

INSTALLATION AND OPERATION MANUAL



CWGE24MS2

COMMERCIAL GRADE MANAGED LAYER 2+ ETHERNET SWITCH WITH 20 × 100/1000BASE-FX + 4 × GIGABIT COMBO PORTS

v1.0 November 29, 2016

The ComNet CWGE24MS2 has twenty 100/1000Base-FX SFP ports and four Gigabit combo ports that allow for TX or FX transmission. All SFP ports utilize ComNet SFP modules for fiber, connector type and distance. The IEEE802.3-compliant unit offers multiple Ethernet redundancy protocols (ERPS G.8032 and MSTP/RSTP/STP) which protect your applications from network interruptions or temporary malfunctions by redirecting transmission within the network. The CWGE24MS2 implements complete Layer 2 to Layer 4 ACLs to restrict access to your sensitive network resources by filtering specific packets based on TCP/UDP ports, source and destination IP addresses or particular network devices. Furthermore, DHCP snooping, TACACS+, ARP, IEEE 802.1X and Port Security provide additional tools to manage access and levels of use of the network. These defence mechanisms of the CWGE24MS2 along with advanced DoS auto prevention deliver robust network security and enables network administrators to offer more stable services on a more secure network.

Contents

Regulatory Compliance Statement	5
Warranty	5
Disclaimer	5
Safety Indications	5
Copyright	5
FCC Warning	6
CE	6
Overview	7
Introduction	7
Software Features	8
Hardware Features	10
Hardware Overview	11
Front Panel	11
Installation	13
Desktop Installation	13
Mounting on a Rack	13
Getting Connected	13
Powering On the Unit	13
Installing the SFP modules and Fiber Cable	14
Connecting a Copper Cable	14
Connecting to the Console	15
Connecting to Computer or a LAN	15
LED Indicators	16
GUI Login	22
System Information	23
Basic Settings	25
General Settings	25
MAC Management	38
CLI Configuration	45

Advanced Settings	53
Bandwidth Control	53
DHCPv6	70
IGMP Snooping	72
VLAN	94
DHCP Option	122
Dual Homing	133
ERPS	136
Link Aggregation	143
Link Layer Discovery Protocol (LLDP)	151
Loop Detection	155
PPPoE IA	159
Static Route	168
STP	173
UDLD	195
Security	200
IP Source Guard	200
ACL	218
802.1x	224
Port Security	233
TACACS+	236
Monitor	241
Alarm	241
Hardware Information	242
Port Statistics	243
Port Utilization	244
RMON Statistics	245
SFP Information	247
Traffic Monitor	249

Management	252
SNMP	252
Auto Provision	263
Mail Alarm	266
Maintenance	270
System log	276
User Account	278

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

Warranty

ComNet warrants that all ComNet products are free from defects in material and workmanship for a specified warranty period from the invoice date. ComNet will repair or replace products found by ComNet to be defective within this warranty period. This warranty does not cover product modifications or repairs done by persons other than ComNet-approved personnel, and this warranty does not apply to ComNet products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

Disclaimer

Information in this publication is intended to be accurate. ComNet shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ComNet reserves the right to revise the contents of this publication without notice.

Safety Indications

- » The equipment can only be accessed by trained ComNet service personnel.
- » This equipment should be installed in secured location.

Copyright

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photo copying, recording or otherwise, without the prior written permission of the publisher.

FCC Warning

This equipment has been tested and found to comply with the limits for a class A device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

CE

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Overview

Introduction

The ComNet CWGE24MS2 has twenty 100/1000Base-FX SFP ports and four Gigabit combo ports that allow for TX or FX transmission. All SFP ports utilize ComNet SFP modules for fiber, connector type and distance. The IEEE802.3-compliant unit offers multiple Ethernet redundancy protocols (ERPS G.8032 and MSTP/RSTP/STP) which protect your applications from network interruptions or temporary malfunctions by redirecting transmission within the network. The CWGE24MS2 implements complete Layer 2 to Layer 4 ACLs to restrict access to your sensitive network resources by filtering specific packets based on TCP/UDP ports, source and destination IP addresses or particular network devices. Furthermore, DHCP snooping, TACACS+, ARP, IEEE 802.1X and Port Security provide additional tools to manage access and levels of use of the network. These defence mechanisms of the CWGE24MS2 along with advanced DoS auto prevention deliver robust network security and enables network administrators to offer more stable services on a more secure network.

In this guide, the term "Switch" (first letter upper case) refers to the CWGE24MS2 Switch, and "switch" (first letter lower case) refers to other switches.

Software Features

Network Functions

- » Port-based Mirroring
- » GARP/GVRP Support
- » 4K Active VLAN
- » IGMP Snooping v1/v2/v3
- » IGMP Querier
- » MVR
- » DHCP Relay/Option 82
- » Dual Homing
- » Link Aggregation
- » Link Layer Discovery Protocol
- » Loop Detection, Auto Recovery Timer
- » STP/RSTP/MSTP
- » ERPS (G8032v2)
- » SFP DDMI Support
- » RMON Statistics
- » Static Route
- » Network Security
- » Access Control List (L2/L3/L4)
- » MAC Limitation
- » Port Security
- » 802.1x Port Authentication
- » TACACS+
- » Traffic management & QoS
- » Port Priority
- » Rate Limitation
- » Storm Control
- » Port Isolation
- » 802.1Q Tag-based VLAN
- » Auto MDI/MDI-X

Network Management

- » Command Line Interface, Telnet
- » Web GUI
- » SNMP v1/v2c/v3
- » Management VLAN
- » Auto Provisioning
- » System log
- » Firmware Upgradable
- » Configuration Upload/Download
- » LED, SNMP trap, and email alarm

Specifications

- » IEEE 802.3 10Base-T
- » IEEE 802.3u 100Base-TX/FX
- » IEEE 802.3ab 1000Base-T
- » IEEE 802.3z 1000Base-SX/LX
- » IEEE 802.3x Flow Control
- » IEEE 802.1d Spanning Tree Protocol
- » IEEE 802.1w Rapid Spanning Tree Protocol
- » IEEE 802.1s Multiple Spanning Tree Protocol
- » IEEE 802.1q VLAN Tagging
- » IEEE 802.1p Class of Service
- » IEEE 802.1x Port Authentication
- » IEEE 802.1ab Link Layer Discovery Protocol
- » IEEE 802.3ad Port Trunk with LACP
- » ITU-T G8032v2 Ethernet Ring Protection Switching

Hardware Features

Performance

» Switching fabric	48 Gbps
» L2 forwarding	35.7 Mpps
» MAC Entries	16 K
» Jumbo frame	10 K

Ports

- » 20-slot 100FX/Gigabit SFP
- » 4 × Gigabit Combo (10/100/1000 RJ-45 or 100FX/GbE SFP)
- » 1 × DB-9 console

Maximum Distances

» RJ-45	up to 100 m
» SC/SFP	up to 120 km
» Console	15 m

Mechanical & Environmental

» Operating temperature	0°C to 50°C
» Storage temperature	-20°C to 70°C
» Operating humidity	10% to 90% RH
» Storage humidity	5% to 95% RH

Power

» Front access AC power	100-240 V, 50~60Hz
» 12V DC battery back-up	
» Power consumption	Max. 25 W (System)

Dimensions & Weight

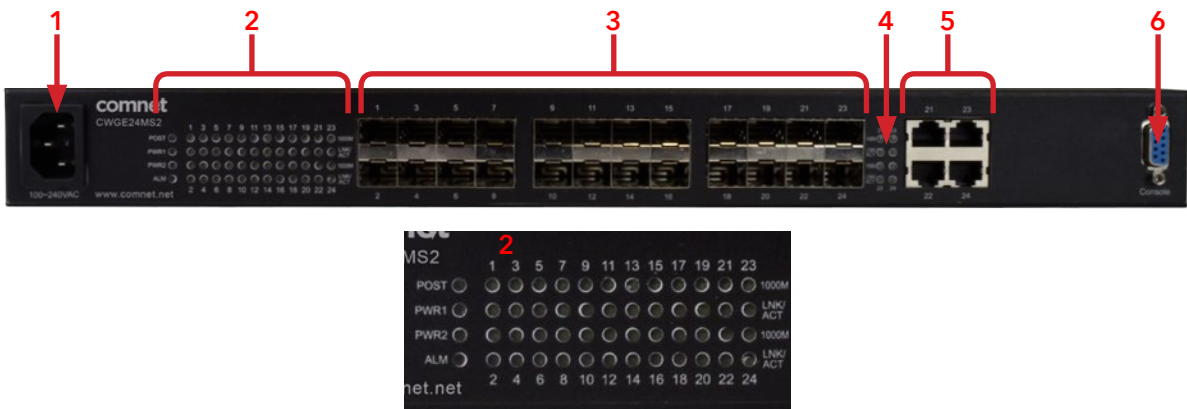
» Dimensions (WxHxD)	440 × 44 × 284mm, 19" rack-mountable
» Weight	3.7 kg

Hardware Overview

Front Panel

The following table describes the labels that are affixed to the CWGE24MS.

Port	Description
SFP ports	20 × 100BaseX
Giga Ethernet Port	4 × Gigabit Combo (10/100/1000 RJ-45 or 100FX/GbE SFP)
Console	Use RS-232 with DB9 connector to manage switch.



CWGE24MS Front Panel

- 1. Power Connector
- 2. LEDs for Post, Power, Alarm; Speed/Link/Activity for 24 SFP ports
- 3. 100/1000Base-X Fiber port on SFP
- 4. LED for Ethernet ports 1000Mbps Speed/Link/Activity status
- 5. 10/100/1000Base-T(X) Ethernet port and 100/1000Base-X SFP (combo port)
- 6. Console port (DB9)

Connectors

The Switch utilizes ports with copper and SFP fiber port connectors functioning under Fast Ethernet/Gigabit Ethernet standards.

100FX/1000Base-SX/LX SFP Ports

The 100/1000Base-SX/LX (SFP) ports support network speeds of 100Mbps or 1000Mbps, and is designed to house 100Mbps/Gigabit SFP modules.

Gigabit Combo

There are four Gigabit Combo ports on the CWGE24MS2. Combo ports have both an RJ-45 interface and an SFP slot, of which one can be in use at any one time. The RJ-45 ports operate at 10/100/1000 Mbps, while the SFP ports are capable of operating at 100Mbps or 1000 Mbps.

The Gigabit copper ports have the same number as its corresponding SFP slot. This means that once an SFP slot is connected, the correspondingly numbered RJ-45 port (21, 22, 23 or 24) will not function

Installation

The location chosen for installing the Switch may affect its performance. When selecting a site, we recommend considering the following rules:

Install the Switch in an appropriate place. See Technical Specifications for the acceptable temperature and humidity ranges.

Install the Switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.

Leave at least 10cm of space at the front and rear of the unit for ventilation.

Desktop Installation

Follow the instructions listed below to install the Switch in a desktop location.

Locate the Switch in a clean, flat and safe position that has convenient access to AC power.

Affix the four self-adhesive rubber pads to the underside of the Switch.

Apply AC power to the Switch (The green PWR LED on the front panel should light up).

Connect cables from the network partner devices to the ports on the front panel (The green LNK LED on the upper right of the port should light).

Warning: Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.

Mounting on a Rack

Attach brackets to each side of the switch and place the brackets in the rack's slots. Insert and tighten screws to securely attach the bracket to the rack on each side.

Getting Connected

The Switch is capable of connecting up to 24 network devices in fiber connection at Fast Ethernet, or Gigabit Ethernet speeds.

Powering On the Unit

The Switch uses an AC power supply 100~240VAC, 50~60 Hz. The Switch's power supply automatically self-adjusts to the local power source and may be powered on without having any or all LAN segment cables connected.

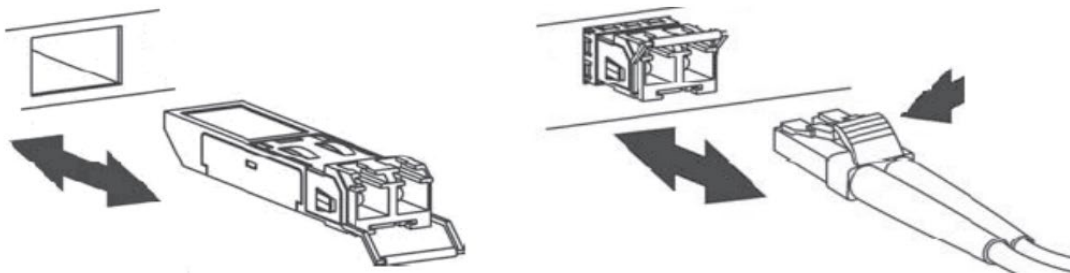
- » Insert the power cable plug directly into the receptacle located at the front of the device.
- » Plug the power adapter into an available socket.

Note: *For international use, you may need to change the AC power adapter cord. You must use a power cord set that has been approved for the receptacle type and electrical current in your country.*

- » Check the front-panel LEDs as the device is powered on to verify that the Power LED is lit. If not, check that the power cable is correctly and securely plugged in.

Installing the SFP modules and Fiber Cable

- » Slide the selected SFP module into the selected SFP slot (Make sure the SFP module is aligned correctly with the inside of the slot)
- » Insert and slide the module into the SFP slot until it clicks into place
- » Remove any rubber plugs that may be present in the SFP module's mouth
- » Align the fiber cable's connector with the SFP module's mouth and insert the connector
- » Slide the connector in until a click is heard
- » If you want to pull the connector out, first push down the release clip on top of the connector to release the connector from the SFP module.



To properly connect fiber cabling: Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

Note: *When inserting the cable, be sure the tab on the plug clicks into position to ensure that it is properly seated.*

Check the corresponding port LED on the Switch to be sure that the connection is valid. (Refer to the LED chart).

Connecting a Copper Cable

The RJ-45 Ethernet port fully supports auto-sensing and auto-negotiation.

- » Insert one end of a Category 3/4/5/5e (see recommendation above) type twisted-pair cable into an available RJ-45 port on the Switch and the other end into the port of the network node.
- » Check the corresponding port LED on the Switch to ensure that the connection is valid. (Refer to LED chart)

Connecting to the Console

The console port (DB-9) provides the out-of-band management facility. Use null modem cable to connect the console port on the Switch and the other end into the COM port of the computer.

Connecting to Computer or a LAN

You can use Ethernet cable to connect computers directly to the switch ports. You can also connect hubs/switches to the switch ports by Ethernet cables. You can use either the crossover or straight-through Ethernet cable to connect computers, hubs, or switches.

Notice: Use a twisted-pair Cat5e Ethernet cable to connect the 1000BASE-T port otherwise the link speed will not be able to reach 1Gbps.

LED Indicators

This Switch is equipped with Unit LEDs to enable you to determine the status of the Switch, as well as Port LEDs to display what is happening in all your connections. They are as follows:

Unit LEDs		
LED	Condition	Status
POWER (Green)	Illuminated	Power on
	Off	Power off or fail
POST (Green)	Illuminated	Switch is ready and running ok
	Blinking	Switch is booting
	Off	Switch is not ready or failed
ALARM (Red)	Illuminated	Alarm for over threshold of system temperature, fan speed or voltage
	Off	Switch is in normal condition
LNK/ACT (Dual Color) (for 1~20th Fiber ports)	Green on	1000Mbps Ethernet link-up
	Amber on	100Mbps Ethernet link-up
	Blinking	Receiving or transmitting data
	Off	Port disconnected or link failed
LNK (Green) (for 21~24th Fiber ports)	Illuminated	Link-up
	Off	Port disconnected or link failed
ACT (Green) (for 21~24th Fiber ports)	Blinking	Receiving or transmitting data
LNK/ACT (Green) (for 21~24th Copper ports)	Illuminated	Link-up
	Blinking	Receiving or transmitting data
	Off	Port disconnected or link failed
1000 (Green) (for 21~24th copper ports)	Illuminated	1000Mbps
	Off	10/100Mbps

Management Options

This system may be managed out-of-band through the console port on the front panel or in-band by using Telnet. The user may also choose web-based management, accessible through a Web browser.

Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a Web browser.

SNMP-based Management

You can manage the Switch with SNMP Manager Software. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Configuring the Switch via Console Port

Prior to accessing the switch's onboard agent via a network connection, you must first configure by giving a valid IP address, subnet mask, and default gateway, using an out-of-band connection or the BOOTP protocol.

After configuring the Switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network or via internet. The onboard configuration program can be accessed by using Telnet from any computer attached to the network. It can also be managed with any computer using a Web browser.

Access the Switch via a terminal emulator (such as Putty, HyperTerminal, Tera Term...) attached to the console port. The console port is set at the factory with the following default COM port properties. Configure your own terminal to match the following:

Use terminal emulation software with the following settings:

Default Settings for the Console Port

Setting	Default Value
Terminal Emulation	VT100
Baud Rate	38400
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

Press [ENTER] to open the login screen.

Setting	Default Value
Default Username	admin
Default Password	admin

Note: *Ensure that the terminal or PC you are using to make this connection is configured to match the above settings. Otherwise the connection will not work.*

Then press [ENTER] to open the login screen with the "Default Value" for Username and Password as "admin".

Management by Telnet

Activate your workstation's command prompt program and access your Switch via the Internet by typing in the correct IP address (factory default IP address is 192.168.10.1 - connect directly via console port to configure a unique IP address). Your command prompt program will allow use of the Telnet protocol.

Connect your computer to one of the Ethernet ports.

Open a Telnet session to the Switch's IP address. If this is your first login, use the default values.

Setting	Default Value
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Management VLAN	1
Default Username	admin
Default Password	admin

Make sure your computer IP address is in the same subnet, unless you are accessing the Switch through one or more routers.

How to enter the CLI

Press [Enter] key to enter the login command prompt when below message is displayed on the screen.

Please press Enter to activate this console

Input “*admin*” to enter the CLI mode when below message is displayed on the screen.

CWGE24MS2 login:

You can execute a few limited commands when CLI prompt is displayed as below.

CWGE24MS2>

If you want to execute more powerful commands, you must enter the privileged mode.

Input command “*enable*”

CWGE24MS2>enable

Input a valid username and password when below prompt are displayed.

user:admin

password:admin

CWGE24MS2#

CLI command concept

Node	Command	Description
enable	show hostname	This command displays the system's network name.
configure	reboot	This command reboots the system.
eth0	ip address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
interface	show	This command displays the current port configurations.
acl	show	This command displays the current access control profile.
vlan	show	This command displays the current VLAN configurations.

The Node type:

- » enable
- » Its command prompt is "CWGE24MS2#".
- » It means these commands can be executed in this command prompt.

configure

Its command prompt is "CWGE24MS2(config)#".

It means these commands can be executed in this command prompt.

In Enable code, executing command "*configure terminal*" enter the configure node.

```
CWGE24MS2# configure terminal
```

eth0

Its command prompt is "CWGE24MS2(config-if)#".

It means these commands can be executed in this command prompt.

In Configure code, executing command "*interface eth0*" enter the eth0 interface node.

```
CWGE24MS2(config)#interface eth0
```

```
CWGE24MS2(config-if)#
```

interface

Its command prompt is "CWGE24MS2(config-if)#".

It means these commands can be executed in this command prompt.

In Configure code, executing command "*interface gig Ethernet1/0/5*" enter the interface port 5 node.

Or

In Configure code, executing command "*interface fast Ethernet1/0/5*" enter the interface port 5 node.

Note: dependent on your port speed, gig Ethernet1/0/5 for gigabit Ethernet ports and fast Ethernet1/0/5 for fast Ethernet ports.

```
CWGE24MS2(config)#interface gig Ethernet1/0/5
```

```
CWGE24MS2(config-if)#
```


vlan

Its command prompt is "CWGE24MS2(config-vlan)#".

It means these commands can be executed in this command prompt.

In Configure code, executing command "*vlan 2*" enter the vlan 2 node.

Note: where the "2" is the vlan ID.

```
CWGE24MS2(config)#vlan 2
```

```
CWGE24MS2(config-vlan)#
```

acl

Its command prompt is "CWGE24MS2(config-acl)#".

It means these commands can be executed in this command prompt.

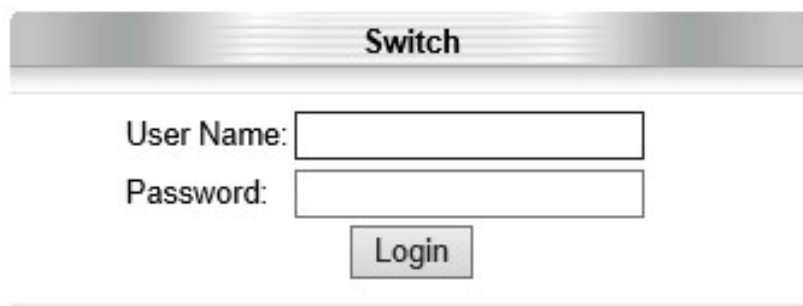
In Configure code, executing command "*access-list test*" enter the access-list test node.

Note: where the "test" is the profile name.

```
CWGE24MS2(config)#access-list test
```

```
CWGE24MS2(config-acl)#
```

GUI Login



Switch

User Name:

Password:

Login

Parameter	Description
User ID	Enter the user name.
Password	Enter the password.

Default:

User name: admin,
Password: admin.

CLI Configuration

Node	Command	Description
enable	show hostname	This command displays the system's network name.
enable	show interface eth0	This command displays the current Eth0 configurations.
enable	show model	This command displays the system information.
enable	show running-config	This command displays the current operating configurations.
enable	show system-info	This command displays the system's CPU loading and memory information.
enable	show uptime	This command displays the system up time.

System Information

System Information

System Information

Model Name	CWGE24MS2
Host Name	CWGE24MS2
Boot Code Version	V1.3.4.S0
Firmware Version	V1.0.3.S0
Built Date	Thu Nov 17 19:24:22 CST 2016
DHCP Client	Disabled
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:22:3b:0b:80:30
Serial Number	00016A005744
Management VLAN	1
CPU Loading	<div style="display: inline-block; width: 100px; height: 10px; background: linear-gradient(to right, blue, gray);"></div> 11 %
Memory Information	Total: 118932 KB, Free: 89440 KB, Usage: 24.8 %
Current Time	2014-1-1, 0:7:0
System Uptime	0 day(s), 00:07:19.
DHCPv6 Client	Disabled
IPv6 Link Local	fe80::222:3bff:fe0b:8030/64
IPv6 Default Gateway	
IPv6 Global	

Parameter	Description
Model Name	This field displays the model name of the Switch.
Host name	This field displays the name of the Switch.
Boot Code Version	This field displays the boot code version.
Firmware Version	This field displays the firmware version.
Built Date	This field displays the built date of the firmware.
DHCP Client	This field displays whether the DHCP client is enabled on the Switch.
IP Address	This field indicates the IP address of the Switch.
Subnet Mask	This field indicates the subnet mask of the Switch.
Default Gateway	This field indicates the default gateway of the Switch.
MAC Address	This field displays the MAC (Media Access Control) address of the Switch.

Parameter	Description
Serial Number	The serial number assigned by manufacture for identification of the unit.
Management VLAN	This field displays the VLAN ID that is used for the Switch management purposes.
CPU Loading	This field displays the percentage of your Switch's system load.
Memory Information	This field displays the total memory the Switch has and the memory which is currently available (Free) and occupied (Usage).
Current Time	This field displays current date (yyyy-mm-dd) and time (hh:mm:ss).
DHCPv6 Client	This field displays whether the DHCPv6 client is enabled on the Switch.
IPv6 Link Local	This field displays the Switch's link local IP address for IPv6.
IPv6 Default Gateway	This field displays the default gateway for IPv6.
IPv6 Global	This field displays the Switch's global IP address for IPv6.
Refresh	Click this to update the information in this screen.

Basic Settings

General Settings

System

Introduction

Management VLAN

To specify a VLAN group which can access the Switch.

- » The valid VLAN range is from 1 to 4094.
- » If you want to configure a management VLAN, the management VLAN should be created first and the management VLAN should have at least one member port.

Host Name

The hostname is same as the SNMP system name. Its length is up to 64 characters.

The first 16 characters of the hostname will be configured as the CLI prompt.

Default Settings

- › The default Hostname is CWGE24MS2
- › The default DHCP client is disabled.
- › The default Static IP is 192.168.10.1
- › Subnet Mask is 255.255.255.0
- › Default Gateway is 0.0.0.0
- › Management VLAN is 1.

CLI Configuration

Node	Command	Description
enable	ping IPADDR [-c COUNT]	This command sends an echo request to the destination host. The -c parameter allow user to specific the packet count. The default count is 4.
enable	ping IPADDR [-s SIZE]	This command sends an echo request to the destination host. The -s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [-c COUNT -s SIZE]	This command sends an echo request to the destination host. The -c parameter allow user to specific the packet count. The default count is 4. The -s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [-s SIZE -c COUNT]	This command sends an echo request to the destination host. The -c parameter allow user to specific the packet count. The default count is 4. The -s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
configure	reboot	This command reboots the system.
configure	hostname STRINGS	This command sets the system's network name.
configure	interface eth0	This command enters the eth0 interface node to configure the system IP.
configure	configure terminal	This command changes the mode to config mode.
configure	interface eth0	This command changes the mode to eth0 mode.
eth0	show	This command displays the eth0 configurations.
eth0	ip address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
eth0	ip address default-gateway A.B.C.D	This command configures the system default gateway.
eth0	ip dhcp client (disable enable renew)	This command configures a DHCP client function for the system. Disable: Use a static IP address on the switch. Enable & Renew: Use DHCP client to get an IP address from DHCP server.
eth0	management vlan VLANID	This command configures the management vlan.
eth0	ip ipv6-address AAAA:BBB B:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH/M	This command configures a global scope of IPv6 address and subnet mask for the system.
eth0	ip ipv6-address default-gateway AAAA:BBB:CCC C:DDDD:EEEE:FFFF:GGGG:HHHH	This command configures a default gateway for the system.
eth0	ip ipv6-dhcp client (disable enable renew)	This command configures a DHCPv6 client function for the system. Disable: Use a static IP address on the switch. Enable & Renew: Use DHCPv6 client to get an IP address from DHCPv6 server.

Example: The procedures to configure an IP address for the Switch.

To enter the configure node.

```
CWGE24MS2#configure terminal
```

```
CWGE24MS2(config)#
```

To enter the ETH0 interface node.

```
CWGE24MS2(config)#interface eth0
```

```
CWGE24MS2(config-if)#
```

To get an IP address from a DHCP server.

```
CWGE24MS2(config-if)#ip dhcp client enable
```

To configure a static IP address and a gateway for the Switch.

```
CWGE24MS2(config-if)#ip address 192.168.202.111/24
```

```
CWGE24MS2(config-if)#ip address default-gateway 192.168.202.1
```

To configure a static global IPv6 address and a gateway for the Switch.

Please set the static global IPv6 address first.

```
CWGE24MS2(config-if)#ip ipv6-address 3ffe::1235/64
```

And the set the IPv6 default gateway address.

```
CWGE24MS2(config-if)#ip ipv6-address default-gateway 3ffe::1234
```

Web Configuration

General Settings

System
Jumbo Frame
SNTP
Management Host

System Settings

Hostname

Management VLAN

IPv4 Settings

DHCP Client Disable ▾ Renew

IP Address

Subnet Mask

Default Gateway

IPv6 Settings

DHCPv6 Client Disable ▾ Renew

Global Address

Default Gateway Set ▾

Apply
Refresh

Parameter	Description
IP Address	Configures a IPv4 address for your Switch in dotted decimal notation. For example, 192.168.0.254.
Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.1.
IPv6 Settings	
DHCPv6 Client	Select Enable to allow the Switch to automatically get an IP address from a DHCPv6 server. Click Renew to have the Switch re-get an IP address from the DHCP server. Select Disable if you want to configure the Switch's IP address manually.
Global Address	Configure a global IPv6 address for the Switch.
Default Gateway	Set - Set an IPv6 default gateway for the Switch. Unset - Unset the IPv6 default gateway for the Switch.
Apply	Click this button to take effect the settings.
Refresh	Click this button to reset the fields to the last setting.

Jumbo Frame

Introduction

Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumbo frames can enhance data transmission efficiency in a network. The bigger the frame size, the better the performance.

Notice:

The jumbo frame settings will apply to all ports.

If the size of a packet exceeds the jumbo frame size, the packet will be dropped.

The available values are 1522, 1536, 1552, 9010, 9216, 10240.

Default Settings

The default jumbo frame is 10240 bytes.

CLI Configuration

Node	Command	Description
enable	show jumboframe	This command displays the current jumbo frame settings.
configure	jumboframe (10240 1522 1536 1552 9010 9216)	This command configures the maximum number of bytes of frame size for all ports.
configure	interface IFNAME	This command enters the interface configure node.
interface	jumboframe (10240 1522 1536 1552 9010 9216)	This command configures the maximum number of bytes of frame size.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	jumboframe (10240 1522 1536 1552 9010 9216)	This command configures the maximum number of bytes of frame size.

Web Configuration

General Settings

System
Jumbo Frame
SNTP
Management Host

Jumbo Frame Settings

Port
 From: 1 ▾ To: 1 ▾

frame size
10240 ▾

Apply Refresh

Port	Jumbo Frame	Port	Jumbo Frame
1	10240	2	10240
3	10240	4	10240
5	10240	6	10240
7	10240	8	10240
9	10240	10	10240
11	10240	12	10240
13	10240	14	10240
15	10240	16	10240
17	10240	18	10240
19	10240	20	10240
21	10240	22	10240
23	10240	24	10240

Parameter	Description
Port	This field specifies a port or a range of ports for configuration.
Frame Size	This field configures the maximum number of bytes of frame size for specified port(s).
Apply	Click this button to take effect the settings.
Refresh	Click this button to reset the fields to the last setting.

SNTP

Introduction

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. A less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time is known as the Simple Network Time Protocol (SNTP). NTP provides Coordinated Universal Time (UTC). No information about time zones or daylight saving time is transmitted; this information is outside its scope and must be obtained separately.

UDP Port: 123.

Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

Note:

- » The SNTP server always replies the UTC current time.
- » When the Switch receives the SNTP reply time, the Switch will adjust the time with the time zone configuration and then configure the time to the Switch.
- » If the time server's IP address is not configured, the Switch will not send any SNTP request packets.
- » If no SNTP reply packets, the Switch will retry every 10 seconds forever.
- » If the Switch has received SNTP reply, the Switch will re-get the time from NTP server every 24 hours.
- » If the time zone and time NTP server have been changed, the Switch will repeat the query process.
- » No default SNTP server.

Default Settings

Current Time:

Time: 0:3:51 (UTC)

Date: 1970-1-1

Time Server Configuration:

Time Zone : +00:00

IP Address: 0.0.0.0

DayLight Saving Time Configuration:

State : disabled

Start Date: None.

End Date : None.

CLI Configuration

Node	Command	Description
enable	show time	This command displays current time and time configurations.
configure	time HOUR:MINUTE:SECOND	Sets the current time on the Switch. hour: 0-23 min: 0-59 sec: 0-59 Note: If you configure Daylight Saving Time after you configure the time, the Switch will apply Daylight Saving Time.
configure	time date YEAR/MONTH/ DAY	Sets the current date on the Switch. year: 1970- month: 1-12 day: 1-31
configure	time daylight-saving-time	This command enables the daylight saving time.
configure	no time daylight-saving-time	This command disables daylight saving on the Switch.
configure	time daylight-saving-time start-date (first second third fourth last) (Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH HOUR	This command sets the start time of the Daylight Saving Time.
configure	time daylight-saving-time end-date (first second third fourth last) (Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH HOUR	This command sets the end time of the Daylight Saving Time.
configure	time ntp-server (disable enable)	This command disables / enables the NTP server state.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of your time server.
configure	time ntp-ipv6-server IP_ ADDRESS	This command sets the IPv6 address of your time server.
configure	time ntp-server domain- name STRING	This command sets a domain name of your time server.
configure	time timezone STRING	Configures the time difference between UTC (formerly known as GMT) and your time zone. Valid Range: -1200 ~ +1200.

Example:

```
CWGE24MS2(config)#time ntp-server 192.5.41.41
CWGE24MS2(config)#time timezone +0800
CWGE24MS2(config)#time ntp-server enable
CWGE24MS2(config)#time daylight-saving-time start-date first Monday 6 0
CWGE24MS2(config)#time daylight-saving-time end-date last Saturday 10 0
```

Web Configuration

General Settings

SystemJumbo FrameSNTPManagement Host

Current Time and Date

Current Time00:13:57 (UTC)

Current Date2014-01-01

Time and Date Settings

☐ Manual

New Time2014.1.1 / 0:13:57 (yyyy.mm.dd / hh:mm:ss)

☒ Enable Network Time Protocol

NTP Server☐ntp0.fau.de - Europe

☒IP192.168.10.254

Time Zone+0000

Daylight Saving Settings

StateDisable

Start DateFirst Sunday of January at 0 o'clock

End DateFirst Sunday of January at 0 o'clock

ApplyRefresh

Parameter	Description
Current Time and Date	
Current Time	This field displays the time you open / refresh this menu.
Current Date	This field displays the date you open / refresh this menu.

Parameter	Description
Time and Date Setting	
Manual	Select this option if you want to enter the system date and time manually.
New Time	Enter the new date in year, month and day format and time in hour, minute and second format. The new date and time then appear in the Current Date and Current Time fields after you click Apply.
Enable Network Time Protocol	Select this option to use Network Time Protocol (NTP) for the time service.
NTP Server	Select a pre-designated time server or type the IP address or type the domain name of your time server. The Switch searches for the timeserver for up to 60 seconds.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Settings	
State	Select Enable if you want to use Daylight Saving Time. Otherwise, select Disable to turn it off.
Start Date	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving Time. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and 2:00. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving Time. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and 2:00. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Management Host

Introduction

The feature limits the hosts which can manage the Switch. That is, any hosts can manage the Switch via telnet or web browser. If the user has configured one or more management hosts, the Switch can be managed by these hosts only. The feature allows the user to configure up to 3 management IP host entries.

Default Settings

The default is none, any host can manage the Switch via telnet or web browser.

CLI Configuration

Node	Command	Description
enable	show interface eth0	The command displays the all of the interface eth0 configurations.
eth0	show	The command displays the all of the interface eth0 configurations.
eth0	management host A.B.C.D	The command adds a management host address.
eth0	no management host A.B.C.D	The command deletes a management host address.

Example:

```
CWGE24MS2#configure terminal
```

```
CWGE24MS2(config)#interface eth0
```

```
CWGE24MS2(config-if)#management host 192.168.200.106
```


Web Configuration

General Settings

System

Jumbo Frame

SNTP

Management Host

Management Host Settings

Management Host

Apply

Refresh

Management Host List

No.	Management Host	Action
1	192.168.10.100	<div>Delete</div>
2	192.168.10.101	<div>Delete</div>
3	192.168.10.102	<div>Delete</div>

Parameter	Description
Management Host	This field configures the management host.
Apply	Click this button to take effect the settings.
Refresh	Click this button to begin configuring this screen afresh.
Management Host List	
No.	This field displays a sequential number for each management host.
Management Host	This field displays the management host.
Action	Click the Delete button to remove the specified entry.

MAC Management

Introduction

Dynamic Address:

The MAC addresses are learnt by the switch. When the switch receives frames, it will record the source MAC, the received port and the VLAN in the address table with an age time. When the age time is expired, the address entry will be removed from the address table.

Static Address:

The MAC addresses are configured by users. The static addresses will not be aged out by the switch; it can be removed by user only. The maximum static address entry is up to 256.

The MAC Table (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's MAC Table. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered).

- » The Switch uses the MAC Table to determine how to forward frames. See the following figure.
- » The Switch examines the received frame and learns the port from which this source MAC address came.
 - › The Switch checks to see if the frame's destination MAC address matches a source MAC address already learnt in the MAC Table.
 - › If the Switch has already learnt the port for this MAC address, then it forwards the frame to that port.
 - › If the Switch has not already learnt the port for this MAC address, then the frame is flooded to all ports. If too much port flooding, it may lead to network congestion.
 - › If the Switch has already learnt the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

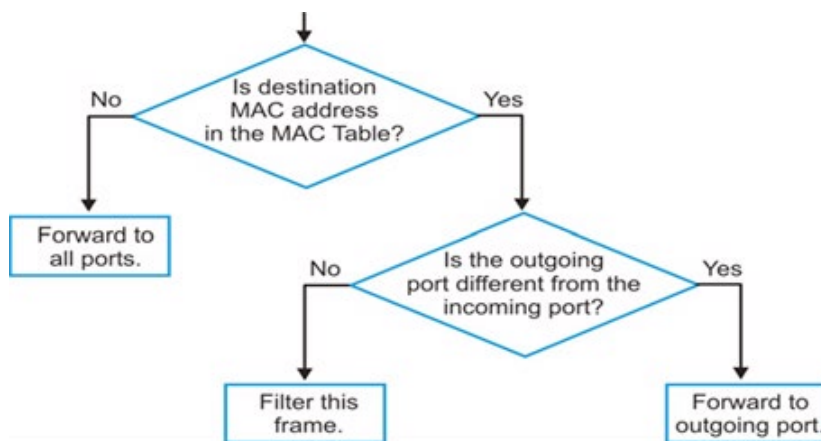


Figure MAC Table Flowchart

Default Settings

The default MAC address table age time is 300 seconds.

The Maximum static address entry is 256.

CLI Configuration

Node	Command	Description
enable	show mac-address-table aging-time	This command displays the current MAC address table age time.
enable	show mac-address-table (static dynamic)	This command displays the current static/dynamic unicast address entries.
enable	show mac-address-table mac MACADDR	This command displays information of a specific MAC.
enable	show mac-address-table port PORT_ID	This command displays the current unicast address entries learnt by the specific port.
configure	mac-address-table static MACADDR vlan VLANID port PORT_ID	This command configures a static unicast entry.
configure	no mac-address-table static MACADDR vlan VLANID	This command removes a static unicast entry from the address table.
configure	mac-address-table aging-time VALUE	This command configures the mac table aging time.
configure	clear mac address-table dynamic	This command clears the dynamic address entries.

Example:

```
CWGE24MS2(config)#mac-address-table static 00:11:22:33:44:55 vlan 1 port 1
```

Web Configuration

Static MAC

A static Media Access Control (MAC) address is an address that has been manually entered in the MAC address table, and do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port, so this may reduce the need for broadcasting.

MAC Address Management

Static MAC Settings

MAC Table

Age Time Setting

Refusal MAC Settings

Static MAC Settings

MAC Address

VLAN ID

Port

1

Apply

Refresh

Static MAC Table

MAC Address	VLAN ID	Port	Action
00:22:3b:0b:80:30	1	CPU	

Total counts : 1

Parameter	Description
Static MAC Settings	
MAC Address	Enter the MAC address of a computer or device that you want to add to the MAC address table. Valid format is hh:hh:hh:hh:hh:hh.
VLAN ID	Enter the VLAN ID to apply to the computer or device.
Port	Enter the port number to which the computer or device is connected.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Static MAC Table	
MAC Address	This field displays the MAC address of a manually entered MAC address entry.
VLAN ID	This field displays the VID of a manually entered MAC address entry.
Port	This field displays the port number of a manually entered MAC address entry. The MAC address with port CPU means the Switch’s MAC addresses itself.
Action	Click Delete to remove this manually entered MAC address entry from the MAC address table. You cannot delete the Switch’s MAC address from the static MAC address table.

MAC Table

MAC Address Management

Static MAC Settings **MAC Table** Age Time Setting Refusal MAC Settings

MAC Table

Show Type: Static ▼ Apply Refresh Clear

MAC Address	Type	VLAN ID	Port/Trunk ID
00:22:3b:0b:80:30	Static	1	CPU

Total counts : 1

Page UP Page Down Page: 1/1 Page: 1 Apply

Parameter	Description
Show Type	Select All, Static, Dynamic or Port and then click Apply to display the corresponding MAC address entries on this screen.
Apply	
Refresh	Click this to update the information in the MAC table.
MAC Address	This field displays a MAC address.
Type	This field displays whether this entry was entered manually (Static) or whether it was learned by the Switch (Dynamic).
VLAN ID	This field displays the VLAN ID of the MAC address entry.
Port	This field displays the port number the MAC address entry is associated. It displays CPU if it is the entry for the Switch itself. The CPU means that it is the Switch's MAC.
Total Counts	This field displays the total entries in the MAC table.

Age Time Settings

MAC Address Management

Static MAC Settings MAC Table **Age Time Setting** Refusal MAC Settings

Age Time Setting

Age Time 300 (sec) (Range: 20-500 or 0:disable)

Apply Refresh

Parameter	Description
Age Time	Configure the age time; the valid range is from 20 to 500 seconds. The default value is 300 seconds.
Apply	Click Apply to take effect the settings.
Refresh	Click this to update the information in the MAC table.

