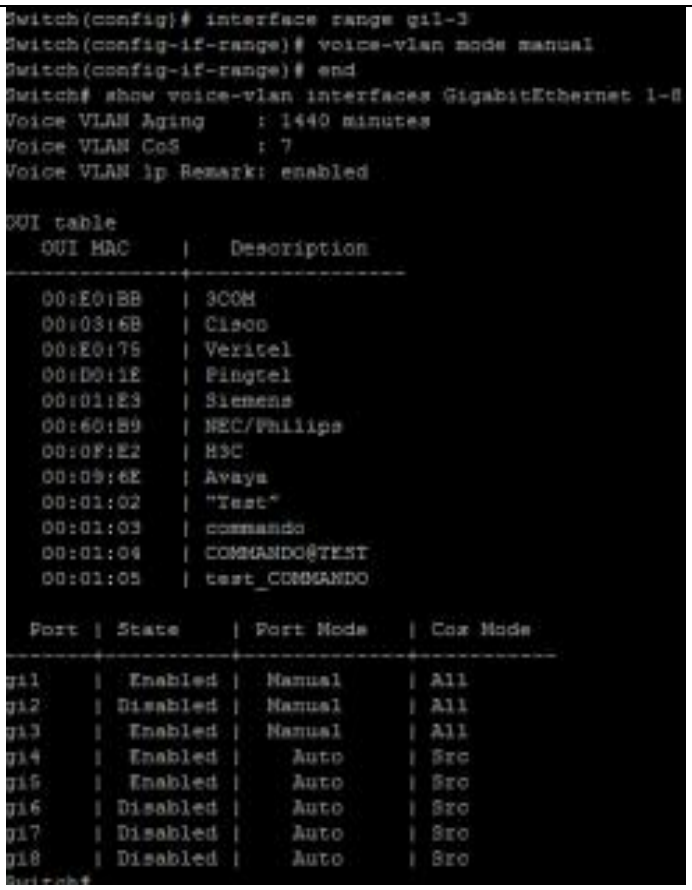
Use the voice-vlan mode global configuration command to configure the voice VLAN mode for interface. Use the **"no"** form to restore to default mode. You can verify your setting by entering the show voice-vlan interfaces Privileged EXEC command.

Switch#**configure terminal**
Switch(config)#**interface** {Interface-ID}
Switch(config-if)#**voice-vlan mode (auto|manual)**

Switch(config-if)#**no voice-vlan mode**

Syntax	**voice-vlan mode (auto|manual)** **no voice-vlan mode**
Parameter	**Auto** Specifies that the port is identified as a candidate to join the voice VLAN. When a packet with a source OUI MAC address that identifies the remote equipment as voice equipment is seen on the port, the port joins the voice VLAN as a tagged port. **manual** Specifies that the port is manually assigned to the voice VLAN.
Default	The default is auto mode.
Mode	Interface Configuration
Example	The following example how to configure voice mode to manual Switch#**configure terminal** Switch(config)#**interface range** gi1-3 Switch(config-if)#**voice-vlan mode manual** Switch# **show voice-vlan interfaces** GigabitEthernet 1-8

© 2024 COMMANDO Networks Inc., USA. All rights reserved.



```
Switch(config)# interface range gi1-3
Switch(config-if-range)# voice-vlan mode manual
Switch(config-if-range)# end
Switch# show voice-vlan interfaces GigabitEthernet 1-8
Voice VLAN Aging     : 1440 minutes
Voice VLAN CoS       : 7
Voice VLAN ip Remark: enabled

OUI table
   OUI MAC     |   Description
---------------+-----------------
   00:E0:BB    | 3COM
   00:03:6B    | Cisco
   00:E0:75    | Veritel
   00:D0:1E    | Pingtel
   00:01:E3    | Siemens
   00:60:B9    | NEC/Philips
   00:0F:E2    | H3C
   00:09:6E    | Avaya
   00:01:02    | "Test"
   00:01:03    | commando
   00:01:04    | COMMANDO@TEST
   00:01:05    | test_COMMANDO

  Port | State     | Port Mode    | Cos Mode
-------+-----------+--------------+-----------
gi1    |  Enabled  |  Manual      | All
gi2    | Disabled  |  Manual      | All
gi3    |  Enabled  |  Manual      | All
gi4    |  Enabled  |    Auto      | Src
gi5    |  Enabled  |    Auto      | Src
gi6    | Disabled  |    Auto      | Src
gi7    | Disabled  |    Auto      | Src
gi8    | Disabled  |    Auto      | Src
Switch#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36.8 VOICE-VLAN AGING-TIME

Use the voice vlan aging-time global configuration command to configure the voice VLAN aging timeout. Use the **"no"** form to restore to default time. You can verify your setting by entering the show voice vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **voice-vlan aing-time** *<30-65536>*

Switch(config)# **no voice-vlan aing-time**

Syntax	**voice-vlan aing-time** *<30-65536>* **no voice-vlan aing-time**
Parameter	*<30-65536>* Specify the voice VLAN aging timeout interval in minutes
Default	The default aging-timeout value is 1440 minutes
Mode	Global Configuration

Example	The following example shows how to set aging time.
	Switch#**configure terminal**
	Switch(config)# **voice-vlan aging-time** 720
	Switch# **show voice-vlan**
	`Switch(config)# voice-vlan aging-time 720`
	`Switch(config)# end`
	`Switch# show voice-vlan`
	`Administrate Voice VLAN state   : enabled`
	`Voice VLAN ID       : 2`
	`Voice VLAN Aging    : 720 minutes`
	`Voice VLAN CoS      : 7`
	`Voice VLAN 1p Remark: enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

36.9 SHOW VOICE-VLAN

Use the show voice vlan command in EXEC mode to display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is OUI.

Switch# **show voice-vlan**
Switch# **show voice-vlan interfaces** *{IF_PORTS}*

Syntax	**show voice-vlan** **show voice-vlan interfaces** *{IF_PORTS}*
Parameter	*IF_PORTS* Specifies interfaces to display voice VLAN settings in oui mode
Mode	Privileged EXEC

Example	The following example show how to display voice vlan oui mode settings
	Switch# **show voice-vlan**
	`Switch# show voice-vlan`
	`Administrate Voice VLAN state   : enabled`
	`Voice VLAN ID       : 2`
	`Voice VLAN Aging    : 720 minutes`
	`Voice VLAN CoS       : 7`
	`Voice VLAN 1p Remark: enabled`
	`Switch#`
	
	Switch# **show voice-vlan interfaces GigabitEthernet 1-4**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# show voice-vlan interfaces GigabitEthernet 1-4
Voice VLAN Aging    : 720 minutes
Voice VLAN CoS      : 7
Voice VLAN 1p Remark: enabled

OUI table
   OUI MAC     |   Description
---------------+-----------------
   00:E0:BB    | 3COM
   00:03:6B    | Cisco
   00:E0:75    | Veritel
   00:D0:1E    | Pingtel
   00:01:E3    | Siemens
   00:60:B9    | NEC/Philips
   00:0F:E2    | H3C
   00:09:6E    | Avaya
   00:01:02    | "Test"
   00:01:03    | commando
   00:01:04    | COMMANDO@TEST
   00:01:05    | test_COMMANDO

  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+-----------
gi1    |  Enabled |  Manual     | All
gi2    | Disabled |  Manual     | All
gi3    |  Enabled |  Manual     | All
gi4    |  Enabled |    Auto     | Src
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37. IPv4 Management and Interfaces

To manage the device by using the telnet configuration utility, the IPv4 device management IP address by default is 192.168.0.1 is access IP. You can set VLAN IP address accordingly to access switch and you can also create loopback interfaces.

Types of Interfaces in E3000 Switch

Trunk interface:

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

Hybrid interface:

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

Tunnel Interface:

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

Access Interface:

An access interface generally connects to a PC/Host or server that cannot identify VLAN tags or is used when VLANs do not need to be differentiated. Access interfaces

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

can only receive and send untagged frames and can add only a unique VLAN tag to untagged frames.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.1 IPv4 Routes

Static IPv4 Routes: A static IPv4 route is a pre-determined path that network information must follow to reach a specific host or network.
Destination: To Specify the destination IPv4 address of the packets.
Subnet Mask: To Specify the subnet mask of the destination IPv4 address.
Next Hop: To Specify the IPv4 gateway address to which the packet should be sent next.
Distance: Specify the administrative distance, which is the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv4 routing table. The valid value ranges from 1 to 255 and the default value is 1.

Default IPv4 Routes: The default route is a special type of static route, which specifies a path that the device should use if the destination address is not included in any other routes. Therefore, a default route can solve this problem, if no route to the destination is specified, the device will send the packets to a specific device, that is, the default gateway. Then the default gateway will forward the packets to the destination. A default route consists of three parts mainly Destination, Subnet Mask and Next Hop (Gateway). The destination and subnet mask are both the fixed value 0.0.0.0, which means arbitrary destination IP addresses that are not matched by other route entries.

Routing table: Routing table is used for a Layer 3 device (in this configuration guide, it means the switch) to forward packets to the correct destination. When the switch receives packets of which the source IP address and destination IP address are in different subnets, it will check the routing table, find the correct outgoing interface then forward the packets. The routing table mainly contains two types of routing entries: Dynamic routing entries and Static routing entries.
Dynamic routing entries: Dynamic routing entries are automatically generated by the switch for connected networks. The switch uses dynamic routing protocols to automatically calculate the best route to forward packets.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Static routing entries: Static routing entries are manually added non-aging routing entries. In a simple network with a small number of devices, you only need to configure static routes to ensure that the devices from different subnets can communicate with each other. On a complex large-scale network, static routes ensure stable connectivity for important applications because the static routes remain unchanged even when the topology changes.

To reduce costs, generally most enterprises use L2+/L3 switches to connect internal devices and an egress router/L3 Switch to connect to an ISP network for access the ISP network, the Layer 3 switch and egress router need to interwork at Layer 3. Most Layer 3 switches do not support routed interfaces or IP based interfaces or support limited routed interfaces. Generally, a VLAN interface is used as a Layer 3 interface to communicate with other Layer 3 interface of the router/ L3 switch and then static route or a dynamic routing protocol is configured to implement Layer 3 connectivity between the L3 switch and egress router/ other L3 Switch.

Interface based VLAN assignment is the simplest and most effective method which is deployed in E3000 Switch. VLANs are assigned based on interfaces. After an interface is added to a VLAN, the interface can forward packets from the VLAN. Ethernet interfaces are classified into access, trunk, and hybrid interfaces according to the connected interfaces to the Ethernet interfaces and number of VLANs from which untagged frames are permitted to access interface. The E3000 switch processes only tagged frames and an access interface connected to devices only receive and send untagged frames, so the access interface needs to add a VLAN tag to received frames. That is, you must configure the default VLAN for the access interface. After the default VLAN is configured, the access interface joins the VLAN. An access interface needs to process only untagged frames. If a user connects a switching device to a user side interface without permission, the user side interface may receive tagged frames. You can configure the user side interface to discard tagged frames, preventing unauthorized access.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.2 STATIC ROUTING

Static routing is a type of network routing technique for manual configuration and selection of a network route, usually managed by the network administrator.

Static Routing

Routing is one of the most essential procedures in data communication. It ensures that data travels from one network to another with optimal speed and minimal delay, and that its integrity is maintained in the process. Static routing is considered the simplest form of routing.

Broadly, routing is performed in two different ways:

- Dynamic routing continuously updates its routing table with paths and their cost/metric, while making optimal routing decisions based on changing network operating environments.