Refusal (Black-hole MAC)

Introduction

These types of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries. Blackhole entries are configured for filtering out frames with specific source or destination MAC addresses

Notice: User can configure up to 20 entries.

CLI Configuration

Node	Command	Description
enable	show mac-address-table refusal	This command displays the current refusal MAC address only.
configure	mac-address-table refusal MACADDR vlan VLANID	This command configures a refusal MAC on a specific VLAN.
configure	mac-address-table refusal MACADDR	This command configures a refusal MAC.

Example: The procedures to configure a refusal MAC address

To enter the configure node.

CWGE24MS2#configure terminal

To configure a refusal MAC address for all ports and all vlans.

```
CWGE24MS2(config)#mac-address-table refusal 00:11:22:33:44:55
```

To configure a refusal MAC address for all ports on a specific vlan.

```
CWGE24MS2(config)#mac-address-table refusal 00:11:22:33:44:55 vlan 1.
```

Web Configuration

MAC Address Management

Static MAC Settings | **MAC Table** | Age Time Setting | **Refusal MAC Settings**

Refusal MAC Settings

MAC Address: VLAN ID: Any

Apply Refresh

Refusal MAC Table

MAC Address	VLAN ID	Action
00:11:22:33:44:55	Any	Delete

Total counts : **1**

Parameter	Description
MAC Address	Enter the MAC address of a computer or device that you want to refuse. Valid format is hh:hh:hh:hh:hh:hh.
VLAN ID	Enter the VLAN ID to apply to the computer or device.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
MAC Address	This field displays a MAC address.
VLAN ID	This field displays the VLAN ID of the MAC address entry.
Action	Click Delete to remove this manually entered MAC address entry from the refusal MAC address table.
Total Counts	This field displays the total entries in the refusal MAC table.

Port Mirror

Introduction

Port-based Mirroring

The Port-Based Mirroring is used on a network switch to send a copy of network packets sent/received on one or a range of switch ports to a network monitoring connection on another switch port (Monitor to Port). This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

Port Mirroring, together with a network traffic analyzer, helps to monitor network traffic. Users can monitor the selected ports (Source Ports) for egress and/or ingress packets.

Source Mode:

- Ingress : The received packets will be copied to the monitor port.
- Egress : The transmitted packets will be copied to the monitor port.
- Both : The received and transmitted packets will be copied to the monitor port.

Note:

- » The monitor port cannot be a trunk member port.
- » The monitor port cannot be ingress or egress port.
- » If the Port Mirror function is enabled, the Monitor-to Port can receive mirrored packets only.
- » If a port has been configured as a source port and then user configures the port as a destination port, the port will be removed from the source ports automatically.

Default Settings

Mirror Configurations:

- State : Disable
- Monitor port : 1
- Ingress port(s) : None
- Egress port(s) : None

CLI Configuration

Node	Command	Description
enable	show mirror	This command displays the current port mirroring configurations.
configure	mirror (disable enable)	This command disables / enables the port mirroring on the switch.
configure	mirror destination port PORT_ID	This command specifies the monitor port for the port mirroring.
configure	mirror source ports PORT_LIST mode (both ingress egress)	This command adds a port or a range of ports as the source ports of the port mirroring.
configure	no mirror source ports PORT_LIST	This command removes a port or a range of ports from the source ports of the port mirroring.

Example:

```
CWGE24MS2#configure terminal
```

```
CWGE24MS2(config)#mirror enable
```

```
CWGE24MS2(config)#mirror destination port 2
```

```
CWGE24MS2(config)#mirror source ports 3-11 mode both
```

Web Configuration

Port Mirroring

Port Mirroring Settings

State Disable ▾

Monitor to Port 1 ▾

All Ports : - ▾

Source Port	Mirror Mode	Source Port	Mirror Mode
1	Disable ▾	2	Disable ▾
3	Disable ▾	4	Disable ▾
5	Disable ▾	6	Disable ▾
7	Disable ▾	8	Disable ▾
9	Disable ▾	10	Disable ▾
11	Disable ▾	12	Disable ▾
13	Disable ▾	14	Disable ▾
15	Disable ▾	16	Disable ▾
17	Disable ▾	18	Disable ▾
19	Disable ▾	20	Disable ▾
21	Disable ▾	22	Disable ▾
23	Disable ▾	24	Disable ▾

Apply
Refresh

Parameter	Description
State	Select Enable to turn on port mirroring or select Disable to turn it off.
Monitor to Port	Select the port which connects to a network traffic analyzer.
All Ports	Settings in this field apply to all ports. Use this field only if you want to make some settings the same for all ports. Use this field first to set the common settings and then make adjustments on a port-by-port basis.
Source Port	This field displays the number of a port.
Mirror Mode	Select Ingress, Egress or Both to only copy the ingress (incoming), egress (outgoing) or both (incoming and outgoing) traffic from the specified source ports to the monitor port. Select Disable to not copy any traffic from the specified source ports to the monitor port.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Port Settings

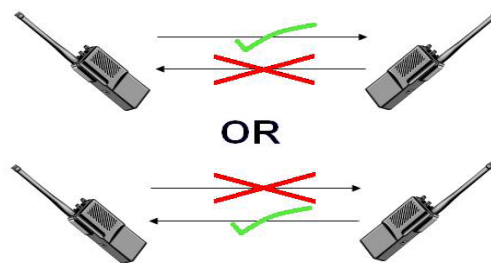
Introduction

Duplex mode

A duplex communication system is a system composed of two connected parties or devices that can communicate with one another in both directions.

Half Duplex:

A half-duplex system provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.



Full Duplex:

A full-duplex, or sometimes double-duplex system, allows communication in both directions, and, unlike half-duplex, allows this to happen simultaneously. Land-line telephone networks are full-duplex, since they allow both callers to speak and be heard at the same time.



» Loopback Test

A loopback test is a test in which a signal is sent from a communications device and returned (looped back) to it as a way to determine whether the device is working right or as a way to pin down a failing node in a network. One type of loopback test is performed using a special plug, called a wrap plug that is inserted in a port on a communications device. The effect of a wrap plug is to cause transmitted (output) data to be returned as received (input) data, simulating a complete communications circuit using a single computer.

» Auto MDI-MDIX

Auto-MDIX (automatic medium-dependent interface crossover) is a computer networking technology that automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately, thereby removing the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. When it is enabled, either type of cable can be used or the interface automatically corrects any incorrect cabling.

For Auto-MDIX to operate correctly, the speed on the interface and duplex setting must be set to "auto". Auto-MDIX was developed by HP engineers Dan Dove and Bruce Melvin.

» Auto Negotiation

Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode.

If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

» Flow Control

A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill and resend later.

The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Note: 1000 Base-T doesn't support force mode.

Default Settings

The default port Speed & Duplex is auto for all ports.

The default port Flow Control is Off for all ports.

CLI Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
configure	interface IFNAME	This command enters the interface configure node.
interface	show	This command displays the current port configurations.
interface	loopback (none mac)	This command tests the loopback mode of operation for the specific port.
interface	flowcontrol (off on)	This command disables / enables the flow control for the port.
interface	speed (auto 10-full 10-half 100-full 100-half 1000-full)	This command configures the speed and duplex for the port.
interface	shutdown	This command disables the specific port.
interface	no shutdown	This command enables the specific port.
interface	description STRINGs	This command configures a description for the specific port.
interface	no description	This command configures the default port description.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	description STRINGs	This command configures a description for the specific ports.
if-range	no description	This command configures the default port description for the specific ports.
if-range	shutdown	This command disables the specific ports.
if-range	no shutdown	This command enables the specific ports.
if-range	speed (auto 10-full 10-half 100-full 100-half 1000-full)	This command configures the speed and duplex for the port.

Example:

```
CWGE24MS2#configure terminal
```

```
CWGE24MS2(config)#interface gi1/0/1
```

```
CWGE24MS2(config-if)#speed auto
```

Web Configuration

Port Settings

General Settings

Information

Port Settings

Port	State	Speed/Duplex	Flow Control
From: 1 To: 1	Enable	Auto	Off

Apply

Refresh

Port Status

Port	State	Speed/Duplex	Flow Control	Link Status
1	Enabled	Auto	Off	Link Down
2	Enabled	Auto	Off	Link Down
3	Enabled	Auto	Off	Link Down
4	Enabled	Auto	Off	Link Down
5	Enabled	Auto	Off	Link Down
6	Enabled	Auto	Off	Link Down
7	Enabled	Auto	Off	Link Down
8	Enabled	Auto	Off	Link Down
9	Enabled	Auto	Off	Link Down
10	Enabled	Auto	Off	Link Down
11	Enabled	Auto	Off	Link Down
12	Enabled	Auto	Off	Link Down
13	Enabled	Auto	Off	Link Down
14	Enabled	Auto	Off	Link Down
15	Enabled	Auto	Off	Link Down
16	Enabled	Auto	Off	Link Down
17	Enabled	Auto	Off	Link Down
18	Enabled	Auto	Off	Link Down
19	Enabled	Auto	Off	Link Down
20	Enabled	Auto	Off	Link Down
21	Enabled	Auto	Off	Link Down
22	Enabled	Auto	Off	Link Down
23	Enabled	Auto	Off	Link Down
24	Enabled	Auto	Off	100M / Full / Off

Parameter	Description
Port	Select a port or a range ports you want to configure on this screen.
State	Select Enable to activate the port or Disable to deactivate the port.
Speed/Duplex	Select the speed and duplex mode of the port. The choices are: <ul style="list-style-type: none">• Auto• 10 Mbps / Full Duplex• 10 Mbps / Half Duplex• 100 Mbps / Full Duplex• 100 Mbps / Half Duplex• 1000 Mbps / Full Duplex
Flow Control	Select On to enable access to buffering resources for the port thus ensuring lossless operation across network switches. Otherwise, select Off to disable it.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port	This field displays the port number.
State	This field displays whether the port is enabled or disabled.
Speed/Duplex	This field displays the speed either 10M, 100M or 1000M and the duplex mode Full or Half.
Flow Control	This field displays whether the port's flow control is On or Off.
Link Status	This field displays the link status of the port. If the port is up, it displays the port's speed, duplex and flow control setting. Otherwise, it displays Link Down if the port is disabled or not connected to any device.

Information:

Port Settings

General Settings
Information

Port Settings

Port
 From: 1 To: 1

Description
 gigabitethernet1/0/1

Apply
Refresh

Port Status

Port	Description	Status	Uptime	Medium Mode
1	gigabitethernet1/0/1	Normally	0 days 0:0:0	Fiber
2	gigabitethernet1/0/2	Normally	0 days 0:0:0	Fiber
3	gigabitethernet1/0/3	Normally	0 days 0:0:0	Fiber
4	gigabitethernet1/0/4	Normally	0 days 0:0:0	Fiber
5	gigabitethernet1/0/5	Normally	0 days 0:0:0	Fiber
6	gigabitethernet1/0/6	Normally	0 days 0:0:0	Fiber
7	gigabitethernet1/0/7	Normally	0 days 0:0:0	Fiber
8	gigabitethernet1/0/8	Normally	0 days 0:0:0	Fiber
9	gigabitethernet1/0/9	Normally	0 days 0:0:0	Fiber
10	gigabitethernet1/0/10	Normally	0 days 0:0:0	Fiber
11	gigabitethernet1/0/11	Normally	0 days 0:0:0	Fiber
12	gigabitethernet1/0/12	Normally	0 days 0:0:0	Fiber
13	gigabitethernet1/0/13	Normally	0 days 0:0:0	Fiber
14	gigabitethernet1/0/14	Normally	0 days 0:0:0	Fiber
15	gigabitethernet1/0/15	Normally	0 days 0:0:0	Fiber
16	gigabitethernet1/0/16	Normally	0 days 0:0:0	Fiber
17	gigabitethernet1/0/17	Normally	0 days 0:0:0	Fiber
18	gigabitethernet1/0/18	Normally	0 days 0:0:0	Fiber
19	gigabitethernet1/0/19	Normally	0 days 0:0:0	Fiber
20	gigabitethernet1/0/20	Normally	0 days 0:0:0	Fiber
21	gigabitethernet1/0/21	Normally	0 days 0:0:0	None
22	gigabitethernet1/0/22	Normally	0 days 0:0:0	None
23	gigabitethernet1/0/23	Normally	0 days 0:0:0	None
24	gigabitethernet1/0/24	Normally	0 days 0:38:11	Copper

Parameter	Description
Port	Select a port or a range ports you want to configure on this screen.
Description	Configures a meaningful name for the port(s).
Port Status	
Port	This field displays the port number.
Description	The meaningful name for the port.
Status	The field displays the detail port status if the port is blocked by some protocol.
Uptime	The sustained time from last link up.
Medium Mode	The current working medium mode, copper or fiber, for the port.

Advanced Settings

Bandwidth Control

QoS

Introduction

Each egress port can support up to 8 transmit queues. Each egress transmit queue contains a list specifying the packet transmission order. Every incoming frame is forwarded to one of the 8 egress transmit queues of the assigned egress port, based on its priority. The egress port transmits packets from each of the 8 transmit queues according to a configurable scheduling algorithm, which can be a combination of Strict Priority (SP) and/or Weighted Round Robin (WRR).

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to give preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The Switch supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 7 (Class 7) – the highest priority queue – to 0 (Class 0) – the lowest priority queue.

The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

Priority	: 0 1 2 3 4 5 6 7
Queue	: 2 0 1 3 4 5 6 7

Priority scheduling is implemented by the priority queues stated above. The Switch will empty the four hardware priority queues in order, beginning with the highest priority queue, 7, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

QoS Enhancement

You can configure the Switch to prioritize traffic even if the incoming packets are not marked with IEEE 802.1p priority tags or change the existing priority tags based on the criteria you select. The Switch allows you to choose one of the following methods for assigning priority to incoming packets on the Switch:

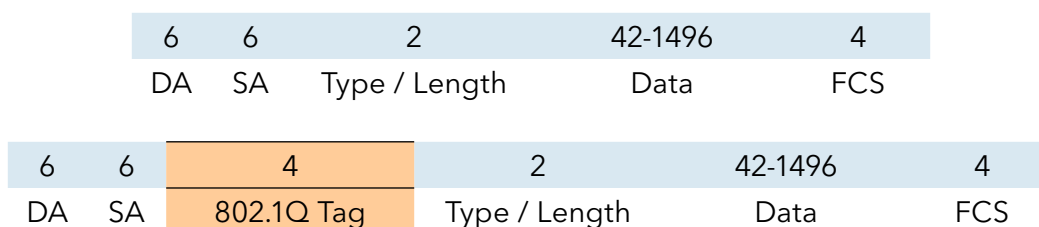
- » 802.1p Tag Priority - Assign priority to packets based on the packet's 802.1p tagged priority.
- » Port Based QoS - Assign priority to packets based on the incoming port on the Switch.
- » DSCP Based QoS - Assign priority to packets based on their Differentiated Services Code Points (DSCPs).

Note: *Advanced QoS methods only affect the internal priority queue mapping for the Switch. The Switch does not modify the IEEE 802.1p value for the egress frames. You can choose one of these ways to alter the way incoming packets are prioritized or you can choose not to use any QoS enhancement setting on the Switch.*

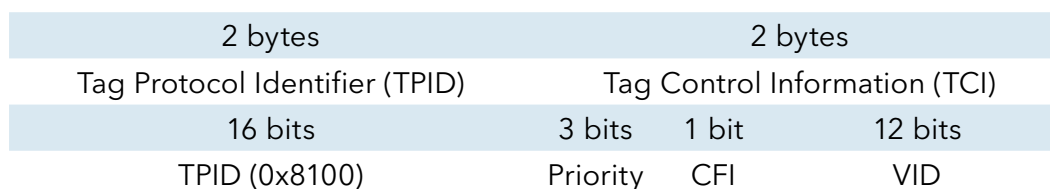
802.1p Priority

When using 802.1p priority mechanism, the packet is examined for the presence of a valid 802.1p priority tag. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

Ethernet Packet:



802.1Q Tag:



- » Tag Protocol Identifier (TPID): a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame.
- » Tag Control Information (TCI)
 - › Priority Code Point (PCP): a 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different

classes of traffic (voice, video, data, etc.).

- › Canonical Format Indicator (CFI): a 1-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format. It is always set to zero for Ethernet switches. CFI is used for compatibility between Ethernet and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be bridged to an untagged port.
- › VLAN Identifier (VID): a 12-bit field specifying the VLAN to which the frame belongs. A value of 0 means that the frame doesn't belong to any VLAN; in this case the 802.1Q tag specifies only a priority and is referred to as a priority tag. A value of hex 0xFFF is reserved for implementation use. All other values may be used as VLAN identifiers, allowing up to 4094 VLANs. On bridges, VLAN 1 is often reserved for management.

Priority Levels

PCP: Priority Code Point.

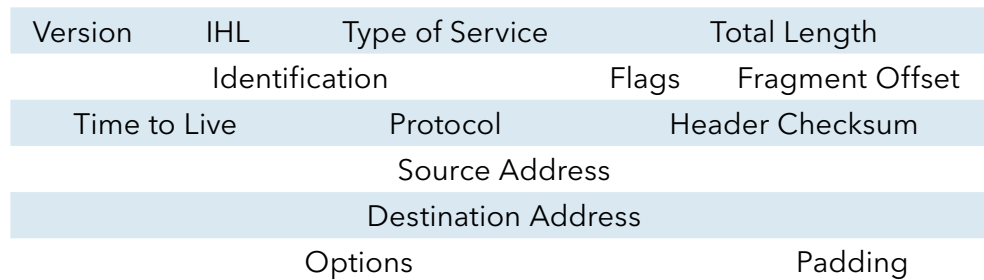
PCP	Network Priority	Traffic Characteristics
1	0 (lowest)	Background
0	1	Best Effort
2	2	Excellent Effort
3	3	Critical Applications
4	4	Video, <100ms latency
5	5	Video, < 10ms latency
6	6	Internetwork Control
7	7 (highest)	Network Control

DiffServ (DSCP)

Differentiated Services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing Quality of Service (QoS) guarantees on modern IP networks. DiffServ can, for example, be used to provide low-latency, guaranteed service (GS) to critical network traffic such as voice or video while providing simple best-effort traffic guarantees to non-critical services such as web traffic or file transfers.

Differentiated Services Code Point (DSCP) is a 6-bit field in the header of IP packets for packet classification purposes. DSCP replaces the outdated IP precedence, a 3-bit field in the Type of Service byte of the IP header originally used to classify and prioritize types of traffic.

When using the DiffServ priority mechanism, the packet is classified based on the DSCP field in the IP header. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.



Example Internet Datagram Header

IP Header Type of Service: 8 bits

The Type of Service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Several networks offer service precedence, which somehow treats high precedence traffic as more important than other traffic (generally by accepting only traffic above certain precedence at time of high load). The major choice is a three way tradeoff between low-delay, high-reliability, and high-throughput.

Bits 0-2: Precedence.

Bit 3: 0 = Normal Delay, 1 = Low Delay.

Bits 4: 0 = Normal Throughput, 1 = High Throughput.

Bits 5: 0 = Normal Reliability, 1 = High Reliability.

Bit 6-7: Reserved for Future Use.

```

0    1    2    3    4    5    6    7
+----+----+----+----+----+----+----+----+
| PRECEDENCE | D | T | R | 0 | 0 |
+----+----+----+----+----+----+----+----+

```

Precedence

- 111 - Network Control
- 110 - Internetwork Control
- 101 - CRITIC/ECP
- 100 - Flash Override
- 011 - Flash
- 010 - Immediate
- 001 - Priority
- 000 - Routine

The use of the Delay, Throughput, and Reliability indications may increase the cost (in some sense) of the service. In many networks better performance for one of these parameters is coupled with worse performance on another. Except for very unusual cases at most two of these three indications should be set.

The type of service is used to specify the treatment of the datagram during its transmission through the internet system. Example mappings of the internet type of service to the actual service provided on networks such as AUTODIN II, ARPANET, SATNET, and PRNET is given in "Service Mappings".

The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway control originators only.

If the actual use of these precedence designations is of concern to a particular network, it is the responsibility of that network to control the access to, and use of, those precedence designations.

DSCP	Priority	DSCP	Priority	DSCP	Priority
0	0	1	0	2	0
...					
60	0	61	0	62	0
63	0				

Example:

IP Header

DSCP=50 => 45 C8 . . .

Queuing Algorithms

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

» Strict-Priority (SPQ)

The packets on the high priority queue are always service firstly.

» Weighted round robin (WRR)

Round Robin scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin (WRR) scheduling uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue Weight field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

Default Settings

QoS mode : High First (SPQ)

The mappings of the Priority to Queue are:

PRI0 0 ==> COSQ 2
PRI0 1 ==> COSQ 0
PRI0 2 ==> COSQ 1
PRI0 3 ==> COSQ 3
PRI0 4 ==> COSQ 4
PRI0 5 ==> COSQ 5
PRI0 6 ==> COSQ 6
PRI0 7 ==> COSQ 7

The DiffServ is disabled on the switch.

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
----	-----	----	-----	----	-----	----	-----
00	0	01	0	02	0	03	0
04	0	05	0	06	0	07	0
08	0	09	0	10	0	11	0
12	0	13	0	14	0	15	0
16	0	17	0	18	0	19	0
20	0	21	0	22	0	23	0
24	0	25	0	26	0	27	0
28	0	29	0	30	0	31	0
32	0	33	0	34	0	35	0
36	0	37	0	38	0	39	0
40	0	41	0	42	0	43	0
44	0	45	0	46	0	47	0
48	0	49	0	50	0	51	0
52	0	53	0	54	0	55	0
56	0	57	0	58	0	59	0
60	0	61	0	62	0	63	0

Note: If the DiffServ is disabled, the 802.1p tag priority will be used.

CLI Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the service queue.
enable	show qos mode	This command displays the current QoS scheduling mode of IEEE 802.1p.
configure	queue cos-map PRIORITY QUEUE_ID	This command configures the 802.1p priority mapping to the service queue.
configure	no queue cos-map	This command configures the 802.1p priority mapping to the service queue to default.
configure	qos mode high-first	This command configures the QoS scheduling mode to high_first, each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets.
configure	qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE	This command configures the QoS scheduling mode to Weighted Round Robin.
interface	default-priority	This command allows the user to specify a default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine which of the hardware priority queues the packet is forwarded to. Default: 0.
interface	no default-priority	This command configures the default priority for the specific port to default (0).
enable	show diffserv	This command displays DiffServ configurations.
configure	diffserv (disable enable)	This command disables / enables the DiffServ function.
configure	diffserv dscp VALUE priority VALUE	This command sets the DSCP-to-IEEE 802.1q mappings.

Web Configuration

Port Priority

QoS

Port Priority
IP DiffServ (DSCP)
Priority/Queue Mapping
Schedule Mode

Port Priority Settings

All Ports 802.1p priority : - ▾

Port	802.1p priority	Port	802.1p priority
1	0 ▾	2	0 ▾
3	0 ▾	4	0 ▾
5	0 ▾	6	0 ▾
7	0 ▾	8	0 ▾
9	0 ▾	10	0 ▾
11	0 ▾	12	0 ▾
13	0 ▾	14	0 ▾
15	0 ▾	16	0 ▾
17	0 ▾	18	0 ▾
19	0 ▾	20	0 ▾
21	0 ▾	22	0 ▾
23	0 ▾	24	0 ▾

Apply
Refresh

Parameter	Description
All Ports 802.1p priority	Use this field to set a priority for all ports. The value indicates packet priority and is added to the priority tag field of incoming packets. The values range from 0 (lowest priority) to 7 (highest priority).
Port	This field displays the number of a port.
802.1p Priority	Select a priority for packets received by the port. Only packets without 802.1p priority tagged will be applied the priority you set here.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

IP DiffServ (DSCP)

QoS

Port Priority
IP DiffServ (DSCP)
Priority/Queue Mapping
Schedule Mode

DSCP Settings

Mode Tag Over DSCP ▼

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
DSCP 0	0 ▼	DSCP 1	0 ▼	DSCP 2	0 ▼	DSCP 3	0 ▼
DSCP 4	0 ▼	DSCP 5	0 ▼	DSCP 6	0 ▼	DSCP 7	0 ▼
DSCP 8	0 ▼	DSCP 9	0 ▼	DSCP 10	0 ▼	DSCP 11	0 ▼
DSCP 12	0 ▼	DSCP 13	0 ▼	DSCP 14	0 ▼	DSCP 15	0 ▼
DSCP 16	0 ▼	DSCP 17	0 ▼	DSCP 18	0 ▼	DSCP 19	0 ▼
DSCP 20	0 ▼	DSCP 21	0 ▼	DSCP 22	0 ▼	DSCP 23	0 ▼
DSCP 24	0 ▼	DSCP 25	0 ▼	DSCP 26	0 ▼	DSCP 27	0 ▼
DSCP 28	0 ▼	DSCP 29	0 ▼	DSCP 30	0 ▼	DSCP 31	0 ▼
DSCP 32	0 ▼	DSCP 33	0 ▼	DSCP 34	0 ▼	DSCP 35	0 ▼
DSCP 36	0 ▼	DSCP 37	0 ▼	DSCP 38	0 ▼	DSCP 39	0 ▼
DSCP 40	0 ▼	DSCP 41	0 ▼	DSCP 42	0 ▼	DSCP 43	0 ▼
DSCP 44	0 ▼	DSCP 45	0 ▼	DSCP 46	0 ▼	DSCP 47	0 ▼
DSCP 48	0 ▼	DSCP 49	0 ▼	DSCP 50	0 ▼	DSCP 51	0 ▼
DSCP 52	0 ▼	DSCP 53	0 ▼	DSCP 54	0 ▼	DSCP 55	0 ▼
DSCP 56	0 ▼	DSCP 57	0 ▼	DSCP 58	0 ▼	DSCP 59	0 ▼
DSCP 60	0 ▼	DSCP 61	0 ▼	DSCP 62	0 ▼	DSCP 63	0 ▼

Apply
Refresh

Parameter	Description
Mode	"Tag Over DSCP" or "DSCP Over Tag". "Tag Over DSCP" means the 802.1p tag has higher priority than DSCP.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Priority/Queue Mapping

QoS

Port Priority IP DiffServ (DSCP) **Priority/Queue Mapping** Schedule Mode

Priority/Queue Mapping Settings

Priority	Queue ID
0	1 ▼
1	0 ▼
2	2 ▼
3	3 ▼
4	4 ▼
5	5 ▼
6	6 ▼
7	7 ▼

Parameter	Description
Reset to Default	Click this button to reset the priority to queue mappings to the defaults.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Queue ID	Select the number of a queue for packets with the priority level.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Schedule Mode

Queue ID	Weight Value (Range:1~127)
0	<input type="text"/>
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>

Parameter	Description
Schedule Mode	Select Strict Priority (SP) or Weighted Round Robin (WRR). Note: Queue weights can only be changed when Weighted Round Robin is selected. Weighted Round Robin scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights.
Queue ID	This field indicates which Queue (0 to 7) you are configuring. Queue 0 has the lowest priority and Queue 7 the highest priority.
Weight Value	You can only configure the queue weights when Weighted Round Robin is selected. Bandwidth is divided across the different traffic queues according to their weights.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Rate Limitation

Storm Control

Introduction

A broadcast storm means that your network is overwhelmed with constant broadcast or multicast traffic. Broadcast storms can eventually lead to a complete loss of network connectivity as the packets proliferate.

Storm Control protects the Switch bandwidth from flooding packets, including broadcast packets, multicast packets, and destination lookup failure (DLF). The Rate is a threshold that limits the total number of the selected type of packets. For example, if the broadcast and multicast options are selected, the total amount of packets per second for those two types will not exceed the limit value.

Broadcast storm control limits the number of broadcast, multicast and unknown unicast (also referred to as Destination Lookup Failure or DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and unknown unicast packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and unknown unicast packets in your network.

Storm Control unit: 652pps.

Default Settings

Broadcast Storm Control : 652pps.

Multicast Storm Control : None.

DLF Storm Control : 652pps.

CLI Configuration

Node	Command	Description
enable	show storm-control	This command displays the current storm control configurations.
configure	storm-control rate RATE_LIMIT type (bcast mcast DLF bcast+mcast bcast+DLF mcast+DLF bcast+mcast+DLF) ports PORTLISTS	This command enables the bandwidth limit for broadcast or multicast or DLF packets and set the limitation.
configure	no storm-control type (bcast mcast DLF bcast+mcast bcast+DLF mcast+DLF bcast+mcast+DLF) ports PORTLISTS	This command disables the bandwidth limit for broadcast or multicast or DLF packets.

Example:

CWGE24MS2#configure terminal

CWGE24MS2(config)#storm-control rate 1 type broadcast ports 1-6

CWGE24MS2(config)#storm-control rate 1 type multicast ports 1-6

CWGE24MS2(config)#storm-control rate 1 type DLF ports 1-6

Web Configuration

Rate Limitation									
Storm Control					Bandwidth Limitation				
Storm Control Settings									
Port		Rate			Type				
From: 1 ▼ To: 1 ▼		0 (units)			Mcast(Multicast) ▼				
(Disable:0. One unit is about 652 pps.)									
Apply					Refresh				
Storm Control Status									
Port	Rate(units)	Multicast	Broadcast	DLF	Port	Rate(units)	Multicast	Broadcast	DLF
1	1	Disable	Enable	Enable	2	1	Disable	Enable	Enable
3	1	Disable	Enable	Enable	4	1	Disable	Enable	Enable
5	1	Disable	Enable	Enable	6	1	Disable	Enable	Enable
7	1	Disable	Enable	Enable	8	1	Disable	Enable	Enable
9	1	Disable	Enable	Enable	10	1	Disable	Enable	Enable
11	1	Disable	Enable	Enable	12	1	Disable	Enable	Enable
13	1	Disable	Enable	Enable	14	1	Disable	Enable	Enable
15	1	Disable	Enable	Enable	16	1	Disable	Enable	Enable
17	1	Disable	Enable	Enable	18	1	Disable	Enable	Enable
19	1	Disable	Enable	Enable	20	1	Disable	Enable	Enable
21	1	Disable	Enable	Enable	22	1	Disable	Enable	Enable
23	1	Disable	Enable	Enable	24	1	Disable	Enable	Enable

Parameter	Description
Port	Select the port number for which you want to configure storm control settings.
Rate	Select the number of packets (of the type specified in the Type field) per second the Switch can receive per second.
Type	Select Broadcast - to specify a limit for the amount of broadcast packets received per second. Multicast - to specify a limit for the amount of multicast packets received per second. DLF - to specify a limit for the amount of DLF packets received per second.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Bandwidth Limitation

Introduction

The rate limitation is used to control the rate of traffic sent or received on a network interface.

Rate Limitation unit: Mbs.

Default Settings

All ports' Ingress and Egress rate limitation are disabled.

CLI Configuration

Node	Command	Description
enable	show bandwidth-limit	This command displays the current rate control configurations.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for outgoing packets and set the limitation.
configure	no bandwidth-limit egress ports PORTLISTS	This command disables the bandwidth limit for outgoing packets.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for incoming packets and set the limitation.
configure	no bandwidth-limit ingress ports PORTLISTS	This command disables the bandwidth limit for incoming packets.

Example:

```
CWGE24MS2#configure terminal
```

```
CWGE24MS2(config)#bandwidth-limit egress 1 ports 1-8
```

```
CWGE24MS2(config)#bandwidth-limit ingress 1 ports 1-8
```


Web Configuration

Rate Limitation					
Storm Control		Bandwidth Limitation			
Bandwidth Limitation Settings					
Port		Ingress		Egress	
From:	1 ▼ To: 1 ▼	0 (Mbs)		0 (Mbs)	
(Disable:0)					
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>					
Bandwidth Limitation Status					
Port	Ingress (Mbs)	Egress (Mbs)	Port	Ingress (Mbs)	Egress (Mbs)
1	0	0	2	0	0
3	0	0	4	0	0
5	0	0	6	0	0
7	0	0	8	0	0
9	0	0	10	0	0
11	0	0	12	0	0
13	0	0	14	0	0
15	0	0	16	0	0
17	0	0	18	0	0
19	0	0	20	0	0
21	0	0	22	0	0
23	0	0	24	0	0

Parameter	Description
Port	Selects a port that you want to configure.
Ingress	Configures the rate limitation for the ingress packets.
Egress	Configures the rate limitation for the egress packets.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

DHCPv6

DHCPv6 Options

CLI Configurations

Node	Command	Description
enable	show ipv6 dhcp-options	This command displays the IPv6 DHCP option configurations.
configure	ipv6 dhcp-options option_18 (disable enable)	This command enables/disables the IPv6 DHCP option 18.
configure	ipv6 dhcp-options option_37	This command enables/disables the IPv6 DHCP option 37.

Web Configurations

Option 18

Parameter	Description
Option 18 State	The field enables / disables the option 18.

Option 37

Parameter	Description
Option 37 State	The field enables / disables the option 37.

DHCPv6 Relay

CLI Configurations

Node	Command	Description
enable	show ipv6 dhcp relay	This command displays the IPv6 DHCP Relay configurations.
configure	ipv6 dhcp relay (enable disable)	This command enables/disables the IPv6 DHCP Relay.
configure	ipv6 dhcp relay hops_count_limit <1-32>	This command configures hop count limitation for IPv6 DHCP Relay.
configure	ipv6 dhcp relay vlan STRINGS	This command enables the IPv6 DHCP Relay in a vlan or a range of vlan.
configure	no ipv6 dhcp relay vlan STRINGS	This command disables the IPv6 DHCP Relay in a vlan or a range of vlan.

Web Configurations

DHCPv6 Relay

DHCPv6 Relay Settings

State Disable ▾

Hops Count Limit 32 (Range:1-32)

VLAN State Add ▾

DHCPv6 Server IP

Apply
Refresh

DHCPv6 Relay Status

DHCPv6 Relay State	Disabled
Hops Count Limit	32
Enabled on VLAN	None
DHCPv6 Server IP	

Parameter	Description
State	The field enables / disables the Ipv6 DHCP Relay.
Hops Count Limit	The field configures the hops count limit for the IPv6 DHCP Relay.
VLAN State	The field enables / disables the Ipv6 DHCP Relay in a vlan or a range of vlans.
DHCPv6 Server IP	The field configures the DHCPv6 server's IP.

IGMP Snooping

IGMP Snooping

Introduction

The IGMP snooping is for multicast traffic. The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch can perform IGMP snooping on up to 4094 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first VLANs that send IGMP packets. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

Immediate Leave

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN. (Immediate Leave is only supported on IGMP Version 2 hosts).

The switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the switch sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Fast Leave

The switch allow user to configure a delay time. When the delay time is expired, the switch removes the interface from the multicast group.

Last Member Query Interval

Last Member Query Interval: The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages.

Without Immediate Leave, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP specific query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is

INS_CWGE24MS2_REV-

removed from multicast group membership.

IGMP Querier

There is normally only one Querier per physical network. All multicast routers start up as a Querier on each attached network. If a multicast router hears a Query message from a router with a lower IP address, it MUST become a Non-Querier on that network. If a router has not heard a Query message from another router for [Other Querier Present Interval], it resumes the role of Querier. Routers periodically [Query Interval] send a General Query on each attached network for which this router is the Querier, to solicit membership information. On startup, a router SHOULD send [Startup Query Count] General Queries spaced closely together [Startup Query Interval] in order to quickly and reliably determine membership information. A General Query is addressed to the all-systems multicast group (224.0.0.1), has a Group Address field of 0, and has a Max Response Time of [Query Response Interval].

Port IGMP Querier Mode

» Auto:

The Switch uses the port as an IGMP query port if the port receives IGMP query packets.

» Fixed:

The Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). The Switch always forwards the client's report/leave packets to the port.

Normally, the port is connected to an IGMP server.

» Edge:

The Switch does not use the port as an IGMP query port. The IGMP query packets received by this port will be dropped.

Normally, the port is connected to an IGMP client.

Note: *The Switch will forward the IGMP join and leave packets to the query port.*

Configurations:

Users can enable/disable the IGMP Snooping on the Switch. Users also can enable/disable the IGMP Snooping on a specific VLAN. If the IGMP Snooping on the Switch is disabled, the IGMP Snooping is disabled on all VLANs even some of the VLAN IGMP Snooping are enabled.

Default Settings

If received packets are not received after 400 seconds, all multicast entries will be deleted.

The default global IGMP snooping state is disabled.

The default VLAN IGMP snooping state is disabled for all VLANs.

The unknown multicast packets will be dropped.

The default port Immediate Leave state is disabled for all ports.

The default port Querier Mode state is auto for all ports.

The IGMP snooping Report Suppression is disabled.

Notices:

There are a global state and per VLAN states. When the global state is disabled, the IGMP snooping on the Switch is disabled even per VLAN states are enabled. When the global state is enabled, user must enable per VLAN states to enable the IGMP Snooping on the specific VLAN.

CLI Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
enable	show igmp-snooping counters	This command displays the current IGMP snooping counters.
enable	show igmp-snooping querier	This command displays the current IGMP Queriers.
enable	show multicast	This command displays the multicast group in IP format.
configure	clear igmp-snooping counters	This command clears all of the IGMP snooping counters.
configure	igmp-snooping (disable enable)	This command disables / enables the IGMP snooping on the switch.
configure	igmp-snooping vlan VLANID	This command enables the IGMP snooping function on a VLAN or range of VLANs.
configure	no igmp-snooping vlan VLANID	This command disables the IGMP snooping function on a VLAN or range of VLANs.
configure	igmp-snooping unknown-multicast (drop flooding)	This command configures the process for unknown multicast packets when the IGMP snooping function is enabled. drop: Drop all of the unknown multicast packets.
configure	igmp-snooping report-suppression (disable enable)	This command disables / enables the IGMP snooping report suppression function on the switch.

Node	Command	Description
configure	clear igmp-counters	This command clears the IGMP snooping counters.
configure	clear igmp-counters (port vlan)	This command clears the IGMP snooping counters for port or vlan.
interface	igmp-querier-mode (auto fixed edge)	This command specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default:auto)
interface	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific interface.
interface	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific interface.
interface	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific interface.
interface	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific interface.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific ports.
if-range	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific ports.
if-range	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific ports.
if-range	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific ports.
if-range	igmp-querier-mode (auto fixed edge)	This command specifies whether or not and under what conditions the ports is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default:auto)

Example:

```

CWGE24MS2(config)#igmp-snooping enable
CWGE24MS2(config)#igmp-snooping vlan 1
CWGE24MS2(config)#igmp-snooping querier enable
CWGE24MS2(config)#igmp-snooping querier vlan 1
CWGE24MS2(config)#interface 1/0/1
CWGE24MS2(config-if)#igmp-immediate-leave
CWGE24MS2(config-if)#igmp-querier-mode fixed
CWGE24MS2(config-if)#igmp-snooping group-limit 20

```

Web Configuration

General Settings

IGMP Snooping

General Settings
Port Settings
Querier Settings

IGMP Snooping Settings

IGMP Snooping State

Report Suppression State

IGMP Snooping VLAN State

Unknown Multicast Packets

Enable ▼

Enable ▼

Add ▼ 1

Drop ▼

IGMP Snooping Status

IGMP Snooping State	Enabled
Report Suppression State	Enabled
IGMP Snooping VLAN State	1
Unknown Multicast Packets	Drop

Parameter	Description
IGMP Snooping State	Select Enable to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select Disable to deactivate the feature.
Report Suppression State	Select Enable/Disable to activate/deactivate IGMP Snooping report suppression function.
IGMP Snooping VLAN State	Select Add and enter VLANs upon which the Switch is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLANs. Select Delete and enter VLANs on which to have the Switch not perform IGMP snooping.
Unknown Multicast Packets	Specify the action to perform when the Switch receives an unknown multicast frame. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
IGMP Snooping State	This field displays whether IGMP snooping is globally enabled or disabled.
Report Suppression State	This field displays whether IGMP snooping report suppression is enabled or disabled.
IGMP Snooping VLAN State	This field displays VLANs on which the Switch is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any port yet.
Unknown Multicast Packets	This field displays whether the Switch is set to discard or flood unknown multicast packets.