- Static routing performs routing decisions with preconfigured routes in the routing table, which can be changed manually only by administrators. Static routes are normally implemented in those situations where the choices in route selection are limited, or there is only a single default route available. Also, static routing can be used if you have only few devices for route configuration and there is no need for route change in the future.

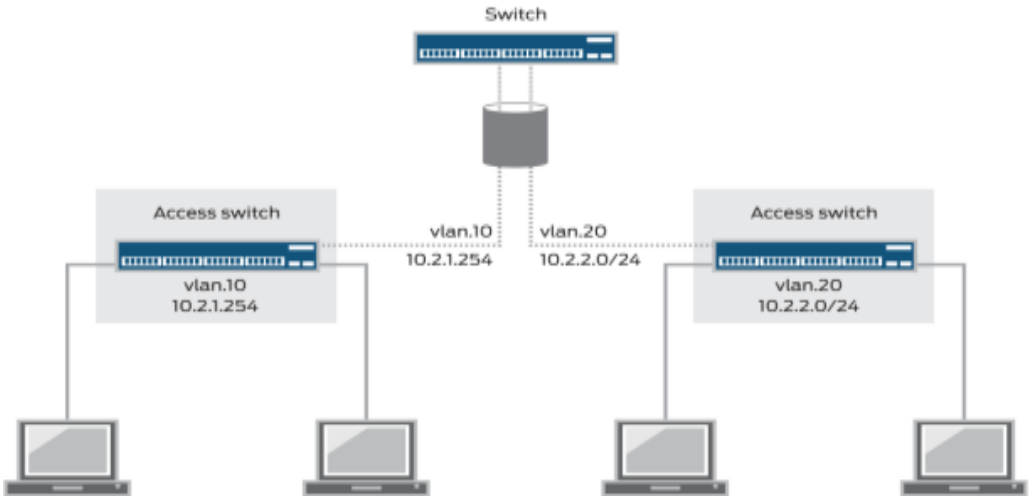


Fig 37.1 Static route for inter LAN routing

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.3 VLAN INTERFACE

Use the interface vlan global configuration command to config ip Interface on the device. Use the ip address command in vlan interface mode to configure the Device's ip address. Use the **"no"** ip address command to delete the configured ip address. Use the **"no"** interface vlan command to delete ip interface on the device. You can verify your setting by entering the show ip interface vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **interface vlan**{VLAN-ID}
Switch(config-if)# **ip address** {ip-addr}/{mask}

Switch(config)# **no interface vlan** {VLAN-ID}
Switch(config-if)# **no ip address**

Syntax	**interface vlan** **ip address ipaddr mask** **no interface vlan** **no ip address**
Parameter	**ipaddr** Specify IPv4 address for switch **mask** Specify net mask address for switch
Default	The vlan interface and ip address are not configured by default.
Mode	Global configuration and vlan interface configuration

Example	The following example shows how to config ip interface.
	Switch#**configure terminal**
	Switch(config)# **interface vlan** 2
	Switch(config-if)# **ip address** 192.168.1.2/24
	Switch# **show ip interface**
	`Switch#  show ip interface`
	
	`IP Address  I/F  I/F Status admin/oper  Type  Status  Roles`
	`1.1.1.1/30  Loopback1  UP/UP  Static  Valid  primary`
	`192.168.0.1/24  VLAN 1  UP/UP  Static  Valid  primary`
	`192.168.1.2/24  VLAN 2  UP/UP  Static  Valid  primary`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.4 IPV4 ROUTES

Use the ip route command in global mode to configure a static route rule. Use the **"no"** ip route command to delete a static routing rule. You can verify your setting by entering the show ip route Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **ip route** {dest-ipaddr} **mask** {Dest-router-ipaddr}

Switch(config)# **no ip route** {dest-ipaddr} **mask** {Dest-router-ipaddr}

Syntax	**ip route** dest-ipaddr **mask router-ipaddr** **no ip route** dest-ipaddr **mask router-ipaddr**
Parameter	**dest-ipaddr** Destination ip address prefix **mask** Destination ip address prefix mask **router-ipaddr** Forwarding router's ip address
Default	Static route is not configured by default.
Mode	Global Configuration mode.
Example	The following example shows how to configure a static route. Switch#**configure terminal** Switch(config)# **vlan** 2 Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport trunk allowed vlan add** 2 Switch(config)# **interface vlan** 2 Switch(config-if)# **ip address** 192.168.3.1 255.255.255.0 Switch(config)# **ip route** 1.1.1.1 255.0.0.0 192.168.3.11 Switch# **show ip route**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch(config)# vlan 2
Switch(config-vlan)# interface GigabitEthernet 2
Switch(config-if)# switchport trunk allowed vlan add 2
Switch(config-if)# exit
Switch(config)# interface vlan 2
Switch(config-if)# ip address 192.168.2.1 255.255.255.0
Switch(config-if)# ip route 1.1.1.1 255.0.0.0 192.168.3.11
Switch(config)# exit
Switch# show ip route
Codes: > - best, C - connected, S - static

S>  1.0.0.0/8 [1/1] via 192.168.3.11, VLAN 2
C>  192.168.1.0/24 is directly connected, VLAN 2
C>  192.168.2.0/24 is directly connected, VLAN 2
C>  192.168.3.0/24 is directly connected, VLAN 2
C>  192.168.100.0/24 is directly connected, MGMT VLAN
Switch#
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.5 IPV4 ARP

Use the arp command to add a static arp entry. Use the **"no"** arp command to delete a static arp entry. You can verify your setting by entering the show arp Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **arp** {ip-addr mac-addr} **vlan** {VLAN-ID}

Switch(config)# **no arp** {ip-addr mac-addr} **vlan** {VLAN-ID}

Syntax	**arp**{ip-addr mac-addr} **vlan** {VLAN-ID} **no arp**{ip-addr mac-addr} **vlan** {VLAN-ID}
Parameter	**ip-addr** IP address of ARP entry **mac-addr** MAC address of ARP entry **vlanid** Vlan ID of this arp entry
Default	The device contains ARP entries of the vlan interface.
Mode	Global Configuration mode
Example	The following example shows how to configure and view a static arp entry. Switch#**configure terminal** Switch(config)# **arp** 192.168.3.22 00:00:11:11:11:11 **vlan** 2 Switch# **show arp** Switch(config)# arp 192.168.3.22 00:00:11:11:11:11 vlan 2 Switch(config)# exit Switch# show arp VLAN Interface IP address HW address Status vlan 1 192.168.100.1 ac:a0:16:42:45:40 Dynamic vlan 1 192.168.100.4 08:00:23:3b:02:3b Dynamic vlan 1 192.168.100.25 e0:d5:5e:d0:dd:e5 Dynamic vlan 1 192.168.100.27 e0:d5:5e:32:b1:92 Dynamic vlan 1 192.168.100.54 50:3e:aa:26:24:3c Dynamic vlan 1 192.168.100.69 e0:d5:5e:32:b1:22 Dynamic vlan 2 192.168.3.22 00:00:11:11:11:11 Static Total number of entries: 7

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.6 IPV6 INTERFACE

Use the interface vlan global configuration command to config ip interface on the device. Use the ipv6 enable command in vlan interface mode to enable ipv6 function. Use the **"no"** ipv6 enables command to disable ipv6 function. Use the **"no"** interface vlan command to delete ip interface on the device. You can verify your setting by entering the show ipv6 interface vlanPrivileged EXEC command.

Switch#**configure terminal**
Switch(config)# **interface vlan** {VLAN-ID}
Switch(config-if)# **ipv6 enable**

Switch(config-if)# **no ipv6 enable**

Syntax	**interface vlan** {VLAN-ID} **ipv6 enable** **no interface vlan** {VLAN-ID} **no ipv6 enable**
Parameter	Vlanid Vlan id for vlan interface
Default	The vlan interface are not configured by default. IPv6 is disabled.
Mode	Global configuration and vlan interface configuration

Example	The following example shows how to config ip interface.
	Switch#**configure terminal**
	Switch(config)# **interface vlan 2**
	Switch(config-if)# **ipv6 enable**
	Switch# **show ipv6 interface vlan 2**
	`Switch(config)# interface vlan 2`
	`Switch(config-if)# ipv6 enable`
	`Switch(config-if)# end`
	`Switch# show ipv6 interface vlan 2`
	`VLAN 2 is up/down`
	`IPv6 is enabled, link-local address is fe80::2e0:4cff:fe00:0 (TENTATIVE)`
	`IPv6 Forwarding is disabled`
	`No global unicast address is configured`
	`ND DAD is enabled, number of DAD attempts: 1`
	`Stateless autoconfiguration is enabled`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.7 IPV6 ADDRESS

Use the ipv6 address command in vlan interface mode to config a manual ipv6 address. Use the **"no"** ipv6 address command in vlan interface mode to delete all manual ipv6 addresses on this vlan interface. You can verify your setting by entering the show ipv6 interface vlan Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **interface** {Interface-ID}
Switch(config-if)# **ipv6 address ipv6-addr**

Switch(config-if)# **no ipv6 address**

Syntax	**ipv6 address ipv6-addr** **no ipv6 address**
Parameter	ipv6-addr Manually configured ipv6 address
Default	The vlan interface are not configured by default. IPv6 is disabled
Mode	Global configuration and vlan interface configuration

Example	The following example shows how to config ip interface.
	Switch#**configure terminal**
	Switch(config)# **interface vlan** 2
	Switch(config-if)# **ipv6 address** 2001:01::01:01/64
	Switch# **show ipv6 interface vlan** 2
	`Switch(config)# interface vlan 2`
	`Switch(config-if)# ipv6 address 2001:01::01:01/64`
	`Switch(config-if)# end`
	`Switch# show ipv6 interface vlan 2`
	`VLAN 2 is up/down`
	`IPv6 is enabled, link-local address is fe80::2e0:4cff:fe00:0 (TENTATIVE)`
	`IPv6 Forwarding is disabled`
	`Global unicast address(es):`
	`IPv6 Global Address Type`
	`2001:1::1:1/64 (TEN) Manual`
	`ND DAD is enabled, number of DAD attempts: 1`
	`Stateless autoconfiguration is enabled`

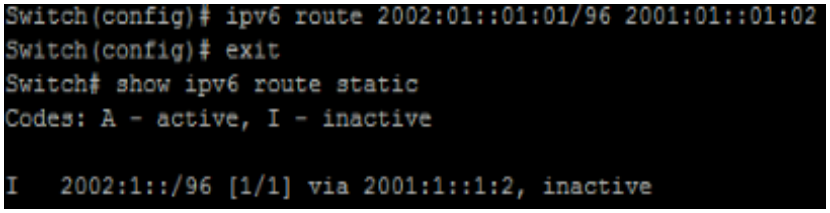
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.8 IPV6 ROUTES

Use the ipv6 route command to configure a static ipv6 routing entry. Use the **"no"** ipv6 address command to delete a static ipv6 routing entry. You can verify your setting by entering the show ipv6 route staticPrivileged EXEC command.

Switch#**configure terminal**
Switch(config)# **ipv6 route ipv6-addr/length route-ipv6-addr**

Switch(config)# **no ipv6 address ipv6-addr/length**

Syntax	**ipv6 route ipv6-addr/length route-ipv6-addr** **no ipv6 address ipv6-addr/length**
Parameter	**ipv6-addr/length** Destination ipv6 prefix and length **route-ipv6-addr** Forwarding router's ipv6 address
Default	The ipv6 routing entry is not configured by default.
Mode	Global configuration and vlan interface configuration.
Example	The following example shows how to configure an ipv6 routing entry. Switch#**configure terminal** Switch(config)# **ipv6 route 2002:01::01:01/96 2001:01::01:02** Switch# **show ipv6 route static** 

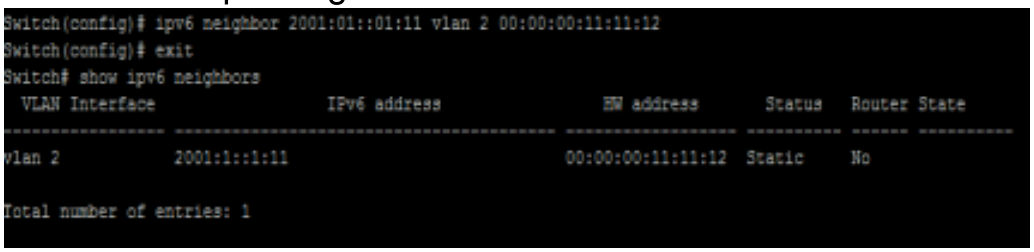
© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.9 IPV6 NEIGHBORS

Use the ipv6 neighbor command to configure a static ipv6 neighbor entry. Use the **"no"** ipv6 neighbor command to delete ipv6 neighbor entry. You can verify your setting by entering the show ipv6 neighbors Privileged EXEC command.

Switch#**configure terminal**
Switch(config)# **ipv6 neighbor [ipv6-addr] vlan [vlan-id] macaddr**

Switch(config)# **no ipv6 neighbor**

Syntax	**ipv6 neighbor** ipv6-addr **vlan** vlan-id **macaddr** **no ipv6 neighbor**
Parameter	**ipv6-addr** Neighbor ipv6 address **vlanid** Vlan interface number **macaddr** MAC address of ipv6 neighbor entry
Mode	Global configuration
Example	The following example shows how to configure an ipv6 neighbor entry. Switch#**configure terminal** Switch(config)# **ipv6 neighbor** 2001:01::01:11 **vlan** 2 00:00:00:11:11:12 Switch# **show ipv6 neighbors** 

```
Switch(config)# ipv6 neighbor 2001:01::01:11 vlan 2 00:00:00:11:11:12
Switch(config)# exit
Switch# show ipv6 neighbors
  VLAN Interface               IPv6 address                HW address       Status   Router State
---------------- ------------------------------------- ----------------- ---------- ------ ----------
vlan 2           2001:1::1:11                          00:00:00:11:11:12  Static     No

Total number of entries: 1
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.10 RIP ROUTES

Routing Information Protocol (RIP) is used in small-scale networks, having hop count less than 16. It is distance-vector routing protocol & exchanges routing information through User Datagram Protocol (UDP) packets with port number 520. RIP employs the hop count as the metric to measure the distance to the destination. In RIP, by default, the number of hops from the router to its directly connected network is 0. The number of hops from the Router to a network that is reachable through another Router is 1, and so on. The hop count (the metric) equals the number of Routers along the path from the local network to the destination network. To speed up route convergence, RIP defines the hop count as an integer that ranges from 0 to 15. A hop count that is greater than or equal to 16 is classified as infinite, indicating that the destination network or host is unreachable. Due to the hop limit, RIP is not applicable to large-scale networks.

RIP Versions

RIP version 1 (RIP-1), a classful routing protocol

RIP version 2 (RIP-2), a classless routing protocol

RIP supports split horizon, poison reverse, and triggered update, which improves the performance and prevents routing loops. It is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source & the destination network. It is one of a family of IP Routing protocols & is an Interior Gateway Protocol (IGP) designed to distribute routing information within an Autonomous System (AS).

Basically, RIP is a distance vector routing protocol which has default AD value 120 & works on the application layer of OSI model with port number 520. Typically, the best path is the path with the fewest hops. A hop is another router through which packets must travel to reach the destination. If RIP receives a RIP update from another router/switch that contains a path with fewer hops than the path stored in the route table, the system replaces the older route with the newer one. The system then

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

includes the new path in the updates it sends to other RIP routers. A router/switch running RIP sends the contents of its routing table to each of its adjacent routers every 30 seconds by default.

Features of RIP

1. Updates of the network are exchanged periodically.

2. Updates (routing information) are always broadcast.

3. Full routing tables are sent in updates.

4. Routers/Switches always trust on routing information received from neighbor routers. This is also known as Routing on rumor.

The disadvantages of RIP include:

Increased network traffic: RIP checks with its neighboring routers every 30 seconds, which increases network traffic.

Maximum hop count limitation: RIP has a maximum hop count of 15, which means that on large networks, other remote routers may not be able to be reached.

Comparison of RIP v1 & RIP v2

RIPv1	RIPv2
Classful	Classless
Automatic summarization to the class boundary	Manual summarization on per interface basis
Network masks not included in the advertisements	Network masks included in the advertisements
Advertisements use broadcast destination address 255.255.255.255	Advertisements use reserved multicast destination address 224.0.0.9
No authentication support	2 authentication methods (clear text, MD5)

Steps to Configure RIP in E3000 Switch

1. Create any VLAN for routing purpose from 2 to 4094.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2. Assign IP address to created VLAN as per other connected router/switch IP address as they required to be in same network.

3. Go to Interface where you connected L3 Switch/Router and assign Created VLAN in access mode.

4. Enable RIP.

5. Add connected Network ID to RIP

6. Check the learn route with RIP.

Switch#**configure terminal**
Switch(config)# **rip**
Switch(config)# **no rip**

Syntax	**Rip** **no rip**
Parameter	Network ID
Default	RIP is not configured by default.
Mode	Global Configuration mode.
Example	The following example shows how to configure a RIP route. Switch#**configure terminal** Switch(config)# **interface vlan2** Switch(config-if)#**ip address 192.168.1.2/24** Switch(config-if)#**interface gi1** Switch(config-if)#**switchport mode access** Switch(config-if)#**switchport access vlan 2** Switch(config-if)# **exit** Switch(config)# **router-id** 1.1.1.1 Switch(config)# **rip** Switch(config-rip)# **network** 192.168.0.0/24 Switch(config-rip)# **network** 192.168.1.0/24

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# config terminal
Switch(config)# interface vlan2
Switch(config-if-vlan2)#  ip address 192.168.1.2/24
Switch(config-if-vlan2)# interface gil
Switch(config-if-gil)#  switchport mode access
Switch(config-if-gil)#  switchport access vlan 2
Switch(config-if-gil)# exit
Switch(config)# router-id  1.1.1.1
```

Switch# show ip route

```
Switch#  show ip route
Codes: > - best, C - connected, S - static R - rip
 O - ospf, I - isis, B - BGP

C>  1.1.1.0/30 is directly connected, Loopback1
C>  192.168.0.0/24 is directly connected, VLAN 1
C>  192.168.1.0/24 is directly connected, VLAN 2
R>  192.168.2.0/24 [120/2] via 192.168.1.1, VLAN 2
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

37.11 OSPF ROUTES

OSPF is an Interior Gateway Protocol (IGP) is link-state Interior Gateway Protocol (IGP) developed by the Internet Engineering Task Force (IETF). OSPF Version 2 as defined in RFC 2328 is designed for IPv4. OSPF constructs network topologies and routing tables by dividing an Autonomous System (AS) into one or more logical areas, Advertising routes by sending Link State Advertisements (LSAs), Exchanging OSPF packets between devices in an OSPF area to synchronize routing information.