Port Settings

IGMP Snooping

General Settings
Port Settings
Querier Settings

Port Settings

Port	Querier Mode	Immediate Leave	Group Limit
From: 1 To: 1	Auto	Disable	256

Apply
Refresh

Port Status

Port	Querier Mode	Immediate Leave	Group/Limit	Port	Querier Mode	Immediate Leave	Group/Limit
1	Auto	Disable	0/256	2	Auto	Disable	0/256
3	Auto	Disable	0/256	4	Auto	Disable	0/256
5	Auto	Disable	0/256	6	Auto	Disable	0/256
7	Auto	Disable	0/256	8	Auto	Disable	0/256
9	Auto	Disable	0/256	10	Auto	Disable	0/256
11	Auto	Disable	0/256	12	Auto	Disable	0/256
13	Auto	Disable	0/256	14	Auto	Disable	0/256
15	Auto	Disable	0/256	16	Auto	Disable	0/256
17	Auto	Disable	0/256	18	Auto	Disable	0/256
19	Auto	Disable	0/256	20	Auto	Disable	0/256
21	Auto	Disable	0/256	22	Auto	Disable	0/256
23	Auto	Disable	0/256	24	Auto	Disable	3/256

Parameter	Description
Querier Mode	Select the desired setting, Auto, Fixed, or Edge. Auto means the Switch uses the port as an IGMP query port if the port receives IGMP query packets. Fixed means the Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). Edge means the Switch does not use the port as an IGMP query port. In this case, the Switch does not keep a record of an IGMP router being connected to this port and the Switch does not forward IGMP join or leave packets to this port.
Immediate Leave	Select individual ports on which to enable immediate leave.
Group Limit	Configures the maximum group for the port or a range of ports.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields.
Port	The port ID.
Querier Mode	The Querier mode setting for the specific port.
Immediate Leave	The Immediate Leave setting for the specific port.
Group Counts	The current joining group count and the maximum group count.

IGMP Snooping Querier

CLI Configurations

Node	Command	Description
configure	igmp-snooping querier (disable enable)	This command disables / enables the IGMP snooping querier on the Switch.
configure	igmp-snooping querier vlan VLANIDs	This command enables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	no igmp-snooping querier vlan VLANIDs	This command disables the IGMP snooping querier function on a VLAN or range of VLANs.

Web Configurations

IGMP Snooping

General Settings

Port Settings

Querier Settings

Querier Settings

Querier State

Enable

Querier VLAN State

Add

1

Apply

Refresh

Querier Status

Querier State

Enable

Querier VLAN State

1

Parameter	Description
Querier State	This field configures the global Querier state.
Querier VLAN State	This field enables the Querier state in a vlan or a range of vlan.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields to the last setting.
Querier State	This field indicates the current global Querier status.
Querier VLAN State	This field indicates the Querier status in vlan.

IGMP Snooping Filtering

The IGMP Snooping Filter allows users to configure one or some of range or multicast address to drop or to forward them.

CLI Configurations

Node	Command	Description
enable	show igmp-snooping filtering	This command displays the IGMP snooping filtering configurations.
configure	igmp-snooping filtering (enable disable)	This command enables/disables the IGMP snooping filtering profiles on the Switch.
configure	igmp-snooping filtering profile	This command enters the IGMP snooping filtering profiles configuration node.
configure	no igmp-snooping filtering all	This command removes all of the IGMP snooping filtering profiles from the Switch.
configure	no igmp-snooping filtering STRINGS	This command removes the IGMP snooping filtering profiles by name from the Switch.
config-igmp	Group GROUP_ID start-address START-ADDR end-address END-ADDR	This command configures the group configurations, including group index and start multicast address and end multicast address.
config-igmp	type (deny permit)	This command configures the type of deny or permit for the group.
config-igmp	no group GROUP-ID	This command removes the group configurations.
config-igmp	no group all	This command removes all of the group configurations.
config-igmp	type (deny permit)	This command configures the type of deny or permit for the group.
interface	igmp-snooping filtering profile STRING	This command enables the IGMP snooping filtering profiles on the specific port.
interface	no igmp-snooping filtering profile STRINGS	This command disables the IGMP snooping filtering profiles on the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-config	igmp-snooping filtering profile STRING	This command enables the IGMP snooping filtering profiles on the range of ports.
if-config	no igmp-snooping filtering profile STRINGS	This command disables the IGMP snooping filtering profiles on the range of ports.

Web Configurations

General Settings

IGMP Snooping Filter

General Settings

Group Settings

Port Settings

IGMP Snooping Filter Settings

State:

Disable

Profile

Type

Deny

Apply

Refresh

IGMP Snooping Filter Status

Profile	Type	Ports	Action
---------	------	-------	--------

Parameter	Description
IGMP Filtering State	This field configures the global IGMP Filtering state.
Profile	This field creates the IGMP Filtering profile.
Type	The field configures the type of action for the profile.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields to the last setting.
IGMP Filtering Status	
Profile	The profile name.
Type	The type of action.
Ports	The field indicates the ports that the IGMP Filtering profile is activated.
Action	Click the “Delete” button to delete the profile.

Group Settings

IGMP Snooping Filter

General Settings

Group Settings

Port Settings

Group Settings

Profile :

Group	Start Address	End Address
1 <div></div>	<div></div>	<div></div>

Apply

Refresh

Group Status

Profile	Type	Group	Start Address	End Address	Action
---------	------	-------	---------------	-------------	--------

Parameter	Description
Profile	This field selects the profile which you want to configure the group.
Group	This field selects the group index.
Start Address	The field configures the first multicast address of the group.
End Address	The field configures the last multicast address of the group.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields to the last setting.

Port Settings

IGMP Snooping Filter

General Settings

Group Settings

Port Settings

Ports Settings

Profile :

Activate on Ports

Select All

Deselect All

1357911131517192123

24681012141618202224

Apply

Refresh

Ports Status

Profile	Type	Port
---------	------	------

Parameter	Description
Profile	This field selects the profile which you want to activate on the ports.
Activate IGMP Filtering on Ports	Selects the ports which you want to activate the IGMP Filtering profile.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields to the last setting.

TECH SUPPORT: 1.888.678.9427

INS_CWGE24MS2_REV-
10/05/16 PAGE 82

MVR

Introduction

MVR refers to Multicast VLAN Registration that enables a media server to transmit multicast stream in a single multicast VLAN while clients receiving multicast VLAN stream can reside in different VLANs. Clients in different VLANs intend to join or leave the multicast group simply by sending the IGMP Join/leave message to a receiver port. The receiver port belonging to one of the multicast groups can receive multicast stream from media server. Without support of MVR, the Multicast stream from media server and subscriber must reside in the same VLAN.

- » Source ports : The Stream source ports.
- » Receiver ports : The Client ports.
- » Tagged ports : Configure the tagged ports for source ports or receiver ports.

MVR Mode

» Dynamic Mode:

If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will be forwarded to a multicast router through its source port. Multicast router knows which multicast groups exist on which interface dynamically.

» Compatible mode:

If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will not be transmitted to a multicast router.

Operation Mode

» Join Operation:

A subscriber sends an IGMP report message to the switch to join the appropriate multicast. The next depends on whether the IGMP report matches the switch configured multicast MAC address. If it matches, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of MVLAN.

» Leave Operation:

Subscriber sends an IGMP leave message to the switch to leave the multicast. The switch CPU sends an IGMP group-specific query through the receiver port VLAN. If there is another subscriber in the VLAN, subscriber must respond within the max response time. If there is no subscriber, the switch would eliminate this receiver port.

» Immediate Leave Operation:

Subscriber sends an IGMP leave message to the switch to leave the multicast. Subscribers do not need to wait for the switch CPU to send an IGMP group-specific query through the receiver port VLAN. The switch will immediately eliminate this receiver port.

Figure-1:

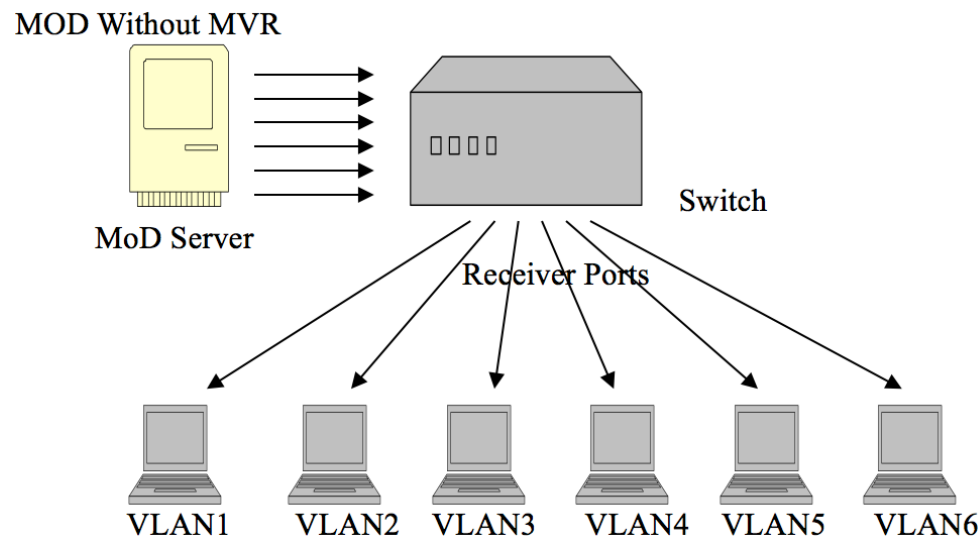
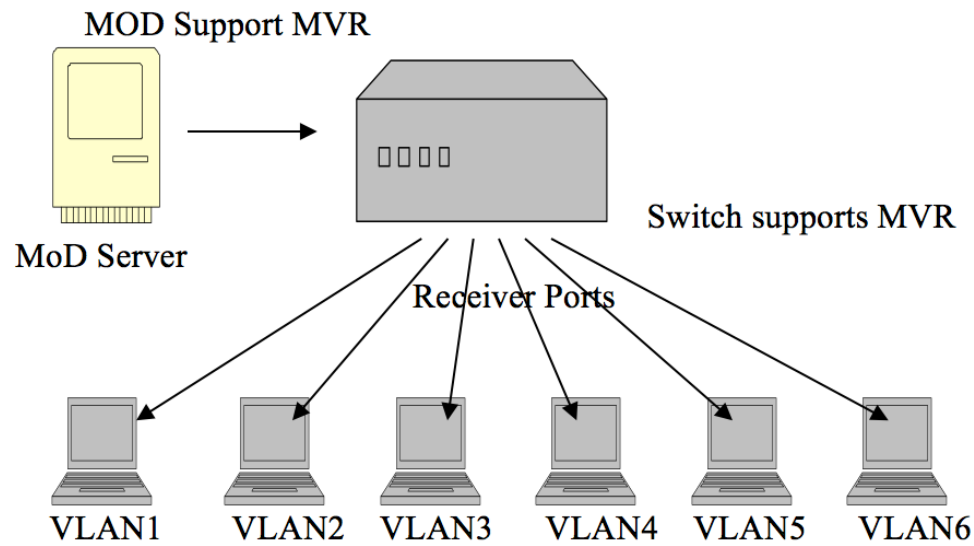


Figure-2:



Default Settings

There is no MVR vlan.

Default configuration for a new MVR:

MVR VLAN Information

VLAN ID	: 2
Name	: MVR2
Active	: Enabled
Mode	: Dynamic
Source Port(s)	: None
Receiver Port(s)	: None
Tagged Port(s)	: None

The Switch allows user to create up to 250 groups.

The Switch allows user to create up to 16 MVRs.

Notices

- » IGMP snooping and MVR can be independently enabled.
- » IGMP snooping and MVR use the same IGMP timers.
- » MVR can recognize IGMPv3 reports.
- » About the IGMPv3 report, switch doesn't treat those group records with the following group record types as membership reports. Those group record types are MODE_IS_INCLUDE, CHANGE_TO_INCLUDE_MODE, ALLOW_NEW_SOURCES and BLOCK_OLD_SOURCES.
- » Don't use the group address X.0.0.1 for your multicast stream. It is because the system detects and records the 224.0.0.1 for dynamic querier port. The group address X.0.0.1 may conflict with 224.0.0.1.
- » Because the lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. When you configure group address, the Switch compares the lower 23 bits only.
- » CLI command "group 1 start-address 224.1.1.1 6", it creates 6 groups. That is, one IP, one group.
- » The MVR name should be the combination of the digit or the alphabet.
- » The group name should be the combination of the digit or the alphabet.

CLI Configuration

Node	Command	Description
enable	show mvr	This command displays the current MVR configurations.
enable	show mvr vlan VLANID	This command displays the current MVR configurations of the specific VLAN.
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
configure	mvr VLANID	This command configures the MVR configurations for the specific VLAN.
configure	no mvr VLANID	This command disables the MVR configurations for the specific VLAN.
MVR	group NAME	This command configures a group configuration for the MVR.
MVR	no group NAME	This command removes the group configurations from the MVR.
MVR	inactive	This command disables the MVR settings.
MVR	no inactive	This command enables the MVR settings.
MVR	mode (dynamic compatible)	This command configures the mode for the MVR. Dynamic : Sends IGMP report to all MVR source ports in the multicast VLAN. Compatible : Sets the Switch not to send IGMP report.
MVR	name STRING	This command configures the name for the MVR.
MVR	no name	This command configures the default name for the MVR.
MVR	receiver-port PORTLIST	This command sets the receiver port(s). Normally the source ports are connected to the streaming client.
MVR	no receiver-port PORTLIST	This command removes a port or range of ports from the receiver port(s).
MVR	source-port PORTLIST	This command sets the source port(s). Normally the source ports are connected to the streaming server.
MVR	no source-port PORTLIST	This command removes a port or range of ports from the source port(s).
MVR	tagged PORTLIST	This command sets the tagged port(s). Same as the VLAN tagged port.
MVR	no tagged PORTLIST	This command removes a port or range of ports from the tagged port(s).
MVR	priority-override (disable enable)	This command enables/disables the multicast priority override.

Web Configuration

MVR Settings

Multicast VLAN Registration

MVR Settings

Group Settings

MVR Settings

VLAN

Name

Priority Override

Disable

State

Enable

Mode

Dynamic

802.1p Priority

0

Source Ports

(ex.1,3,5-8)

Receiver Ports

(ex.1,3,5-8)

Tagged Ports

(ex.1,3,5-8)

Apply

Refresh

MVR Status

Parameter	Description
VLAN ID	Configures a VLAN.
NAME	Configures a name for the MVR.
Priority Override	Enable / Disable for the priority override.
State	Enables / Disables the MVR.
Mode	Configures the mode for the MVR.
802.1p Priority	The priority for these multicast group packets.
Source Ports	Configures the source port(s) for the MVR. Normally the source ports are connected to the streaming server.
Receive Ports	Configures the receive port(s) for the MVR. Normally the source ports are connected to the streaming client
Tagged Ports	Configures the tagged port(s) for the MVR. Same as the VLAN tagged port.

Group Settings

Multicast VLAN Registration

MVR Settings

Group Settings

Group Settings

MVR VLAN

▼

Group Name

Start Address

Quantity:

Apply

Refresh

Group Status

Parameter	Description
MVR VLAN	Select a MVR VLAN.
Group Name	Configures the group name.
Start Address	Configures the multicast start address.
Quantity	Configures the quantity of the multicast address.

Multicast Address

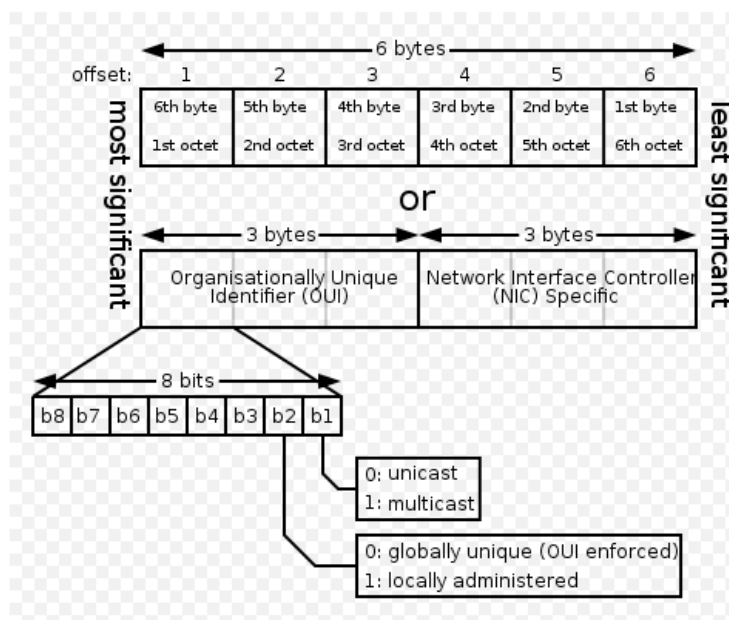
Introduction

A multicast address is associated with a group of interested receivers. According to RFC 3171, addresses 224.0.0.0 to 239.255.255.255, the former Class D addresses, are designated as multicast addresses in IPv4.

The IANA owns the OUI MAC address 01:00:5e, therefore multicast packets are delivered by using the Ethernet MAC address range 01:00:5e:00:00:00 - 01:00:5e:7f:ff:ff. This is 23 bits of available address space.

The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. This means that there is ambiguity in delivering packets. If two hosts on the same subnet each subscribe to a different multicast group whose address differs only in the first 5 bits, Ethernet packets for both multicast groups will be delivered to both hosts, requiring the network software in the hosts to discard the unrequired packets.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.



IP multicast address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	The All Hosts multicast group that contains all systems on the same network segment
224.0.0.2	The All Routers multicast group that contains all routers on the same network segment
224.0.0.5	The Open Shortest Path First (OSPF) AllSPFRouters address. Used to send Hello packets to all OSPF routers on a network segment
224.0.0.6	The OSPF AllDRouters address. Used to send OSPF routing information to OSPF designated routers on a network segment
224.0.0.9	The RIP version 2 group address, used to send routing information using the RIP protocol to all RIP v2-aware routers on a network segment
224.0.0.10	EIGRP group address. Used to send EIGRP routing information to all EIGRP routers on a network segment
224.0.0.13	PIM Version 2 (Protocol Independent Multicast)
224.0.0.18	Virtual Router Redundancy Protocol
224.0.0.19 - 21	IS-IS over IP
224.0.0.22	IGMP Version 3 (Internet Group Management Protocol)
224.0.0.102	Hot Standby Router Protocol Version 2
224.0.0.251	Multicast DNS address
224.0.0.252	Link-local Multicast Name Resolution address
224.0.1.1	Network Time Protocol address
224.0.1.39	Cisco Auto-RP-Announce address
224.0.1.40	Cisco Auto-RP-Discovery address
224.0.1.41	H.323 Gatekeeper discovery address

CLI Configuration

Node	Command	Description
enable	show mac-address-table multicast	This command displays the current static/dynamic multicast address entries.
enable	show mac-address-table multicast vlan VLANID	This command displays the current static/dynamic multicast address entries with a specific vlan.
configure	mac-address-table multicast MACADDR vlan VLANID ports PORTLIST	This command configures a static multicast entry.
configure	no mac-address-table multicast MACADDR	This command removes a static multicast entry from the address table.

Web Configuration

Multicast Address

Static Multicast Address Settings

VLAN ID	MAC Address	Port
1 ▾	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>

Multicast Address Table

VLAN ID	MAC Address	Status	Port	Action
1	01:00:5e:00:00:fc	Dynamic	24	<input type="button" value="Delete"/>
1	01:00:5e:00:00:07	Dynamic	24	<input type="button" value="Delete"/>
1	01:00:5e:00:00:fb	Dynamic	24	<input type="button" value="Delete"/>
1	01:00:5e:00:01:18	Dynamic	24	<input type="button" value="Delete"/>
1	01:00:5e:00:01:3c	Dynamic	24	<input type="button" value="Delete"/>

Total counts : **5**

Parameter	Description
VLAN ID	Configures the VLAN that you want to configure.
MAC Address	Configures the multicast MAC which will not be aged out. Valid format is hh:hh:hh:hh:hh:hh.
Port	Configures the member port for the multicast address.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.

Explicit Host Tracking

This capability enables the Switch to track each individual host that is joined to a particular group or channel and to achieve minimal leave latencies when hosts leave a multicast group or channel.

Notice:

Before configuring the `ip igmp explicit-tracking` command, IGMP must be enabled.

When explicit host tracking is enabled, the router uses more memory than if explicit tracking is disabled because the router must store the membership state of all hosts on the interface.

CLI Configurations

Node	Command	Description
enable	show ip multicast	This command shows the IGMP snooping membership information.
enable	show igmp-snooping membership	This command shows the IGMP snooping host membership information.
configure	igmp-snooping explicit-tracking	This command enables the IGMP snooping explicit host tracking on the Switch.
configure	no igmp-snooping explicit-tracking	This command disables the IGMP snooping explicit host tracking on the Switch.

Web Configurations

Explicit Host Tracking

Explicit Host Tracking Settings

Explicit Host Tracking State Disable ▾

Apply
Refresh

IGMP Snooping Membership Table

Port	Multicast Group	VID	Timeout	Host IP
24	224.0.0.7	1	124	
24	224.0.0.251	1	244	
24	224.0.0.252	1	236	
24	224.0.1.24	1	238	
24	224.0.1.60	1	244	

Parameter	Description
Explicit Tracking state	The field enables/disables the IGMP Snooping explicit host tracking state on the Switch.
IGMP Snooping Membership Table	
Index	This field indicates the index of the entry.
Port	This field indicates the port of the entry.
Multicast Group	This field indicates the multicast address of the entry.
VID	This field indicates the vlan of the entry.
Timeout	This field indicates the remaining time in the table of the entry.
Host IP	This field indicates the host IP which joins the multicast group.

VLAN

Port Isolation

Introduction

The port isolation is a port-based virtual LAN feature. It partitions the switching ports into virtual private domains designated on a per port basis. Data switching outside of the port's private domain is not allowed. It will ignore the packets' tag VLAN information.

This feature is a per port setting to configure the egress port(s) for the specific port to forward its received packets. If the CPU port (port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the Switch.

If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. CPU refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.

Example: If you want to allow port-1 and port-3 to talk to each other, you must configure as below:

```
CWGE24MS2(config)#interface 1/0/1
CWGE24MS2(config-if)#port-isolation ports 3
CWGE24MS2(config-if)#exit
; Allow the port-1 to send its ingress packets to port-3.
```

```
CWGE24MS2(config)#interface 1/0/3
CWGE24MS2(config-if)#port-isolation ports 1
CWGE24MS2(config-if)#exit
; Allow the port-3 to send its ingress packets to port-1
```

CLI Configuration

Node	Command	Description
enable	show port-isolation	This command displays the current port isolation configurations. "V" indicates the port's packets can be sent to that port. "- " indicates the port's packets cannot be sent to that port.
interface	port-isolation ports PORTLISTS	This command configures a port or a range of ports to egress traffic from the specific port.
interface	no port-isolation	This command configures all ports to egress traffic from the specific port.

Example:

```
CWGE24MS2(config)#interface 1/0/2
CWGE24MS2(config-if)#port-isolation ports 3-10
```

Web Configuration

Port Isolation

Port Isolation Settings

Port

From: 1 To: 1

Egress Port :

Select All

Deselect All

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24 0 (CPU)

Apply

Refresh

Port Isolation Status

Port	Egress Port																								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
2	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
3	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
4	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
5	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
6	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
7	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
8	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
9	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
10	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
11	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
12	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
13	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
14	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
15	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
16	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
17	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
18	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
19	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
20	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
21	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v

Parameter	Description
Port	Select a port number to configure its port isolation settings. Select All Ports to configure the port isolation settings for all ports on the Switch.
Egress Port	An egress port is an outgoing port, that is, a port through which a data packet leaves. Selecting a port as an outgoing port means it will communicate with the port currently being configured.
Select All/ Deselect All	Click Select All to mark all ports as egress ports and permit traffic. Click Deselect All to unmark all ports and isolate them. Deselecting all ports means the port being configured cannot communicate with any other port.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
Port Isolation Status	"V" indicates the port's packets can be sent to that port. "-" indicates the port's packets cannot be sent to that port.

802.1Q VLAN

Introduction

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VID- VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q. It has 12 bits and allow the identification of 4096 (2^{12}) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each

other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 bytes	3 bits	1 bit	12 bits

» Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

» 802.1Q Port base VLAN

With port-based VLAN membership, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members of the same VLAN. The network administrator typically performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

As with other VLAN approaches, the packets forwarded using this method do not leak into other VLAN domains on the network. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN without the intervention of a Layer 3 device.

The device that is attached to the port likely has no understanding that a VLAN exists. The device simply knows that it is a member of a subnet and that the device should be able to talk to all other members of the subnet by simply sending information to the cable segment. The switch is responsible for identifying that the information came from a specific VLAN and for ensuring that the information gets to all other members of the VLAN. The switch is further responsible for ensuring that ports in a different VLAN do not receive the information.

This approach is quite simple, fast, and easy to manage in that there are no complex lookup tables required for VLAN segmentation. If port-to-VLAN association is done with an application-specific integrated circuit (ASIC), the performance is very good. An ASIC allows the port-to-VLAN mapping to be done at the hardware level.

Default Settings

The default PVID is 1 for all ports.

The default Acceptable Frame is All for all ports.

All ports join in the VLAN 1.

Notice: The maximum VLAN group is 4094.

CLI Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1~4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1~4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	name STRING	This command assigns a name for the specific VLAN. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
vlan	no name	This command configures the vlan name to default. Note: The default vlan name is "VLAN"+vlan_ID, VLAN1, VLAN2,...
vlan	add PORTLISTS	This command adds a port or a range of ports to the vlan.
vlan	fixed PORTLISTS	This command assigns ports for permanent member of the vlan.
vlan	no fixed PORTLISTS	This command removes all fixed member from the vlan.
vlan	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.
vlan	no tagged PORTLISTS	This command removes all tagged member from the vlan.
vlan	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.
vlan	no untagged PORTLISTS	This command removes all untagged member from the vlan.
interface	acceptable frame type (all tagged untagged)	This command configures the acceptable frame type. all - acceptable all frame types. tagged - acceptable tagged frame only. untagged - acceptable untagged frame only.
interface	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
interface	no pvid	This command configures 1 for the port default VLAN ID.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	pvid VLANID	This command configures a VLAN ID for the port default VLAN ID.
if-range	no pvid	This command configures 1 for the port default VLAN ID.
configure	vlan range STRINGS	This command configures a range of vlans.
configure	no vlan range STRINGS	This command removes a range of vlans.
vlan-range	add PORTLISTS	This command adds a port or a range of ports to the vlans.

Node	Command	Description
vlan-range	fixed PORTLISTS	This command assigns ports for permanent member of the VLAN group.
vlan-range	no fixed PORTLISTS	This command removes all fixed member from the vlans.
vlan-range	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no tagged PORTLISTS	This command removes all tagged member from the vlans.
vlan-range	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no untagged PORTLISTS	This command removes all untagged member from the vlans.

Example:

```
CWGE24MS2#configure terminal
CWGE24MS2(config)#vlan 2
CWGE24MS2(config-vlan)#fixed 1-6
CWGE24MS2(config-vlan)#untagged 1-3
```

Web Configuration

VLAN Settings

VLAN				
VLAN Settings		Tag Settings	Port Settings	
VLAN Settings				
VLAN ID		VLAN Name	Member Port	
From: <input type="text"/>	To: <input type="text"/>	<input type="text"/>	<input type="text"/>	
		<input type="button" value="Apply"/>	<input type="button" value="Refresh"/>	
VLAN List				
VLAN ID	VLAN Name	VLAN Status	Member Port	Action
1	VLAN1	Static	1-24	

Parameter	Description
VLAN ID	Enter the VLAN ID for this entry; the valid range is between 1 and 4094.
VLAN Name	Enter a descriptive name for the VLAN for identification purposes. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
Member Port	Enter the port numbers you want the Switch to assign to the VLAN as members. You can designate multiple port numbers individually by using a comma (,) and by range with a hyphen (-).
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
VLAN List	
VLAN ID	This field displays the index number of the VLAN entry. Click the number to modify the VLAN.
VLAN Name	This field displays the name of the VLAN.
VLAN Status	This field displays the status of the VLAN. Static or Dynamic (802.1Q VLAN).
Member Port	This field displays which ports have been assigned as members of the VLAN. This will display None if no ports have been assigned.
Action	Click Delete to remove the VLAN. The VLAN 1 cannot be deleted.

Tag Settings

VLAN

VLAN Settings

Tag Settings

Port Settings

Tag Settings

VLAN ID

From:

To:

Tag Port :

☐ Select All

☐ Deselect All

☐ 1 ☐ 3 ☐ 5 ☐ 7

☐ 9 ☐ 11 ☐ 13 ☐ 15

☐ 17 ☐ 19 ☐ 21 ☐ 23

☐ 2 ☐ 4 ☐ 6 ☐ 8

☐ 10 ☐ 12 ☐ 14 ☐ 16

☐ 18 ☐ 20 ☐ 22 ☐ 24

Apply

Refresh

Tag Status

VLAN ID	Tag Ports	UnTag Ports
1		1-24

Parameter	Description
VLAN ID	Select a VLAN ID to configure its port tagging settings.
Tag Port	Selecting a port which is a member of the selected VLAN ID will make it a tag port. This means the port will tag all outgoing frames transmitted with the VLAN ID.
Select All	Click Select All to mark all member ports as tag ports.
Deselect All	Click Deselect All to mark all member ports as untag ports.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Tag Status	
VLAN ID	This field displays the VLAN ID.
Tag Ports	This field displays the ports that have been assigned as tag ports.
Untag Ports	This field displays the ports that have been assigned as untag ports.

Port Settings

VLAN

VLAN Settings
Tag Settings
Port Settings

Port Settings

Port
 From: 1 ▼ To: 1 ▼

PVID
1 ▼

Acceptable Frame
All ▼

Apply
Refresh

Port Status

Port	PVID	Acceptable Frame	Port	PVID	Acceptable Frame
1	1	All	2	1	All
3	1	All	4	1	All
5	1	All	6	1	All
7	1	All	8	1	All
9	1	All	10	1	All
11	1	All	12	1	All
13	1	All	14	1	All
15	1	All	16	1	All
17	1	All	18	1	All
19	1	All	20	1	All
21	1	All	22	1	All
23	1	All	24	1	All

Parameter	Description
Port	Select a port number to configure from the drop-down box. Select All to configure all ports at the same time.
PVID	Select a PVID (Port VLAN ID number) from the drop-down box.
Acceptable Frame	Specify the type of frames allowed on a port. Choices are All, VLAN Untagged Only or VLAN Tagged Only. <ul style="list-style-type: none"> - Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. - Select VLAN Tagged Only to accept only tagged frames on this port. All untagged frames will be dropped. - Select VLAN Untagged Only to accept only untagged frames on this port. All tagged frames will be dropped.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Port Status	
Port	This field displays the port number.
PVID	This field displays the Port VLAN ID number.
Acceptable Frame	This field displays the type of frames allowed on the port. This will either display All or VLAN Tagged Only or VLAN Untagged Only.

GARP/GVRP

Introduction

GARP and GVRP are industry-standard protocols that are described in IEEE 802.1p. GVRP is a GARP application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

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 that are connected through 802.1Q trunk ports.

GVRP makes use of GID and GIP, which provide the common state machine descriptions and the common information propagation mechanisms defined for use in GARP-based applications. GVRP prunes trunk links so that only active VLANs will be sent across trunk connections. GVRP expects to hear join messages from the switches before it will add a VLAN to the trunk. GVRP updates and hold timers can be altered. GVRP ports run in various modes to control how they will prune VLANs. GVRP can be configured to dynamically add and manage VLANs to the VLAN database for trunking purposes.

In other words, GVRP allows the propagation of VLAN information from device to device. With GVRP, a single switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically. An end-node can be plugged into any switch and be connected to that end-node's desired VLAN. For end-nodes to make use of GVRP, they need GVRP-aware Network Interface Cards (NICs). The GVRP-aware NIC is configured with the desired VLAN or VLANs, then connected to a GVRP-enabled switch. The NIC communicates with the switch, and VLAN connectivity is established between the NIC and switch.

Registration Mode:

- » Normal: The normal registration mode allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the trunk port. Normal mode is the default.
- » Forbidden: The forbidden registration mode deregisters all VLANs (except VLAN 1) and prevents any further VLAN creation or registration on the trunk port.
- » Fixed: The fixed registration mode allows manual creation and registration of VLANs, prevents VLAN deregistration, and registers all known VLANs on other ports on the trunk port. (Same as the static VLAN)

GVRP Timer:

Join Timer: Specifies the maximum number of milliseconds the interface waits before sending VLAN advertisements.

Leave Timer: Specifies the number of milliseconds an interface waits after receiving a leave message before the interface leaves the VLAN specified in the message.

Leaveall Timer: Specifies the interval in milliseconds at which Leave All messages are sent on interfaces. Leave All messages help to maintain current GVRP VLAN membership information in the network.

The value for leave must be greater than three times the join value (leave \geq join * 3).

The value for leaveall must be greater than the value for leave (leaveall > leave).

Default Settings

The default port Join Time is 20 for all ports.

The default port Leave Time is 60 for all ports.

The default port Leaveall Time is 1000 for all ports.

The default port Hold Time is 10 for all ports.

CLI Configuration

Node	Command	Description
enable	show gvrp configuration	This command displays the GVRP configurations.
enable	show gvrp statistics	This command displays the GVRP configurations on a port or all ports.
enable	show garp timer	This command displays the timers for the GARP.
configure	gvrp (disable enable)	This command disables / enables the GVRP on the switch.
configure	no gvrp configuration	This command set GVRP configuration to its defaults.
interface	gvrp (disable enable)	This command disables / enables the GVRP on the specific port.
interface	gvrp registration (normal forbidden)	This command configures the registration mode for the GVRP on the specific port.
interface	no gvrp configuration	This command set GVRP configuration to its defaults for the specific port.
interface	garp join-time VALUE leave-time VALUE leaveall-time VALUE	This command configures the join time / leaves time / leave all time for the GARP on the specific port.
interface	no garp time	This command configures the join time / leaves time / leaves all time to default for the GARP on the specific port.

Web Configuration

GVRP Settings

GARP VLAN Registration Protocol					
GVRP			GARP Timer		
GVRP Settings					
GVRP State Disable ▾					
Port		State		Registration Mode	
From: 1 ▾ To: 1 ▾		Disable ▾		Normal ▾	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>					
GVRP Status					
Port	State	Registration Mode	Port	State	Registration Mode
1	Disabled	-	2	Disabled	-
3	Disabled	-	4	Disabled	-
5	Disabled	-	6	Disabled	-
7	Disabled	-	8	Disabled	-
9	Disabled	-	10	Disabled	-
11	Disabled	-	12	Disabled	-
13	Disabled	-	14	Disabled	-
15	Disabled	-	16	Disabled	-
17	Disabled	-	18	Disabled	-
19	Disabled	-	20	Disabled	-
21	Disabled	-	22	Disabled	-
23	Disabled	-	24	Disabled	-

Parameter	Description
GVRP State	Select Enable to activate GVRP function to exchange VLAN configuration information with other GVRP switches. Select Disable to deactivate the feature.
Port	Select the port that you want to configure the GVRP settings.
State	Select Enable to activate the port GVRP function. Select Disable to deactivate the port GVRP function.
Registration Mode	Select Normal to allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the trunk port. Select Forbidden to deregister all VLANs (except VLAN 1) and prevents any further VLAN creation or registration on the trunk port.

GARP Timer

GARP VLAN Registration Protocol				
GVRP		GARP Timer		
GARP Timer Settings				
Port From: <input type="text" value="1"/> To: <input type="text" value="1"/>		Join Time <input type="text" value="20"/>	Leave Time <input type="text" value="60"/>	Leave All Time <input type="text" value="1000"/>
2*Join Time < Leave Time < Leave All Time Time unit: (centi-sec)				
		<input type="button" value="Apply"/>	<input type="button" value="Refresh"/>	
GARP Timer Status				
Port	Join Time	Hold Time	Leave Time	Leave All Time
1	20	10	60	1000
2	20	10	60	1000
3	20	10	60	1000
4	20	10	60	1000
5	20	10	60	1000
6	20	10	60	1000
7	20	10	60	1000
8	20	10	60	1000
9	20	10	60	1000
10	20	10	60	1000
11	20	10	60	1000
12	20	10	60	1000
13	20	10	60	1000
14	20	10	60	1000
15	20	10	60	1000
16	20	10	60	1000
17	20	10	60	1000
18	20	10	60	1000
19	20	10	60	1000
20	20	10	60	1000
21	20	10	60	1000
22	20	10	60	1000
23	20	10	60	1000

Parameter	Description
Join Time	Specifies the maximum number of milliseconds the interface waits before sending VLAN advertisements.
Leave Time	Specifies the number of milliseconds an interface waits after receiving a leave message before the interface leaves the VLAN specified in the message.
Leaveall Time	Specifies the interval in milliseconds at which Leave All messages are sent on interfaces. Leave All messages help to maintain current GVRP VLAN membership information in the network.

MAC-based VLAN

Introduction

The MAC base VLAN allows users to create VLAN with MAC address. The MAC address can be the leading three or more bytes of the MAC address.

For example, 00:01:02 or 00:03:04:05 or 00:01:02:03:04:05.

When the Switch receives packets, it will compare MAC-based VLAN configures. If the SA is matched the MAC-based VLAN configures, the Switch replace the VLAN with user configured and them forward them.

For example:

Configurations: 00:01:02, VLAN=23, Priority=2.

The packets with SA=00:01:02:xx:xx:xx will be forwarded to VLAN 22 member ports.

Notices: The 802.1Q port base VLAN should be created first.

CLI Configuration

Node	Command	Description
enable	show mac-vlan	This command displays the all of the mac-vlan configurations.
configure	mac-vlan STRINGS vlan VLANID priority <0-7>	This command creates a mac-vlan entry with the leading three or more bytes of mac address and the VLAN and the priority.
configure	no mac-vlan entry STRINGS	This command deletes a mac-vlan entry.
configure	no mac-vlan all	This command deletes all of the mac-vlan entries.

Example:

```
CWGE24MS2(config)#mac-vlan 00:01:02:03:04 vlan 111 priority 1
CWGE24MS2(config)#mac-vlan 00:01:02:22:04 vlan 121 priority 1
CWGE24MS2(config)#mac-vlan 00:01:22:22:04:05 vlan 221 priority 1
```

Web Configuration

MAC VLAN

MAC VLAN Settings

MAC Address	VLAN	Priority
<input type="text"/>	<input type="text"/> (1~4094)	<input type="text" value="0"/> ▼

Ex: 00:01:02 will only filter 3 bytes of source mac address.
 00:01:02:03:04 will only filter 5 bytes of source mac address.
 00:01:02:03:04:05 will filter all bytes of source mac address.

MAC VLAN Table

Index	MAC Address	VLAN	Priority	Action
-------	-------------	------	----------	--------

Parameter	Description
MAC Address	Configures the leading three or more bytes of the MAC address.
VLAN	Configures the VLAN.
Priority	Configures the 802.1Q priority.
Action	Click the "Delete" button to delete the protocol VLAN profile.

Protocol-based VLAN

Introduction

The Protocol based VLAN allows users to create VLAN with packet frame type. The packet frame type can be one of the three frame types: EthernetII, NonLLC-SNAP and LLC-SNAP. If configuring the Ethernet II frame type, the configuration will be more detail with the ethernet type.

When the user configures the protocol VLAN as LLC-SNAP, VLAN:22, ports list: 1-3.

If the Switch receives packets with LLC-SNAP frame type from port 1 to 3, the packets' VLAN will be replaced with VLAN 22 and be forwarded to VLAN 22 member ports.

Notices: The 802.1Q port base VLAN should be created first.

CLI Configuration

Node	Command	Description
enable	show protocol-vlan	This command displays the all of the protocol-vlan configurations.
configure	protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with ethernetII frame type.
configure	protocol-vlan frame-type nonLLC-SNAP vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with nonLLC-SNAP frame type.
configure	protocol-vlan frame-type LLC-SNAP vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with LLC-SNAP frame type.
configure	no protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLANID	This command deletes a protocol-vlan entry with ethernetII frame type.
configure	no protocol-vlan frame-type nonLLC-SNAP vlan VLANID	This command deletes a protocol-vlan entry with nonLLC-SNAP frame type and vlan.
configure	no protocol-vlan frame-type LLC-SNAP vlan VLANID	This command deletes a protocol-vlan entry with LLC-SNAP frame type and vlan.
configure	no protocol-vlan all	This command deletes all of the protocol-vlan entries.