In an OSPF network, each router generates a link-state advertisement (LSA) based on its surrounding network topology and transmits this LSA in an update packet to other routers in the network. The OSPF works by Exchanging Hello packets to establish OSPF neighbor relationships, Flooding LSAs to advertise link state information form their LSDBs to create a weighted, directed graph, Using an SPF algorithm to calculate and generate routes, Maintaining and updating routing tables by any topology changes.

OSPF packets

Hello packet: Hello packets are sent periodically by OSPF-enabled interfaces to discover and maintain OSPF neighbor relationships. These packets contain information about the Designated Router (DR), Backup Designated Router (BDR), and known neighbors on the same network.

Database Description (DD) packet: After an adjacency is established, it uses DD packets to describe their own LSDBs for LSDB synchronization. A DD packet contains the header of each LSA in an LSDB and is the summary of all LSAs.

Link State Request (LSR) packet: After DD packets exchanged, they send LSR packets to request each other's LSAs. The LSR packets contain the summaries of the requested LSAs.

Link State Update (LSU) packet: It uses an LSU packet to transmit LSAs requested by its neighbors or to flood its own updated LSAs. The LSU packet contains a set of LSAs.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Link State Acknowledgment Packets: These packet to make the flooding of link state advertisements reliable, flooded advertisements are explicitly acknowledged. This acknowledgment is accomplished through the sending and receiving of Link State Acknowledgment packets.

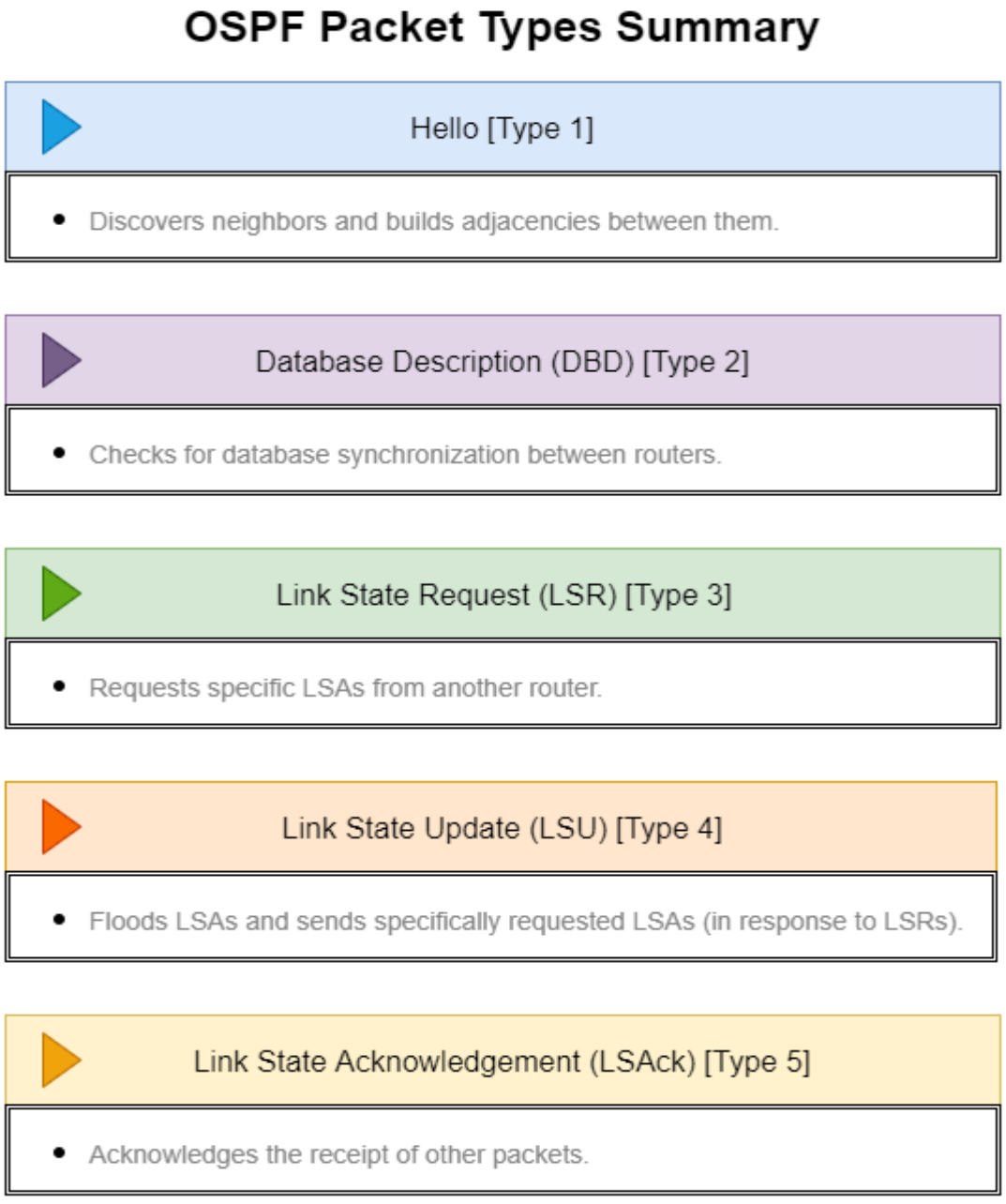


Fig 37.11.1 OSPF Packet type summary

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

OSPF Network Types

Broadcast: Networks using Ethernet or Fiber Distributed Data Interface (FDDI) at the link layer are broadcast networks by default.

Non-Broadcast Multi-Access (NBMA): Networks using frame relay (FR) or X.25 at the link layer are NBMA networks by default.

Point-to-Multipoint (P2MP): No networks are P2MP networks by default, regardless of the link layer protocol used by the network. Networks may be changed to P2MP networks. Typical practice is to change partial-meshed NBMA networks to P2MP networks.

Point-to-Point (P2P): Networks using Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), or Link Access Procedure Balanced (LAPB) at the link layer are P2P networks.

OSPF Network Type	Uses DR/BDR	Default Hello/Dead Interval (seconds)	Dynamic Neighbor Discovery	More Than Two Routers Allowed in Subnet?
Point-to-point	No	10/40	Yes	No
Broadcast	Yes	10/40	Yes	Yes
Nonbroadcast	Yes	30/120	No	Yes
Point-to-multipoint	No	30/120	Yes	Yes
Point-to-multipoint nonbroadcast	No	30/120	No	Yes
Loopback	No	—	—	No

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Common terms used in OSPF Process

OSPF Routers

The four types of OSPF routers as follows:

Internal routers: Internal routers are routers that belong to the same OSPF region as their directly connected networks. Because they belong to only one area, these routers have a single link-state database.

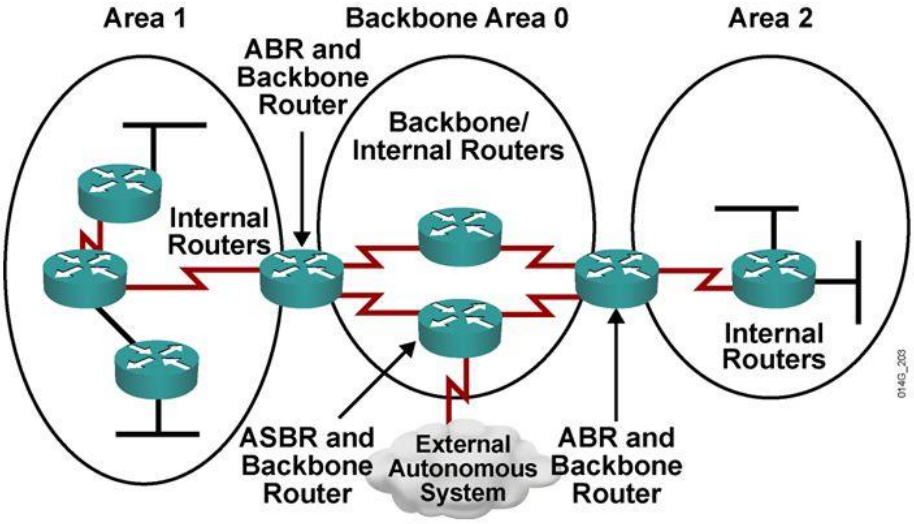
Area Borders Routers (ABRs): They are linked to various OSPF areas, a network can have several ABRs.