Example:

CWGE24MS2(config)#protocol-vlan frame-type LLC-SNAP vlan 12 ports 1-2

CWGE24MS2(config)#protocol-vlan frame-type nonLLC-SNAP vlan 13 ports 3-4

CWGE24MS2(config)#protocol-vlan frame-type ethernetII ether-type 0800 vlan 14 ports 1-2

Web Configuration

Protocol VLAN

Protocol VLAN Settings

Frame Type	Ethernet Type	VLAN	Port List
EthernetII ▾	<input type="text"/>	<input type="text"/> (1~4094)	<input type="text"/>

Apply

Refresh

Protocol VLAN Table

Index	Frame Type	Ethernet Type	VLAN	Port List	Action
-------	------------	---------------	------	-----------	--------

Parameter	Description
Frame Type	Select one of three frame types, "EthernetIU" and "NonLLC-SNAP" and "LLC-SNAP".
Ethernet type	Input the Ethernet type for the EthernetII frame type.
VLAN	Configure the VLAN ID.
Port List	Configure the member ports.
Action	Click the "Delete" button to delete the protocol VLAN profile.

Q-in-Q VLAN (VLAN Stacking)

Introduction

Q-in-Q tunneling is also known as VLAN stacking. Both of them use 802.1q double tagging technology. Q-in-Q is required by ISPs (Internet Service Provider) that need Transparent LAN services (TLS), and the service provider has their own set of VLAN, independent of customer VLANs. Typically, each service provider VLAN interconnects a group of sites belonging to a customer. However, a service provider VLAN could also be shared by a set of customers sharing the same end points and quality of service requirements of the VLAN. Double tagging is considered to be a relatively simpler way of implementing transparent LAN. This is accomplished by encapsulating Ethernet Frame. A second or outer VLAN tag is inserted in Ethernet frames sent over the ingress PE (Provider Edge). This VLAN tag corresponds to the VLAN of the Service Provider (SP). When the frame reaches the destination PE, the SP VLAN is stripped off. The DA of the encapsulated frame and the VLAN ID are used to take further L2 decisions, similar to an Ethernet frame arriving from a physical Ethernet port. The SP VLAN tag determines the VPLS (Virtual Private LAN Service) membership. Double tagging aggregates multiple VLANs within another VLAN and provides a private, dedicated Ethernet connection between customers to reach their subnet transparently across multiple networks. Thus service providers can create their own VLANs without interfering with customer VLANs by using double tagging. This allows them to connect customers to ISPs and ASPs (Application Service Provider).

The ports that are connected to the service provider VLANs are called tunnel ports, and the ports that are connected to the customer VLANs are called access (subscriber/customer) ports. When a port is configured as tunnel port, all the outgoing packets on this port will be sent out with SPVLAN (SPVID and 1p priority) tag. The incoming packet can have two tags (SPVLAN + CVLAN), one tag (SPVLAN or CVLAN), or no tag. In all cases, the packet is sent out with a SPVLAN tag. When a port is configured as an access port, the incoming traffic can have only a CVLAN (CVID and 1p priority) tag or no tag. Hence, all the packets that are being sent out of access ports will be untagged or single tagged (CVLAN). When a port is configured as a normal port, it will ignore the frames with double tagging.

Double Tagging Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

TPID	Priority	VID
------	----------	-----

TPID (Tag Protocol Identifier) is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. The value of this field is 0x8100 as defined in IEEE 802.1Q. Other vendors may use a different value, such as 0x9100.

Tunnel TPID is the VLAN stacking tag type the Switch adds to the outgoing frames sent through a Tunnel Port of the service provider's edge devices

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for. "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. SP VID is the VID for the second or outer (service provider's) VLAN tag. CVID is the VID for the first or inner (Customer's) VLAN tag.

The frame formats for an untagged Ethernet frame; a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) are shown as following.

untagged frame	DA	SA	Len or Etype	Data	FCS						
single-tagged frame	DA	SA	TPID	P	VID	Len or Etype	Data	FCS			
double-tagged frame	DA	SA	Tunnel TPID	P	VID	TPID	P	VID	Len or Etype	Data	FCS

DA: Destination Address

SA: Source Address

Tunnel TPID: Tag Protocol Identifier added on a tunnel port

P: 802.1p priority

VID: VLAN ID

Len or Etype: Length or Ethernet frame type

Data: Frame data

FCS: Frame Check Sequence

VLAN Stacking Port Roles

Each port can have three VLAN stacking "roles", Normal, Access Port and Tunnel Port.

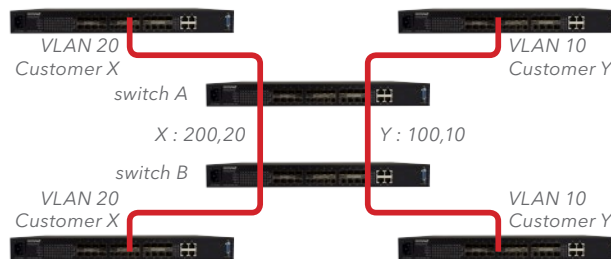
- » Select Normal for "regular" (non-VLAN stacking) IEEE 802.1Q frame switching.
- » Select Access Port for ingress ports on the service provider's edge devices. The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.
- » Select Tunnel Port for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).

NOTE: *In order to have the double tagged frames switching correctly, user has to configure a service provider's VLAN (SPVLAN) on the Q-in-Q switch. Then, the double tagged frames can be switched according to the SP VID. The SPVLAN should include all the related Tunnel and Access ports. Also, user has to configure the Tunnel posts as tagged ports and the Access ports as untagged ports.*

Port-based Q-in-Q

Q-in-Q encapsulation is to convert a single tagged 802.1Q packet into a double tagged Q-in-Q packet. The Q-in-Q encapsulation can be based on port or traffic. Port-based Q-in-Q is to encapsulate all the packets incoming to a port with the same SPVID outer tag. The mode is more inflexible.

In the following example figure, both X and Y are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 100 to distinguish customer X and tag 200 to distinguish customer Y at edge device A and then stripping those tags at edge device B as the data frames leave the network.



This example shows how to configure switch A with ports 1 on the Switch to tag incoming frames with the service provider's VID of 200 (ports are connected to customer X network) and configure port 7 to service provider's VID of 100 (ports are connected to customer Y network). This example also shows how to set the priority for port 1 to 3 and port 7 to 4.

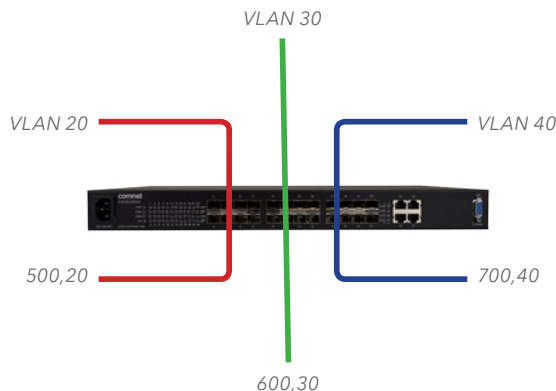
```

CWGE24MS2(config)# vlan-stacking port-based
CWGE24MS2(config)# vlan-stacking tpid-table index 2 value 88a8
CWGE24MS2(config)# vlan 10
CWGE24MS2(config-vlan)# fixed 7,8
CWGE24MS2(config-vlan)# tagged 7
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# vlan 100
CWGE24MS2(config-vlan)# fixed 7,8
CWGE24MS2(config-vlan)# tagged 8
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# vlan 20
CWGE24MS2(config-vlan)# fixed 1,2
CWGE24MS2(config-vlan)# tagged 1
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# vlan 200
CWGE24MS2(config-vlan)# fixed 1,2
CWGE24MS2(config-vlan)# tagged 2
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# interface gigaethernet1/0/1
CWGE24MS2(config-if)# vlan-stacking port-based role access
CWGE24MS2(config-if)# vlan-stacking spvid 200
CWGE24MS2(config-if)# vlan-stacking priority 3
CWGE24MS2(config)# interface gigaethernet1/0/2
CWGE24MS2(config-if)# vlan-stacking port-based role tunnel
CWGE24MS2(config-if)# vlan-stacking tunnel-tpid index 2
CWGE24MS2(config)# interface gigaethernet1/0/7
CWGE24MS2(config-if)# vlan-stacking port-based role access
CWGE24MS2(config-if)# vlan-stacking spvid 100
CWGE24MS2(config-if)# vlan-stacking priority 4
CWGE24MS2(config)# interface gigaethernet1/0/8
CWGE24MS2(config-if)# vlan-stacking port-based role tunnel
CWGE24MS2(config-if)# vlan-stacking tunnel-tpid index 2
CWGE24MS2(config-if)# exit
CWGE24MS2(config)# exit
CWGE24MS2# show vlan-stacking
CWGE24MS2# show vlan-stacking tpid-table
CWGE24MS2# show vlan-stacking portbased-qinq

```

Selective Q-in-Q

The traffic based Q-in-Q is also called Selective Q-in-Q. Selective Q-in-Q allows the Switch to add different outer VLAN tags to the incoming frames received on one port according to their inner VLAN tags. In the Selective Q-in-Q mode, switch performs traffic classification for the traffic incoming to a port based on the VLAN ID. When a user uses different VLAN IDs for different services, traffic can be classified according to the VLAN ID. For example, the VLAN ID 20 for surfing on the internet by PC, VLAN ID 30 for IPTV and VLAN ID 40 for VIP customers. After receiving user data, the switch labels the traffic of surfing on the Internet by PC with 500 as a SPVID outer tag, IPTV with 600, and VIP customers with 700.



This following example shows how to configure ports 3 on the Switch to tag incoming frames with the different service provider's VID and priority.

```
CWGE24MS2(config)# vlan-stacking selective
CWGE24MS2(config)# vlan-stacking tpid-table index 6 value 9100
CWGE24MS2(config)# vlan 20
CWGE24MS2(config-vlan)# fixed 3,4
CWGE24MS2(config-vlan)# tagged 3
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# vlan 30
CWGE24MS2(config-vlan)# fixed 3,4
CWGE24MS2(config-vlan)# tagged 3
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# vlan 40
CWGE24MS2(config-vlan)# fixed 3,4
CWGE24MS2(config-vlan)# tagged 3
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# vlan 500
CWGE24MS2(config-vlan)# fixed 3,4
CWGE24MS2(config-vlan)# tagged 4
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# vlan 600
CWGE24MS2(config-vlan)# fixed 3,4
CWGE24MS2(config-vlan)# tagged 4
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# vlan 700
CWGE24MS2(config-vlan)# fixed 3,4
```

```
CWGE24MS2(config-vlan)# tagged 4
CWGE24MS2(config-vlan)# exit
CWGE24MS2(config)# vlan-stacking selective-qinq rule1
CWGE24MS2(config-qinq)# cvids 20
CWGE24MS2(config-qinq)# priority 2
CWGE24MS2(config-qinq)# spvid 500
CWGE24MS2(config-qinq)# access-ports 3
CWGE24MS2(config-qinq)# tunnel-ports 4
CWGE24MS2(config-qinq)# active
CWGE24MS2(config-qinq)# show
CWGE24MS2(config-qinq)# exit
CWGE24MS2(config)# vlan-stacking selective-qinq rule2
CWGE24MS2(config-qinq)# cvids 30
CWGE24MS2(config-qinq)# priority 5
CWGE24MS2(config-qinq)# spvid 600
CWGE24MS2(config-qinq)# access-ports 3
CWGE24MS2(config-qinq)# tunnel-ports 4
CWGE24MS2(config-qinq)# active
CWGE24MS2(config-qinq)# show
CWGE24MS2(config-qinq)# exit
CWGE24MS2(config)# vlan-stacking selective-qinq rule3
CWGE24MS2(config-qinq)# cvids 40
CWGE24MS2(config-qinq)# priority 7
CWGE24MS2(config-qinq)# spvid 700
CWGE24MS2(config-qinq)# access-ports 3
CWGE24MS2(config-qinq)# tunnel-ports 4
CWGE24MS2(config-qinq)# active
CWGE24MS2(config-qinq)# show
CWGE24MS2(config-qinq)# exit
CWGE24MS2(config)# interface interface 1/0/4
CWGE24MS2(config-if)# vlan-stacking tunnel-tpid index 6
CWGE24MS2(config-if)# exit
CWGE24MS2(config)# exit
CWGE24MS2# show vlan-stacking
CWGE24MS2# show vlan-stacking tpid-table
CWGE24MS2# show vlan-stacking selective-qinq
```

Default Setting: VLAN Stacking is disabled.

CLI Configuration

Node	Command	Description
enable	show vlan-stacking	This command displays the current vlan-stacking type.
enable	show vlan-stacking selective-qinq	This command displays the selective Q-in-Q configurations.
enable	show vlan-stacking portbased-qinq	This command displays the port-based q-in-Q configurations.
enable	show vlan-stacking tpid-inform	This command displays the TPID configurations.
configure	vlan-stacking (disable port-based selective)	This command disable the vlan stacking or enable the vlan-stacking with port-based or selective on the switch.
configure	vlan-stacking selective-qinq STRINGS	This command creates a selective Q-in-Q profile with the name.
configure	no vlan-stacking selective-qinq STRINGS	This command removes the selective Q-in-Q profile with the name.
configure	vlan-stacking tpid-table index <2-6> value STRINGS	This command configures TPID table.
interface	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
interface	vlan-stacking port-based role (tunnel access normal)	This command sets VLAN stacking port role.
interface	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
interface	vlan-stacking tunnel-tpid index <1-6>	This command sets TPID for a Q-in-Q tunnel port.
configure	interface range gigabitethernet1/0/ ORTLISTS	This command enters the interface configure node.
if-range	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
if-range	vlan-stacking port-based role (tunnel access normal)	This command sets VLAN stacking port role.
if-range	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
if-range	vlan-stacking tunnel-tpid index <1-6>	This command sets TPID for a Q-in-Q tunnel port.
qinq	active	This command enables the selective Q-in-Q profile.
qinq	inactive	This command disables the selective Q-in-Q profile.
qinq	cvid VLANID	This command specifies the customer's VLAN range on the incoming packets.
qinq	spvid VLANID	This command sets the service provider's VLAN ID for outgoing packets in selective Q-in-Q.

Node	Command	Description
qinq	priority <0-7>	This command sets priority in selective Q-in-Q.
qinq	access-ports PORTLISTS	This command specifies the access ports to apply the rule.
qinq	tunnel-ports PORTLISTS	This command specifies the tunnel ports to apply the rule.
qinq	end	The command exits the CLI Q-in-Q node and enters the CLI enable node.
qinq	exit	The command exits the CLI Q-in-Q node and enter the CLI configure node.
qinq	show	The command shows the current selective Q-in-Q profile configurations.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	vlan-stacking port-based priority <0~7>	This command sets the priority in port based Q-in-Q.
if-range	vlan-stacking port-based role (tunnel access normal)	This command sets VLAN stacking port role.
if-range	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
if-range	vlan-stacking tunnel-tpid index <1-6>	This command sets TPID for a Q-in-Q tunnel port.

Web Configuration

VLAN Stacking

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

VLAN Stacking Settings

Action Disable ▼

Tunnel TPID Index	TPID
1 (Default) ▼	8100 (0000~ffff)

Port	Tunnel TPID Index
From: 1 ▼ To: 1 ▼	1 (Default) ▼

Apply
Refresh

VLAN Stacking Status

Tunnel TPID Index	TPID
1	8100
2	8100
3	8100
4	8100
5	8100
6	8100

Port	Tunnel TPID Index (TPID)	Port	Tunnel TPID Index (TPID)
1	1 (8100)	2	1 (8100)
3	1 (8100)	4	1 (8100)
5	1 (8100)	6	1 (8100)
7	1 (8100)	8	1 (8100)
9	1 (8100)	10	1 (8100)
11	1 (8100)	12	1 (8100)
13	1 (8100)	14	1 (8100)
15	1 (8100)	16	1 (8100)
17	1 (8100)	18	1 (8100)
19	1 (8100)	20	1 (8100)
21	1 (8100)	22	1 (8100)
23	1 (8100)	24	1 (8100)

Parameter	Description
Action	Select one of the three modes, Disable or Port-Based or Selective for the VLAN stacking.
Configures the TPID Table: The TPID table has 6 entries.	
Tunnel TPID Index	Selects the table index.
TPID	Configures the TPID.
Configures the Port TPID:	
Port	Selects a port or a range of ports which you want to configure.
Tunnel TPID Index	Configures the index of the TPID Table for the specific ports.

Port-Based Q-in-Q

Q-in-Q

VLAN Stacking

Port-based Q-in-Q

Selective Q-in-Q

Port-based Q-in-Q Settings

Port	Role	SPVID	Priority
From: 1 To: 1	Normal	1 (1~4094)	0

Apply

Refresh

Port-based Q-in-Q Status

Port	Role	SPVID	Priority	Port	Role	SPVID	Priority
1	Normal	1	0	2	Normal	1	0
3	Normal	1	0	4	Normal	1	0
5	Normal	1	0	6	Normal	1	0
7	Normal	1	0	8	Normal	1	0
9	Normal	1	0	10	Normal	1	0
11	Normal	1	0	12	Normal	1	0
13	Normal	1	0	14	Normal	1	0
15	Normal	1	0	16	Normal	1	0
17	Normal	1	0	18	Normal	1	0
19	Normal	1	0	20	Normal	1	0
21	Normal	1	0	22	Normal	1	0
23	Normal	1	0	24	Normal	1	0

Parameter	Description
Port	Selects a port or a range of ports which you want to configure.
Role	Selects one of the three roles, Normal and Access and Tunnel, for the specific ports.
SPVID	Configures the service provider's VLAN.
Priority	Configures the priority for the specific ports.

Selective Q-in-Q

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

Selective Q-in-Q Settings

Name	<input type="text"/>	
Access Ports	<input type="text"/>	(ex. 1,3,5-6)
Tunnel Ports	<input type="text"/>	(ex. 1,3,5-6)
CVID	<input type="text"/>	(Range: 1~4094)
SPVID	<input type="text"/>	(Range: 1~4094)
Priority	<input type="text" value="0"/>	
Action	<input type="text" value="Disable"/>	

Selective Q-in-Q Status

No.	Name	Access Ports	Tunnel Ports	CVID	SPVID	Priority	Action	Delete

Parameter	Description
Name	Configures the selective Q-in-Q profile name.
Access Ports	Configures a port or a range of ports for the access ports.
Tunnel Ports	Configures a port or a range of ports for the tunnel ports.
CVID	Configures a customer's VLAN.
SPVID	Configures a service provider's VLAN.
Priority	Configures an 802.1Q priority for the profile.
Action	Enables / Disables the profile.

DHCP Option

Option 66/67

Introduction

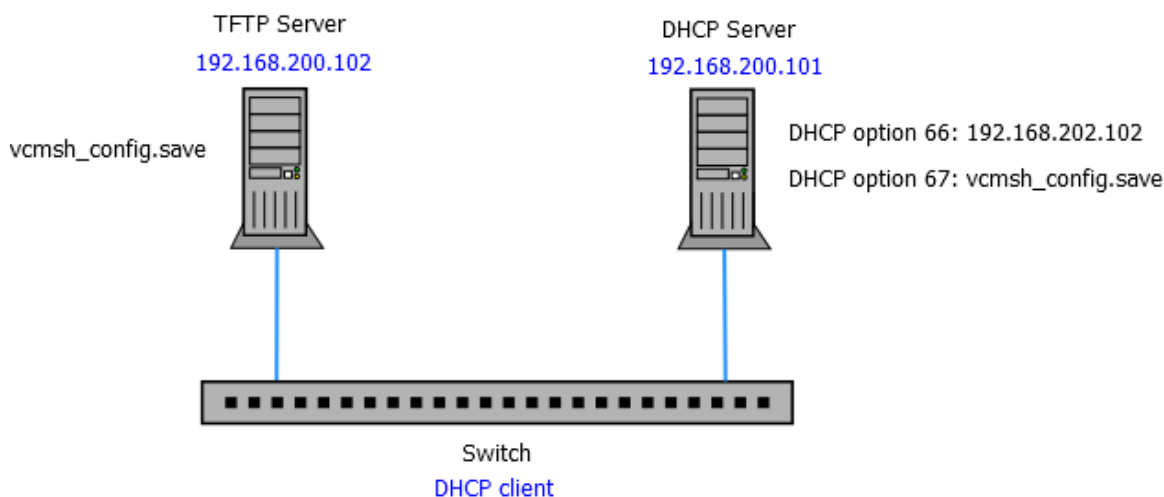
The Dynamic Host Configuration Protocol (DHCP) is used by device for requesting Internet Protocol parameters, such as an IP address from a network server. The protocol operates based on the client-server model.

When the Switch connects to a network, its DHCP client software in the operating system sends a broadcast query requesting necessary information. Any DHCP server on the network may service the request. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, and time servers, and "DHCP option 66 and 67".

DHCP option 66 is used to identify a TFTP server when the "TFTP server name" field in the DHCP header has been used for DHCP options. DHCP option 67 is used to identify a TFTP server when the "file name" field in the DHCP header has been used for DHCP options. If DHCP server supply "DHCP option 66 and 67" then the user can set it. When the switch connects to a network, the switch will get DHCP option 66 and 67's information from DHCP server. The user can put the configure file on the TFTP server. The Switch will download configure file from TFTP server automatically and it will take effect the configuration file immediately.

The procedures to use the DHCP option 66 and 67:

Configurations:



- » Set DHCP option 66 and 67's information on the DHCP server as below:
 - › DHCP option 66: 192.168.202.102
 - › DHCP option 67: `vcmsh_config.save`
- » Put configuration file "`vcmsh_config.save`" in TFTP server.
- » Enable DHCP option 66 and 67 on the Switch.

- » Enable DHCP client on the Switch.
- » When the Switch gets an IP from DHCP server, the DHCP server also gives the option 66's and 67's information to the Switch.
- » When the Switch gets the option 66 and 67 information, it downloads the configuration file from TFTP server automatically.
- » The Switch will take effect the configuration file immediately.
- » If the configuration file has an auto-backup command, the Switch backups the current system configuration to the TFTP server automatically.

Notice: The auto-backup command should be the last command in the configuration file.

CLI Configuration

Node	Command	Description
enable	show dhcp-options	This command displays the configurations and status for the DHCP option 66 and 67.
configure	dhcp-options option_66_67 (disable enable)	This command disables / enables the DHCP option 66 and 67 on the Switch.
configure	dhcp-options option_66_67 auto-backup	This command uploads the current configurations to TFTP server. The file name is vcmsh_config_MODEL-NAME_MAC if you didn't specify a filename for it.
configure	dhcp-options option_66_67 auto-backup file FILENAME	This command configures a filename for the auto-backup function.

Web Configuration

Parameter	Description
State	Select this option to enable / disable the DHCP option 66 and 67 on the Switch.
TFTP IP	The TFTP server's IP address gotten from the DHCP option 66.
TFTP File Name	The configuration filename gotten from the DHCP option 67.
Apply	Click Apply to save your changes to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.

Option 82

Introduction

DHCP Option 82 is the "DHCP Relay Agent Information Option". Option 82 was designed to allow a DHCP Relay Agent to insert circuit specific information into a request that is being forwarded to a DHCP server. Specifically the option works by setting two sub-options: Circuit ID and Remote ID.

The DHCP option 82 is working on the DHCP snooping or/and DHCP relay.

The switch will monitor the DHCP packets and append some information as below to the DHCPDISCOVER and DHCPREQUEST packets. The switch will remove the DHCP Option 82 from the DHCPOFFER and DHCPACK packets. The DHCP server will assign IP domain to the client dependent on these information.

The maximum length of the information is 32 characters.

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

When you enable the DHCP snooping information option 82 on the switch, this sequence of events occurs:

- » The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- » When the switch receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote-ID suboption) and the port identifier, vlan-mod-port, from which the packet is received (the circuit-ID suboption).
- » If the IP address of the relay agent is configured, the switch adds the IP address in the DHCP packet.
- » The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- » The DHCP server receives the packet. If the server is option-82 capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.
- » The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

Option Frame Format:

Code	Len	Agent Information Field					
82	N	i1	i2	i3	i4	...	iN

The Agent Information field consists of a sequence of SubOpt/Length/Value tuples for each sub-option, encoded in the following manner:

Sub-Option	Len	Sub-Option Value					
1	N	s1	s2	s3	s4	...	sN

DHCP Agent Sub-option Code	Sub-Option Description
-----	-----
1	Agent Circuit ID Sub-option
2	Agent Remote ID Sub-option

Circuit ID Sub-option Format:

Suboption Type	Length	Information
0x01		Circuit Form

Remote ID Suboption Frame Format:

Suboption Type	Length	Type	Length	MAC Address
0x02	8	0	6	6

Circuit Form:

The circuit form is a flexible architecture. It allows user to combine any information or the system configurations into the circuit sub-option.

The Circuit Form is a string format. And its maximum length is 100 characters.

The keyword, %SPACE, will be replaced with a space character.

The other keywords get system configurations from the system and then replace the keyword and its leading code in the Circuit form. Eventually, the content of the circuit form is part of the payload on the DHCP option 82 packet.

Rules:

- » The keyword must have a leading code '%'. For example: %HOSTNAME.
- » If there are any characters following the keywords, you must add '+' between the keyword and character. For example: %HOSTNAME+/.
- » If there are any characters before the keyword, you must add '+' between the character and the keyword. For example: Test+%HOSTNAME.

Keyword:

- | | |
|----------|--|
| HOSTNAME | - Add the system name into the Circuit sub-option.. |
| SPACE | - Add a space character. |
| SVLAN | - Add the service provider VLAN ID into the Circuit sub-option.
If the service provider VLAN is not defined, the system will return PVLAN. |
| CVLAN | - Add the customer VLAN ID into the Circuit sub-option. If the CVLAN is not defined, the system returns 0. |
| PORT | - Add the transmit port ID into the Circuit sub-option. |
| FRAME | - Add the frame ID into the Circuit sub-option.
The frame ID is configured with the CLI command, "dhcp-options option82 circuit_frame VALUE". Or GUI Circuit Frame. |
| SHELF | - Add the shelf ID into the Circuit sub-option. The shelf ID is configured with the CLI command, "dhcp-options option82 circuit_shelf VALUE". Or GUI Circuit Shelf. |
| SLOT | - Add the slot ID into the Circuit sub-option. The slot ID is configured with the CLI command, "dhcp-options option82 circuit_slot VALUE". Or GUI Circuit Slot. |

For Example:

```
HOSTNAME=CWGE24MS2.
SVLAN=44.
CVLAN=32.
```

Circuit Form=RD+%SPACE+Department+%SPACE+%HOSTNAME+%SPACE+%PORT+_+%SVLAN+. +%CVLAN

The circuit sub-option result is: RD Department CWGE24MS2 1_44.32

Default Settings

DHCP Option 82 state	: disabled.
Circuit Frame	: 1.
Circuit Shelf	: 0.
Circuit Slot	: 0.
Circuit ID String	: %HOSTNAME+%SPACE+eth/+%FRAME+/%SHELF+/%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN
Remote ID String	: %HOSTNAME+%SPACE+eth/+%FRAME+/%SHELF+/%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN

CLI Configuration

Node	Command	Description
enable	show dhcp-options	This command displays the DHCP options configurations.
configure	dhcp-options option82 (disable enable)	This command disables / enables the DHCP option 82 on the Switch.
configure	dhcp-options option82 circuit_id	This command configures the information of the circuit ID sub-option.
configure	dhcp-options option82 remote_id	This command configures the information of the remote ID sub-option.
configure	dhcp-options option82 circuit_frame VALUE	This command configures the frame ID for the circuit sub-option.
configure	dhcp-options option82 circuit_shelf VALUE	This command configures the shelf ID for the circuit sub-option.
configure	dhcp-options option82 circuit_slot VALUE	This command configures the slot ID for the circuit sub-option.

Web Configuration

DHCP Options

Option 66 & 67

Option 82

DHCP Option 82 Settings

Option 82 State

Disable

Option 82 Frame

1

Option 82 Shelf

0

Option 82 Slot

0

Circuit-ID String

%HOSTNAME+%SPACE+eth/+%FRAME+/%SHELF+/%SLOT+:%PORT+

Remote-ID String

%HOSTNAME+%SPACE+eth/+%FRAME+/%SHELF+/%SLOT+:%PORT+

DHCP Option 82 Port Settings

Port

1

Option 82 State

Enable

Circuit-ID String

Remote-ID String

Apply

Refresh

DHCP Option 82 Port Status

Port 1

Option 82 State

Enable

Circuit-ID String

Remote-ID String

Port 2

Option 82 State

Enable

Circuit-ID String

Remote-ID String

Parameter	Description
State	Select this option to enable / disable the DHCP option 82 on the Switch.
Circuit Frame	The frame ID for the circuit sub-option.
Circuit Shelf	The shelf ID for the circuit sub-option.
Circuit Slot	The slot ID for the circuit sub-option.
Circuit-ID String	The String of the circuit ID sub-option information.
Remote-ID String	The String of the remote ID sub-option information.
Apply	Click Apply to save your changes to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.

DHCP Option 82 Port Settings

Port	The port ID.
Circuit-ID String	The String of the circuit ID sub-option information for the specific port.
Remote-ID String	The String of the remote ID sub-option information for the specific port.

DHCP Option 82 Port Status

The field displays all of the ports' configurations.

DHCP Relay

Introduction

Because the DHCPDISCOVER message is a broadcast message, and broadcasts only cross other segments when they are explicitly routed, you might have to configure a DHCP Relay Agent on the router interface so that all DHCPDISCOVER messages can be forwarded to your DHCP server. Alternatively, you can configure the router to forward DHCP messages and BOOTP message. In a routed network, you would need DHCP Relay Agents if you plan to implement only one DHCP server.

The DHCP Relay that either a host or an IP router that listens for DHCP client messages being broadcast on a subnet and then forwards those DHCP messages directly to a configured DHCP server. The DHCP server sends DHCP response messages directly back to the DHCP relay agent, which then forwards them to the DHCP client. The DHCP administrator uses DHCP relay agents to centralize DHCP servers, avoiding the need for a DHCP server on each subnet.

Most of the time in small networks DHCP uses broadcasts however there are some circumstances where unicast addresses will be used. A router for such a subnet receives the DHCP broadcasts, converts them to unicast (with a destination MAC/IP address of the configured DHCP server, source MAC/IP of the router itself). The field identified as the GIADDR in the main DHCP page is populated with the IP address of the interface on the router it received the DHCP request on. The DHCP server uses the GIADDR field to identify the subnet the device and select an IP address from the correct pool. The DHCP server then sends the DHCP OFFER back to the router via unicast which then converts it back to a broadcast and out to the correct subnet containing the device requesting an address.

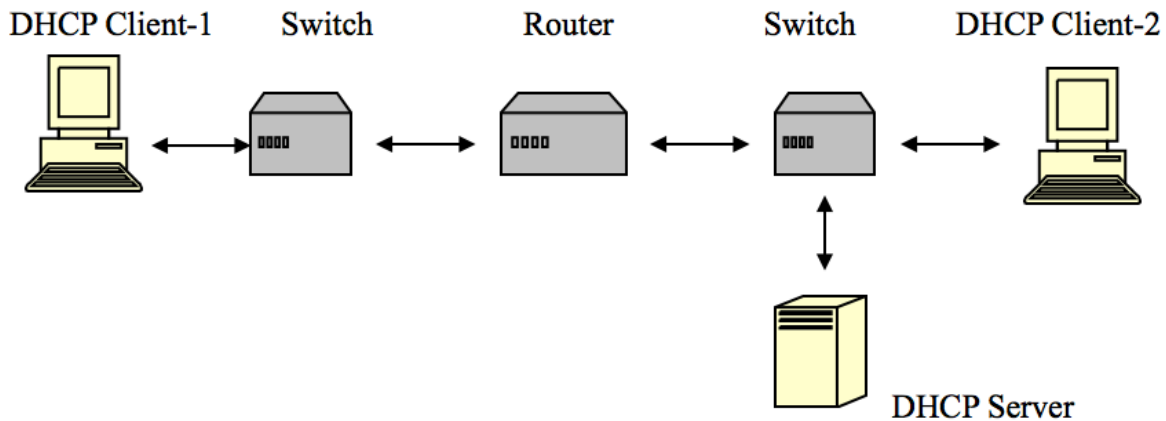
Configurations:

Users can enable/disable the DHCP Relay on the Switch. Users also can enable/disable the DHCP Relay on a specific VLAN. If the DHCP Relay on the Switch is disabled, the DHCP Relay is disabled on all VLANs even some of the VLAN DHCP Relay are enabled.

Applications

» Application-1 (Over a Router)

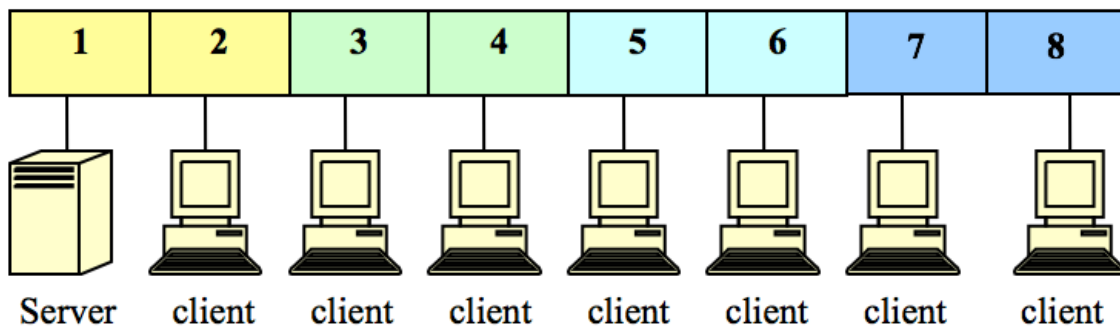
The DHCP client-1 and DHCP client-2 are located in different IP segments. But they allocate IP address from the same DHCP server.



» Application-2 (Local in different VLANs)

The DHCP client-1 and DHCP client-2 are located in different VLAN. But they allocate IP address from the same DHCP server.

Switch DHCP Relay agent



VLAN 1: port 1, 2 (Management VLAN)

VLAN 2: port 3, 4

VLAN 3: port 5, 6

VLAN 4: port 7, 8

DHCP Server => Port 1.

DHCP Client => Port 2, 3, 4, 5, 6, 7, 8.

Result: Hosts connected to port 2,3,4,5,6,7,8 can get IP from DHCP server.

Note: The DHCP Server must connect to the management VLAN member ports.

The DHCP Relay in management VLAN should be enabled.

Default Settings

The default global DHCP relay state is disabled.

The default VLAN DHCP relay state is disabled for all VLANs.

The default DHCP server is 0.0.0.0

CLI Configuration

Node	Command	Description
enable	show dhcp relay	This command displays the current configurations for the DHCP relay.
configure	dhcp relay (disable enable)	This command disables/enables the DHCP relay on the switch.
configure	dhcp relay vlan VLAN_ RANGE	This command enables the DHCP relay function on a VLAN or a range of VLANs.
configure	no dhcp relay vlan VLAN_RANGE	This command disables the DHCP relay function on a VLAN or a range of VLANs.
configure	dhcp helper-address IP_ADDRESS	This command configures the DHCP server's IP address.
configure	no dhcp helper-address	This command removes the DHCP server's IP address.

Example:

```

CWGE24MS2#configure terminal
CWGE24MS2(config)# interface eth0
CWGE24MS2(config-if)# ip address 172.20.1.101/24
CWGE24MS2(config-if)# ip address default-gateway 172.20.1.1
CWGE24MS2(config)#dhcp relay enable
CWGE24MS2(config)# dhcp relay vlan 1
CWGE24MS2(config)# dhcp helper-address 172.20.1.1

```

Web Configuration

DHCP Relay

DHCP Relay Settings

State

Disable ▾

VLAN State

Add ▾

DHCP Server IP

0.0.0.0

Apply

Refresh

DHCP Relay Status

DHCP Relay State	Disabled
Enabled on VLAN	None
DHCP Server IP	0.0.0.0

Parameter	Description
State	Enables / disables the DHCP relay for the Switch.
VLAN State	Enables / disables the DHCP relay on the specific VLAN(s).
DHCP Server IP	Configures the DHCP server’s IP address.

Dual Homing

Introduction

Dual Homing is a network topology in which a device is connected to the network by way of two independent access points (points of attachment). One access point is the primary connection, and the other is a standby connection that is activated in the event of a failure of the primary connection.

How Dual-Homing Works?

Assume the primary connection and secondary connections are connected to Internet by different way. For example, primary connection is connected to a physical network but secondary connection is connected to a wireless network. When enable dual homing feature, device will default connect to Internet by primary connection and secondary connection will be shutdown. If the port or all ports of primary connection are link-down, the device will replace primary connection by secondary connection to connect to Internet. At this situation, if secondary connection is also link-down, device will do nothing. Secondary connection only works as primary connection disconnecting.

Default Settings

Dual-Homing Configurations:

State	: Disable.
Primary Channel	: -
Secondary Channel	: -

Detail Status:

Primary Channel Status	: -
Secondary Channel Status	: -

Notices

If the channel is a single port, then the port cannot add into any trunk group.

CLI Configuration

Node	Command	Description
enable	show dual-homing	This command displays the dual-homing information.
configure	dual-homing (disable enable)	This command disables / enables the dual-homing function for the system.
configure	dual-homing primary-channel (port trunk) VALUE	This command sets the dual-homing primary channel for the system. The channel can be a single port or a trunk group.
configure	no dual-homing primary-channel	This command removes the dual-homing primary channel for the system.
configure	dual-homing secondary-channel (port trunk) VALUE	This command sets the dual-homing secondary channel for the system. The channel can be a single port or a trunk group.
configure	no dual-homing secondary-channel	This command removes the dual-homing secondary channel for the system.

Example:

```
CWGE24MS2(config)# link-aggregation 1 ports 5-6
CWGE24MS2(config)# link-aggregation 1 enable
CWGE24MS2(config)# dual-homing primary-channel port 2
CWGE24MS2(config)# dual-homing secondary -channel trunk 1
CWGE24MS2(config)# dual-homing enable
```

Web Configuration

Dual Homing

Dual Homing Settings

State Disable ▾

Group ID 1 ▾

Group State Disable ▾

Primary Channel Add ▾ Port ▾ 0

Secondary Channel Add ▾ Port ▾ 0

Apply
Refresh

Dual Homing Status

Group Id	1
Group State	Disabled
Primary Channel	None
Secondary Channel	None
Group Id	2
Group State	Disabled
Primary Channel	None
Secondary Channel	None
Group Id	3
Group State	Disabled
Primary Channel	None
Secondary Channel	None
Group Id	4
Group State	Disabled
Primary Channel	None
Secondary Channel	None

Parameter	Description
State	Enables / disables the Dual-Homing for the Switch.
Primary channel	Configures the primary channel. The channel can be single port or a trunk group.
Secondary channel	Configures the secondary channel. The channel can be single port or a trunk group.

ERPS

Introduction

The ITU-T G.8032 Ethernet Ring Protection Switching feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

The Ethernet ring protection functionality includes the following:

- » Loop avoidance
- » The use of learning, forwarding, and Filtering Database (FDB) mechanisms

Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL) and under normal conditions this ring link is blocked, i.e., not used for service traffic. One designated Ethernet ring node, the RPL owner node, is responsible to block traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL owner node is responsible for unblocking its end of the RPL, unless the RPL has failed, allowing the RPL to be used for traffic. The other Ethernet ring node adjacent to the RPL, the RPL neighbour node, may also participate in blocking or unblocking its end of the RPL.

The Ethernet rings could support a multi-ring/ladder network that consists of conjoined Ethernet rings by one or more interconnection points. The protection switching mechanisms and protocol defined in this Recommendation shall be applicable for a multi-ring/ladder network, if the following principles are adhered to:

- » R-APS channels are not shared across Ethernet ring interconnections;
- » on each ring port, each traffic channel and each R-APS channel are controlled (e.g., for blocking or flushing) by the Ethernet ring protection control process (ERP control process) of only one Ethernet ring;
- » Each major ring or sub-ring must have its own RPL.

In an Ethernet ring, without congestion, with all Ethernet ring nodes in the idle state (i.e., no detected failure, no active automatic or external command and receiving only "NR, RB" R-APS messages), with less than 1200 km of ring fibre circumference and fewer than 16 Ethernet ring nodes, the switch completion time (transfer time as defined in [ITU-T G.808.1]) for a failure on a ring link shall be less than 50 ms.

The ring protection architecture relies on the existence of an APS protocol to coordinate ring protection actions around an Ethernet ring.

The Switch supports up to six rings.

Guard timer -- All ERNs use a guard timer. The guard timer prevents the possibility of forming a closed loop and prevents ERNs from applying outdated R-APS messages. The guard timer

activates when an ERN receives information about a local switching request, such as after a switch fail (SF), manual switch (MS), or forced switch (FS). When this timer expires, the ERN begins to apply actions from the R-APS it receives. This timer cannot be manually stopped.

Wait to restore (WTR) timer -- The RPL owner uses the WTR timer. The WTR timer applies to the revertive mode to prevent frequent triggering of the protection switching due to port flapping or intermittent signal failure defects. When this timer expires, the RPL owner sends a R-APS (NR, RB) through the ring.

Wait to Block (WTB) timers -- This wait-to-block timer is activated on the RPL owner. The RPL owner uses WTB timers before initiating an RPL block and then reverting to the idle state after operator-initiated commands, such as for FS or MS conditions, are entered. Because multiple FS commands are allowed to co-exist in a ring, the WTB timer ensures that the clearing of a single FS command does not trigger the re-blocking of the RPL. The WTB timer is defined to be 5 seconds longer than the guard timer, which is enough time to allow a reporting ERN to transmit two R-APS messages and allow the ring to identify the latent condition. When clearing a MS command, the WTB timer prevents the formation of a closed loop due to the RPL owner node applying an outdated remote MS request during the recovery process.

Hold-off timer -- Each ERN uses a hold-off timer to delay reporting a port failure. When the timer expires, the ERN checks the port status. If the issue still exists, the failure is reported. If the issue does not exist, nothing is reported.

ERPS revertive and non-revertive switching

ERPS considers revertive and non-revertive operation. In revertive operation, after the condition(s) causing a switch has cleared, the traffic channel is restored to the working transport entity, i.e. blocked on the RPL. In the case of clearing of a defect, the traffic channel reverts after the expiry of a WTR timer, which is used to avoid toggling protection states in case of intermittent defects. In non-revertive operation, the traffic channel continues to use the RPL, if it is not failed, after a switch condition has cleared.

Control VLAN:

The pure ERPS control packets domain only, no other packets are transmitted in this vlan to guarantee no delay for the ERPS. So when you configure a Control VLAN for a ring, the vlan should be a new one. The ERPS will create this control vlan and its member ports automatically. The member port should have the Left and Right ports only.

In ERPS, the control packets and data packets are separated in different vlans.

The control packets are transmitted in a vlan which is called the Control VLAN.

Instance:

For ERPS version 2, the instance is a profile specifies a control vlan and a data vlan or multiple data vlans for the ERPS. In ERPS, it can separate the control packets and data packets in different vlans. The control packets is in the Control VLAN and the data packets can be in one or multiple data vlan. And then user can assign an instance to an ERPS ring easily.

In ERPS version 1, if a port is blocked by ERPS, all packets are blocked.

In ERPS version 2, if a port is blocked by a ring of ERPS, only the packets belong to the vlans in the instance are blocked.

Notice:

Control VLAN and Instance:

In CLI or Web configurations, there are the Control VLAN and the Instance settings.

If the Control VLAN is configured for a ring and you want to configure an instance for the ring. The control vlan of the instance must be same as the Control VLAN; otherwise, you will get an error. If you still want to use this instance, you can change the Control VLAN to same as the control vlan of the instance first. And then configures the instance.

CLI Configuration

Node	Command	Description
enable	show erps	This command displays the ERPS configurations.
enable	show erps instance	This command displays the ERPS instance configurations.
enable	show erps instance INSTANCE_ID	This command displays the specific ERPS instance configurations.
configure	erps enable	This command enables the global ERPS on the Switch.
configure	no erps enable	This command disables the global ERPS on the Switch.
configure	erps ring-id VALUE	This command creates an ERPS ring and its ID and enter ERPS node.
configure	erps instance	This command enters the instance configure node.
configure	no erps ring-id VALUE	This command creates an ERPS ring and enter ERPS node to configure detail ring configurations.
erps-ring	show	This command displays the configurations of the ring.
erps-ring	control-vlan	This command configures a control-vlan for the ERPS ring.
erps-ring	guard-timer	This command configures the Guard Timer for the ERPS ring. (default:500ms)
erps-ring	holdoff-timer	This command configures the Hold-off Timer for the ERPS ring. (default:0 ms)
erps-ring	left-port PORTID type [owner neighbor normal]	This command configures the left port and type for the ERPS ring.
erps-ring	mel VALUE	This command configures a Control MEL for the ERPS ring.
erps-ring	name STRING	This command configures a name for the ERPS ring.
erps-ring	revertive	This command configures the revertive mode for the ERPS ring.
erps-ring	no revertive	This command configures the non-revertive mode for the ERPS ring.
erps-ring	right-port PORTID type [owner neighbor normal]	This command configures the right port and type for the ERPS ring.
erps-ring	ring enable	This command enables the ring.
erps-ring	no ring enable	This command disables the ring.
erps-ring	version	This command configures a version for the ERPS ring.
erps-ring	wtr-timer	This command configures the WTR Timer for the ERPS ring. (default: 5 minutes)
config-erps- inst	instance INSTANCE_ID control-vlan VLAN_ID data-vlan VLAN_ID	This command configures a new instance and specifies its control vlan and data vlan.
config-erps- inst	no instance INSTANCE_ID	This command removes an instance.
config-erps- inst	show	This command displays all of the instance configurations.

Web configuration

Ring Settings:

ERPS

Ring Settings
Instance Settings

ERPS Global Settings

Global State Enable ▼

ERPS Ring Settings

Ring ID (1~255)
Ring Name
Instance (0:Disable, 0~30)
Control VLAN (1~4094)
Holdoff Timer (ms) (0~10000)
MEL (0~7)
Left Port None ▼ Normal ▼

State Disable ▼
Revertive Enable ▼
Ring Type Major-ring ▼
Version v2 ▼
WTR Timer (sec) (5~720)
Guard Timer (ms) (10~2000)
Right Port None ▼ Normal ▼

Apply Refresh

ERPS Ring Status

Ring ID	1	State	Disabled
Ring Name	Ring1	Revertive	Enable
Instance	None	Ring Type	Major-ring
Control VLAN	2	Version	v2
Holdoff Timer (ms)	0	WTR Timer (sec)	300
MEL	7	Guard Timer (ms)	500
Left Port	1	Right Port	2
Left Port Type	RPL Owner	Right Port Type	RPL Normal
Left Port Status	No connection	Right Port Status	No connection
Ring Status	Initialization		

Delete

Parameter	Description
Global State	Enables / disables the global ERPS state.
Ring ID	Configures the ring ID. The Valid value is from 1 to 255.
State	Enables/ disables the ring state.
Ring Name	Configures the ring name.(Up to 32 characters)
Revertive	Enables / disables the revertive mode.
Instance	Configures the instance for the ring. The Valid value is from 0 to 30. 0-Disable means the ERPS is running in version 1. The control VLAN of the instance should be same as below Control VLAN.
Control VLAN	Configures the Control VLAN which is the ERPS control packets domain for the ring.
Version	Configures the version for the ring.
Hold-off Timer	Configures the Hold-off time for the ring. The Valid value is from 0 to 10000 (ms).
WTR Timer	Configures the WTR time for the ring. The Valid value is from 5 to 12 (min).
MEL	Configures the Control MEL for the ring. The Valid value is from 0 to 7. The default is 7.
Guard Timer	Configures the Guard time for the ring. The Valid value is from 10 to 2000 (ms).
Left Port	Configures the left port and its type for the ring. The valid port type is one of Owner, Neighbor or Normal.
Right Port	Configures the right port and its type for the ring. The valid port type is one of Owner, Neighbor or Normal.
ERPS Status	
Ring ID	The ring ID.
Ring Name	The ring name.
State	The ring state.
Revertive	The ring revertive mode.
Control VLAN	The ring Control VLAN.
Version	The protocol version on the ring.
Holdoff Timer	The Hold-off time.
WTR Timer	The WTR time.
MEL	The Control MEL.
Guard Timer	The Guard time.
Left Port	The left port.
Left Port Type	The left port type.
Right Port	The right port.
Right Port Type	The right port type.
WTB Timer	The WTB time.
Ring Status	The current ring status.
Left Port Status	The current left port status.
Right Port Status	The current right port status.

Instance Settings:

ERPS

Ring Settings

Instance Settings

Instance Settings

Instance

Control VLAN

Data VLAN

Apply

Refresh

Instance Status

Instance	1	Data VLAN	1
Control VLAN	2		

Delete

Parameter	Description
Instance Settings	
Instance	Configures the instance ID. The valid value is from 1 to 31.
Control VLAN	Configures the control vlan for the instance. The valid value is from 1 to 4094.
Data VLAN	Configures the data vlan for the instance. The valid value is from 1 to 4094. It can be one or multiple vlans.
Instance Status	
Instance	The instance ID.
Control VLAN	The control vlan of the instance.
Data VLAN	The data vlan of the instance.

Link Aggregation

Static Trunk

Introduction

Link Aggregation (Trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports. The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

Default Settings

The default group Link Aggregation state is disabled for all groups.

The default group Link Aggregation load balance is source MAC and destination MAC for all groups.

Maximum link aggregation group	: 8
Maximum port in link aggregation group	: 8.

CLI Configuration

Node	Command	Description
enable	show link-aggregation	The command displays the current trunk configurations.
configure	link-aggregation [GROUP_ID] (disable enable)	The command disables / enables the trunk on the specific trunk group.
configure	link-aggregation [GROUP_ID] interface PORTLISTS	The command adds ports to a specific trunk group.
configure	no link-aggregation [GROUP_ID] interface PORTLISTS	The commands delete ports from a specific trunk group.

Example:

```
CWGE24MS2#configure terminal
```

```
CWGE24MS2(config)#link-aggregation 1 enable
```

```
CWGE24MS2(config)#link-aggregation 1 ports 1-4
```

Web Configuration

Link Aggregation

Static Trunk
LACP
LACP Info.

Static Trunk Settings

Group State Group 1 ▾ Disable ▾

Load Balance MAC ▾

Member Ports

☐ Select All ☐ Deselect All

☐ 1 ☐ 3 ☐ 5 ☐ 7

☐ 9 ☐ 11 ☐ 13 ☐ 15

☐ 17 ☐ 19 ☐ 21 ☐ 23

☐ 2 ☐ 4 ☐ 6 ☐ 8

☐ 10 ☐ 12 ☐ 14 ☐ 16

☐ 18 ☐ 20 ☐ 22 ☐ 24

Apply Refresh

Trunk Group Status

Group ID	State	Load Balance	Member Ports
1	Disabled	MAC	
2	Disabled	MAC	
3	Disabled	MAC	
4	Disabled	MAC	
5	Disabled	MAC	
6	Disabled	MAC	
7	Disabled	MAC	
8	Disabled	MAC	

Member Ports: T is Trunk member port but no link, A is Trunk member and link up.

Parameter	Description
Group State	Select the group ID to use for this trunk group, that is, one logical link containing multiple ports. Select Enable to use this static trunk group.
Load Balance	Configures the load balance algorithm for the specific trunk group.
Member Ports	Select the ports to be added to the static trunk group.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
Trunk Group Status	
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
State	This field displays if the trunk group is enabled or disabled.
Load Balance	This field displays the load balance policy for the trunk group.
Member Ports	This field displays the assigned ports that comprise the static trunk group.

LACP

Introduction

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention.

Please note that:

- » You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- » LACP only works on full-duplex links.
- » All ports in the same trunk group must have the same media type, speed, and duplex mode and flow control settings.
- » Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

System Priority:

The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP), the smaller the number, the higher the priority level.

System ID:

The LACP system ID is the combination of the LACP system priority value and the MAC address of the router.

Administrative Key:

The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:

- » Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium.
- » Configuration restrictions that you establish.

Port Priority:

The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Default Settings

The default System Priority is 32768.

The default group LACP state is disabled for all groups.

CLI Configuration

Node	Command	Description
enable	show lacp counters [GROUP_ID]	This command displays the LACP counters for the specific group or all groups.
enable	show lacp internal [GROUP_ID]	This command displays the LACP internal information for the specific group or all groups.
enable	show lacp neighbor [GROUP_ID]	This command displays the LACP neighbor's information for the specific group or all groups.
enable	show lacp port_priority	This command c displays the port priority for the LACP.
enable	show lacp sys_id	This command displays the actor's and partner's system ID.
configure	lacp (disable enable)	This command disables / enables the LACP on the switch.
configure	lacp GROUP_ID (disable enable)	This command disables / enables the LACP on the specific trunk group.
configure	clear lacp counters [PORT_ID]	This command clears the LACP statistics for the specific port or all ports.
configure	lacp system-priority <1-65535>	This command configures the system priority for the LACP. Note: The default value is 32768.
configure	no lacp system-priority	This command configures the default for the system priority for the LACP.
interface	lacp port_priority <1-65535>	This command configures the priority for the specific port. Note: The default value is 32768.
interface	no lacp port_priority	This command configures the default for the priority for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	lacp port_priority <1-65535>	This command configures the priority for the specific ports. Note: The default value is 32768.
if-range	no lacp port_priority	This command configures the default for the priority for the specific ports.

Web Configuration

LACP Settings

Link Aggregation

Static Trunk
LACP
LACP Info.

LACP Settings

State Disable ▾

System Priority 32768

Group LACP Group 1 ▾ Disable ▾

Port Priority From: - ▾ ~ - ▾ :

Apply
Refresh

LACP Group Status

Group ID	LACP State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

LACP Port Priority Status

Port	Priority	Port	Priority
1	32768	2	32768
3	32768	4	32768
5	32768	6	32768
7	32768	8	32768
9	32768	10	32768
11	32768	12	32768
13	32768	14	32768
15	32768	16	32768
17	32768	18	32768
19	32768	20	32768
21	32768	22	32768

Parameter	Description
State	Select Enable from the drop down box to enable Link Aggregation Control Protocol (LACP). Select Disable to not use LACP.
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group LACP	Select a trunk group ID and then select whether to Enable or Disable Group Link Aggregation Control Protocol for that trunk group.
Port Priority	Select a port or a range of ports to configure its (their) LACP priority.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
LACP Group Status	
Group ID	The field identifies the LACP group ID.
LACP State	This field displays if the group has LACP enabled.
LACP Port Priority Status	
Port	The field identifies the port ID.
Priority	The field identifies the port's LACP priority.

LACP Info.

Link Aggregation

Static Trunk
LACP
LACP Info.

LACP Information

Group ID

Group ID	1						
Neighbors Information							
Port	System Priority	System ID	Port	Age	Port State	Port Priority	Oper Key
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
Internal Information							
Port	Port Priority	Admin Key	Oper Key	Port State			
1	32768	1	1	0x45			
2	32768	2	2	0x45			

Neighbor Information: '-' means the port is link down.

Parameter	Description
Group ID	Select a LACP group that you want to view.
Neighbors Information	
Port	The LACP member port ID.
System Priority	LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)
System ID	The neighbor Switch's system ID.
Port	The direct connected port Id of the neighbor Switch.
Age	The available time period of the neighbor Switch LACP information.
Port State	The direct connected port's state of the neighbor Switch.
Port Priority	The direct connected port's priority of the neighbor Switch.
Oper Key	The Oper key of the neighbor Switch.
Internal Information	
Port	The LACP member port ID.
Port Priority	The port priority of the LACP member port.
Admin Key	The Admin key of the LACP member port.
Oper Key	The Oper key of the LACP member port.
Port State	The port state of the LACP member port.

Link Layer Discovery Protocol (LLDP)

Introduction

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802® LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

Default Settings

The LLDP on the Switch is disabled.

Tx Interval : 30 seconds.

Tx Hold : 4 times.

Time To Live : 120 seconds.

Port	Status	Port	Status
----	-----	----	-----
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable
7	Enable	8	Enable
9	Enable	10	Enable
11	Enable	12	Enable
13	Enable	14	Enable
15	Enable	16	Enable
17	Enable	18	Enable
19	Enable	20	Enable
21	Enable	22	Enable
23	Enable	24	Enable

CLI Configuration

Node	Command	Description
enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all of the ports' neighbor information.
configure	lldp (disable enable)	This command globally enables / disables the LLDP function on the Switch.
configure	lldp tx-interval	This command configures the interval to transmit the LLDP packets.
configure	lldp tx-hold	This command configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)
interface	lldp-agent (disable enable rx-only tx-only)	This command configures the LLDP agent function. disable - Disable the LLDP on the specific port. enable - Transmit and Receive the LLDP packet on the specific port. tx-only - Transmit the LLDP packet on the specific port only. rx-only - Receive the LLDP packet on the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	lldp-agent (disable enable rx-only tx-only)	This command configures the LLDP agent function. disable - Disable the LLDP on the specific port. enable - Transmit and Receive the LLDP packet on the specific port. tx-only - Transmit the LLDP packet on the specific port only. rx-only - Receive the LLDP packet on the specific port.

Web Configuration

LLDP

Settings
Neighbor

LLDP Settings

State Disable ▾

Tx Interval 30 seconds

Tx Hold 4 times

Time To Live 120 seconds

Port

From: 1 ▾ To: 1 ▾

State

Enable ▾

Apply
Refresh

LLDP Status

Port	State	Port	State
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable
7	Enable	8	Enable
9	Enable	10	Enable
11	Enable	12	Enable
13	Enable	14	Enable
15	Enable	16	Enable
17	Enable	18	Enable
19	Enable	20	Enable
21	Enable	22	Enable
23	Enable	24	Enable

Parameter	Description
State	Globally enables / disables the LLDP on the Switch.
Tx Interval	Configures the interval to transmit the LLDP packets.
Tx Hold	Configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)
Time To Live	The hold time for the Switch's information.
Port	The port range which you want to configure.
State	Enables / disables the LLDP on these ports.
LLDP Status	
Port	The Port ID.
State	The LLDP state for the specific port.

LLDP

SettingsNeighbor

LLDP Neighbor Information

Port21▼Apply

Local Port 21	
Remote Port ID	1
Chassis ID	00-22-3b-02-01-74
System Name	CNGE11FX3TX8MSPOE
System Description	ComNetFirmware Version 1.0.0 2016-10-19T14:07:17-04:00
System Capabilities	Bridge/Switch (enabled)
Management IP	192.168.10.2
Time To Live	120 seconds

Parameter	Description
Port	Select the port(s) which you want to display the port’s neighbor information.
Local Port	The local port ID.
Remote Port ID	The connected port ID.
Chassis ID	The neighbor’s chassis ID.
System Name	The neighbor’s system name.
System Description	The neighbor’s system description.
System Capabilities	The neighbor’s capability.
Management Address	The neighbor’s management address.
Time To Live	The hold time for the neighbor’s information.

Loop Detection

Introduction

Loop detection is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

The loop detection function sends probe packets periodically to detect if the port connect to a network in loop state. The Switch shuts down a port if the Switch detects that probe packets loop back to the same port of the Switch.

Loop Recovery:

When the loop detection is enabled, the Switch will send one probe packets every two seconds and then listen this packet. If it receives the packet at the same port, the Switch will disable this port. After the time period, recovery time, the Switch will enable this port and do loop detection again.

The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop detection feature.

Default Settings

The default global Loop-Detection state is disabled.

The default Loop Detection Destination MAC is 00:22:3b:aa:aa:ab

The default Port Loop-Detection state is disabled for all ports.

The default Port Loop-Detection status is unblocked for all ports.

The loop detection on the Switch is disabled.

Loop Detection Destination MAC=00:22:3b:aa:aa:ab

Recovery Port	State	Status	State	Time	Recovery Port	State	Status	State	Time
----	-----	-----	-----	----	----	-----	-----	-----	----
1	Disabled	Normal	Enabled	1	2	Disabled	Normal	Enabled	1
3	Disabled	Normal	Enabled	1	4	Disabled	Normal	Enabled	1
5	Disabled	Normal	Enabled	1	6	Disabled	Normal	Enabled	1
7	Disabled	Normal	Enabled	1	8	Disabled	Normal	Enabled	1
9	Disabled	Normal	Enabled	1	10	Disabled	Normal	Enabled	1
11	Disabled	Normal	Enabled	1	12	Disabled	Normal	Enabled	1
13	Disabled	Normal	Enabled	1	14	Disabled	Normal	Enabled	1
15	Disabled	Normal	Enabled	1	16	Disabled	Normal	Enabled	1
17	Disabled	Normal	Enabled	1	18	Disabled	Normal	Enabled	1
19	Disabled	Normal	Enabled	1	20	Disabled	Normal	Enabled	1
21	Disabled	Normal	Enabled	1	22	Disabled	Normal	Enabled	1
23	Disabled	Normal	Enabled	1	24	Disabled	Normal	Enabled	1

CLI Configuration

Node	Command	Description
enable	show loop-detection	This command displays the current loop detection configurations.
configure	loop-detection (disable enable)	This command disables / enables the loop detection on the switch.
configure	loop-detection address MACADDR	This command configures the destination MAC for the loop detection special packets.
configure	no loop-detection address	This command configures the destination MAC to default (00:0b:04:AA:AA:AB).
interface	loop-detection (disable enable)	This command disables / enables the loop detection on the port.
interface	no shutdown	This command enables the port. It can unblock port blocked by loop detection.
interface	loop-detection recovery (disable enable)	This command enables / disables the recovery function on the port.
interface	loop-detection recovery time VALUE	This command configures the recovery period time.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	loop-detection (disable enable)	This command disables / enables the loop detection on the ports.
if-range	loop-detection recovery (disable enable)	This command enables / disables the recovery function on the port.
if-range	loop-detection recovery time VALUE	This command configures the recovery period time.

Example:

```
CWGE24MS2(config)#loop-detection enable
```

```
CWGE24MS2(config)#interface 1/0/1
```

```
CWGE24MS2(config-if)#loop-detection enable
```


Web Configuration

Loop Detection

Loop Detection Settings

State Disable ▾

MAC Address 00:22:3b:aa:aa:ab

Port	State	Action	Loop Recovery	Recovery Time (min)
From: 1 ▾ To: 1 ▾	Disable ▾	None ▾	Enable ▾	1 (Range: 1-60)

Apply
Refresh

Loop Detection Status

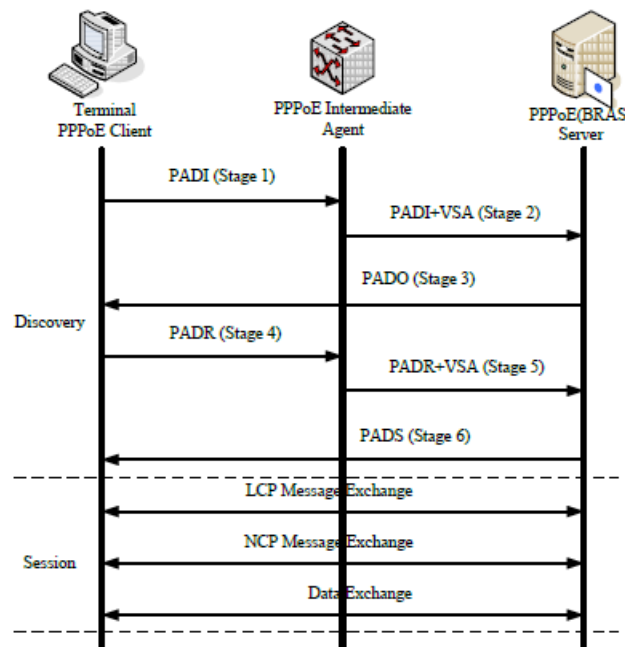
Port	State	Status	Loop Recovery	Recovery Time (min)
1	Disabled	Normal	Enabled	1
2	Disabled	Normal	Enabled	1
3	Disabled	Normal	Enabled	1
4	Disabled	Normal	Enabled	1
5	Disabled	Normal	Enabled	1
6	Disabled	Normal	Enabled	1
7	Disabled	Normal	Enabled	1
8	Disabled	Normal	Enabled	1
9	Disabled	Normal	Enabled	1
10	Disabled	Normal	Enabled	1
11	Disabled	Normal	Enabled	1
12	Disabled	Normal	Enabled	1
13	Disabled	Normal	Enabled	1
14	Disabled	Normal	Enabled	1
15	Disabled	Normal	Enabled	1
16	Disabled	Normal	Enabled	1
17	Disabled	Normal	Enabled	1
18	Disabled	Normal	Enabled	1
19	Disabled	Normal	Enabled	1
20	Disabled	Normal	Enabled	1
21	Disabled	Normal	Enabled	1
22	Disabled	Normal	Enabled	1
23	Disabled	Normal	Enabled	1

Parameter	Description
State	Select this option to enable loop guard on the Switch.
MAC Address	Enter the destination MAC address the probe packets will be sent to. If the port receives these same packets the port will be shut down.
Port	Select a port on which to configure loop guard protection.
State	Select Enable to use the loop guard feature on the Switch.
Loop Recovery	Select Enable to reactivate the port automatically after the designated recovery time has passed.
Recovery Time	Specify the recovery time in minutes that the Switch will wait before reactivating the port. This can be between 1 to 60 minutes.
Apply	Click Apply to save your changes to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Loop Guard Status	
Port	This field displays a port number.
State	This field displays if the loop guard feature is enabled.
Status	This field displays if the port is blocked.
Loop Recovery	This field displays if the loop recovery feature is enabled.
Recovery Time (min)	This field displays the recovery time for the loop recovery feature.

PPPoE IA

Introduction

PPPoE Intermediate Agent (PPPoE IA) is placed between a subscriber and BRAS to help the service provider BRAS distinguish between end hosts connected over Ethernet to an access switch. On the access switch, PPPoE IA enables Subscriber Line Identification by appropriately tagging Ethernet frames of different users. (The tag contains specific information like which subscriber is connected to the switch and VLAN.) PPPoE IA acts as mini security firewall between host and BRAS by intercepting all PPPoE Active Discovery (PAD) messages on a per-port per-vlan basis. It provides specific security feature such as verifying the intercepted PAD message from untrusted port, inserting and removing VSA Tags (vendor-specific tag) into and from PAD messages.



PPPoE Discovery Stage

- » The PPPoE client broadcasts a PADI packet that contains information about the service type it requests.
- » PPPoE IA intercepts PPPoE discovery frames from the client and inserts a unique line identifier (circuit-id /remote-id) using the PPPoE Vendor-Specific tag (0x0105) to PADI (PPPoE Active Discovery Initiation) packets. The PPPoE IA forwards these packets to the PPPoE server after the insertion.
- » After receiving a PADI packet that it can serve, a PPPoE server replies with a PADO packet. The destination address of the PADO packet is the unicast packet of the host that sent the PADI.
- » Depending on the network topology, since the PADI was broadcast, the PPPoE client may receive PADO packets sent by multiple PPPoE servers. Among these PPPoE servers, the PPPoE client selects the one whose PADO packet arrived the earliest and unicasts a PADR packet to the PPPoE server.

- » Depending on the network topology, since the PADI was broadcast, the PPPoE client may receive PADO packets sent by multiple PPPoE servers. Among these PPPoE servers, the PPPoE client selects the one whose PADO packet arrived the earliest and unicasts a PADR packet to the PPPoE server.
- » PPPoE IA intercepts PPPoE discovery frames from the client and inserts a unique line identifier (circuit-id /remote-id) using the PPPoE Vendor-Specific tag (0x0105) to PADR (PPPoE Active Discovery Request) packets. The PPPoE IA forwards these packets to the PPPoE server after the insertion.
- » The PPPoE server generates a unique session ID for the session and sends the session ID to the PPPoE client through a PADS packet. If no error occurs, the session will thus be established and PPPoE moves on to the Session stage.

PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the Switch adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 1 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	#1	#2
------------------------------------	----------------	--------------	-----------	-----------

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, #1 and #2. The Value is the 32-bit number 0x00000DE9, which stands for the "ADSL Forum" IANA entry. #1 and #2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client.

Sub-Option Format

There are two types of sub-option: "Agent Circuit ID Sub-option" and "Agent Remote ID Suboption". They have the following formats.

Table 2 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (64 bytes)

Table 3 PPPoE IA Remote ID Sub-option Format

SubOpt	Length	Value
0x02 (1 byte)	N (1 byte)	MAC Address or String (64 bytes)

The 0x01 in the first field identifies this as an Agent Circuit ID sub-option and 0x02 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field. The Switch

takes the Circuit ID string you manually configure for a VLAN on a port as the highest priority and the Circuit ID string for a port as the second priority. In addition, the Switch puts the PPPoE client's MAC address into the Agent Remote ID Sub-option if you do not specify any user-defined string.

Flexible Circuit ID Syntax with Identifier String and Variables

If you do not configure a Circuit ID string for a VLAN on a specific port or for a specific port, the Switch adds the user-defined identifier string and variables into the Agent Circuit ID Sub-option. The system variables can be the host name of the access node (Switch), the port number of the PPPoE client and/or the VLAN ID on the PPPoE packet.

Table 4 PPPoE IA System Variable

System Variable	Description
%HOSTNAME	Host name of access node(Switch)
%SPACE	Space key(ASCII 0x20)
%PORT	Port number of the client
%SVLAN	Service provider VLAN ID
%CVLAN	Client VLAN ID

PS. %SVLAN equal to %CVLAN

Users can freely combined circuit ID, using the '+' symbol to links system variables and identifier strings, in order to meet specific requirements.

EX: CLI Command

pppoe intermediate-agent format-type user-defined %HOSTNAME+%SPACE+atm+%SPACE+/0/0/+%PORT+:+%CVLAN

Table 5: PPPoE IA Circuit ID Sub-option Format: User-defined String and Variables

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	Host Name (x bytes)
	Space (1 byte)	atm (3 bytes)
	Space (1 byte)	/0/0/ (5 bytes)
	Port ID (2 bytes)	:
		(1 byte)
		CVLAN ID (4 bytes)

WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string for a specific VLAN on a port or for a specific port, and no set the flexible Circuit ID syntax in the Switch, the Switch automatically generates a Circuit ID string according to the default Circuit ID syntax which is defined in the DSL Forum Working Text (WT)-101. The default access node identifier is the host name of the PPPoE intermediate agent and the eth indicates "Ethernet", and the slot id is 0.

SubOpt Length

Value

0x01 (1 byte)	N (1 byte)	Access node identifier	Space (1 byte)	eth (3 bytes)	Space (1 byte)	Slot ID (1 byte)	/ (1 byte)	Port ID (2 bytes)	: (1 byte)	CVLAN ID (4 bytes)
------------------	---------------	---------------------------	-------------------	------------------	-------------------	---------------------	---------------	----------------------	---------------	-----------------------

Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- » If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.

If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s).

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

- » The trusted ports can keep/replace/strip vendor-tag of PADO and PADS packet.
- » Keep: means that the PPPoE agent will keep original vendor-tag in the PADO/PADS packet.
- » Replace: means that the PPPoE agent will replace the vendor-tag in the PADO/PADS packet with its own vendor-tag.
- » Strip: means that the PPPoE agent will strip the vendor-tag in the PADO/PADS packet(Default).

Untrusted ports are connected to subscribers.

- » If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s).

- » The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

CLI Configuration

Node	Command	Description
enable	show pppoe intermediate-agent configuration	This command displays the current configurations for the PPPoE IA.
enable	show pppoe intermediate-agent statistics	This command displays the current statistics for the PPPoE IA.
enable	show pppoe intermediate-agent statistics by-vlan <VLAN-list>	This command displays the current statistics by specific VLANs for the PPPoE IA.
configure	clear pppoe intermediate-agent statistics	This command clears the statistics for the PPPoE IA.
configure	clear pppoe intermediate-agent statistics by-vlan <VLAN-list>	This command clears the statistics by specific VLANs for the PPPoE IA.
configure	pppoe intermediate-agent <enable disable>	This command disables / enables the PPPoE IA on the switch.
configure	pppoe intermediate-agent format-type user-defined <user-defined-string>	This command configures the user defined circuit ID string for the PPPoE IA.
configure	pppoe intermediate-agent vlan <VLAN-list>	This command enables the PPPoE IA on either (a) a specific VLAN, (b) a comma separated list like "x,y," or (c) a range like "x-y".
configure	pppoe intermediate-agent circuit-id-vlan <VLAN-list>	This command enables the PPPoE IA circuit-id on either (a) a specific VLAN, (b) a comma separated list like "x,y," or (c) a range like "x-y".
configure	pppoe intermediate-agent remote-id-vlan <VLAN-list>	This command enables the PPPoE IA remote-id on either (a) a specific VLAN, (b) a comma separated list like "x,y," or (c) a range like "x-y".
configure	no pppoe intermediate-agent format-type user-defined	This no command removes the user defined circuit ID for the PPPoE IA.
configure	no pppoe intermediate-agent vlan	This no command disables PPPoE IA on all VLANs.
configure	no pppoe intermediate-agent vlan <VLAN-list>	This no command disables the PPPoE IA on specific VLANs.
configure	no pppoe intermediate-agent circuit-id-vlan	This no command disables the PPPoE IA circuit-id on all VLANs.
configure	no pppoe intermediate-agent circuit-id-vlan <VLAN-list>	This no command disables the PPPoE IA circuit-id on specific VLANs.
configure	no pppoe intermediate-agent remote-id-vlan	This no command disables the PPPoE IA remote-id on all VLANs.
configure	no pppoe intermediate-agent remote-id-vlan <VLAN-list>	This no command disables the PPPoE IA remote-id on specific VLANs.

Node	Command	Description
interface	pppoe intermediate-agent <enable disable>	This command disables / enables the PPPoE IA on specific interface for the PPPoE IA.
interface	pppoe intermediate-agent trust	This command sets a physical interface as trusted port.
interface	pppoe intermediate-agent format-type <circuit-id remote-id> <id-string>	This command sets circuit ID or remote ID string on specific interface for the PPPoE IA.
interface	pppoe intermediate-agent vendor-tag <keep replace strip>	This command is used to set the retransmitting policy of the specific interface for the PADO/PADS packet. Default:Keep
interface	pppoe intermediate-agent vlan <VLAN-list>	This command enables the PPPoE IA on specific VLANs of interface.
interface	no pppoe intermediate-agent trust	This command sets a physical interface as untrusted port.
interface	no pppoe intermediate-agent format-type <circuit-id remote-id>	This command removes circuit ID or remote ID string on specific interface for the PPPoE IA
interface	no pppoe intermediate-agent vendor-tag	The command sets the retransmitting policy of the specific interface as "keep".
interface	no pppoe intermediate-agent vlan	This command disables the PPPoE IA on all VLANs.
interface	no pppoe intermediate-agent vlan <VLAN-list>	This command disables the PPPoE IA on specific VLANs of interface.
if-pppoe-vlan	pppoe intermediate-agent format-type <circuit-id remote-id> <id-string>	This command sets circuit ID or remote ID string on specific VLANs of interface for the PPPoE IA.
if-pppoe-vlan	no pppoe intermediate-agent format-type <circuit-id remote-id>	This command removes circuit ID or remote ID string on specific VLANs of interface for the PPPoE IA.

Example:

```

CWGE24MS2(config)#pppoe intermediate-agent enable
CWGE24MS2(config)#pppoe intermediate-agent vlan 1-100,200,300
CWGE24MS2(config)#pppoe intermediate-agent circuit-id-vlan 1-100,200,300
CWGE24MS2(config)#pppoe intermediate-agent remote-id-vlan 1-100,200,300
CWGE24MS2(config)#pppoe intermediate-agent format-type user-defined %HOSTNAME+%SPACE+atm+%SPACE+/0/0/+%PORT+:+%CVLAN
CWGE24MS2(config)#interface 1/0/1
CWGE24MS2(config-if)#pppoe intermediate-agent enable
CWGE24MS2(config-if)#interface 1/0/8
CWGE24MS2(config-if)#pppoe intermediate-agent enable
CWGE24MS2(config-if)#pppoe intermediate-agent trust
CWGE24MS2(config-if)#pppoe intermediate-agent vlan 1
CWGE24MS2(if-pppoe-vlan)#

```


Web Configuration

Global Configuration

PPPoE IA Global Configuration

Global Configuration

Port Configuration

Statistics

PPPoE IA Global Configurations

PPPoE-IA

Disable ▾

User-Defined-String

Ex: %HOSTNAME+%SPACE+atm+/1/0/+%PORT+.0200:%CVLAN

PPPoE IA VLAN Configurations

PPPoE IA

Add ▾

(1,2,10-20,...,4094)

Circuit-ID

Add ▾

(1,2,10-20,...,4094)

Remote-ID

Add ▾

(1,2,10-20,...,4094)

Apply

Refresh

Parameter	Description
PPPoE-IA	Selects Enable to activate the PPPoE-IA or Disable to deactivate the PPPoE-IA.
User-Defined-String	User defined circuit ID string for the PPPoE IA.
PPPoE IA VLAN	Selects Add to increase the PPPoE-IA Vlan or Remove to delete the PPPoE-IA Vlan.
Circuit-ID VLAN	Selects Add to increase the Circuit-ID Vlan or Remove to delete the Circuit-ID Vlan.
Remote-ID VLAN	Selects Add to increase the Remote-ID Vlan or Remove to delete the Remote-ID Vlan.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Port Configuration

PPPoE IA Port Configuration

Global Configuration

Port Configuration

Statistics

PPPoE IA Port Configurations

Port

1

State

Disable

Trusted

No

Vendor-Tag

Strip

Circuit-ID String

Remote-ID String

PPPoE IA Interface Vlan Configurations

VLAN

Add

(1,2,10-20,...,4094)

Circuit-ID String

Remote-ID String

Apply

Refresh

PPPoE IA Port Status

Port

1

Show

PPPoE IA

Disable

Trusted

No

Policy

Strip

Circuit-ID String

Remote-ID String

Interface VLAN

Circuit-ID String

Remote-ID String

Parameter	Description
Port Number	Selects a port number you want to configure on this screen
State	Selects Enable to activate the port or Disable to deactivate the port
Trusted	Selects yes to sets a physical interface as trusted port
Vendor-Tag	Set the retransmitting policy of the specific interface for the PADO/PADS packet<keep replace strip>. Default:Keep
Circuit-ID String	User defined circuit ID string on specific interface for the PPPoE IA
Remote ID String	User defined remote ID string on specific interface for the PPPoE IA
Interface VLAN	Selects Add to increase the interface Vlan or Remove to delete the interface Vlan
Circuit-ID String	User defined circuit ID string on specific interface vlan for the PPPoE IA
Remote-ID String	User defined remote ID string on specific interface vlan for the PPPoE IA
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port	Selects a port number you want to display its configurations.
Show	Show the configurations of the port.

Statistics

PPPoE IA Statistics

Global Configuration

Port Configuration

Statistics

PPPoE IA Statistics

Vlan

Vlan1			<input type="button" value="Clear"/>
PPPoE discovery packet	Received	Forwarded	Dropped
PADI	0	0	0
PADO	0	0	0
PADR	0	0	0
PADS	0	0	0
PADT	0	0	0
Malformed packet	0	0	0

Parameter	Description
VLAN	Displays the current statistics of the vlan for the PPPoE IA.
PPPoE discovery packet	PPPoE packet type
Received	Total received packet
Forwarded	Total forwarded packet
Dropped	Total dropped packet
Show	Show the statistics of the vlan.
clear	Clear the statistics of the vlan.

Static Route

Introduction

Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. Static routes use less bandwidth than dynamic routes. No CPU cycles are used to calculate and analyze routing updates.

IP forwarding

IP forwarding provides on end to end delivery of IP packet between hosts with help of routers. Routing database plays import role in forwarding the packets. Routers populate its routing database either by manual configurations or by using dynamic routing protocols.

IP forwarding works as router as well as Inter VLAN routing with trunk stick.

Manual routing configurations are called as Static routes. Static routes are permanent routes; we can delete those routes with manual configurations only.

Whenever an IP packet received by a router then it fetches destination IP address and it will do the lookup in routing table to find the longest prefix match route. Packet is forwarded on the assigned next-hop in the route.

CLI configuration

Node	Command	Description
enable	show ip forwarding status	This command displays the current configuration of the ip forwarding status.
enable	show ip routes (all ipv4 ipv6)	This command displays the configurations of IPv4 or IPv6 or both routes from routing table.
enable	show ip arp (all ipv4 ipv6)	This command displays dynamic and static IPv4 or IPv6 or both ARP entries in ARP table.
enable	show ip hosts (all ipv4 ipv6)	This command displays assigned IPv4 or IPv6 or both addresses for interfaces in router.
configure	ip forwarding enable	This command enables layer 3 IPv4 and IPv6 forwarding/routing globally.
configure	no ip forwarding enable	This command disables layer 3 IPv4 and IPv6 forwarding/routing globally. This will delete all assigned IP addresses and static routes from interfaces.
configure	ip arp proxy enable	This command enables route to act as an ARP proxy globally; It will be useful in InterVLAN routing.
configure	no ip arp proxy enable	This command disables route to act as an ARP proxy.
configure	ipv4 arp <IPv4_ADDR> <MAC_ADDR>	This command allows adding static IPv4 ARP entry in ARP table.
configure	ip6 arp <IPv6_ADDR> <MAC_ADDR>	This command allows adding static IPv6 ARP entry in ARP table.