Autonomous Systems Boundary Routers (ASBRs): They are connected to many ASs and communicate with routers in other ASs to exchange routing information. The transferred external routing information is advertised by ASBRs throughout their AS.

Backbone Routers: Backbone routers are routers with interfaces that exclusively connect to the backbone area (BRs).

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Types of OSPF Routers



Router ID

A router ID is a 32-bit integer, which uniquely identifies an OSPF router in an AS. Each OSPF router has a router ID. A router ID is in the same format as an IP address. To ensure OSPF stability in actual network deployment, it is recommended that the IP address of a loopback interface on a router be used as the router ID of this router. A router ID can be manually configured or automatically selected by a router. If no router ID is manually configured for a router, the router automatically selects an interface IP address as its router ID.

The router ID selection rules are as follows:

1. The router preferentially selects the largest IP address among loopback interface addresses as the router ID.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2. If no loopback interface is configured, the router selects the largest IP address among interface addresses as the router ID.

3. A switch can obtain a router ID again only after a router ID is reconfigured for the switch or an OSPF router ID is reconfigured and the OSPF process restarts.

DR/BDR Election process

DR election rules are used to elect a DR only when routers with different router IDs or configured with different DR priorities are started at the same time. The election rules are that the device with the highest DR priority is elected as DR and the device with the second highest DR priority as BDR. A router with a DR priority of 0 can be a DR other only. If routers have the same DR priority, the router with the greatest router ID is elected as the DR, the router with the second greatest router ID becomes the BDR, and other routers are DR others.

Area

There are five types of OSPF areas as follows.

Backbone area (area 0): The backbone area also called Area 0 or area 0.0.0.0 forms the core of OSPF networks. All other areas should be connected to the backbone area either by a direct link or by virtual link configuration. It is required to have interfaces in both backbone area and (at least one) non-backbone area is called Area Border Routers (ABR). Inter area routing happens via ABRs. The backbone area is the logical and physical structure for the OSPF domain and is attached to all non-zero areas in the OSPF domain. The backbone area is responsible for distributing routing information between non-backbone areas. The backbone must be contiguous and provides backbone connectivity via interfaces or virtual links.

Standard area: Regular (nonbackbone) areas can have several subtypes: standard area, stub area, totally stubby area, not-so-stubby area (NSSA), and totally stubby NSSA. It is basically a nonbackbone area that must be connected to the backbone area it accepts intra-area, inter-area, external and a default route.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

Stub Area: It has a single exit point (ABR) typically used in hub and spoke network & It accepts intra-area routes but does not accept external summary routes from non-OSPF sources. It uses default route to send packets to an external network

Totally Stubby Area: Cisco proprietary & it does not accept external AS routes or inter-area routes; recognizes only intra-area routes and the default route

NSSA (Not-So-Stubby Atra): It recognizes intra-area, inter-area routes and the default route (0.0.0.0) & allows external routes from an ASBR but these routes are marked with O N1 or O N2

Totally Stubby NSSA: Cisco proprietary & It does not accept external AS routes or inter-area routes. It recognizes only intra-area routes and the default route and allows local ASBR only and thereby external routers this router inserts into the area are marked with O N1 or O N2

LSA

Link State Advertisements (LSA) are flooding updates which allow the OSPF network to create a map of the network. It is based on Dijkstra's Shortest Path First Algorithm.

LSA Type 1 (Router LSA): It describes the interfaces of the local router that are participating in OSPF and the neighbors the local OSPF speaker has established.

LSA Type 2 (Network LSA): The Type 2 LSA is sent by the Designated Router into the local area. This LSA describes all of the routers that are attached to that Ethernet segment.

LSA Type 3 (Summary LSA): The Summary (Type 3) LSA is used for advertising prefixes learned from the Type 1 and Type 2 LSAs into a different area. The Area Border Router (ABR) separates areas, and it is this device that advertises the Type 3 LSA.

LSA Type 4 (Summary ASBR LSA): The Autonomous System Boundary Router (ASBR) to inform routers in different areas about the existence of ASBR, the Type 4 LSA is

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

used. This Summary LSA provides the router ID of the ASBR. Area Border Router is responsible for this information into the next area.

LSA Type 5 (Autonomous system external LSA): It is used for the actual prefixes that are coming in from the other ASBR. The OSPF ASBR creates these LSAs and they are sent to the Area Border Routers for used in other areas.

LSA Type 6 (Multicast OSPF LSA): It is used for Multicast OSPF.

LSA Type 7 (Not-so-stubby area LSA): An NSSA makes use of type 7 LSAs, which are essentially type 5 LSAs in disguise. This allows an ASBR to advertise external links to an ABR, which converts the type 7 LSAs into type 5 before flooding them to the rest of the OSPF domain.

LSA Type 8 (External attribute LSA for BGP): They are called External Attribute LSAs and are used to transit BGP attributes through an OSPF network while BGP destinations are conveyed via LSA Type 5 packets.

LSA Types 9, 10, and 11 "Opaque": LSA types used for application-specific purposes

LSA Type	Description
1	Router LSA
2	Network LSA
3	Summary LSA
4	ASBR summary LSA
5	Autonomous system LSA
6-11	Other types

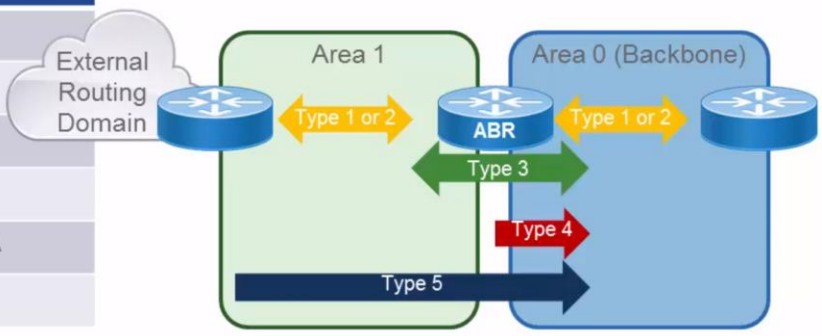


Fig 37.11.2 LSA Types

OSPF Route

There are six types of route types like Intra-Area (O), Inter-Area (O IA), External Type 1 (E1), NSSA Type 1 (N1), External Type 2 (E2), NSSA Type 2 (N2) .

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

We also distinguish between different types of routes in routing tables:

OSPF route typical route marked with O in routing table & it indicates OSPF protocol is used for origin of the route

Default route: A route used to propagate traffic to an external area; marked with O*IA

Intra-area routes: The routes originated and learned in the same area, i.e., internal to the area and marked with O

Inter-area routes: The routes originated in other OSPF areas & marked with O IA

External routes: The routes from other autonomous system (AS), external to the particular OSPF area & it appear as O E1 or O E2 in a standard area and as O N1 or O N2 in a NSSA or totally NSSA area.