Node	Command	Description
configure	no ipv4 arp <IPv4_ADDR> <MAC_ADDR>	This command deletes a static IPv4 ARP entry from ARP table.
configure	no ipv6 arp <IPv6_ADDR> <MAC_ADDR>	This command deletes a static IPv6 ARP entry from ARP table.
configure	interface vlan VLAN-ID	This command enters the L3 interface node.
L3 interface	ipv4 address A.B.C.D/M	This command assigns a specified IPv4 interface route to the interface. We can assign multiple IPv4 interface route to a single interface with different IP segment. If this configuration is a first IP assigning to the interface then automatically interface is enabled for routing.
L3 interface	ipv6 address <IPv6_ADDR>/M	This command assigns a specified IPv6 interface route to the interface. We can assign only one IPv6 interface route for an interface vlan. If this configuration is a first IP assigning to the interface then it automatically enables the interface with routing.
L3 interface	no ipv4 address A.B.C.D/M	This command deletes a specified IPv4 interface route from the interface vlan. This command deletes all dependent static routes on the specified IPv4 interface route. If there is no assigned IP addresses for the specified interface after deleting then it will automatically disables routing in interface.
L3 interface	no ipv4 address <IPv6_ADDR>/M	This command deletes a specified IPv6 interface route from the interface. This command deletes all dependent static routes on the specified IPv6 interface route. If there is no assigned IP addresses for the specified interface after deleting then it will automatically disables routing in interface vlan.
L3 interface	ipv4 route A.B.C.D/M A.B.C.D	This command configures an IPv4 static route onto the specified interface vlan.
L3 interface	ipv6 route <IPv6_ADDR>/M <IPv6_ADDR>	This command configures an IPv6 static route onto the specified interface vlan.
L3 interface	no ipv4 route A.B.C.D/M A.B.C.D	This command deletes a specified IPv4 static route from an interface vlan.
L3 interface	no ipv6 route <IPv6_ADDR>/M <IPv6_ADDR>	This command deletes a specified IPv6 static route from an interface vlan.

Example:

IP Forwarding Enable: This command is used to enable ip forwarding (routing).
CWGE24MS2(config)#ip forwarding enable

IP Forwarding Disable: This command is used to disable ip forwarding.
CWGE24MS2(config)#no ip forwarding enable

ARP proxy enable: This command is used to enable ARP proxy.
CWGE24MS2(config)#ip arp proxy enable

ARP proxy disable: This command is used to disable ARP proxy.
CWGE24MS2(config)#no ip arp proxy enable

Add a static IPv4/IPv6 ARP entry: This command is used to add a static IPv4/IPv6 ARP entries.
CWGE24MS2(config)#ipv4 arp 192.168.20.1 00:11:22:33:44:55
CWGE24MS2(config)#ipv6 arp 1234:ab::ccdd 00:11:22:33:44:55

Deletes a static IPv4/IPv6 ARP entry: This command is used to delete static IPv4/IPv6 ARP entries
CWGE24MS2(config)#no ipv4 arp 192.168.20.1 00:11:22:33:44:55
CWGE24MS2(config)#no ipv6 arp 1234:ab::ccdd 00:11:22:33:44:55

Assigning a IPv4/IPv6 interface router: This command is used to add an IPv4/IPv6 interface route to a interface vlan.

```
CWGE24MS2(config)#interface vlan 1
CWGE24MS2(config-if-vlan-l3)#
CWGE24MS2(config-if-vlan-l3)#ipv4 address 192.168.20.1/24
CWGE24MS2(config-if-vlan-l3)#ipv6 address 1234:ab::ccdd/120
```

Deleting IPv4/IPv6 address: This command is used to delete an IPv4/IPv6 interface route from a interface vlan.

```
CWGE24MS2(config-if-vlan-l3)#no ipv4 address 192.168.20.1/24
CWGE24MS2(config-if-vlan-l3)#no ipv6 address 1234:ab::ccdd/120
```

Adding static IPv4/IPv6 route: This command is used to add an IPv4/IPv6 static route to a interface vlan.

```
CWGE24MS2(config-if-vlan-l3)#ipv4 address 192.168.20.1/24 192.168.20.1
CWGE24MS2(config-if-vlan-l3)#ipv6 address 1234:ab::ccdd/120 1234:ab::ccdd
```

Deleting static IPv4/IPv6 route: This command is used to delete an IPv4/IPv6 static route form an interface vlan.

```
CWGE24MS2(config-if-vlan-l3)#no ipv4 address 192.168.20.1/24 192.168.20.1
CWGE24MS2(config-if-vlan-l3)#no ipv6 address 1234:ab::ccdd/120 1234:ab::ccdd
```

Web configuration

Static Route

Global Settings

IP Forwarding

Disable

IP ARP Proxy

Enable

IPv4 ARP Table

Add

IP:

MAC:

IPv6 ARP Table

Add

IP:

MAC:

Route Settings

VLAN:

IPv4

Add

Interface Route

IP/M:

IP:

IPv6

Add

Interface Route

IP/M:

IP:

Apply

Refresh

Status

Type:

ARP

All

Show

Parameter	Description
Global Settings	
IP Forwarding	Enables / disables the IP forwarding globally.
IP ARP Proxy	Enables / disables the route to act as an ARP proxy globally.
IPv4 ARP Table	Adds a static IPv4 ARP entry in the ARP table. / Deletes a static IPv4 ARP entry from the ARP table.
IP:	The IP address for the entry.
MAC:	The MAC address for the entry.
IPv6 ARP Table	Adds a static IPv6 ARP entry in the ARP table. / Deletes a static IPv6 ARP entry from the ARP table.
IP:	The IP address for the entry.
MAC:	The MAC address for the entry.
Route Settings	
vlan	Specifies an interface vlan.

Parameter	Description
IPv4	Adds an IPv4 Interface Route / Static Route onto the interface vlan. / Deletes an IPv4 Interface Route / Static Route from the interface vlan. Selects the route type, Interface Route or Static Route.
IP/M:	The IP address and the netmask for the entry.
IP:	The static route address for the Static Route type only.
IPv6	Adds an IPv6 Interface Route / Static Route onto the interface vlan. / Deletes an IPv6 Interface Route / Static Route from the interface vlan. Selects the route type, Interface Route or Static Route.
IP/M:	The IP address and the netmask for the entry.
IP:	The static route address for the Static Route type only.
Status	Shows the ARP table / Host table / Route configurations.

STP

STP/RSTP

Introduction

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

- » IEEE 802.1D Spanning Tree Protocol
- » IEEE 802.1w Rapid Spanning Tree Protocol

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database.

In STP, the port states are Blocking, Listening, Learning, Forwarding.

In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this document, "STP" refers to both STP and RSTP.

STP Terminology

- » The root bridge is the base of the spanning tree.
- » Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 27 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

Forward Time (Forward Delay):

This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.

Max Age:

This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

Hello Time:

This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

PathCost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge, the slower the media, the higher the cost.

How STP Works?

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed. Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

802.1D STP

The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. It is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation. In the OSI model for computer networking, STP falls under the OSI layer-2. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for

manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

The Spanning Tree Protocol (STP) is defined in the IEEE Standard 802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the tree, leaving a single active path between any two network nodes.

STP switch port states

- » Blocking - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.
- » Listening - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state.
- » Learning - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)
- » Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
- » Disabled - Not strictly part of STP, a network administrator can manually disable a port

802.1w RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

RSTP bridge port roles:

- » Root - A forwarding port that is the best port from Nonroot-bridge to Rootbridge
- » Designated - A forwarding port for every LAN segment
- » Alternate - An alternate path to the root bridge. This path is different than using the root port.
- » Backup - A backup/redundant path to a segment where another bridge port already connects.
- » Disabled - Not strictly part of STP, a network administrator can manually disable a port

Edge Port:

They are attached to a LAN that has no other bridges attached. These edge ports transition directly to the forwarding state. RSTP still continues to monitor the port for BPDUs in case a bridge is connected. RSTP can also be configured to automatically detect edge ports. As soon as the bridge detects a BPDU coming to an edge port, the port becomes a non-edge port.

Forward Delay:

The range is from 4 to 30 seconds. This is the maximum time (in seconds) the root device will wait

before changing states (i.e., listening to learning to forwarding).

Transmission Limit:

This is used to configure the minimum interval between the transmissions of consecutive RSTP BPDUs. This function can only be enabled in RSTP mode. The range is from 1 to 10 seconds.

Hello Time:

Set the time at which the root switch transmits a configuration message. The range is from 1 to 10 seconds.

Bridge priority:

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will become the root device.

Port Priority:

Set the port priority in the switch. Low numeric value indicates a high priority. A port with lower priority is more likely to be blocked by STP if a network loop is detected. The valid value is from 0 to 240.

Path Cost:

The valid value is from 1 to 200000000. Higher cost paths are more likely to be blocked by STP if a network loop is detected.

BPDU Guard

This is a per port setting. If the port is enabled in BPDU guard and receive any BPDUs, the port will be set to disable to avoid the error environments. User must enable the port by manual.

BPDU Filter

It is a feature to filter sending or receiving BPDUs on a switch port. If the port receives any BPDUs, the BPDUs will be dropped.

Notice:

If both of the BPDUs filter and BPDUs guard are enabled, the BPDUs filter has the high priority.

Root Guard

The Root Guard feature forces an interface to become a designated port to prevent surrounding switches from becoming a root switch. In other words, Root Guard provides a way to enforce the root bridge placement in the network. The Root Guard feature prevents a Designated Port from becoming a Root Port. If a port on which the Root Guard feature receives a superior BPDUs, it moves the port into a root-inconsistent state (effectively equal to a listening state), thus maintaining the current Root Bridge status. The port can be moved to forwarding state if no superior BPDUs received by this port for three hello times.

Default Settings

STP/RSTP	: disabled.
STP/RSTP mode	: RSTP.
Forward Time	: 15 seconds.
Hello Time	: 2 seconds.
Maximum Age	: 20 seconds.
System Priority	: 32768.
Transmission Limit	: 3 seconds.
Per port STP state	: enabled.
Per port Priority	: 128.
Per port Edge port	: disabled.
Per port BPDU filter	: disabled.
Per port BPDU guard	: disabled.
Per port BPDU Root guard	: disabled.
Per port Path Cost	: depend on port link speed.

Example: Bandwidth -> STP Port Cost Value

10 Mbps	->	100
100 Mbps	->	19
1 Gbps	->	4
10 Gbps	->	2

CLI Configuration

Node	Command	Description
enable	show spanning-tree active	This command displays the spanning tree information for only active port(s)
enable	show spanning-tree blockedports	This command displays the spanning tree information for only blocked port(s)
enable	show spanning-tree port detail PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree statistics PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree summary	This command displays the summary of port states and configurations
enable	clear spanning-tree counters	This command clears spanning-tree statistics for all ports.
enable	clear spanning-tree counters PORT_ID	This command clears spanning-tree statistics for a specific port.
configure	spanning-tree (disable enable)	This command disables / enables the spanning tree function for the system.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	This command configures the bridge times (forward-delay,max-age,hello-time).

Node	Command	Description
configure	no spanning-tree algorithm-timer	This command configures the default values for forward-time & max-age & hello-time.
configure	spanning-tree forward-time <4-30>	This command configures the bridge forward delay time (sec).
configure	no spanning-tree forward-time	This command configures the default values for forward-time.
configure	spanning-tree hello-time <1-10>	This command configures the bridge hello time(sec).
configure	no spanning-tree hello-time	This command configures the default values for hello-time.
configure	spanning-tree max-age <6-40>	This command configures the bridge message max-age time(sec).
configure	no spanning-tree max-age	This command configures the default values for max-age time.
configure	spanning-tree mode (rstp stp)	This command configures the spanning mode.
configure	spanning-tree pathcost method (short long)	This command configures the pathcost method.
configure	spanning-tree priority <0-61440>	This command configures the priority for the system.
configure	no spanning-tree priority	This command configures the default values for the system priority.
interface	spanning-tree (disable enable)	This command configures enables/disables the STP function for the specific port.
interface	spanning-tree bpduguard (disable enable)	This command configures enables/disables the bpduguard function for the specific port.
interface	spanning-tree rootguard (disable enable)	This command configures enables/disables the BPDUGuard function for the specific port.
interface	spanning-tree edge-port (disable enable)	This command enables/disables the edge port setting for the specific port.
interface	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-2000000000.
interface	no spanning-tree cost	This command configures the path cost to default for the specific port.
interface	spanning-tree port-priority <0-240>	This command configures the port priority for the specific port. Default: 128.

Node	Command	Description
interface	no spanning-tree port-priority	This command configures the port priority to default for the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	spanning-tree (disable enable)	This command configures enables/disables the STP function for the specific port.
if-range	spanning-tree bpdupfilter (disable enable)	This command configures enables/disables the bpdupfilter function for the specific port.
if-range	spanning-tree bpduguard (disable enable)	This command configures enables/disables the bpduguard function for the specific port.
if-range	spanning-tree rootguard (disable enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
if-range	spanning-tree edge-port (disable enable)	This command enables/disables the edge port setting for the specific port.
if-range	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-2000000000.
if-range	no spanning-tree cost	This command configures the path cost to default for the specific port.
if-range	spanning-tree port-priority <0-240>	This command configures the port priority for the specific port. Default: 128.
if-range	no spanning-tree port-priority	This command configures the port priority to default for the specific port.

Web Configuration

General Settings

Spanning Tree Protocol		
General Settings	Port Parameters	STP Status
Spanning Tree Protocol Settings		
State	Disable ▾	
Mode	RSTP ▾	
Bridge Parameters		
Forward Delay	15 (Range:4-30)	Relationships: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$ $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Max Age	20 (Range:6-40)	
Hello Time	2 (Range:1-10)	
Priority	32768 (Range:0-61440)	
Pathcost Method	Short ▾	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>		

Parameter	Description
-----------	-------------

State	Select Enabled to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
-------	--

Mode	Select to use either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
------	---

Forward Time	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.
--------------	---

Max Age	<p>This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals.</p> <p>Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.</p>
---------	---

Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
------------	--

Parameter	Description
Priority	<p>Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.</p> <p>Enter a value from 0~61440.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge.</p> <p>Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.</p>
Pathcost	<p>Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.</p>

Port Parameters

Spanning Tree Protocol

General Settings

Port Parameters

STP Status

Port Parameters Settings

Port	Active	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
From: 1 To: 1	Enable	250	128	Disable	Disable	Disable	Disable

Apply

Refresh

Port Status

Port	Active	Role	Status	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
1	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
2	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
3	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
4	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
5	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
6	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
7	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
8	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
9	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
10	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
11	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
12	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
13	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
14	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
15	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
16	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
17	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
18	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
19	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
20	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
21	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
22	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
23	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
24	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled

Parameter	Description
Port	Selects a port that you want to configure.
Active	Enables/Disables the spanning tree function for the specific port.
Path Cost	Configures the path cost for the specific port.
Priority	Configures the priority for the specific port.

Parameter	Description
Edge Port	Configures the port type for the specific port. Edge or Non-Edge.
BPDU Filter	Enables/Disables the BPDU filter function for the specific port.
BPDU Guard	Enables/Disables the BPDU guard function for the specific port.
ROOT Guard	Enables/Disables the BPDU root guard function for the specific port.
Port Status	
Active	The state of the STP function.
Role	The port role. Should be one of the Alternated / Designated / Root / Backup / None.
Status	The port's status. Should be one of the Discarding / Blocking / Listening / Learning / Forwarding / Disabled.
Path Cost	The port's path cost.
Priority	The port's priority.
Edge Port	The state of the edge function.
BPDU Filter	The state of the BPDU filter function.
BPDU Guard	The state of the BPDU guard function.
ROOT Guard	The state of the BPDU Root guard function.

STP Status

Spanning Tree Protocol

General Settings

Port Parameters

STP Status

Current Root Status

MAC Address	Priority	Max Age	Hello Time	Forward Delay
00:1f:6c:c5:a9:de	32768	20	2	15

Current Bridge Status

MAC Address	Priority	Max Age	Hello Time	Forward Delay	Path Cost	Root Port
00:22:3b:0b:80:30	32768	20	2	15	19	24

Refresh

Parameter	Description
Current Root Status	
MAC address	This is the MAC address of the root bridge.
Priority	Root refers to the base of the spanning tree (the root bridge). This field displays the root bridge's priority. This Switch may also be the root bridge.
MAX Age	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Hello Time	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Forward Delay	This is the time (in seconds) the root switch will wait before changing states.
Current Bridge Status	
MAC address	This is the MAC address of the current bridge.
Priority	<p>Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.</p> <p>Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.</p>
MAX Age	<p>This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals.</p> <p>Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network.</p>

Parameter	Description
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch.
Forward Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.
Root Cost	This is the number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.

MSTP

Introduction

MSTP (IEEE 802.1S Multiple STP), which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs.

Multiple Spanning-Tree Regions:

For switches to participate in multiple spanning-tree (MST) instances, you must consistently configure the switches with the same MST configuration information. A collection of interconnected switches that have the same MST configuration comprises an MST region. The MST configuration determines to which MST region each switch belongs. The configuration includes the name of the region, the revision number, and the MST instance-to-VLAN assignment map. You configure the switch for a region by using the spanning-tree mst configuration global configuration command, after which the switch enters the MST configuration mode. From this mode, you can map VLANs to an MST instance by using the instance MST configuration command, specify the region name by using the name MST configuration command, and set the revision number by using the revision MST configuration command.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can support up to 16 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

Boundary Ports

A boundary port is a port that connects an MST region to a single spanning-tree region running RSTP, or to a single spanning-tree region running 802.1D, or to another MST region with a different MST configuration. A boundary port also connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

At the boundary, the roles of the MST ports do not matter, and their state is forced to be the same as the IST port state (MST ports at the boundary are in the forwarding state only when the IST port is forwarding). An IST port at the boundary can have any port role except a backup port role.

On a shared boundary link, the MST ports wait in the blocking state for the forward-delay time to expire before transitioning to the learning state. The MST ports wait another forward-delay time before transitioning to the forwarding state.

If the boundary port is on a point-to-point link and it is the IST root port, the MST ports transition to the forwarding state as soon as the IST port transitions to the forwarding state.

If the IST port is a designated port on a point-to-point link and if the IST port transitions to the forwarding state because of an agreement received from its peer port, the MST ports also immediately transition to the forwarding state.

If a boundary port transitions to the forwarding state in an IST instance, it is forwarding in all MST instances, and a topology change is triggered. If a boundary port with the IST root or designated port role receives a topology change notice external to the MST cloud, the MSTP switch triggers a topology change in the IST instance and in all the MST instances active on that port.

Interoperability with 802.1D STP:

A switch running MSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MSTP BPDU (version 3) associated with a different region, or an RSTP BPDU (version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Also, a switch might continue to assign a boundary role to a port when the switch to which this switch is connected has joined the region. To restart the protocol migration process (force the renegotiation with neighboring switches), you can use the clear spanning-tree detected-protocols privileged EXEC command.

If all the legacy switches on the link are RSTP switches, they can process MSTP BPDUs as if they are RSTP BPDUs. Therefore, MSTP switches send either a version 0 configuration and TCN BPDUs or version 3 MSTP BPDUs on a boundary port. A boundary port connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

CLI Configurations

Node	Command	Description
enable	show spanning-tree mst configuration	This command displays the MSTP configurations.
enable	show spanning-tree mst instance	This command displays all of the instance configurations of the MSTP.
enable	show spanning-tree mst instance <0-63>	This command displays specific instance configurations of the MSTP.
enable	show spanning-tree mst instance <0-63> interface IFNAME	This command displays specific instance configurations on an interface of the MSTP.
enable	show spanning-tree mst interface IFNAME	This command displays the configurations on an interface of the MSTP.
enable	show spanning-tree mst root	This command displays the root bridge configurations.
configure	spanning-tree (disable enable)	This command enables / disables the spanning tree.
configure	spanning-tree mode mst	This command configures the mode of the spanning tree. (one of the three modes STP/RSTP/MSTP.)
configure	spanning-tree mst forward-time	This command configures the forward time for the MSTP.
configure	no spanning-tree mst forward-time	This command resets the forward time for the MSTP. The default forward delay time is 15 seconds.
configure	spanning-tree mst hello-time	This command configures the hello time for the MSTP.
configure	no spanning-tree mst hello-time	This command resets the hello time for the MSTP. The default hello time is 2 seconds.
configure	spanning-tree mst max-age	This command configures the maximum age time for the MSTP.
configure	no spanning-tree mst max-age	This command resets the maximum age time for the MSTP. The default maximum age time is 20 seconds.
configure	spanning-tree mst max-hops	This command configures the maximum hop count.
configure	no spanning-tree mst max-hops	This command resets the maximum hop count. The default maximum hop count is 20.
configure	spanning-tree mst instance STRING priority <0-61440>	This command resets the maximum hop count. The default maximum hop count is 20.
configure	no spanning-tree mst instance STRING priority	This command resets the priority for the specific instance.

Node	Command	Description
interface	spanning-tree mst instance STRING cost <1-200000000>	This command configures a cost on the specific port for the MSTP.
interface	no spanning-tree mst instance STRING cost	This command resets the cost on the specific port for the MSTP.
interface	spanning-tree mst instance STRING port- priority <0-240>	This command configures a priority on the specific port for the MSTP.
interface	no spanning-tree mst instance STRING port- priority	This command resets the priority on the specific port for the MSTP.
configure	spanning-tree mst configuration	This command enters the MSTP configure node.
configure	no spanning-tree mst configuration	This command resets all of configurations for the MSTP.
mst	apply	This command applies configurations to current instant.
mst	instance	This command configures the instance and vlan map.
mst	name	This command configures a region name for the MSTP.
mst	no name	This command reset the region name for the MSTP.
mst	revision	This command configures the revision for the MSTP.
mst	no revision	This command resets the revision for the MSTP.
mst	show (current pending)	This command shows the MSTP configures. Current - the working configurations. Pending - the not applied configurations.

Specifying the MST Region Configuration and Enabling MSTP

For two or more switches to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same name. A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can support up to 16 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

```
CWGE24MS2(config)#spanning-tree mst configuration
```

```
CWGE24MS2(config-mst)#name MSTP
```

```
CWGE24MS2(config-mst)#revision 1
```

```
CWGE24MS2(config-mst)#instance 1 vlan 1-10
```


Web Configurations

General Settings

Spanning Tree Protocol

General Settings
Bridge Parameters
Port Parameters
STP Status

Spanning Tree Protocol Settings

State Enable ▾

Mode MSTP ▾

Configuration Parameters

Region Name

Revision (Range:0-65535)

Instance - ▾

VLAN Add ▾

Instance	VLAN	Action
0	1-4094	

Parameter	Description
State	Select Enabled to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP).
Mode	Selects the Spanning Tree running mode. STP - Spanning Tree Protocol. RSTP - Rapid Spanning Tree Protocol. MSTP - Multiple Spanning Tree Protocol.

Configuration Parameters

Region Name	Configures the region name for the Switch.
Revision	Configures the revision for the Switch.
Instance	Selects an instance which you want to configure.
VLAN	Select one or more vlans which will join the instance. Note: the vlan will be removed from instance 0 automatically.

Instance and vlan map table

Instance	The instance.
VLAN	The vlan in the instance.
Action	Click Delete button to delete this instance.

Bridge Parameters

Spanning Tree Protocol

General Settings
Bridge Parameters
Port Parameters
STP Status

Bridge Parameters Settings

Forward Time

15

(Range:4-30)

Hello Time

2

(Range:1-10)

Max Age

20

(Range:6-40)

Max Hops

20

(Range:1-40)

Instance

0 ▼

Priority

32768

(Range:0-61440)

Apply
Refresh

Bridge Parameters Status

Forward Time	15	Hello Time	2
Max Age	20	Max Hops	20
Instance		Priority	
0		32768	

Parameter	Description
Forward Time	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Max Hops	
Instance	Selects an instance which you want to configure.
Priority	Configures the priority for the instance. Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Enter a value from 0~61440. The lower the numeric value you assign, the higher the priority for this bridge. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.

Port Parameters

Spanning Tree Protocol

General Settings

Bridge Parameters

Port Parameters

STP Status

Port Parameters Settings

Instance

0

Port

From: 1 To: 1

Path Cost

200000000

Priority

128

Port

From: 1 To: 1

Active

Enable

Edge Port

Disable

BPDU Filter

Disable

BPDU Guard

Disable

ROOT Guard

Disable

Apply

Refresh

Port Status

Port	Active	Role	Status	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
1	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
2	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
3	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
4	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
5	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
6	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
7	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
8	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
9	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
10	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
11	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
12	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
13	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
14	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
15	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
16	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
17	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
18	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
19	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
20	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
21	Enabled	Designated	Forwarding	20000	128	Disabled	Disabled	Disabled	Disabled
22	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
23	Enabled	Disabled	Blocking	200000000	128	Disabled	Disabled	Disabled	Disabled
24	Enabled	Root	Forwarding	200000	128	Disabled	Disabled	Disabled	Disabled

Parameter	Description
Instance	Selects a instance that you want to configure.
Port	Selects a port or a range of ports that you want to configure.
Path Cost	Configures the path cost for the specific port.
Priority	Configures the priority for the specific port.
Port	Selects a port or a range of ports that you want to configure.
Active	Enables/Disables the spanning tree function for the specific port.
Edge Port	Configures the port type for the specific port. Edge or Non-Edge.
BPDU Filter	Enables/Disables the BPDU filter function for the specific port.
BPDU Guard	Enables/Disables the BPDU guard function for the specific port.
ROOT Guard	Enables/Disables the BPDU root guard function for the specific port.
Port Status	
Active	The state of the STP function.
Role	The port role. Should be one of the Alternated / Designated / Root / Backup / None.
Status	The port's status. Should be one of the Discarding / Blocking / Listening / Learning / Forwarding / Disabled.
Path Cost	The port's path cost.
Priority	The port's priority.
Edge Port	The state of the edge function.
BPDU Filter	The state of the BPDU filters function.
BPDU Guard	The state of the BPDU guards function.
ROOT Guard	The state of the BPDU Root guard function.

STP Status

Spanning Tree Protocol

General Settings

Port Parameters

STP Status

Current Root Status

MAC Address	Priority	Max Age	Hello Time	Forward Delay
00:1f:6c:c5:a9:de	32768	20	2	15

Current Bridge Status

MAC Address	Priority	Max Age	Hello Time	Forward Delay	Path Cost	Root Port
00:22:3b:0b:80:30	32768	20	2	15	19	24

Refresh

Parameter	Description
Current Root Status	
Instance	The Instance ID.
MAC address	This is the MAC address of the root bridge.
Priority	Root refers to the base of the spanning tree (the root bridge). This field displays the root bridge's priority. This Switch may also be the root bridge.
Root Cost	This is the path cost to the root bridge.
MAX Age	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Hello Time	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Forward Delay	This is the time (in seconds) the root switch will wait before changing states.
Root Port	This is the port to the root bridge.
Current Bridge Status	
Instance	This is the MAC address of the current bridge.
MAC address	This is the MAC address of the bridge.
Priority	This is the priority of the Switch.

UDLD

Introduction

The UDLD (UniDirectional Link Detection) protocol is used to detect and/or disable unidirectional connections before they create dangerous situations such as Spanning Tree loops or other protocol malfunctions.

The UDLD protocol was implemented to help correct certain assumptions made by other protocols and in particular to help the STP to function properly so as to avoid the creation of dangerous Layer 2 loops.

UDLD is meant to be a Layer 2 detection protocol that works on top of existing Layer 1 detection mechanisms defined by the IEEE standards.

Network systems typically check for miss wiring or unidirectional problems at the physical layer. The physical layer defines the actual physical components such as connectors and cables. So, physical layer only checks for open lines or port malfunctions and would not detect a miss wired systems.

But, UDLD performs mutual neighbor identification; in addition, it performs neighbor acknowledgement on top of the Logical Link Control (LLC) layer and thus is able to discover logical one-way miscommunication between neighbors even when either one of PHY layer mechanisms has deemed the transmission medium bidirectional.

Notice:

The port blocked by UDLD can be recovered automatically or you can execute the CLI command, "no shutdown", in interface node. You can configure the recovery interval with CLI command, "errdisable recovery interval VALUE".

CLI Configurations

Node	Command	Description
enable	show uddl status	This command displays the UDLD global settings.
enable	show uddl interface	This command displays the ports' settings.
enable	show uddl neighbor	This command displays the port's neighbor information.
configure	uddl enable	This command enables the global UDLD state.
configure	no uddl enable	This command disables the global UDLD state.
configure	uddl message interval-time VALUE	This command configures the interval time of sending.
configure	uddl message interval-time reset	This command configures the interval time to default value. (7 seconds)
configure	errdisable recovery interval VALUE	This command configures the recovery interval time if ports is blocked by UDLD. (Default is 0, no recovery time, valid value is 30 ~ 86400 seconds.)
interface	no shutdown	This command enables the specific ports.
interface	uddl port enable	This command enables the uddl state for the specific port.
interface	no uddl port enable	This command disables the uddl state for the specific port.
interface	uddl port aggressive	This command configures the uddl mode to aggressive mode for the specific port.
interface	no uddl port aggressive	This command configures the uddl mode to normal mode for the specific port.

Default Configurations

1. Message interval time is set to 7
2. Port configuration of UDLD is enabled on all ports.

Case 1: To configure UDLD on port 1 only then disable uddl port configuration on all interfaces except port 1 and enable global UDLD.

```
CWGE24MS2#configure terminal
CWGE24MS2(config)# interface <id> //All interfaces one by one except port 1
CWGE24MS2(config-if)# no uddl port enable
CWGE24MS2(config-if)# exit
CWGE24MS2(config)# uddl enable
```

Case 2: To configure UDLD on all ports

```
CWGE24MS2#configure terminal
CWGE24MS2(config)# uddl enable
```

Case 3: To disable UDLD on all ports

```
CWGE24MS2#configure terminal
CWGE24MS2(config)# no uddl enable
```


Case 4: To disable UDLD on a specific port; example port 1

```
CWGE24MS2#configure terminal
CWGE24MS2(config)# interface <port_1>
CWGE24MS2(config-if)# no udld port enable
```

Case 5: To enable aggressive mode on a specific port; example port 1

```
CWGE24MS2#configure terminal
CWGE24MS2(config)# interface <port_1>
CWGE24MS2(config-if)# udld port aggressive
```

Case 6: To disable aggressive mode on a specific port; example port 1

```
CWGE24MS2#configure terminal
CWGE24MS2(config)# interface <port_1>
CWGE24MS2(config-if)# no udld port aggressive
```

Web Configurations

Port Settings:

UDLD

Port Settings

Neighbors

UDLD Port Settings

State

Disable

Message Time Interval

7

seconds

Recovery Interval

0

seconds

Port

State

Aggressive

From:

1

To:

1

Enable

Disable

Apply

Refresh

UDLD Port Status

Port	State	Aggressive	Detection State	Operational State
1	Enable	Disabled	Unknown	UDLD Down
2	Enable	Disabled	Unknown	UDLD Down
3	Enable	Disabled	Unknown	UDLD Down
4	Enable	Disabled	Unknown	UDLD Down
5	Enable	Disabled	Unknown	UDLD Down
6	Enable	Disabled	Unknown	UDLD Down
7	Enable	Disabled	Unknown	UDLD Down
8	Enable	Disabled	Unknown	UDLD Down
9	Enable	Disabled	Unknown	UDLD Down
10	Enable	Disabled	Unknown	UDLD Down
11	Enable	Disabled	Unknown	UDLD Down
12	Enable	Disabled	Unknown	UDLD Down
13	Enable	Disabled	Unknown	UDLD Down
14	Enable	Disabled	Unknown	UDLD Down
15	Enable	Disabled	Unknown	UDLD Down
16	Enable	Disabled	Unknown	UDLD Down
17	Enable	Disabled	Unknown	UDLD Down
18	Enable	Disabled	Unknown	UDLD Down
19	Enable	Disabled	Unknown	UDLD Down
20	Enable	Disabled	Unknown	UDLD Down
21	Enable	Disabled	Unknown	UDLD Down
22	Enable	Disabled	Unknown	UDLD Down
23	Enable	Disabled	Unknown	UDLD Down
24	Enable	Disabled	Unknown	UDLD Down

Parameter	Description
State	Selects Enable or Disable to enable or disable the global UDLD state.
Message Interval Time	Configures the message interval time.
Port	Selects a port or a range of ports to be configured.
State	Selects the port state for above selection.
Aggressive	Selects enable to let the port working in Aggressive mode. Selects disable to let the port working in Normal mode.
UDLD Port Status	
State	Display the current UDLD port state for the specific port.
Aggressive	Display the current Aggressive state for the specific port.
Bidirectional State	Display the current detection state.
Operational State	Display the current operational state.

Neighbors:

UDLD

Port Settings

Neighbors

UDLD Neighbor Information

Select Port: All ▼

Apply

Port	Device Name	Device ID	Port ID	Neighbor State
21	CWGE24MS2	00223B0B8024	Gi1/0/21	Active

Refresh

Parameter	Description
Select Port	Selects Enable or Disable to enable or disable the global UDLD state.
Port	The local port number.
Device Name	The device name of the neighbor Switch.
Device ID	The device ID of the neighbor Switch.
Port ID	The port number of the neighbor Switch connected to this port.
Neighbor State	The operational state of the neighbor Switch.

Security

IP Source Guard

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. 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.

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.

The IP Source Guard features include below functions:

- » DHCP Snooping.
- » DHCP Binding table.
- » ARP Inspection.
- » Blacklist Filter. (arp-inspection mac-filter table)

DHCP Snooping

Introduction

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, which is also referred to as a DHCP snooping binding table.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You can use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

The DHCP snooping binding database contains the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN

in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- » A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from the untrusted port.
- » A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match any of the current bindings.

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).

The source MAC address and source IP address in the packet do not match any of the current bindings.

The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.

The rate at which DHCP packets arrive is too high.

DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again.

Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

- » Enable DHCP snooping on the Switch.
- » Enable DHCP snooping on each VLAN.
- » Configure trusted and untrusted ports.
- » Configure static bindings.

Note:

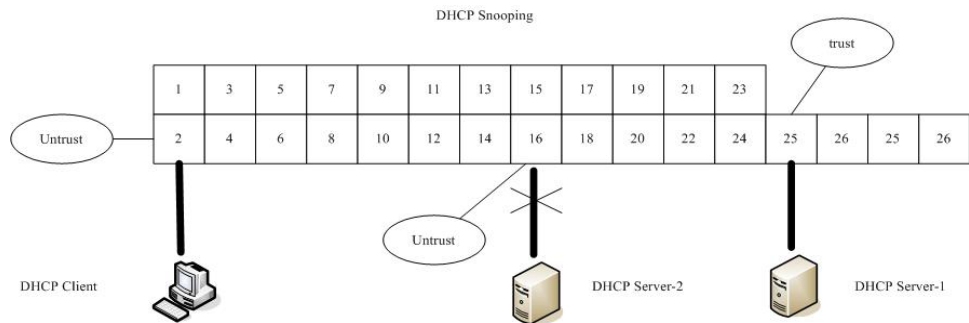
The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

If the port link down, the entries learned by this port in the DHCP snooping binding table will be deleted.

You must enable the global DHCP snooping and DHCP Snooping for vlan first.

The main purposes of the DHCP Snooping are:

- » Create and maintain binding table for ARP Inspection function.
- » Filter the DHCP server’s packets that the DHCP server connects to an untrusted port.



The DHCP server connected to an un-trusted port will be filtered.

Default Settings

The DHCP snooping on the Switch is disabled.

The DHCP snooping is enabled in VLAN(s): None.

Port	Trusted	Maximum Host Count	Port	Trusted	Maximum Host Count
----	-----	-----	----	-----	-----
1	no	32	2	no	32
3	no	32	4	no	32
5	no	32	6	no	32
.

Notices

There are a global state and per VLAN states.

When the global state is disabled, the DHCP Snooping on the Switch is disabled even per VLAN states are enabled.

When the global state is enabled, user must enable per VLAN states to enable the DHCP Snooping on the specific VLAN.

VLAN 1 : port 1-10.

DHCP Client-1 : connect to port 3.

DHCP Server : connect to port 1.

Procedures:

Default environments:

- » DHCP Client-1: ipconfig /release
- » DHCP Client-1: ipconfig /renew
- => DHCP Client-1 can get an IP address.

Enable the global DHCP Snooping.

- » CWGE24MS2(config)#dhcp-snooping
- » DHCP Client-1: ipconfig /release
- » DHCP Client-1: ipconfig /renew
- => DHCP Client-1 can get an IP address.

Enable the global DHCP Snooping and VLAN 1 DHCP Snooping.

- » CWGE24MS2(config)#dhcp-snooping
- » CWGE24MS2(config)#dhcp-snooping vlan 1
- » DHCP Client-1: ipconfig /release
- » DHCP Client-1: ipconfig /renew
- => DHCP Client-1 cannot get an IP address.
- ; Because the DHCP server connects to a un-trust port.

Enable the global DHCP Snooping and VLAN 1 DHCP Snooping.

- » CWGE24MS2(config)#dhcp-snooping
 - » CWGE24MS2(config)#dhcp-snooping vlan 1
 - » CWGE24MS2(config)#interface gi1/0/1
 - » CWGE24MS2(config-if)#dhcp-snooping trust
 - » DHCP Client-1: ipconfig /release
 - » DHCP Client-1: ipconfig /renew
- => DHCP Client-1 can get an IP address.

If you configure a static host entry in the DHCP snooping binding table, and then you want to change the host to DHCP client, the host will not get a new IP from DHCP server, and then you must delete the static host entry first.

CLI Configuration

Node	Command	Description
enable	show dhcp-snooping	This command displays the current DHCP snooping configurations.
configure	dhcp-snooping (disable enable)	This command disables/enables the DHCP snooping on the switch.
configure	dhcp-snooping vlan VLANID	This command enables the DHCP snooping function on a VLAN or range of VLANs.
configure	no dhcp-snooping vlan VLANID	This command disables the DHCP snooping function on a VLAN or range of VLANs.
configure	dhcp-snooping server IPADDR	This command configures a valid DHCP server.
interface	dhcp-snooping host	This command configures the maximum host count for the specific port.
interface	no dhcp-snooping host	This command configures the maximum host count to default for the specific port.
interface	dhcp-snooping trust	This command configures the trust port for the specific port.
interface	no dhcp-snooping trust	This command configures the un-trust port for the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.
if-range	dhcp-snooping host	This command configures the maximum host count for the specific ports.
if-range	no dhcp-snooping host	This command configures the maximum host count to default for the specific ports.
if-range	dhcp-snooping trust	This command configures the trust port for the specific ports.
if-range	no dhcp-snooping trust	This command configures the un-trust port for the specific ports.

Example:

```
CWGE24MS2#configure terminal
CWGE24MS2(config)#dhcp-snooping enable
CWGE24MS2(config)#dhcp-snooping vlan 1
CWGE24MS2(config)#interface 1/0/1
CWGE24MS2(config-if)#dhcp-snooping trust
```

Web Configuration

DHCP Snooping

DHCP Snooping

DHCP Snooping

Port Settings

Server Screening

DHCP Snooping Settings

State

Disable

VLAN State

Add

Apply

Refresh

DHCP Snooping Status

DHCP Snooping State

Disabled

Enabled on VLAN

None

Parameter	Description
State	Select Enable to use DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLANs and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports. Select Disable to not use DHCP snooping.
VLAN State	Select Add and enter the VLAN IDs you want the Switch to enable DHCP snooping on. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-). Select Delete and enter the VLAN IDs you no longer want the Switch to use DHCP snooping on.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
DHCP Snooping Status	
DHCP Snooping State	This field displays the current status of the DHCP snooping feature, Enabled or Disabled.
Enabled on VLAN	This field displays the VLAN IDs that have DHCP snooping enabled on them. This will display None if no VLANs have been set.

Port Settings

DHCP Snooping

DHCP Snooping
Port Settings
Server Screening

Port Settings

Port

Trust

Maximum Host Count

From: To:

(Range: 1-32)

Port Status

Port	Trusted	Maximum Host Count	Port	Trusted	Maximum Host Count
1	NO	32	2	NO	32
3	NO	32	4	NO	32
5	NO	32	6	NO	32
7	NO	32	8	NO	32
9	NO	32	10	NO	32
11	NO	32	12	NO	32
13	NO	32	14	NO	32
15	NO	32	16	NO	32
17	NO	32	18	NO	32
19	NO	32	20	NO	32
21	NO	32	22	NO	32
23	NO	32	24	NO	32

Parameter	Description
Port	Select a port number to modify its maximum host count.
Trust	Configures the specific port if it is a trust port.
Maximum Host Count	Enter the maximum number of hosts (1-32) that are permitted to simultaneously connect to a port.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

DHCP Server Screening

Introduction

The Switch supports DHCP Server Screening, a feature that denies access to rogue DHCP servers. That is, when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients, the valid DHCP server's packets will be passed to the client.

If you want to enable this feature, you must enable the DHCP Snooping function first. The Switch allows users to configure up to three valid DHCP servers.

If no DHCP servers are configured, it means all DHCP server are valid.

CLI Configuration

Node	Command	Description
enable	show dhcp-snooping server	This command displays the valid DHCP server IP.
configure	dhcp-snooping server IPADDR	This command configures a valid DHCP server's IP.
configure	no dhcp-snooping server IPADDR	This command removes a valid DHCP server's IP.

Web Configuration

DHCP Snooping

DHCP Snooping

Port Settings

Server Screening

Server Screening Setting

IP Address

ApplyRefresh

Server Screening List

No.	IP Address	Action
1	192.168.201.1	Delete

Parameter	Description
IP Address	This field configures the valid DHCP server’s IP address.
Apply	Click Apply to configure the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Server Screening List	
No.	This field displays the index number of the DHCP server entry. Click the number to modify the entry.
IP Address	This field displays the IP address of the DHCP server.
Action	Click Delete to remove a configured DHCP server.

Binding Table

Introduction

The DHCP Snooping binding table records the host information learned by DHCP snooping function (dynamic) or set by user (static). The ARP inspection will use this table to forward or drop the ARP packets. If the ARP packets sent by invalid host, they will be dropped. If the Lease time is expired, the entry will be removed from the table.

Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one.

CLI Configuration

Node	Command	Description
enable	show dhcp-snooping binding	This command displays the current DHCP snooping binding table.
configure	dhcp-snooping binding mac MAC_ADDR ip IP_ADDR vlan VLANID port PORT_NO	This command configures a static host into the DHCP snooping binding table.
configure	no dhcp-snooping binding mac MACADDR	This command removes a static host from the DHCP snooping binding table.

Example:

```
CWGE24MS2#configure terminal
CWGE24MS2(config)#dhcp-snooping binding mac 00:11:22:33:44:55 ip 1.1.1.1 vlan 1 port 2
CWGE24MS2(config)#no dhcp-snooping binding mac 00:11:22:33:44:55
CWGE24MS2#show dhcp-snooping binding
```

Web Configuration

Static Entry Settings

DHCP Snooping Binding Table							
Static Entry Settings		Binding Table					
Static Entry Settings							
MAC Address	<input type="text"/>						
IP Address	<input type="text"/>						
VLAN ID	<input type="text"/>						
Port	1 <input type="button" value="v"/>						
				<input type="button" value="Apply"/> <input type="button" value="Refresh"/>			
Static Binding Table							
No.	MAC Address	IP Address	Lease(hour)	VLAN	Port	Type	Action

Parameter	Description
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN ID	Enter the source VLAN ID in the binding.
Port	Specify the port in the binding.
Static Binding Table	
No.	This field displays a sequential number for each binding. Click it to update an existing entry.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease (Hour)	This field displays how long the binding is valid.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding.
Type	This field displays how the Switch learned the binding. Static: This binding was learned from information provided manually by an administrator. Dynamic: This binding was learned by snooping DHCP packets.
Action	Click Delete to remove the specified entry.

Binding Table

Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the dynamic bindings by snooping DHCP packets and from information provided manually in the Static Entry Settings screen.

DHCP Snooping Binding Table

Static Entry Settings

Binding Table

DHCP Snooping Binding Table

Show Type

All

Show

*You can select the dynamic entry and convert it to static status.

*All

☐

MAC Address

IP Address

Lease(hour)

VLAN

Port

Type

Apply

Refresh

Parameter	Description
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Type	This field displays how the Switch learned the binding. Static: This binding was learned from information provided manually by an administrator. Dynamic: This binding was learned by snooping DHCP packets.

ARP Inspection

ARP Inspection

Introduction

Dynamic ARP inspection is a security feature which validates ARP packet in a network by performing IP to MAC address binding inspection. Those will be stored in a trusted database (the DHCP snooping database) before forwarding. Dynamic ARP intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection 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 it updates the local ARP cache or before it forwards the packet to the appropriate destination.

Trusted and untrusted port

- » This setting is independent of the trusted and untrusted setting of the DHCP Snooping.
- » The Switch does not discard ARP packets on trusted ports for any reasons.
- » The Switch discards ARP packets on un-trusted ports if the sender's information in the ARP packets does not match any of the current bindings.
- » Normally, the trusted ports are the uplink port and the untrusted ports are connected to subscribers.

Configurations:

Users can enable/disable the ARP Inspection on the Switch. Users also can enable/disable the ARP Inspection on a specific VLAN. If the ARP Inspection on the Switch is disabled, the ARP Inspection is disabled on all VLANs even some of the VLAN ARP Inspection are enabled.

Default Settings

The ARP Inspection on the Switch is disabled.

The age time for the MAC filter is 5 minutes.

ARP Inspection is enabled in VLAN(s): None.

Port	Trusted	Port	Trusted
----	-----	----	-----
1	no	2	no
3	no	4	no
5	no	6	no
7	no	8	no
9	no	10	no
11	no	12	no
13	no	14	no
15	no	16	no
17	no	18	no
19	no	20	no
21	no	22	no
23	no	24	no

Notices

There are a global state and per VLAN states.

When the global state is disabled, the ARP Inspection on the Switch is disabled even per VLAN states are enabled.

When the global state is enabled, user must enable per VLAN states to enable the ARP Inspection on the specific VLAN.

CLI Configuration

Node	Command	Description
enable	show arp-inspection	This command displays the current ARP Inspection configurations.
configure	arp-inspection (disable enable)	This command disables/enables the ARP Inspection function on the switch.
configure	arp-inspection vlan VLANID	This command enables the ARP Inspection function on a VLAN or range of VLANs.
configure	no arp-inspection vlan VLANID	This command disables the ARP Inspection function on a VLAN or range of VLANs.
interface	arp-inspection trust	This command configures the trust port for the specific port.
interface	no arp-inspection trust	This command configures the un-trust port for the specific port.

Example:

```
CWGE24MS2#configure terminal
CWGE24MS2(config)#arp-inspection enable
CWGE24MS2(config)#arp-inspection vlan 1
CWGE24MS2(config)#interface 1/0/1
CWGE24MS2(config-if)#arp-inspection trust
```

Web Configuration

ARP Inspection

ARP Inspection
Filter Table

ARP Inspection Settings

State Disable ▾

VLAN State Add ▾

Trusted Ports

☐ Select All
☐ Deselect All

☐ 1 ☐ 3 ☐ 5 ☐ 7 ☐ 9 ☐ 11 ☐ 13 ☐ 15 ☐ 17 ☐ 19 ☐ 21 ☐ 23

☐ 2 ☐ 4 ☐ 6 ☐ 8 ☐ 10 ☐ 12 ☐ 14 ☐ 16 ☐ 18 ☐ 20 ☐ 22 ☐ 24

Apply
Refresh

ARP Inspection Status

ARP Inspection State	Disabled
Enabled on VLAN	None
Trusted Ports	None

Parameter	Description
State	Use this to Enable or Disable ARP inspection on the Switch.
VLAN State	Enter the VLAN IDs you want the Switch to enable ARP Inspection for. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-).
Trusted Ports	<p>Select the ports which are trusted and deselect the ports which are untrusted. The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations:</p> <ul style="list-style-type: none"> • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Select All	Click this to set all ports to trusted.
Deselect All	Click this to set all ports to untrusted.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
ARP Inspection Status	
ARP Inspection State	This field displays the current status of the ARP Inspection feature, Enabled or Disabled.
Enabled on VLAN	This field displays the VLAN IDs that have ARP Inspection enabled on them. This will display None if no VLANs have been set.
Trusted Ports	This field displays the ports which are trusted. This will display None if no ports are trusted.

Filter Table

Introduction

Dynamic ARP inspections validates the packet by performing IP to MAC address binding inspection stored in a trusted database (the DHCP snooping database) before forwarding the packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. The switch also periodically deletes entries if the age-time for the entry is expired.

If the ARP Inspection is enabled and the system detects invalid hosts, the system will create a filtered entry in the MAC address table.

When Port link down and ARP Inspection was disabled, Switch will remove the MAC-filter entries learned by this port.

When Port link down and ARP Inspection was enabled, Switch will remove the MAC-filter entries learned by this port.

The maximum entry of the MAC address filter table is 256.

When MAC address filter table of ARP Inspection is full, the Switch receives unauthorized ARP packet, and it automatically creates a SYSLOG and drop this ARP packet. The SYSLOG event happens on the first time.

Default Settings

The mac-filter age time : 5 minutes. (0 – No age)

The maximum mac-filter entries : 256.

CLI Configuration

Node	Command	Description
enable	show arp-inspection mac-filter	This command displays the current ARP Inspection filtered MAC.
configure	arp-inspection mac-filter age VALUE	This command configures the age time for the ARP inspection MAC filter entry.
configure	clear arp-inspection mac-filter	This command clears all of entries in the filter table.
configure	no arp-inspection mac-filter mac MACADDR vlan VLANID	This command removes an entry from the ARP inspection MAC filter table.

Web Configuration

ARP Inspection

ARP Inspection
Filter Table

Filter Age Time Settings

Filter Age Time

5

minutes (Range: 1-10080)

Filter Table

No.	MAC Address	VLAN	Port	Expiry(min)	Action
Total : 0 record(s)					

Parameter	Description
Filter Age Time	This setting has no effect on existing MAC address filters. Enter how long (1-10080 minutes) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Filter Table	
No.	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VLAN	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (min)	This field displays how long (in minutes) the MAC address filter remains in the Switch.
Action	Click Delete to remove the record manually.
Total	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.

ACL

Introduction

L2 Access control list (ACL) is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

L2 ACL function allows user to configure a few rules to reject packets from the specific ingress ports or all ports. These rules will check the packets' source MAC address and destination MAC address. If packets match these rules, the system will do the actions "deny". "deny" means rejecting these packets.

The Action Resolution engine collects the information (action and metering results) from the hit entries: if more than one rule matches, the actions and meter/counters are taken from the policy associated with the matched rule with highest priority.

L2 ACL Support:

1. Filter a specific source MAC address.

Command: source mac host MACADDR

2. Filter a specific destination MAC address.

Command: destination mac host MACADDR

3. Filter a range of source MAC address.

Command: source mac MACADDR MACADDR

The second MACADDR is a mask, for example: ffff.ffff.0000

4. Filter a range of destination MAC address.

Command: destination mac MACADDR MACADDR

The second MACADDR is a mask, for example: ffff.ffff.0000

L3 ACL Support:

1. Filter a specific source IP address.

Command: source ip host IPADDR

2. Filter a specific destination IP address.

Command: destination ip host IPADDR

3. Filter a range of source IP address.

Command: source ip IPADDR IPADDR

The second IPADDR is a mask, for example: 255.255.0.0

4. Filter a range of destination IP address.

Command: destination ip IPADDR IPADDR

L4 ACL Support:

1. Filter a UDP/TCP source port.

2. Filter a UDP/TCP destination port.

Default Settings

Maximum profile : 64.

Maximum profile name length : 16.

Notices

The ACL name should be the combination of the digit or the alphabet.

CLI Configuration

Node	Command	Description
enable	show access-list	This command displays all of the access control profiles.
configure	access-list STRING ip-type (ipv4 ipv6)	This command creates a new access control profile. Where the STRING is the profile name. And you can specify the type, ipv4 or ipv6.
configure	no access-list STRING	This command deletes an access control profile.
acl	show	This command displays the current access control profile.
acl	action (disable drop permit)	This command activates this profile. disable - disable the profile. drop - If packets match the profile, the packets will be dropped. permit - If packets match the profile, the packets will be forwarded.
acl	action dscp remarking <0-63>	This command activates this profile and specify that it is for DSCP remark. And configures the new DSCP value which will be override to all packets matched this profile.

Node	Command	Description
acl	action 802.1p remarking <0-7>	This command activates this profile and specifies that it is for 802.1p remark. And configures the new 802.1p value which will be override to all packets matched this profile.
acl	802.1p VALUE	This command configures the 802.1p value for the profile.
acl	dscp VALUE	This command configures the DSCP value for the profile.
acl	destination mac host MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile.
acl	no destination mac	This command removes the destination MAC from the profile.
acl	ethertype STRING	This command configures the ether type for the profile. Where the STRING is a hex-decimal value. e.g.: 08AA.
acl	no ethertype	This command removes the limitation of the ether type from the profile.
acl	source mac host MACADDR	This command configures the source MAC and mask for the profile.
acl	source mac MACADDR MACADDR	This command configures the source MAC and mask for the profile.
acl	no source mac	This command removes the source MAC and mask from the profile.
acl	source ip host IPADDR	This command configures the source IP address for the profile.
acl	source ip IPADDR IPMASK	This command configures the source IP address and mask for the profile.
acl	no source ip	This command removes the source IP address from the profile.
acl	destination ip host IPADDR	This command configures a specific destination IP address for the profile.
acl	destination ip IPADDR IPMASK	This command configures the destination IP address and mask for the profile.
acl	no destination ip	This command removes the destination IP address from the profile.
acl	l4-source-port IPADDR	This command configures UDP/TCP source port for the profile.
acl	no l4-source-port IPADDR	This command removes the UDP/TCP source port from the profile.
acl	L4-destination-port PORT	This command configures the UDP/TCP destination port for the profile.
acl	no l4-destination-port	This command removes the UDP/TCP destination port from the profile.
acl	vlan VLANID	This command configures the VLAN for the profile.
acl	no vlan	This command removes the limitation of the VLAN from the profile.
acl	source interface PORT_ID	This command configures the source interface for the profile.
acl	no source interface PORT_ID	This command removes the source interface from the profile.

Where the MAC mask allows users to filter a range of MAC in the packets' source MAC or destination MAC.

For example:

```
source mac 00:01:02:03:04:05 ff:ff:ff:ff:00
```

=> The command will filter source MAC range from 00:01:02:03:00:00 to 00:01:02:03:ff:ff

Where the IPMASK mask allows users to filter a range of IP in the packets' source IP or destination IP.

For example:

```
source ip 172.20.1.1 255.255.0.0
```

=> The command will filter source IP range from 172.20.0.0 to 172.20.255.255

Example:

```
CWGE24MS2#configure terminal
CWGE24MS2(config)#access-list 111
CWGE24MS2(config-acl)#vlan 2
CWGE24MS2(config-acl)#source interface 1
CWGE24MS2(config-acl)#show
Profile Name: 111
Activate: disabled
VLAN: 2
Source Interface: 1
Destination MAC Address: any
Source MAC Address: any
Ethernet Type: any
Source IP Address: any
Destination IP Address: any
Source Application: any
Destination Application: any
```

Note: Any: Don't care.

Web Configuration

Access Control List

Access Control List Settings

IP Type

IPv4

Profile Name

Ethernet Type

Any

Source MAC

Any

Destination MAC

Any

DSCP

Any

0

Source IP

Any

Destination IP

Any

IP Protocol

Any

Source Application

Any

Destination Application

Any

Source Interface

Any

--

Action

Disable

VLAN

Any

Mask of Source MAC

Mask of Destination MAC

802.1p

Any

0

Mask of Source IP

Mask of Destination IP

Apply

Refresh

Access Control List Status

IP Type	IPv4		
Profile Name	acl	Action	Disabled
Ethernet Type	Any	VLAN	Any
Source MAC	Any	Mask of Source MAC	None
Destination MAC	Any	Mask of Destination MAC	None
DSCP	Any	802.1p	Any
IP Protocol	Any		
Source IP	Any	Mask of Source IP	None
Destination IP	Any	Mask of Destination IP	None
Source Application	Any	Destination Application	Any
Source Interface	1		
<div>Delete</div>			

Parameter	Description
IP Type	Selects IPv4 / IPv6 type for the profile.
Profile Name	The access control profile name.
Action	Selects Disables / Drop / Permits / DSCP action for the profile.
Ethernet Type	Configures the ethernet type of the packets that you want to filter.
VLAN	Configures the VLAN of the packets that you want to filter.
Source MAC	Configures the source MAC of the packets that you want to filter.
Mask of Source MAC	Configures the bitmap mask of the source MAC of the packets that you want to filter. If the Source MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Source MAC field.
Destination MAC	Configures the destination MAC of the packets that you want to filter.
Mask of Destination MAC	Configures the bitmap mask of the destination MAC of the packets that you want to filter. If the Destination MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Destination MAC field.
DSCP	Configure the DSCP for the profile.
802.1p	Configures the 802.1p for the profile.
Source IP	Configures the source IP of the packets that you want to filter.
Mask of Source IP	Configures the bitmap mask of the source IP of the packets that you want to filter. If the Source IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Source IP field.
Destination IP	Configures the destination IP of the packets that you want to filter.
Mask of Destination IP	Configures the bitmap mask of the destination IP of the packets that you want to filter. If the Destination IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Destination IP field.
IP Protocol	Configures the IP protocol type. The setting will be used for Source Application and Destination Application. TCP:0x06. UDP:0x11.
Source Application	Configures the source UDP/TCP ports of the packets that you want to filter.
Destination Application	Configures the destination UDP/TCP ports of the packets that you want to filter.
Source Interface(s)	Configures one or a range of the source interfaces of the packets that you want to filter.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

802.1x

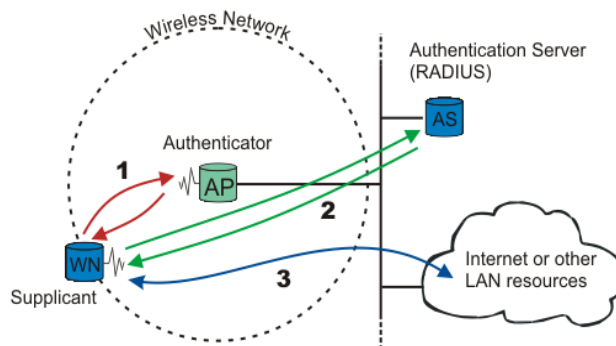
Introduction

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (“port” meaning a single point of attachment to the LAN infrastructure). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. It is used for most wireless 802.11 access points and is based on the Extensible Authentication Protocol (EAP).

802.1X provides port-based authentication, which involves communications between a supplicant, authenticator, and authentication server. The supplicant is often software on a client device, such as a laptop, the authenticator is a wired Ethernet switch or wireless access point, and an authentication server is generally a RADIUS database. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant’s identity is authorized. An analogy to this is providing a valid passport at an airport before being allowed to pass through security to the terminal. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the credentials are valid (in the authentication server database), the supplicant (client device) is allowed to access resources located on the protected side of the network.

Upon detection of the new client (supplicant), the port on the switch (authenticator) is enabled and set to the “unauthorized” state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is blocked at the network layer (Layer 3). The authenticator sends out the EAP-Request identity to the supplicant, the supplicant responds with the EAP-response packet that the authenticator forwards to the authenticating server. If the authenticating server accepts the request, the authenticator sets the port to the “authorized” mode and normal traffic is allowed. When the supplicant logs off, it sends an EAP-logoff message to the authenticator. The authenticator then sets the port to the “unauthorized” state, once again blocking all non-EAP traffic.

The following figure illustrates how a client connecting to an IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password.



When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate users without interacting with a network authentication server. However, there is a limit on the number of users you may authenticate in this way.

Guest VLAN

The Guest VLAN in IEEE 802.1x port authentication on the switch to provide limited services to clients, such as downloading the IEEE 802.1x client. These clients might be upgrading their system for IEEE 802.1x authentication.

When you enable a guest VLAN on an IEEE 802.1x port, the switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

Port Parameters

» Admin Control Direction:

both - drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication.

in - drop only incoming packets on the port when a user has not passed 802.1x port authentication.

» Re-authentication:

Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.

» Reauth-period:

Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.

» Port Control Mode:

auto : Users can access network after authenticating.

force-authorized : Users can access network without authentication.

force-unauthorized : Users cannot access network.

» Quiet Period:

Specify a period of the time the client has to wait before the next re-authentication attempt. This will prevent the Switch from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.

» Server Timeout:

The server-timeout value is used for timing out the Authentication Server.

» Supp-Timeout:

The supp-timeout value is the initialization value used for timing out a Supplicant.

» Max-req Time:

Specify the amount of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.

Default Settings

The default global 802.1x state is disabled.
 The default 802.1x Authentication Method is local.
 The default port 802.1x state is disabled for all ports.
 The default port Admin Control Direction is both for all ports.
 The default port Re-authentication is disabled for all ports.
 The default port Control Mode is auto for all ports.
 The default port Guest VLAN is 0 for all ports. (Guest VLAN is disabled).
 The default port Max-req Time is 2 times for all ports.
 The default port Reauth period is 3600 seconds for all ports.
 The default port Quiet period is 60 seconds for all ports.
 The default port Supp timeout is 30 seconds for all ports.
 The default port Server timeout is 30 seconds for all ports.

CLI Configuration

Node	Command	Description
enable	show dot1x	This command displays the current 802.1x configurations.
enable	show dot1x username	This command displays the current user accounts for the local authentication.
enable	show dot1x accounting-record	This command displays the local accounting records.
configure	dot1x authentication (disable enable)	This command enables/disables the 802.1x authentication on the switch.
configure	dot1x authentic-method (local radius)	This command configures the authentic method of 802.1x.
configure	no dot1x authentic-method	This command configures the authentic method of 802.1x to default.
configure	dot1x radius primary-server-ip <IP> port PORTID	This command configures the primary radius server.
configure	dot1x radius primary-server-ip <IP> port PORTID key KEY	This command configures the primary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID	This command configures the secondary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID key KEY	This command configures the secondary radius server.
configure	no dot1x radius secondary-server-ip	This command removes the secondary radius server.

Node	Command	Description
configure	dot1x username <STRING> passwd <STRING>	This command configures the user account for local authentication.
configure	no dot1x username <STRING>	This command deletes the user account for local authentication.
configure	dot1x accounting (disable enable)	This command enables/disables the dot1x local accounting records.
configure	dot1x guest-vlan VLANID	This command configures the guest vlan.
configure	no dot1x guest-vlan	This command removes the guest vlan.
interface	dot1x admin-control- direction (both in)	This command configures the control direction for blocking packets.
interface	dot1x default	This command sets the port configuration to default settings.
interface	dot1x max-req <1-10>	This command sets the max-req times of a port. (1~10).
interface	dot1x port-control (auto force-authorized force-unauthorized)	This command configures the port control mode on the port.
interface	dot1x authentication (disable enable)	This command enables/disables the 802.1x on the port.
interface	dot1x reauthentication (disable enable)	This command enables/disables re-authentication on the port.
interface	dot1x timeout quiet- period	This command configures the quiet-period value on the port.
interface	dot1x timeout server- timeout	This command configures the server-timeout value on the port.
interface	dot1x timeout reauth- period	This command configures the re-auth-period value on the port.
interface	dot1x timeout supp- timeout	This command configures the supp-timeout value on the port.
interface	dot1x guest-vlan (disable enable)	This command configures the 802.1x state on the port.

Web Configuration

Global Settings

802.1x				
Global Settings		Port Settings		
Global Settings				
State	Disable ▾			
Authentication Method	Local ▾			
Guest VLAN	0			
Primary Radius Server	IPv4 ▾	IP : <input type="text"/>	UDP Port : <input type="text"/>	Shared Key : <input type="text"/>
Secondary Radius Server	IPv4 ▾	IP : <input type="text"/>	UDP Port : <input type="text"/>	Shared Key : <input type="text"/>
Local Authentic User	None ▾	User Name : <input type="text"/> Password : <input type="password"/>		
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>				
Global Status				
State	Disabled			
Authentication Method	Local			
Guest VLAN	0			
Primary Radius Server	IP : -	UDP Port : -	Shared Key : -	
Secondary Radius Server	IP : -	UDP Port : -	Shared Key : -	
Local Authentication User	admin,			

Parameter	Description
State	Select Enable to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Authentication Method	Select whether to use Local or RADIUS as the authentication method. The Local method of authentication uses the "guest" and "user" user groups of the user account database on the Switch itself to authenticate. However, only a certain number of accounts can exist at one time. RADIUS is a security protocol used to authenticate users by means of an external server instead of an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS allows you to validate an unlimited number of users from a central location.
Guest VLAN	Configure the guest vlan.

Parameter	Description
Primary Radius Server	When RADIUS is selected as the 802.1x authentication method, the Primary Radius Server will be used for all authentication attempts.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is 1812.
Share Key	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Second Radius Server	This is the backup server used only when the Primary Radius Server is down.
Global Status	
State	This field displays if 802.1x authentication is Enabled or Disabled.
Authentication Method	This field displays if the authentication method is Local or RADIUS.
Guest VLAN	The field displays the guest vlan.
Primary Radius Server	This field displays the IP address, UDP port and shared key for the Primary Radius Server. This will be blank if nothing has been set.
Secondary Radius Server	This is the backup server used only when the Primary Radius Server is down.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Port Settings

802.1x

Global Settings
Port Settings

Port

From: To:

802.1x State

Admin Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times
<input type="text" value="Both"/>	<input type="text" value="Disable"/>	<input type="text" value="Auto"/>	<input type="text" value="Disable"/>	<input type="text" value="2"/>

Reauth-period	Quiet-period	Supp-timeout	Server-timeout	Reset to Default
<input type="text" value="3600"/>	<input type="text" value="20"/>	<input type="text" value="30"/>	<input type="text" value="16"/>	<input type="checkbox"/>

Note : Please don't set "enable" on all ports at the same time.

Port Status

Port	802.1x State	Admin Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times	Reauth-period	Quiet-period	Supp-timeout	Server-timeout
1	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
2	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
3	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
4	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
5	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
6	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
7	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
8	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
9	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
10	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
11	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
12	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
13	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
14	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
15	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
16	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
17	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
18	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
19	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
20	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
21	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
22	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
23	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
24	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16

Parameter	Description
Port	Select a port number to configure.
802.1x State	Select Enable to permit 802.1x authentication on the port. You must first enable 802.1x authentication on the Switch before configuring it on each port.
Admin Control Direction	Select Both to drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. Select In to drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Re-authentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	Select Auto to require authentication on the port. Select Force Authorized to always force this port to be authorized. Select Force Unauthorized to always force this port to be unauthorized. No packets can pass through this port.
Guest VLAN	Select Disable to disable Guest VLAN on the port. Select Enable to enable Guest VLAN on the port.
Max-req Time	Specify the amount of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.
Reauth period	Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.
Quiet period	Specify a period of the time the client has to wait before the next re-authentication attempt. This will prevent the Switch from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.
Supp timeout	Specify how long the Switch will wait before communicating with the server. The acceptable range for this field is 0 to 65535 seconds.
Server timeout	Specify how long the Switch to time out the Authentication Server. The acceptable range for this field is 0 to 65535 seconds.
Reset to Default	Select this and click Apply to reset the custom 802.1x port authentication settings back to default.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port Status	
Port	This field displays the port number.
802.1x State	This field displays if 802.1x authentication is Enabled or Disabled on the port.

Parameter	Description
Admin Control Direction	This field displays the Admin Control Direction. Both will drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. In will drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Re-authentication	This field displays if the subscriber must periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	This field displays the port control mode. Auto requires authentication on the port. Force Authorized forces the port to be authorized. Force Unauthorized forces the port to be unauthorized. No packets can Pass through the port.
Guest VLAN	This field displays the Guest VLAN setting for hosts that have not passed authentication.
Max-req Time	This field displays the amount of times the Switch will try to connect to the authentication server before determining the server is down.
Reauth period	This field displays how often a client has to re-enter his or her username and password to stay connected to the port.
Quiet period	This field displays the period of the time the client has to wait before the next re-authentication attempt.
Supp timeout	This field displays how long the Switch will wait before communicating with the server.
Server timeout	This field displays how long the Switch will wait before communicating with the client.

Port Security

Introduction

The Switch will learn the MAC address of the device directly connected to a particular port and allow traffic through. We will ask the question: "How do we control who and how many can connect to a switch port?" This is where port security can assist us. The Switch allow us to control which devices can connect to a switch port or how many of them can connect to it (such as when a hub or another switch is connected to the port).

Let's say we have only one switch port left free and we need to connect five hosts to it. What can we do? Connect a hub or switch to the free port! Connecting a switch or a hub to a port has implications. It means that the network will have more traffic. If a switch or a hub is connected by a user instead of an administrator, then there are chances that loops will be created. So, it is best that number of hosts allowed to connect is restricted at the switch level. This can be done using the "port-security limit" command. This command configures the maximum number of MAC addresses that can source traffic through a port.

Port security can sets maximum number of MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses are dropped. It can be use MAC table to check it. The static MAC addresses are included for the limit.

Note: If you configure a port of the Switch from disabled to enabled, all of the MAC learned by this port will be clear.

Default Settings

The port security on the Switch is disabled.

The Maximum MAC per port is 5.

The port state of the port security is disabled.

CLI Configuration

Node	Command	Description
enable	show port-security	This command displays the current port security configurations.
configure	port-security (disable enable)	This command enables / disables the global port security function.
interface	port-security (disable enable)	This command enables / disables the port security function on the specific port.
interface	port-security limit VALUE	This command configures the maximum MAC entries on the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	port-security (disable enable)	This command enables / disables the port security function for the specified ports
if-range	port-security limit VALUE	This command configures the maximum MAC entries for the specified ports.

Web Configuration

Port Security

Port Security
Sticky MAC Settings

Port Security Settings

Port Security Disable ▾

Port		State	Sticky State	Maximum MAC	
From:	1 ▾	To:	1 ▾	Disable ▾	Disable ▾
				5	(1~30)

Apply
Refresh

Port Security Status

Port	State	Sticky State	Maximum MAC	Port	State	Sticky State	Maximum MAC
1	Disable	Disable	5	2	Disable	Disable	5
3	Disable	Disable	5	4	Disable	Disable	5
5	Disable	Disable	5	6	Disable	Disable	5
7	Disable	Disable	5	8	Disable	Disable	5
9	Disable	Disable	5	10	Disable	Disable	5
11	Disable	Disable	5	12	Disable	Disable	5
13	Disable	Disable	5	14	Disable	Disable	5
15	Disable	Disable	5	16	Disable	Disable	5
17	Disable	Disable	5	18	Disable	Disable	5
19	Disable	Disable	5	20	Disable	Disable	5
21	Disable	Disable	5	22	Disable	Disable	5
23	Disable	Disable	5	24	Disable	Disable	5

Parameter	Description
-----------	-------------

Port Security Settings	
------------------------	--

Port Security	Select Enable/Disable to permit Port Security on the Switch.
---------------	--

Port	Select a port number to configure.
------	------------------------------------

State	Select Enable/Disable to permit Port Security on the port.
-------	--

Maximum MAC	The maximum number of MAC addresses allowed per interface. The acceptable range is 1 to 30.
-------------	---

Port Security Status	
----------------------	--

Port	This field displays a port number.
------	------------------------------------

State	This field displays if Port Security is Enabled or Disabled
-------	---

Maximum MAC	This field displays the maximum number of MAC addresses
-------------	---

TACACS+

Introduction

The purpose of this enhancement is to support TACACS+ on the Switch platforms. Terminal Access Controller Access Control System Plus is a security application that provides centralized validation of users attempting to gain access to a router, network access server etc. In order for the TACACS+ feature on the VOLKTEK products to work it would need a TACACS+ server, which would typically be a daemon running on a centralized UNIX or windows NT authentication, authorization and accounting facilities for managing network access points from a single management service.

Product Features

The TACACS+ implementation will support the following features:

- » The implementation will conform to version 1.78 of the TACACS+ draft RFC.
- » Authentication, Authorization and Accounting can be run as well as disabled independently of each other.
- » In case TACACS+ authentication fails on account of the server being unreachable the box can be made to default to a local authentication policy.
- » TACACS+ packet body encryption will be supported.
- » Single Tacacs+ server will be supported.
- » Multiple connect mode will be supported.
- » Syslog messages will be supported.

Functional Description

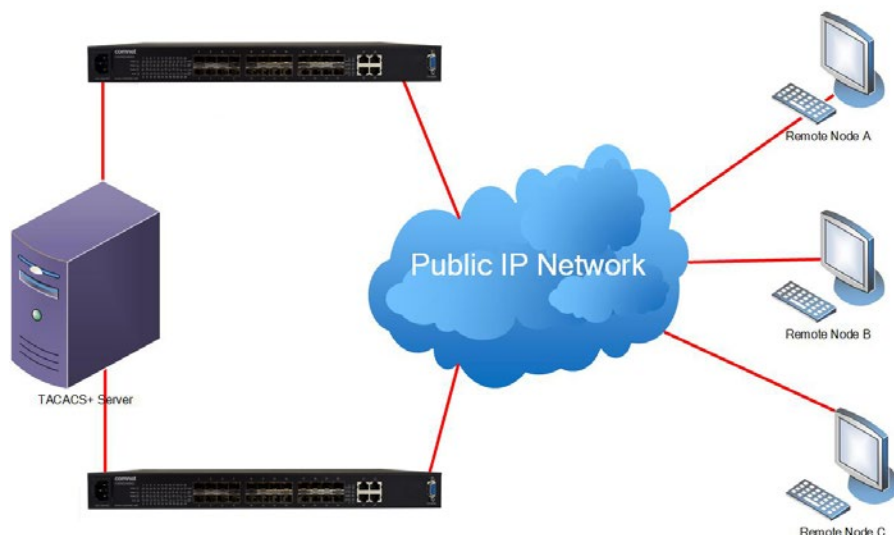
The Tacacs+ implementation will provide the following services:

- » Authentication:
Complete control of authentication through login and password dialog, challenge and response, messaging support etc.
- » Authorization:
Control over user capabilities for the duration of the user session, like setting auto commands, enforcing restrictions on what configuration commands a user may execute, session duration etc.
- » Accounting :
Collecting and sending information used for billing, auditing, and reporting to the TACACS+ daemon.

Each of the above mentioned services can be configured and run independent of the others. The TACACS+ implementation will provide authentication and confidentiality between the router and the TACACS+ daemon. It runs on TCP port 49.

Application:

Remote network access is witnessing a major paradigm shift that from terminal access to LAN access. Single users want to connect to the corporate network in the same way that they connect at work i.e. as a LAN user. This places increased emphasis on network access security. As a result of this network managers are concerned with 3 parameters: authentication, authorization and accounting. This is where TACACS+ enters into the picture. A typical deployment using TACACS+ could be as follow:



Notices

- » TACACS+ service must be enabled before configuring the authentication, authorization and accounting parameters, otherwise it will return error as Tacacs+ service is not enabled.
- » Not allowed to disable the Authentication login mode when both enabled login-mode and login local.
- » Not allowed to disable the Authentication enable mode when both enabled enable-mode and enable local.
- » Not allowed to enable the login-mode local when login-mode is in disable.
- » Not allowed to enable the enable-mode local when enable-mode is in disable.
- » For input CLI, user must supply full command or partial command with TAB (command must be completed). The reason is only the command after user HIT the ENTER is only send to TACACSP server for authorization or accounting. So if this command is partial then subsequently authorization or accounting fails.

CLI Configuration

Mode	Command	Description
Enable	show tacacs-plus	To show the Tacacs+ Statistics.
configure	tacacs-plus server-host <ipaddr>	To set the Tacacs+ Server IP address
configure	no tacacs-plus server-host	To reset the Tacacs+ Server ip address as 0.0.0.0
configure	tacacs-plus server-ipv6-host <ipaddr>	To set the Tacacs+ Server IP v6 address
configure	no tacacs-plus server-ipv6-host	To reset the Tacacs+ Server ip address as default (None).
configure	tacacs-plus server-key <key>	To set the Tacacs+ server key
configure	no tacacs-plus server-key	To reset the Tacacs+ server key as default key(NULL means no key)
configure	tacacs-plus enable	To enable the Tacacs+ service
configure	no tacacs-plus enable	To disable the Tacacs+ service
configure	tacacs-plus authentication login-mode enable	To enable the authentication login mode
configure	no tacacs-plus authentication login-mode enable	To disable the authentication login mode
configure	tacacs-plus authentication login-mode local enable	To enable the authentication login local mode
configure	no tacacs-plus authentication login-mode local enable	To disable the authentication login local mode
configure	tacacs-plus authentication enable-mode enable	To enable the authentication in enable mode.
configure	no tacacs-plus authentication enable-mode enable	To disable the authentication in enable mode.
configure	tacacs-plus authentication enable-mode local enable	To enable the authentication enable local mode
configure	no tacacs-plus authentication enable-mode local enable	To disable the authentication enable local mode
configure	tacacs-plus authorization commands enable	To enable the authorization show commands.
configure	no tacacs-plus authorization commands enable	To disable the authorization show commands.
configure	tacacs-plus authorization exec enable	To enable the authorization configuration commands.
configure	no tacacs-plus authorization exec enable	To disable the authorization configuration commands.

Mode	Command	Description
configure	tacacs-plus accounting commands enable	To enable the level 1 commands for accounting.
configure	no tacacs-plus accounting commands enable	To disable the level 1 commands for accounting.
configure	tacacs-plus accounting exec enable	To enable the level 15 commands for accounting.
configure	no tacacs-plus accounting exec enable	To disable the level15 commands for accounting
configure	tacacs-plus line-console enable	To enable TACACSP on the console port.
configure	no tacacs-plus line-console enable	To disable TACACSP on the console port.

Example:

CWGE24MS2#show tacacs-plus

```

Tacacs+ Server Host      :0.0.0.0
Tacacs+ State            :disabled
Tacacs+ line-console mode :disabled
Authentication Login mode :disabled      Local: disabled
Authentication Enable mode :disabled      Local: disabled
Authorization            :Command:disabled Exec : disabled
Accounting               :Command:disabled Exec : disabled
Authentication Sessions  :0
Authorization Sessions   :0
Accounting Sessions      :0
    
```

Web Configuration

TACACS+			
Global Settings			
State	Disable ▾		
Authentication Console mode	Disable ▾		
Authentication Login Mode	Disable ▾	Local: Disable ▾	
Authentication Enable Mode	Disable ▾	Local: Disable ▾	
Authorization	Command: Disable ▾	Exec: Disable ▾	
Accounting	Command: Disable ▾	Exec: Disable ▾	
TACACS Server	IP Version : IPv4 ▾	Server Address: 0.0.0.0	Server Key : <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>			
Global Status			
State	Disabled		
Authentication Console mode	Disabled		
Authentication Login Mode	Disabled	Local: Disabled	
Authentication Enable Mode	Disabled	Local: Disabled	
Authorization	Command: Disabled	Exec: Disabled	
Accounting	Command: Disabled	Exec: Disabled	
TACACS Server	IP Version: IPv4	Server Address : 0.0.0.0	

Parameter	Description
State	Enables / Disables the Tacacs+ service.
Authentication Login Mode	Enables / Disables the authentication in login mode.
Authentication Enable Mode	Enables / Disables the authentication in Enable mode.
Authorization Command	Enables / Disables the authorization with show commands.
Authorization Exec	Enables / Disables the authorization with configuration commands.
Accounting Command	Enables / Disables the level 1 command for the Accounting.
Accounting Exec	Enables / Disables the level 15 command for the Accounting.
TACACS+ Server	
IP Version	Configures the IPv4 or IPv6 address format.
Server Address	Configures the TACACS server's IP.
TACACS Server Server Key	Configures the server key for the TACACS server.

Monitor

Alarm

Introduction

The feature displays if there are any abnormal situation need process immediately.

CLI Configuration

Node	Command	Description
enable	show alarm-info	This command displays alarm information.

Web Configuration

Alarm Information

Alarm Information

Alarm Status	No Alarm.
Alarm Reason(s)	

Refresh

Parameter	Description
Alarm Information	
Alarm Status	This field indicates if there is any alarm events.
Alarm Reason(s)	This field displays all of the detail alarm events.