E1 are type 1 routes: It is used when there are multiple ASBRs advertising a route to the AS & external cost is added to the internal cost of each link and will add the cost.

E2 are type 2 routes: It is used if only one router is advertising a route to the AS & external cost does not change.

OSPF authentication

Ospf supports null, simple password authentication and MD5 authentication. OSPF MD5 authentication can be configured globally or by interface. Plain text & MD5 authentication among neighboring routers within an area is supported: Configurable routing interface parameters include interface output cost, re-transmission interval, interface transmit delay, router priority, router dead & hello intervals, & authentication key.

Steps to Configure OSPF in E3000

1. Create any VLAN for routing purpose from 2 to 4094.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

2. Assign IP address to created VLAN as per other connected router/switch IP address as they required to be in same network.

3. Go to Interface where you connected L3 Switch/Router and assign Created VLAN in access mode.

4. Enable OSPF.

5. Add connected Network ID to OSPF

6. Check OSPF Route

Switch#**configure terminal**
Switch(config)# **ospf** {Process-ID}

Switch(config)# **no ospf** {Process-ID}

Syntax	**ospf** 1 **no ospf 1**
Parameter	**Network ID and mask**
Default	OSPF is not configured by default.
Mode	Global Configuration mode.
Example	The following example shows how to configure a OSPF route. Switch#**configure terminal** Switch(config)# **interface vlan2** Switch(config-if)#**ip address 192.168.1.2/24** Switch(config-if)#**interface gi1** Switch(config-if)#**switchport mode access** Switch(config-if)#**switchport access vlan** 2 Switch(config-if)# **exit** Switch(config)# **router-id** 1.1.1.1 Switch(config)# **ospf** 1 Switch(config-ospf-1)# **area** 0 Switch(config-ospf-1-area-0.0.0.0)# **network** 192.168.0.0/24 Switch(config-ospf-1-area-0.0.0.0)# **network** 192.168.1.0/24

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch# config terminal
Switch(config)# interface vlan2
Switch(config-if-vlan2)#  ip address 192.168.1.2/24
Switch(config-if-vlan2)# interface gil
Switch(config-if-gil)#  switchport mode access
Switch(config-if-gil)#  switchport access vlan 2
Switch(config-if-gil)# exit
Switch(config)# router-id  1.1.1.1
Switch(config)# ospf 1
Switch(config-ospf-1)#  area 0
Switch(config-ospf-1-area-0.0.0.0)#   network 192.168.0.0/24
Switch(config-ospf-1-area-0.0.0.0)#   network 192.168.1.0/24
```

Switch# show ip route

```
Switch#  show ip route
Codes: > - best, C - connected, S - static R - rip
 O - ospf, I - isis, B - BGP

C>  1.1.1.0/30 is directly connected, Loopback1
C>  192.168.0.0/24 is directly connected, VLAN 1
C>  192.168.1.0/24 is directly connected, VLAN 2
O>  192.168.2.0/24 [110/11] via 192.168.1.1, VLAN 2
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

38. POE

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.

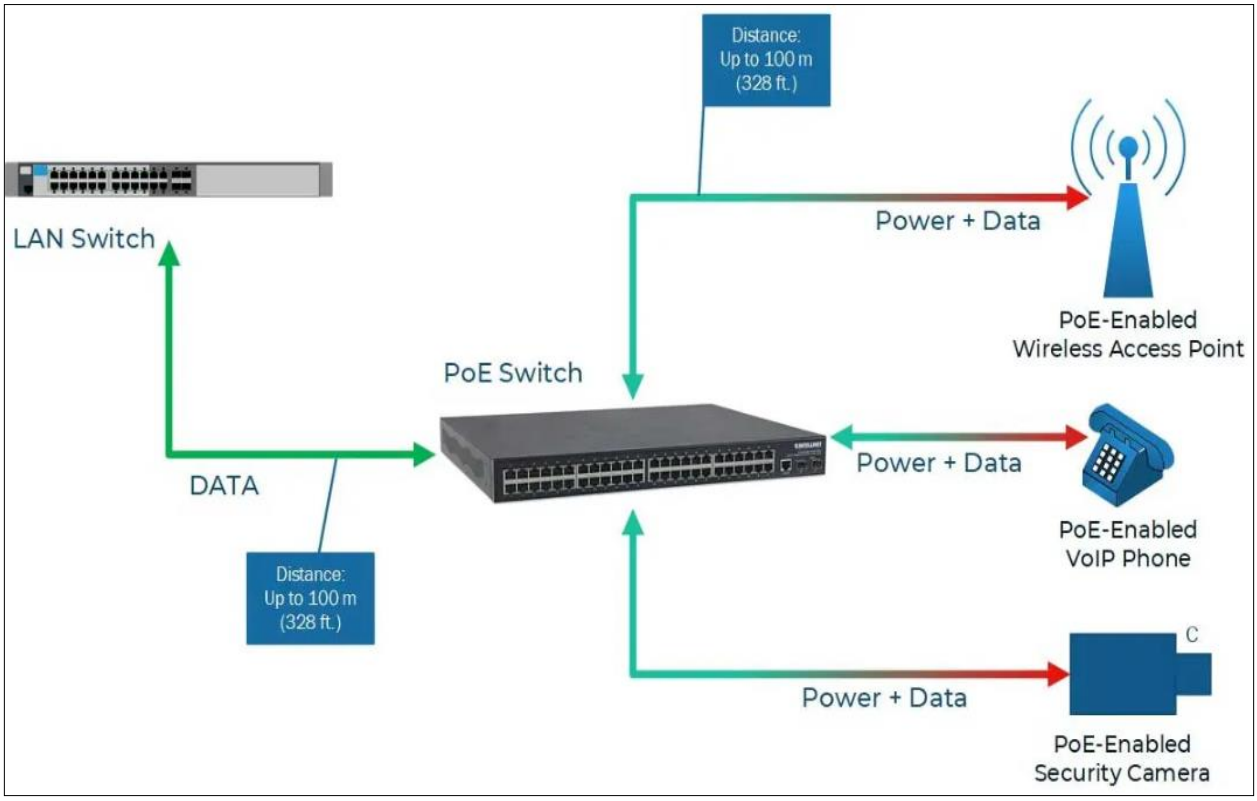


Fig 38.1 PoE Concept

PoE, PoE and PoE+ Comparison Chart

PoE Standard	PoE Common Name	Power Output	Year	Comment
IEEE 802.3af	PoE	15.40W	2003	12.95 W
IEEE 802.3at	PoE+	30W	2009	25.50 W

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

As PoE/PoE+ technology has developed the amount of power that can be sent over Ethernet cable has increased. IEEE-compliant PoE/PoE+ switches and injectors can output anywhere from 12 watts to 30 watts of power per port.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

38.1 POE PORT SETTING

Use the poe command in interface mode to enable port poe power supply. Use the **"no"** poe command in interface mode to disable port poe power supply. You can check the port poe working status by using the show poe Privileged EXEC command.

Switch#**configure terminal**
Switch(config-if)# **poe**

Switch(config-if)# **no poe**

Syntax	**poe** **no poe**
Default	All ports are enabled for poe power supply by default. (Poe-enabled device)
Mode	interface configuration.
Example	The following example shows how to config poe. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **poe** Switch# **show poe**

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

```
Switch#  show poe
  Get poe power:

  Port  |  Enable | State | type | level | actual-    | voltage(V) | current(mA)
        |         |       |      |       | power(mW)  |            |
--------+---------+-------+------+-------+------------+------------+--------------
  gi1       enable    off    AF      0       N/A          N/A          N/A
  gi2       enable    off    AF      0       N/A          N/A          N/A
  gi3       enable    off    AF      0       N/A          N/A          N/A
  gi4       enable    off    AF      0       N/A          N/A          N/A
  gi5       enable    off    AF      0       N/A          N/A          N/A
  gi6       enable    off    AF      0       N/A          N/A          N/A
  gi7       enable    off    AF      0       N/A          N/A          N/A
  gi8       enable    off    AF      0       N/A          N/A          N/A
  gi9       enable     on    AF      0      2028           52           39
  gi10      enable    off    AF      0       N/A          N/A          N/A
  gi11      enable    off    AF      0       N/A          N/A          N/A
  gi12      enable    off    AF      0       N/A          N/A          N/A
  gi13      enable    off    AF      0       N/A          N/A          N/A
  gi14      enable    off    AF      0       N/A          N/A          N/A
  gi15      enable    off    AF      0       N/A          N/A          N/A
  gi16      enable    off    AF      0       N/A          N/A          N/A
  gi17      enable    off    AF      0       N/A          N/A          N/A
  gi18      enable    off    AF      0       N/A          N/A          N/A
  gi19      enable    off    AF      0       N/A          N/A          N/A
  gi20      enable    off    AF      0       N/A          N/A          N/A
  gi21      enable    off    AF      0       N/A          N/A          N/A
  gi22      enable    off    AF      0       N/A          N/A          N/A
  gi23      enable    off    AF      0       N/A          N/A          N/A
  gi24      enable    off    AF      0       N/A          N/A          N/A

  Total used power: 2028 (mW)
  Total reserve power: 0 (mW)
  Current Temperature: 26 (C)
```

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

38.2 POE PORT SCHEDULE SETTING

Use the poe schedule command in interface mode to set port poe power supply time. Use the **"no"** poe schedule command in interface mode to clear port poe power supply time. You can check the port poe work time setting view through the web.

Switch#**configure terminal**
Switch(config-if)#**poe schedule week days hour** {hours}

Switch(config-if)#**no poe schedule week days hour** {hours}

Syntax	**poe schedule week days hour** hours **no poe schedule week days hour** hours
Parameter	days Port poe power supply days hours Port poe power supply hours
Default	All ports open POE function all day by default. (Poe-enabled device)
Mode	interface configuration.

Example	The following example shows how to config poe schedule.
	Switch#**configure terminal**
	Switch(config)# **interface** GigabitEthernet 1
	Switch(config-if)# **poe schedule week mon hour** 1
	Note: The configured time has a deviation of about 0~10 minutes.
	`Switch(config)# interface GigabitEthernet 1`
	`Switch(config-if)# poe schedule week mon hour 1`

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

GLOSSARY

ACL: Access Control List can limit network traffic and restrict access to certain users, ports or mac by allowing and disallowing based on L2/L3/L4 information.

ARP: Address Resolution Protocol converts between IP addresses and MAC addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP: Boot Protocol is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CFM: Connectivity Fault Management provides fault monitoring for end-to-end connections within a designated service area by using continuity check messages which can detect faults in maintenance points, fault verification through loop back messages, and fault isolation with link trace messages.

COS: Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP: Dynamic Host Control Protocol provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP SNOOPING: It is used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

DIFFSERV: Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

DNS: Domain Name Service used for translating host names for network nodes into IP addresses.

DSCP: Differentiated Services Code Point Service uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

EAPOL: Extensible Authentication Protocol over LAN is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A username and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

ERPS: Ethernet Ring Protection Switching can be used to increase the availability and robustness of Ethernet rings, such as those used in Metropolitan Area Networks (MAN). ERPS provides Layer 2 loop avoidance and fast reconvergence in Layer 2 ring topologies, supporting up to 255 nodes in the ring structure. It can also function with IEEE 802.1ag to support link monitoring when non-participating devices exist within the Ethernet ring.

EUI: Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.

GARP: Generic Attribute Registration Protocol is a protocol that can be used by end stations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered end stations.

GMRP: Generic Multicast Registration Protocol allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

GVRP: GARP VLAN Registration Protocol is a way for switches to exchange VLAN information to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

ICMP: Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feedback information about better routing choices.

IEEE 802.1D: Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q: VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign end stations to different virtual LANs and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1P: An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

IEEE 802.1S: An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1W: An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard now incorporated in IEEE 802.1D-2004,

IEEE 802.1X: Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3AC: Defines frame extensions for VLAN tagging.

IEEE 802.3X: Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP: Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

IGMP QUERY: On each subnetwork, one IGMP-capable device will act as the querier that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP PROXY: Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in a simple tree that uses IGMP Proxy.

IGMP SNOOPING: Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IN-BAND MANAGEMENT: Management of the network from a station attached directly to the network.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

IP MULTICAST FILTERING: A process whereby this switch can pass multicast traffic along to participating hosts.

IP PRECEDENCE: The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default but may be configured differently to suit the requirements for specific network applications.

LACP: Link Aggregation Control Protocol allows ports to automatically negotiate

a trunked link with LACP-configured ports on another device.

LAYER 2: Data Link layer in the ISO OSI 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

LINK AGGREGATION: Link aggregation increases bandwidth, provides graceful degradation as failure occurs, and increases availability. It provides network redundancy by load-balancing traffic across all available trunk links.

LLDP: Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities, and configuration settings.

MD5: Message-Digest 5 is an algorithm that is used to create digital signatures. It is intended for use with 32-bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB: Management Information Base is an acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MSTP: Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

MRD: Multicast Router Discovery is used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

Multicast Switching: A process whereby the switch filters incoming multicast frames for services for which no attached host has registered or forwards them to all ports contained within the designated multicast VLAN group.

MVR: Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on-demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or private VLAN groups.

NTP: Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration to synchronize local clocks within the subnet and to national time standards via wire or radio.

OAM: Operation, Administration, and Maintenance provides remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). This section describes functions including enabling OAM for selected ports, loopback testing, and displaying remote device information.

OSPF: Open Shortest Path First (OSPF) is an open link state routing protocol. OSPF routers learn the entire network topology for their "area" (the portion of the network they maintain routes for, usually the entire network for small networks). OSPF routers send event driven updates. If a network is converged for a week, the OSPF routers will send no updates. OSPF has far faster convergence than distance vector protocols such as RIP.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

OUT-OF-BAND Management: The device can be accessed from a station not attached to the network.

PORT MIRRORING: A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be monitored.

PORT TRUNK: Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower speed physical links.

PRIVATE VLANS: Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

QINQ QinQ tunneling: It is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.

QOS: Quality of Service refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS: Remote Authentication Dial-in User Service is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RIP: Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol that has an AD value of 120 uses port number 520.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

RMON: Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP and can set alarms on a variety of traffic conditions, including specific error types.

RSTP: Rapid Spanning Tree Protocol reduces the convergence time for network topology changes.

SMTP: Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

SNMP: Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP: Simple Network Time Protocol allows a device to set its internal clock based on

periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server or can be received via broadcasts sent by NTP servers.

SSH: Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key and encrypt data connections between management clients and the switch.

STA: Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

TACACS+: Terminal Access Controller Access Control System Plus is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

TCP/IP: Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

TELNET: It is a remote communication facility for interfacing to a terminal device over TCP/IP.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.

TFTP: Trivial File Transfer Protocol used for software/firmware downloads.

UDP: User Datagram Protocol provides a datagram mode for packet switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC: Universal Time Coordinate is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN: Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers and allows users to share information and resources as though located on the same LAN.

XMODEM: A protocol used to transfer files between devices. Data is grouped in 128-

byte blocks and error corrected.

© 2024 COMMANDO Networks Inc., USA. All rights reserved.