Hardware Information

Introduction

The feature displays some hardware information to monitor the system to guarantee the network correctly.

- » Displays the board's and CPU's and MAC chip's temperature.
- » Displays the 1.0V and 2.5V and 3.3V input status.

CLI Configuration

Node	Command	Description
enable	show hardware-monitor (C F)	This command displays hardware working information.

Example:

CWGE24MS2#show hardware-monitor C

Temperature(C)	Crent	MAX	MIN	Threshold	Status
BOARD	44.0	44.2	24.0	80.0	Normal
CPU	49.2	49.2	26.5	80.0	Normal
PHY	57.5	57.5	30.0	80.0	Normal

Voltage(V)	Current	MAX	MIN	Threshold	Status
1.0V IN	1.009	1.009	1.009	+/-5%	Normal
1.8V IN	1.768	1.778	1.755	+/-5%	Normal
3.3V IN	3.264	3.264	3.259	+/-5%	Normal

Web Configuration

Hardware Information

Hardware Information

Temperature unit: Celsius(C) Change

Hardware Working Information:

Temperature(C)	Current	MAX	MIN	Threshold	Status
BOARD	26.0	26.0	24.5	80.0	Normal
CPU	32.0	32.2	29.0	80.0	Normal
PHY	29.2	29.5	27.0	80.0	Normal
Voltage(V)	Current	MAX	MIN	Threshold	Status
1.0V IN	1.037	1.037	1.037	+/-5%	Normal
1.8V IN	1.788	1.788	1.788	+/-5%	Normal
3.3V IN	3.280	3.280	3.280	+/-5%	Normal

Power Source Information:

Voltage(V)	Current
12VIN	0.016

Power Source	Power Source 2
--------------	----------------

Refresh

Port Statistics

Introduction

This feature helps users to monitor the ports' statistics, to display the link up ports' traffic utilization only.

CLI Configuration

Node	Command	Description
enable	show port-statistics	This command displays the link up ports' statistics.

Example:

CWGE24MS2#show port-statistics

Port	Packets		Bytes		Errors		Drops	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
----	-----	-----	-----	-----	-----	-----	-----	-----
7	1154	2	108519	1188	0	0	0	0

Web Configuration

Port Statistics								
Port Statistics								
Port	Receive Drops	Transmit Drops	Receive Errors	Transmit Errors	Receive Packets	Transmit Packets	Receive Bytes	Transmit Bytes
21	0	0	0	0	1211	3127	553084	743251
24	0	0	0	0	4629	1702	808507	956924
<input type="button" value="Refresh"/> <input type="button" value="Clear"/>								

Parameter	Description
Port	Select a port or a range of ports to display their statistics.
Rx Packets	The field displays the received packet count.
Tx Packets	The field displays the transmitted packet count.
Rx Bytes	The field displays the received byte count.
Tx Bytes	The field displays the transmitted byte count.
Rx Errors	The field displays the received error count.
Tx Errors	The field displays the transmitted error count.
Rx Drops	The field displays the received drop count.
Tx Drops	The field displays the transmitted drop count.
Refresh	Click this button to refresh the screen quickly.

Port Utilization

Introduction

This feature helps users to monitor the ports' traffic utilization, to display the link up ports' traffic utilization only.

CLI Configuration

Node	Command	Description
enable	show port-utilization	This command displays the link up ports' traffic utilization.

Web Configuration

Port Utilization		
Port Utilization		
Port	Speed	Traffic Utilization (%)
21	1000	0
24	100	0.001
<input type="button" value="Refresh"/>		

Parameter	Description
Port	Select a port or a range of ports to display their RMON statistics.
Speed	The current port speed.
Utilization	The port traffic utilization.
Refresh	Click this button to refresh the screen quickly.

RMON Statistics

Introduction

This feature helps users to monitor or clear the port's RMON statistics.

CLI Configuration

Node	Command	Description
enable	show rmon statistics	This command displays the RMON statistics.
configure	clear rmon statistics [IFNAME]	This command clears one port's or all ports' RMON statistics.

Web Configuration

RMON Statistics			
RMON Statistics			
Port	24	Show	Clear
Port 24 (Active)			
Inbound	Total Octets	867271	
	BroadcastPkts	2044	UnicastPkts 1793
	Non-unicastPkts	3178	MulticastPkts 1134
	FragmentsPkts	0	UndersizePkts 0
	OversizePkts	0	DiscardsPkts 0
	ErrorPkts	0	UnknownProtos 0
	AlignError	0	CRCAlignErrors 0
	Jabbers	0	DropEvents 0
Outbound	Total Octets	1028616	
	BroadcastPkts	1	UnicastPkts 1840
	Non-unicastPkts	219	Collisions 0
	LateCollision	0	SingleCollision 0
	MultipleCollision	0	DiscardsPkts 0
	ErrorPkts	0	
# of packets received with a length of	64 Octets	2259	65to127 Octets 1747
	128to255 Octets	1213	256to511 Octets 934
	512to1023 Octets	296	1024toMax Octets 581

Parameter	Description
Port	Select a port or a range of ports to display their RMON statistics.
Show	Show them.
Clear	Clear the RMON statistics for the port or a range of ports.

SFP Information

Introduction

The SFP information allows user to know the SFP module's information, such as vendor name, connector type, revision, serial number, manufacture date, and to know the DDMI information if the SFP modules have supported the DDMI function.

CLI Configuration

Node	Command	Description
enable	show sfp info port PORT_ID	This command displays the SFP information.
enable	show sfp ddmi port PORT_ID	This command displays the SFP DDMI status.

Web Configuration

SFP Information					
SFP Information					
Port	10 <input type="button" value="Apply"/>				
SFP Information					
Fiber Cable	Link Up				
Connector	LC				
Wavelength(nm)	1310				
Transfer Distance	15km, Single mode				
DDM Supported	YES (Externally Calibrated)				
Vendor Name	COMNET				
Vendor PN	SFP-6				
Vendor rev	1.0				
Vendor SN	160532056				
Date code	160515				
DDMI Information					
	Current	High-Alarm	Low-Alarm	High-Warn	Low-Warn
Temperature(C)	35.332	110.000	-45.000	105.000	-40.000
Voltage(V)	3.331	3.600	2.900	3.500	3.000
Tx Bias(mA)	9.150	90.000	0.000	80.000	0.000
Tx Power(mW)	0.247	0.794	0.063	0.631	0.079
Tx Power(dBm)	-6.079	-0.998	-12.010	-2.004	-11.000
Rx Power(mW)	0.159	3.162	0.001	1.995	0.002
Rx Power(dBm)	-7.982	4.997	-30.000	2.999	-28.495

Parameter	Description
Port	Select a port number to configure.
Apply	Click Apply to display the SFP information.
Fiber Cable	To indicate if the fiber cable is connected.
Connector	Code of optical connector type.
Vendor Name	SFP vendor name.
Vendor PN	Part Number.
Vendor rev	Revision level for part number.
Vendor SN	Serial number (ASCII).
Date Code	Manufacturing date code.

Notice: If the fiber cable is not connected, the Rx Power fields are not available.

Traffic Monitor

Introduction

The function can be enabled / disabled on a specific port or globally be enabled disabled on the Switch.

The function will monitor the broadcast / multicast / broadcast and multicast packets rate. If the packet rate is over the user's specification, the port will be blocked. And if the recovery function is enabled, the port will be enabled after recovery time.

Default Settings

Port	State	Status	Packet Type	Rate(pps)	Packet State	Recovery Time(min)
1	Disabled	Normal	Bcast	1000	Enabled	1
2	Disabled	Normal	Bcast	1000	Enabled	1
3	Disabled	Normal	Bcast	1000	Enabled	1
4	Disabled	Normal	Bcast	1000	Enabled	1
5	Disabled	Normal	Bcast	1000	Enabled	1
6	Disabled	Normal	Bcast	1000	Enabled	1
.

CLI Configuration

Node	Command	Description
enable	show traffic-monitor	This command displays the traffic monitor configurations and current status.
configure	traffic-monitor (disable enable)	This command enables / disables the traffic monitor on the Switch.
interface	traffic-monitor (disable enable)	This command enables / disables the traffic monitor on the port.
interface	traffic-monitor rate RATE_LIMIT type (bcast mcast bcast+mcast)	This command configures the packet rate and packet type for the traffic monitor on the port. bcast - Broadcast packet. mcast - Multicast packet.
interface	traffic-monitor recovery (disable enable)	This command enables / disables the recovery function for the traffic monitor on the port.
interface	traffic-monitor recovery time VALUE	This command configures the recovery time for the traffic monitor on the port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	traffic-monitor (disable enable)	This command enables / disables the traffic monitor on the port.
if-range	traffic-monitor rate RATE_LIMIT type (bcast mcast bcast+mcast)	This command configures the packet rate and packet type for the traffic monitor on the port. bcast - Broadcast packet. mcast - Multicast packet.
if-range	traffic-monitor recovery (disable enable)	This command enables / disables the recovery function for the traffic monitor on the port.
if-range	traffic-monitor recovery time VALUE	This command configures the recovery time for the traffic monitor on the port.

Web Configuration

Traffic Monitor

Traffic Monitor Settings

State Disable ▾

Port	State	Action	Packet Type	Packet Rate (pps)	Recovery State	Recovery Time (min)
From: 1 ▾ To: 1 ▾	Disable ▾	None ▾	Broadcast ▾	100	Enable ▾	1

Apply
Refresh

Traffic Monitor Status

Port	State	Status	Packet Type	Packet Rate(pps)	Recovery State	Recovery Time (min)
1	Disabled	Normal	Broadcast	100	Enabled	1
2	Disabled	Normal	Broadcast	100	Enabled	1
3	Disabled	Normal	Broadcast	100	Enabled	1
4	Disabled	Normal	Broadcast	100	Enabled	1
5	Disabled	Normal	Broadcast	100	Enabled	1
6	Disabled	Normal	Broadcast	100	Enabled	1
7	Disabled	Normal	Broadcast	100	Enabled	1
8	Disabled	Normal	Broadcast	100	Enabled	1
9	Disabled	Normal	Broadcast	100	Enabled	1
10	Disabled	Normal	Broadcast	100	Enabled	1
11	Disabled	Normal	Broadcast	100	Enabled	1
12	Disabled	Normal	Broadcast	100	Enabled	1
13	Disabled	Normal	Broadcast	100	Enabled	1
14	Disabled	Normal	Broadcast	100	Enabled	1
15	Disabled	Normal	Broadcast	100	Enabled	1
16	Disabled	Normal	Broadcast	100	Enabled	1
17	Disabled	Normal	Broadcast	100	Enabled	1
18	Disabled	Normal	Broadcast	100	Enabled	1
19	Disabled	Normal	Broadcast	100	Enabled	1
20	Disabled	Normal	Broadcast	100	Enabled	1
21	Disabled	Normal	Broadcast	100	Enabled	1
22	Disabled	Normal	Broadcast	100	Enabled	1
23	Disabled	Normal	Broadcast	100	Enabled	1
24	Disabled	Normal	Broadcast	100	Enabled	1

Parameter	Description
State	Globally enables / disables the traffic monitor function.
Port	The port range which you want to configure.
State	Enables / disables the traffic monitor function on these ports.
Action	Unblock these ports.
Packet Type	Specify the packet type which you want to monitor.
Packet Rate	Specify the packet rate which you want to monitor.
Recover State	Enables / disables the recovery function for the traffic monitor function on these ports.
Recovery Time	Configures the recovery time for the traffic monitor function on these ports.(Range: 1 - 60 minutes)

Management

SNMP

SNMP

Introduction

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

Support below MIBs:

- » RFC 1157 A Simple Network Management Protocol
- » RFC 1213 MIB-II
- » RFC 1493 Bridge MIB
- » RFC 1643 Ethernet Interface MIB
- » RFC 1757 RMON Group 1,2,3,9

SNMP community act like passwords and are used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default SNMP community is "public" for both SNMP v1 and SNMP v2c before SNMP v3 is enabled. Once SNMP v3 is enabled, the communities of SNMP v1 and v2c have to be unique and cannot be shared.

Network ID of Trusted Host:

The IP address is a combination of the Network ID and the Host ID.

Network ID = (Host IP & Mask).

User need only input the network ID and leave the host ID to 0. If user has input the host ID, such as 192.168.1.102, the system will reset the host ID, such as 192.168.1.0

Note: Allow user to configure the community string and rights only.

User configures the Community String and the Rights and the Network ID of Trusted Host=0.0.0.0, Subnet Mask=0.0.0.0. It means that all hosts with the community string can access the Switch.

Default Settings

SNMP	: disabled.
System Location	: CWGE24MS2. (Maximum length 64 characters)
System Contact	: None. (Maximum length 64 characters)
System Name	: None. (Maximum length 64characters)
Trap Receiver	: None.
Community Name	: None.
The maximum entry for community	: 3.
The maximum entry for trap receiver	: 5.

CLI Configuration

Node	Command	Description
enable	show snmp	This command displays the SNMP configurations.
configure	snmp community STRING (ro rw) trusted-host IPADDR/ right, network ID and mask in IPv4 format. MASK	This command configures the SNMP community name, access right, network ID and mask in IPv4 format.
configure	no snmp community STRING (ro rw) trusted-host IPADDR/ network ID and mask in IPv4 format. MASK	This command deletes the SNMP community name, access right, network ID and mask in IPv4 format.
configure	snmp community STRING (ro rw) trusted-ipv6-host IPADDR/MASK	This command configures the SNMP community name, access right, network ID and mask in IPv6 format.
configure	no snmp community STRING (ro rw) trusted-ipv6-host IPADDR/MASK	This command deletes the SNMP community name, access right, network ID and mask in IPv6 format.
configure	snmp (disable enable)	This command disables/enables the SNMP on the switch.
configure	snmp system-contact STRING	This command configures contact information for the system.
configure	snmp system-location STRING	This command configures the location information for the system.
configure	snmp system-name STRING	This command configures a name for the system. (The System Name is same as the host name)
configure	snmp trap-receiver IPADDR VERSION COMMUNITY	This command configures the trap receiver's configurations, including the IP address, version (v1 or v2c) and community.
configure	no snmp trap-receiver IPADDR VERSION COMMUNITY	This command deletes the trap receiver's configurations, including the IP address, version (v1 or v2c) and community.
configure	snmp trap-ipv6-receiver IPADDR VERSION COMMUNITY	This command configures the trap receiver's configurations, including the IP address in IPv6 format, version (v1 or v2c) and community.
configure	no snmp trap-ipv6-receiver IPADDR VERSION COMMUNITY	This command deletes the trap receiver's configurations, including the IP address in IPv6 format, version (v1 or v2c) and community.

Example:

```

CWGE24MS2#configure terminal
CWGE24MS2(config)#snmp enable
CWGE24MS2(config)#snmp community public rw trusted-host 192.168.200.106/24
CWGE24MS2(config)#no snmp community public rw trusted-host 192.168.200.106/24
CWGE24MS2(config)#snmp community qqz rw trusted-ipv6-host 2100::1234/64
CWGE24MS2(config)#no snmp community qqz rw trusted-ipv6-host 2100::1234/64
CWGE24MS2(config)#snmp trap-receiver 192.168.200.106 v2c public
CWGE24MS2(config)#snmp system-contact IT engineer

```

CWGE24MS2(config)#snmp system-location Branch-Office

Web Configuration

SNMP Setting:

SNMP

SNMP Settings

Community Name

SNMP Settings

SNMP State

Disable ▾

System Name

CWGE24MS2

System Location

System Contact

Apply

Refresh

Parameter	Description
SNMP State	Select Enable to activate SNMP on the Switch. Select Disable to not use SNMP on the Switch.
System Name	Type a System Name for the Switch. (The System Name is same as the host name)
System Location	Type a System Location for the Switch.
System Contact	Type a System Contact for the Switch.
Apply	Click Apply to configure the settings.
Refresh	Click this button to reset the fields to the last setting.

Community Name:

SNMP						
SNMP Settings		Community Name				
Community Name Settings						
Community String	Rights	IP Version	Network ID of Trusted Host	Mask		
<input type="text"/>	Read-Only ▼	IPv4 ▼	<input type="text"/>	<input type="text"/>		
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>						
Community Name List						
No.	Community String	Rights	IP Version	Network ID of Trusted Host	Mask	Action
1	public	Read-Only	IPv4	192.168.10.0	255.255.255.0	<input type="button" value="Delete"/>

Parameter	Description
Community String	Enter a Community string, this will act as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Rights	Select Read-Only to allow the SNMP manager using this string to collect information from the Switch. Select Read-Write to allow the SNMP manager using this string to create or edit MIBs (configure settings on the Switch).
IP Version	Select the IP version.(IPv4 or IPv6)
Network ID of Trusted Host	Type the IP address of the remote SNMP management station in dotted decimal notation, for example 192.168.1.0. or the IPv6 format as 2100::1234.
Mask	Type the subnet mask for the IP address of the remote SNMP management station in dotted decimal notation, for example 255.255.255.0. or the IPv6 format as FFFF:FFFF:FFFF:FFFF::
Apply	Click Apply to configure the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Community Name List

No.	This field indicates the community number. It is used for identification only. Click on the individual community number to edit the community settings.
Community String	This field displays the SNMP community string. An SNMP community string is a text string that acts as a password.

Parameter	Description
Right	This field displays the community string's rights. This will be Read Only or Read Write.
Network ID of Trusted Host	This field displays the IP address of the remote SNMP management station after it has been modified by the subnet mask.
Subnet Mask	This field displays the subnet mask for the IP address of the remote SNMP management station.
Action	Click Delete to remove a specific Community String.

SNMP Trap

Web Configurations

SNMP Trap

Trap Receiver Settings
Trap Event Settings
Port Trap Settings

Trap Receiver Settings

IP Version	IP Address	Version	Community String
IPv4 ▼		v1 ▼	

Trap Receiver List

No.	IP Version	IP Address	Version	Community String	Action
1	IPv4	192.168.10.253	v2c	public	<input type="button" value="Delete"/>

Parameter	Description
IP Version	Selects the IP version, IPv4 or IPv6.
IP Address	Enter the IP address of the remote trap station in dotted decimal notation.
Version	Select the version of the Simple Network Management Protocol to use. v1 or v2c.
Community String	Specify the community string used with this remote trap station.
Apply	Click Apply to configure the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Trap Receiver List	
No.	This field displays the index number of the trap receiver entry. Click the number to modify the entry.
IP Version	This field displays the IP address version.
IP Address	This field displays the IP address of the remote trap station.
Version	This field displays the version of Simple Network Management Protocol in use. v1 or v2c.
Community String	This field displays the community string used with this remote trap station.
Action	Click Delete to remove a configured trap receiver station.

SNMPv3

CLI Configuration

Node	Command	Description
enable	show snmp user	This command displays all snmp v3 users.
enable	show snmp group	This command displays all snmp v3 groups.
enable	show snmp view	This command displays all snmp v3 view.
configure	snmp user USERNAME GROUPNAME noauth	Configures v3 user of non- authentication.
configure	snmp user USERNAME GROUPNAME auth (MD5 SHA) STRINGS	Configures v3 user of authentication.
configure	snmp user USERNAME GROUPNAME priv (MD5 SHA) STRINGS des STRINGS	Configures v3 user of authentication and encryption.
configure	snmp group GROUPNAME noauth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of non- authentication.
configure	snmp group GROUPNAME auth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication.
configure	snmp group GROUPNAME priv (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication and encryption.
configure	snmp view VIEWNAME STRINGS (included excluded)	To identify the subtree.
configure	no snmp user USERNAME GROUPNAME	This command removes a v3 user from switch.
configure	no snmp group GROUPNAME	This command removes a v3 group from switch.
configure	no snmp view VIEWNAME STRINGS	This command removes a v3 view from switch.

Web Configuration

SNMPv3 User

Parameter	Description
User Name	Enter the v3 user name.
Group Name	Map the v3 user name into a group name.
Security Level	Select the security level of the v3 user to use. noauth means no authentication and no encryption. auth means messages are authenticated but not encrypted. priv means messages are authenticated and encrypted.
Auth Algorithm	Select MD5 or SHA Algorithm when security level is auth or priv.
Auth Password	Set the password for this user when security level is auth or priv. (pass phrases must be at least 8 characters long!)
Priv Algorithm	Select DES encryption when security level is priv.
Priv Password	Set the password for this user when security level is priv. (pass phrases must be at least 8 characters long!)
Apply	Click Apply to configure the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
SNMPv3 User Status	
User Name	This field displays the v3 user name.

Group Name This field displays the group name which the v3 user mapping.

Auth Protocol These fields display the security level to this v3 user.

Priv Protocol

Rowstatus This field displays the v3 user rowstatus.

Action Click Delete to remove a v3 user.

SNMPv3 Group

SNMPv3 Configuration

SNMPv3 User
SNMPv3 Group
SNMPv3 View

SNMPv3 Group Settings

Group Name

Security Level

noauth ▼

Read View

Write View

Notify View

SNMPv3 Group Status

Group Name	Security Model	Security Level	Read View	Write View	Notify View	Action
No Entries!						

Parameter	Description
Group Name	Enter the v3 user name.
Security Level	Select the security level of the v3 group to use.
Read View	Note that if a group is defined without a read view than all objects are available to read. (default value is none.)
Write View	if no write or notify view is defined, no write access is granted and no objects can send notifications to members of the group. (default value is none.)
Notify View	By using a notify view, a group determines the list of notifications its users can receive. (default value is none.)
Apply	Click Apply to configure the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
SNMPv3 Group Status	

Parameter	Description
Group Name	This field displays the v3 user name.
Security Model	This field displays the security model of the group. Always displayed v3: User-based Security Model (USM)
Security Level	This field displays the security level to this group.
Read View	These fields display the View list of this group.
Write View	
Notify View	
Action	Click Delete to remove a v3 group.

SNMPv3 View

Parameter	Description
View Name	Enter the v3 view name for creating an entry in the SNMPv3 MIB view table.
View Subtree	The OID defining the root of the subtree to add to (or exclude from) the named view.
View Type	Select included or excluded to define subtree adding to the view or not.
Apply	Click Apply to configure the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
SNMPv3 View Status	
View Name	This field displays the v3 view name.
View Subtree	This field displays the subtree.
View Type	This field displays the subtree adding to the view or not.
Action	Click Delete to remove a v3 view.

Auto Provision

Introduction

Auto provision is a service that service provider can quickly, easily and automatically configure remote device or doing firmware upgrade at remote side.

» When the Auto Provision is enabled, the Switch will download the auto provision information file from the auto provision server first.

The file name is followed below naming rule:

Model_Name_Autoprovision.txt

For Example: *CWGE24MS2_Autoprovision.txt*

The contents of the file are listed below:

```
AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version=CWGE24MS2-096-1.0.3.S0
Firmware_Image_File=CWGE24MS2-096-1.0.3.S0.fw
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File=CWGE24MS2-096-1.0.3.S0.save
Global_Configuration_Reboot=0
Specific_Configuration_State=0
Specific_Configuration_Reboot=0
```

- » If AUTO_PROVISION_VER is biggest than current auto provision version, do step 3; otherwise, wait 24 hours and go back to step 1.
- » If the Firmware_Upgrade_State =1, do step 4; otherwise, do step 6.
- » If the Firmware_Version is difference than current firmware version, download the Firmware_Image_File and upgrade firmware.
- » If upgrade firmware succeeded and Firmware_Reboot=1, let reboot_flag=1.
- » If the Global_Configuration_State =1, download the Global_Configuration_File and upgrade configuration; otherwise, do step 8.
- » If upgrade configuration succeeded and Global_Configuration_Reboot =1, let reboot_flag=1.
- » If the Specific_Configuration_State =1, download the specific configuration file and upgrade configuration; otherwise do step 10. The naming is "Model_Name_" with 12-bit MAC digits, example for following is "CWGE24MS2_00223b0b8030.txt"
- » If upgrade configuration succeeded and Specific_Configuration_Reboot =1, let reboot_flag=1.
- » If reboot_flag=1, save running configuration and reboot the switch; otherwise, wait 24 hours and go back to step 1.

Default Settings

Auto provision configuration profile:

Active : Disable
 Version : 0
 Protocol : FTP
 FTP user/pwd : /
 Folder :
 Server address :

CLI Configuration

Node	Command	Description
enable	show auto-provision	This command displays the current auto provision configurations.
configure	auto-provision	This command enters the auto-provision node.
auto-provision	show	This command displays the current auto provision configurations.
auto-provision	active (enable disable)	This command enables/disables the auto provision function.
auto-provision	server-address IPADDR	This command configures the auto provision server's IP.
auto-provision	protocol (tftp http ftp)	The command configurations the upgrade protocol.
auto-provision	FTP-user username STRING password STRING	The command configurations the username and password for the FTP server.
auto-provision	folder STRING	The command configurations the folder for the auto provision server.
auto-provision	no folder	The command configurations the folder to default.
auto-provision	no FTP-user	The command configurations the username and password to default.

Web Configuration

Auto Provision	
Auto Provision Settings	
State	<input type="text" value="Disable"/>
Status	Disabled
Version	0
Protocol	<input type="text" value="TFTP"/>
Server IP version	<input type="text" value="IPv4"/>
Server IP	<input type="text" value="0.0.0.0"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Folder Path	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>	

Mail Alarm

Introduction

The feature sends an e-mail trap to a predefined administrator when some events occur. The events are listed below:

- | | |
|------------------------|--|
| » System Reboot | : The system warn start or cold start. |
| » Port Link Change | : A port link up or down. |
| » Configuration Change | : The system configurations in the NV-RAM have been updated. |
| » Firmware Upgrade | : The system firmware image has been updated. |
| » User Login | : A user login the system. |
| » Port Blocked | : A port is blocked by looping detection or BPDU Guard. |

Default Settings

Mail-Alarm Configuration:

```
-----
State                : Disabled.
Server IP            : 0.0.0.0
Server Port          : 25
Mail From            :
Mail To              :
```

Trap Event Status:

```
-----
System Reboot        : Disabled.
Port Link Change     : Disabled.
Configuration Change : Disabled.
Firmware Upgrade     : Disabled.
User Login           : Disabled.
Port Blocked         : Disabled.
Alarm                : Disabled.
```

Reference

Default Ports	Server	Authentication	Port
SMTP Server (Outgoing Messages)	Non-Encrypted	AUTH	25 (or 587)
	Secure (TLS)	StartTLS	587
	Secure (SSL)	SSL	465
POP3 Server (Incoming Messages)	Non-Encrypted	AUTH	110
	Secure (SSL)	SSL	995
Googlemail - Gmail	Server	Authentication	Port
SMTP Server (Outgoing Messages)	smtp.gmail.com	SSL	465
	smtp.gmail.com	StartTLS	587
POP3 Server (Incoming Messages)	pop.gmail.com	SSL	995
Outlook.com	Server	Authentication	Port
SMTP Server (Outgoing Messages)	smtp.live.com	StartTLS	587
POP3 Server (Incoming Messages)	pop3.live.com	SSL	995
Yahoo Mail	Server	Authentication	Port
SMTP Server (Outgoing Messages)	smtp.mail.yahoo.com	SSL	465
POP3 Server (Incoming Messages)	pop.mail.yahoo.com	SSL	995
Yahoo Mail Plus	Server	Authentication	Port
SMTP Server (Outgoing Messages)	plus.smtp.mail.yahoo.com	SSL	465
POP3 Server (Incoming Messages)	plus.pop.mail.yahoo.com	SSL	995

CLI Configuration

Node	Command	Description
enable	show mail-alarm	This command displays the Mail Alarm configurations.
configure	mail-alarm (disable enable)	This command disables / enables the Mail Alarm function.
configure	mail-alarm auth-account	This command configures the Mail server authentication account.
configure	mail-alarm mail-from	This command configures the mail sender.
configure	mail-alarm mail-to	This command configures the mail receiver.
configure	mail-alarm server-ip IPADDR server-port VALUE	This command configures the mail server IP address and the TCP port.
configure	mail-alarm server-ip IPADDR server-port Default	This command configures the mail server IP address and configures 25 as the server's TCP port.
configure	mail-alarm trap-event (reboot link-change config firmware login port-blocked alarm) (disable enable)	This command disables / enables mail trap events.

Web Configuration

Mail Alarm

Mail Alarm Settings

State

Disable ▾

Server

IP ▾

0.0.0.0

Server Port

25

(Default:25)

Account Name

Account Password

Mail From

Mail To

Trap State :

☐ Select All

☐ Deselect All

☐ System Reboot

☐ Port Link Change

☐ Configuration Change

☐ Firmware Upgrade

☐ User Login

☐ Port Blocked

☐ Alarm

Apply

Refresh

Parameter	Description
State	Enable / disable the Mail Alarm function.
Server IP	Specifies the mail server’s IP address.
Server Port	Specifies the TCP port for the SMTP.
Account Name	Specifies the mail account name.
Account Password	Specifies the mail account password.
Mail From	Specifies the mail sender.
Mail To	Specifies the mail receiver.
Trap State	Enables / disables the mail trap event states.

Maintenance

CLI Configuration

Node	Command	Description
enable	show config-change-status	This command displays the configurations status if there are default values.
configure	reboot	This command reboots the system.
configure	reload default-config	This command copies a default-config file to replace the current one. Note: The system will reboot automatically to take effect the configurations.
configure	write memory	This command writes current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	This command downloads a new copy of configuration file from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	This command uploads the current configurations file to a TFTP server.
configure	archive download-fw <URL PATH>	This command downloads a new copy of firmware file from TFTP / FTP / HTTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

Example:

```
CWGE24MS2#configure terminal
CWGE24MS2(config)#interface eth0
CWGE24MS2(config-if)#ip address 172.20.1.101/24
CWGE24MS2(config-if)#ip address default-gateway 172.20.1.1
CWGE24MS2(config-if)#management vlan 1
```

Enable the DHCP client function for the switch.

```
CWGE24MS2#configure terminal
CWGE24MS2(config)#interface eth0
CWGE24MS2(config-if)#ip dhcp client enable
```

```
CWGE24MS2#show config-change-status
```

The user configuration file is default.

The configurations have been modified.

Web Configuration

The screenshot shows a web interface for the 'Maintenance' section. At the top, there is a dark blue header with the word 'Maintenance' in white. Below this, there are four tabs: 'Configuration' (which is active and highlighted in dark blue), 'Firmware', 'Reboot', and 'Server'. The main content area is divided into several sections. The first section is 'Save Configuration', which contains the text 'Save the parameter settings of the Switch :' and a 'Save' button. The second section is 'Upload and Download Configuration', which contains two radio button options. The first option is selected and is labeled 'Upload configuration file to your Switch.'; it includes a 'File path' label, a 'Choose File' button, the text 'No file chosen', and an 'Upload' button. The second option is labeled 'Press "Download" to save configuration file to your PC.' and includes a 'Download' button. The third section is 'Reset Configuration', which contains the text 'Reset the factory default settings of the Switch : - IP address will be 192.168.10.1' and a 'Reset' button. The final section is 'The configuration status', which contains the text 'The user configuration file is default. The configuration has been modified.'

Save Configurations

The screenshot shows a 'Save Configurations' dialog box. It has a title bar that says 'Save Configurations'. The main text inside the dialog is 'Save the parameter settings of the Switch :'. Below this text is a 'Save' button.

Press the Save button to save the current settings to the NV-RAM (flash).

Upload / Download Configurations to/from your server

Follow the steps below to save the configuration file to your PC.

- » Select the “Press “Download” to save configurations file to your PC”.
- » Click the “Download” button to start the process.

Follow the steps below to load the configuration file from your PC to the Switch.

- » Select the “Upload configurations file to your Switch”.
- » Select the full path to your configuration file.
- » Click the Upload button to start the process.

Reset the factory default settings of the Switch

Press the Reset button to set the settings to factory default configurations.

The configuration status

Display the configuration status of recorded in the NV-RAM.

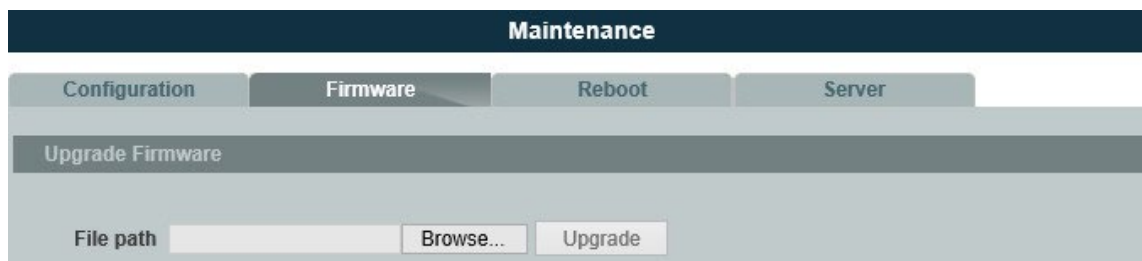
Notice: *If the user has changed any configurations, the message displays “The configurations have been modified!” Otherwise, the message “The configurations are default values.”*

There are two conditions will change message from “The configurations have been modified!” to “The configurations are default values.”

- » Click "Reset configuration" in web management or do cli command, reload default-config.
- » Click "Upload configuration" in web management or do cli command, "archive download-config xxx".

Firmware

Type the path and file name of the firmware file you wish to upload to the Switch in the File path text box or click Browse to locate it. Click Upgrade to load the new firmware.



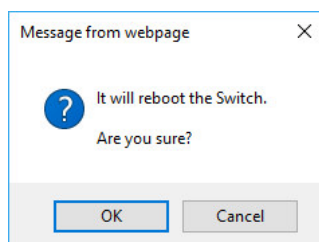
Reboot

Reboot allows you to restart the Switch without physically turning the power off.

Follow the steps below to reboot the Switch.



- » In the Reboot screen, click the Reboot button. The following screen displays.



- » Click OK again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Server Control

The function allows users to enable or disable the SSH or Telnet or Web service individual using the CLI or GUI.

CLI Configuration

Node	Command	Description
enable	show server status	This command displays the current server status.
configure	ssh server	This command enables the ssh on the Switch.
configure	no ssh server	This command disables the ssh on the Switch.
configure	telnet server	This command enables the telnet on the Switch.
configure	no telnet server	This command disables the telnet on the Switch.
configure	web server	This command enables the web on the Switch.
configure	no web server	This command disables the web on the Switch.

Web Configuration

Maintenance

Configuration

Firmware

Reboot

Server

Server Settings

HTTP Server State	Enable ▾	HTTP Server TCP Port	80
HTTPS Server State	Enable ▾		
SNMP v1/v2c Server State	Enable ▾		
SNMP v3 Server State	Enable ▾		
SSH Server State	Enable ▾		
TELNET Server State	Enable ▾	TELNET Server TCP Port	23

Apply

Refresh

Server Status

HTTP Server Status	Enable	HTTP Server TCP Port	80
HTTPS Server Status	Enable		
SNMP v1/v2c Server Status	Enable		
SNMP v3 Server Status	Enable		
SSH Server Status	Enable		
TELNET Server Status	Enable	TELNET Server TCP Port	23

Parameter	Description
Server Settings	
Web Server State	Selects Enable or Disable to enable or disable the Web service.
Telnet Server State	Selects Enable or Disable to enable or disable the Telnet service.
SSH Server State	Selects Enable or Disable to enable or disable the SSH service.
Apply	Click Apply to configure the settings.
Refresh	Click this button to reset the fields to the last setting.
Server Status	
Web Server Status	Displays the current Web service status.
Telnet Server Status	Displays the current Telnet service status.
SSH Server Status	Displays the current SSH service status.

System log

Introduction

The syslog function records some of system information for debugging purpose. Each log message recorded with one of these levels, Alert / Critical / Error / Warning / Notice / Information. The syslog function can be enabled or disabled. The default setting is disabled. The log message is recorded in the Switch file system. If the syslog server's IP address has been configured, the Switch will send a copy to the syslog server.

The log message file is limited in 4KB size. If the file is full, the oldest one will be replaced.

CLI Configuration

Node	Command	Description
enable	show syslog	The command displays the entire log message recorded in the Switch.
enable	show syslog level LEVEL	The command displays the log message with the LEVEL recorded in the Switch.
enable	show syslog server	The command displays the syslog server configurations.
configure	clear syslog	The command clears the syslog message.
configure	syslog-server (disable enable)	The command disables / enables the syslog server function.
configure	syslog-server ipv4-ip IPADDR	The command configures the syslog server's IP address in IPv4 format.
configure	syslog-server ipv6-ip IPADDR	The command configures the syslog server's IP address in IPv6 format.
configure	syslog-server facility	The command configures the syslog facility level.

Example:

```
CWGE24MS2#configure terminal
CWGE24MS2(config)#syslog-server ipv4-ip 192.168.200.106
CWGE24MS2(config)#syslog-server enable
```


Web Configuration

System Log

Syslog Server Settings

Server IP

IPv4

Disable

Facility

(5) Messages generated internally by syslogd

Apply

System Log

Log Level

All

Show

Refresh

Clear

Save

<6> 2014 Jan 1 00:00:00 System Cold Start

<6> 2014 Jan 1 00:00:02 Power source is changed from AC to Battery!

<6> 2014 Jan 1 00:00:02 Port 24 Link Up.

<6> 2014 Jan 1 00:00:03 Port 18 Link Up.

<6> 2014 Jan 1 00:00:03 Port 11 Link Up.

<6> 2014 Jan 1 00:00:03 Port 19 Link Up.

<6> 2014 Jan 1 00:00:03 Port 1 Link Up.

<6> 2014 Jan 1 00:00:03 Port 2 Link Up.

<6> 2014 Jan 1 00:00:03 Port 3 Link Up.

<6> 2014 Jan 1 00:00:03 Port 5 Link Up.

<6> 2014 Jan 1 00:00:03 Port 16 Link Up.

<6> 2014 Jan 1 00:00:03 Port 8 Link Up.

<6> 2014 Jan 1 00:00:03 Port 4 Link Up.

<6> 2014 Jan 1 00:00:03 Port 13 Link Up.

<6> 2014 Jan 1 00:00:03 Port 15 Link Up.

<6> 2014 Jan 1 00:00:03 Port 10 Link Up.

<6> 2014 Jan 1 00:00:03 Port 7 Link Up.

<6> 2014 Jan 1 00:00:03 Port 22 Link Up.

Parameter	Description
Server IP	Enter the Syslog server IP address in dotted decimal notation. For example, 192.168.1.1. Select Enable to activate switch sent log message to Syslog server when any new log message occurred.
Log Level	Select Alert/Critical/Error/Warning/Notice/Information to choose which log message to want see.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

User Account

Introduction

The Switch allows users to create up to 6 user account. The user name and the password should be the combination of the digit or the alphabet. The last admin user account cannot be deleted. Users should input a valid user account to login the CLI or web management.

User Authority:

The Switch supports two types of the user account, admin and normal. The default user's account is username (admin) / password (admin).

- » admin - read / write.
- » normal - read only.
- ; Cannot enter the privileged mode in CLI.
- ; Cannot apply any configurations in web.

Default Settings

Maximum user account : 6.
Maximum user name length : 32.
Maximum password length : 32.
Default user account for privileged mode : admin / admin.

Notices

The Switch allows users to create up to 6 user account.

The user name and the password should be the combination of the digit or the alphabet.

The last admin user account cannot be deleted.

The maximum length of the username and password is 32 characters.

CLI Configuration

Node	Command	Description
enable	show user account	This command displays the current user accounts.
configure	add user USER_ACCOUNT PASSWORD (normal admin)	This command adds a new user account.
configure	delete user USER_ACCOUNT	This command deletes a present user account.

Example:

```
CWGE24MS2#configure terminal
CWGE24MS2(config)#add user q q admin
CWGE24MS2(config)#add user 1 1 normal
```

Web Configuration

User Account

User Account Settings

User Name

User Password

User Authority Normal ▼

User Account List

No.	Name	Authority	Action
1	admin	admin	

Parameter	Description
User Name	Type a new username or modify an existing one.
User Password	Type a new password or modify an existing one. Enter up to 32 alphanumeric or digit characters.
User Authority	Select with which group the user associates: admin (read and write) or normal (read only) for this user account.
Apply	Click Apply to add/modify the user account.
Refresh	Click Refresh to begin configuring this screen afresh.
User Account List	
No.	This field displays the index number of an entry.
User Name	This field displays the name of a user account.
User Password	This field displays the password.
User Authority	This field displays the associated group.
Action	Click the Delete button to remove the user account. Note: You cannot delete the last admin accounts.

MECHANICAL INSTALLATION INSTRUCTIONS

ComNet Customer Service

Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.

Email ComNet Global Service Center: customercare@comnet.net



3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET