LES-2224C-SFP SNMP Fiber Switch

User Manual & Setting Guide

1. **Web interface operation**

2. **Command line interface**

3. **CDP function setting**
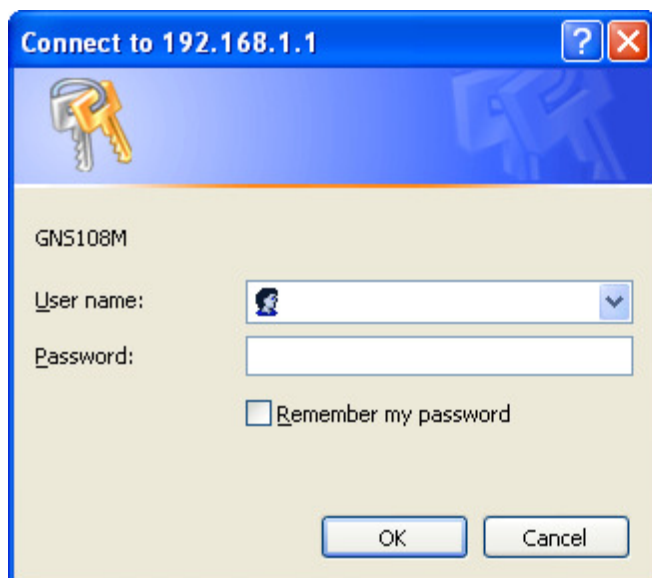
4. **S/W upgrade procedure**

Web interface operation

This section introduces the settings and functions of the web management interface. If you are using IE 5.0, please activate the Java security privilege.
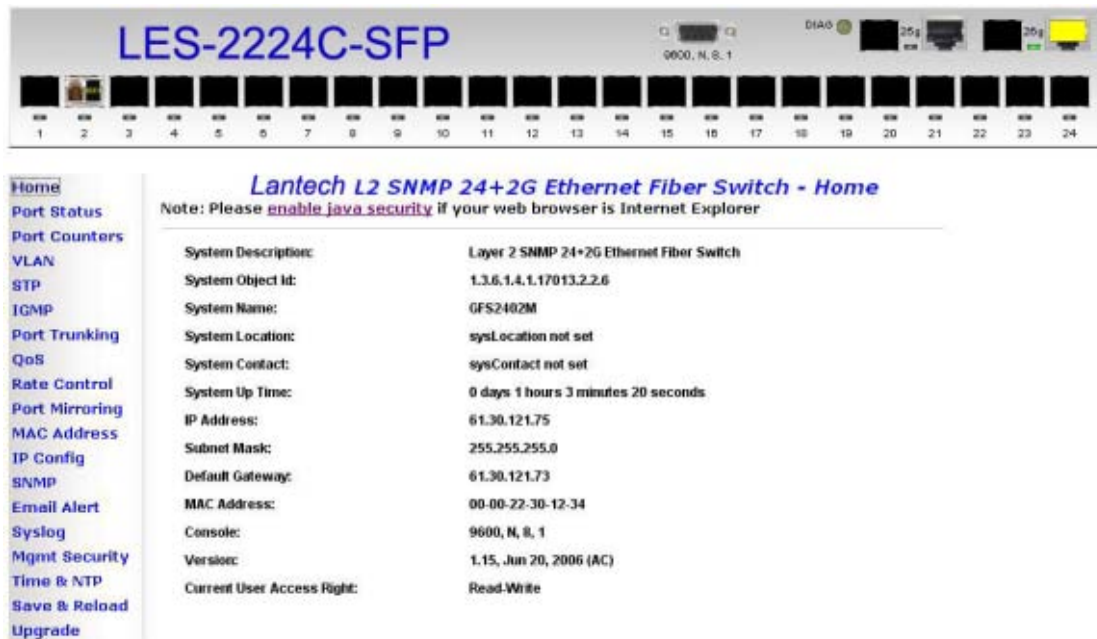
- Tools>Internet Options>Security>Internet>Custom Level>Microsoft VM Java Permissions
- Click on Custom
- Then click on the Java Custom Settings Box below
- Edit Permissions
- Unsigned content
- Run unsigned content
- Enable
- Click ok, click ok
- Click yes

Login to the system:

1. Start IE or other browser.
2. Enter the IP address(The default IP is: 192.168.1.1) of the switch at the URL location.
3. The password screen will appear.
4. Input correct user name and password. There is no default name and password. Just press a key for username. It is necessary to enter password.
5. Click OK then the web management interface will appear.

Home

System Description: the brief description of this switch

System Object ID: the SNMP object ID of this switch.

System Name: the symbolic name of this switch

System Location: the location of this switch

System Contact: the contact person name.

System Uptime: time lasts since last reboot.

IP Address: the IP address of this switch

Subnet Mask: the subnet mask.

Default Gateway: the default gateway of this switch

MAC Address: the MAC address of the switch

Console: RS232 Settings (baud rate, parity, bits, stop bit)

Version: the firmware version

Current User Access Right: Read Write (or Read Only)

   The virtual switch panel is shown on the top of the screen. The LED columns refer to the fiber ports respectively. If the fiber port is linked, the diagram of the plug will show yellow circle, otherwise the plug will be dark.

Port Status

All ports information will be display on this page. When the SFP slot is inserted with module, CPU will try to identify the SFP type and display the information. When the SFP module is linked, the yellow circle will show.

Port 25/26 are gigabit port. UTP and SFP slot are shared with the same port. They cannot work at the same time. The UTP port only works in 1000M speed. It cannot connect with 10M or 100M copper port.

Port Counters

The content for port counters are as below:

1. Bytes RX, TX

2. Frames RX, TX

3. Unicast/Broadcast/Multicast RX

4. Unicast/Broadcast/Multicast TX

5. Error RX, TX

6. InDiscards

7. OutDiscards

8. Undersize

9. Oversize

10. Collision

11. Fragment

VLAN
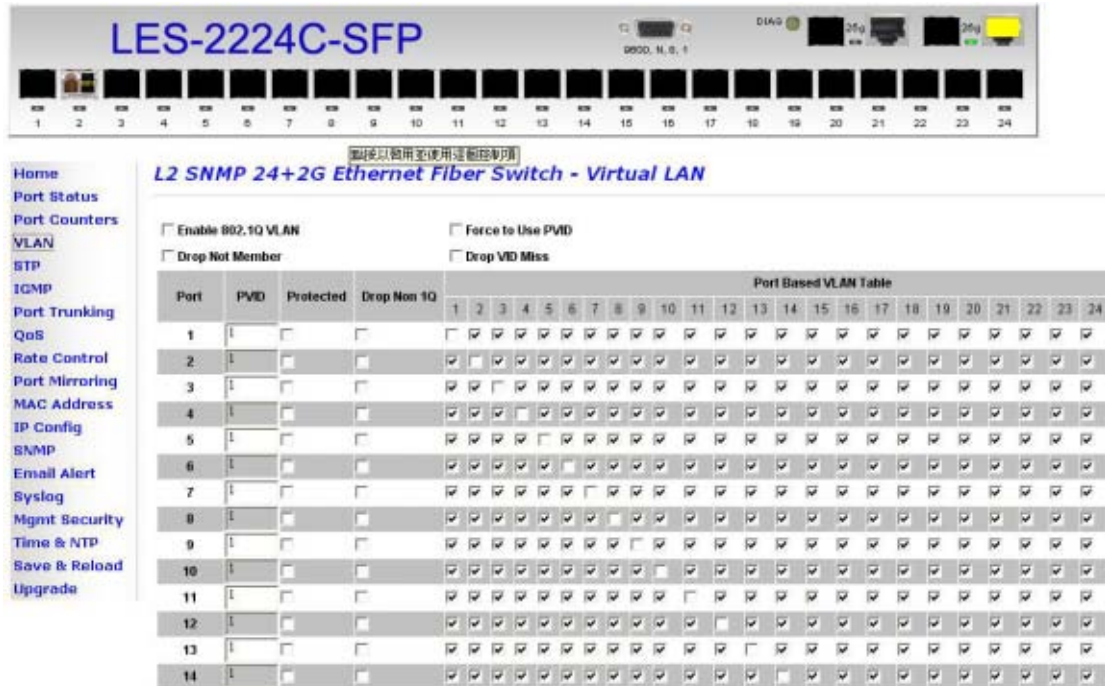
1. Management CPU is port 27
2. There are several VLAN mode can be selected:
    (1) Force to Use PVID: Force to use Default VLAN ID (the tagged frame's VID is ignored)
    (2) Drop Not Member: Drop a frame if the ingress port of the frame is not a member of the frame's VID
    (3) Drop VID Miss: Drop a frame if the frame's VID is not contained in current VLAN table
3. PVID (1..4094): Port Default VLAN ID
4. Protected: Traffic between protected port group members is blocked
5. Drop Non 1Q: Any non-820.1Q frame (without vlan tagged) is dropped
6. Press "Remove All" button will remove all VLANs except VLAN 1

Spanning Tree Protocol(STP)

LES-2224C-SFP

9600, N, 8, 1

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

L2 SNMP 24+2G Ethernet Fiber Switch - Spanning Tree Protocol

Navigation menu:
Home
Port Status
Port Counters
VLAN
STP
IGMP
Port Trunking
QoS
Rate Control
Port Mirroring
MAC Address
IP Config
SNMP
Email Alert
Syslog
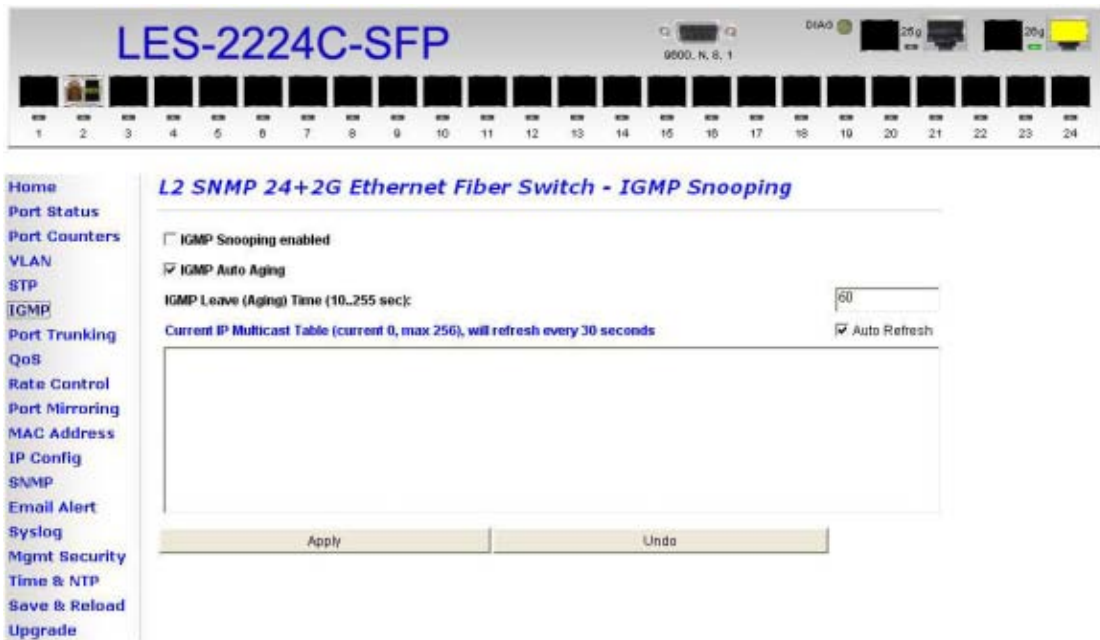Mgmt Security
Time & NTP
Save & Reload
Upgrade

☐ **Enable Spanning Tree Protocol**

Current Spanning Tree Root

MAC Address:	-
Root Priority:	-
Root Max Age (sec):	-
Root Hello Time (sec):	-
Root Forward Delay (sec):	-
Root Path Cost:	-
Root Port:	-

Spanning Tree Bridge Configuration

Priority (0-65535):	32768
Max Age Time (6-200 sec):	20
Hello Time (1-10 sec):	2
Forward Delay (4-200 sec):	15

Spanning Tree Port Configuration

Port	Priority (0..255)	State	Path Cost (1..255)	Root Cost
1	128	-	19	-
2	128	-	19	-
3	128	-	19	-
4	128	-	19	-
5	128	-	19	-
6	128	-	19	-
7	128	-	19	-
8	128	-	19	-
9	128	-	19	-

Once the STP function is enabled, there are 30 seconds which could not access this switch. The user has to wait for the STP function is done, then the system will be work normally.

All parameters can be set in this web page. The user can set them using CLI to do these setting. Please check the command line page for more detail information.

IGMP

The Internet Group Management Protocol(IGMP) is an internal protocol of the internet protocol(IP) suit. This management switch supports IP multicast function. The user can set this IGMP function, then display IGMP snooping information in this page.

Port Trunking

Port	Trunk Group 0 (Ports 1..24)	Trunk Group 1 (Ports 1..24)	Trunk Giga Ports 25-26	Name (RO)
	☐ Enabled	☐ Enabled	☐ Enabled	
1	☐ Member	☐ Member		
2	☐ Member	☐ Member		
3	☐ Member	☐ Member		
4	☐ Member	☐ Member		
5	☐ Member	☐ Member		
6	☐ Member	☐ Member		
7	☐ Member	☐ Member		
8	☐ Member	☐ Member		
9	☐ Member	☐ Member		
10	☐ Member	☐ Member		
11	☐ Member	☐ Member		
12	☐ Member	☐ Member		
13	☐ Member	☐ Member		
14	☐ Member	☐ Member		
15	☐ Member	☐ Member		
16	☐ Member	☐ Member		
17	☐ Member	☐ Member		
18	☐ Member	☐ Member		
19	☐ Member	☐ Member		
20	☐ Member	☐ Member		
21	☐ Member	☐ Member		
22	☐ Member	☐ Member		
23	☐ Member	☐ Member		

There are 2 trunk groups can be assigned for 100M SFP port(port 1 to port 24). The 2 gigabit port can be assigned to one trunk port also.

For 100M SFP port, the trunk port number can up to 4 members in each trunk group.

For two 1000M ports. They are assigned to member automatic when "trunk gigabit port" item is selected.

QoS

1. Force to Use Default Priority: Use the default ingress priority (the tagged frame's priority is ignored)
2. Default Priority: the default ingress priority to use when no other priority information is available
3. Highest Priority: Force all frames from a port to highest queue
4. Use IP Mapping: Use IP (IPv4 and IPv6) for priority, 1 (default)-Use IP fields for priority mapping, 0-Ignore IP priority field
5. Use Tag Mapping: Use IEEE Tags for priority, 1 (default)-Use IEEE 802.1p tag Traffic Class for priority mapping if the frame is tagged, 0-Ignore IEEE 802.1p tag fields even the frame is tagged
6. For DSCP (IP fields, 0..63) priority mapping, please use "dscp-mapping" command in console or telnet

Rate Control

L2 SNMP 24+2G Ethernet Fiber Switch - Rate Limit Control

☐ Count IFG and Preamble   ☐ Drop Over Rate

Port	Ingress Rate Control	Ingress Rate (bits/sec)	Egress Rate Control	Egress Rate (bits/sec)	Name (RO)
1	☐	100M	☐	100M	
2	☐	100M	☐	100M	
3	☐	100M	☐	100M	
4	☐	100M	☐	100M	
5	☐	100M	☐	100M	
6	☐	100M	☐	100M	
7	☐	100M	☐	100M	
8	☐	100M	☐	100M	
9	☐	100M	☐	100M	
10	☐	100M	☐	100M	
11	☐	100M	☐	100M	
12	☐	100M	☐	100M	
13	☐	100M	☐	100M	
14	☐	100M	☐	100M	
15	☐	100M	☐	100M	
16	☐	100M	☐	100M	
17	☐	100M	☐	100M	
18	☐	100M	☐	100M	
19	☐	100M	☐	100M	
20	☐	100M	☐	100M	
21	☐	100M	☐	100M	
22	☐	100M	☐	100M	
23	☐	100M	☐	100M	
24	☐	100M	☐	100M	

1. Count IFG and Preamble: Count interframe gap (IFG) bytes (12 per frame) and Preamble bytes (8 per frame), 1-Counted, 0(default)-Not counted
2. Drop Over Rate: Drop incoming frame if the maximum rate control is exceeded
3. The resolution from 64K to 1792K is 64K, the resolution from 2M to 100M is 1M, the resolution from 104M to 1000M is 8M (for port 25g and 26g)

Note 1: Ingress rate means receiving rate. Egress rate means transmitting tare.
Note 2: In normal condition, the switch will send out "flow control" packet to reduce the transmit rate in link partner. Once the "Drop Over Rate" function is enabled, the packet will be dropped immediately when the rate is exceed the setting rate.

Port-Mirroring

- Sniffer Ingress: Copy packets which come from monitored ports to one sniffer port.

- Sniffer Egress: Copy packets which go out from monitored ports to one sniffer port

MAC Address

L2 SNMP 24+2G Ethernet Fiber Switch - MAC Address

Aging Time (0-1048575 sec, default 300): [300]

Port	Fast Aging Out	Max Dynamic MAC Number (0..8191)	Current Dynamic MAC Number (RO)
1	☐	8191	0
2	☐	8191	0
3	☐	8191	0
4	☐	8191	0
5	☐	8191	0
6	☐	8191	0
7	☐	8191	0
8	☐	8191	0
9	☐	8191	0
10	☐	8191	0
11	☐	8191	0
12	☐	8191	0
13	☐	8191	0
14	☐	8191	0
15	☐	8191	0
16	☐	8191	0
17	☐	8191	0
18	☐	8191	0
19	☐	8191	0
20	☐	8191	0
21	☐	8191	0
22	☐	8191	0
23	☐	8191	0
24	☐	8191	0

The user can get all mac address information in this page. The MAX dynamic MAC number cab be set for each port. The default is 8K users for each port. The switch will drop the packet when the max dynamic MAC number is exceeded and the new packet SA is not exist.

IP Config

This function allows user to set IP configurations. Once this DHCP client function is set to ON, the switch will request its IP address and other settings from a DHCP server in the same network. If the DHCP function is not activated, then user can set his own IP settings. You can also choose the access methods (Telnet, HTTP) for controlling the converter. You can also enable/disable FTP server and TFTP server. For greatest security, FTP and TFTP should be disabled between upgrades.

SNMP

Set the objects of the system group, system name, system location and system contact. There are eight community names which can be assigned Read/Write privileges or Read Only privileges. There are eight trap addresses which can be assigned to receive alarms. Trap messages will be sent to these addresses. If the table is empty, then no traps will be issued. The user can use the Trap options section at the bottom of this screen to select the types of traps to be sent.

Email Alert
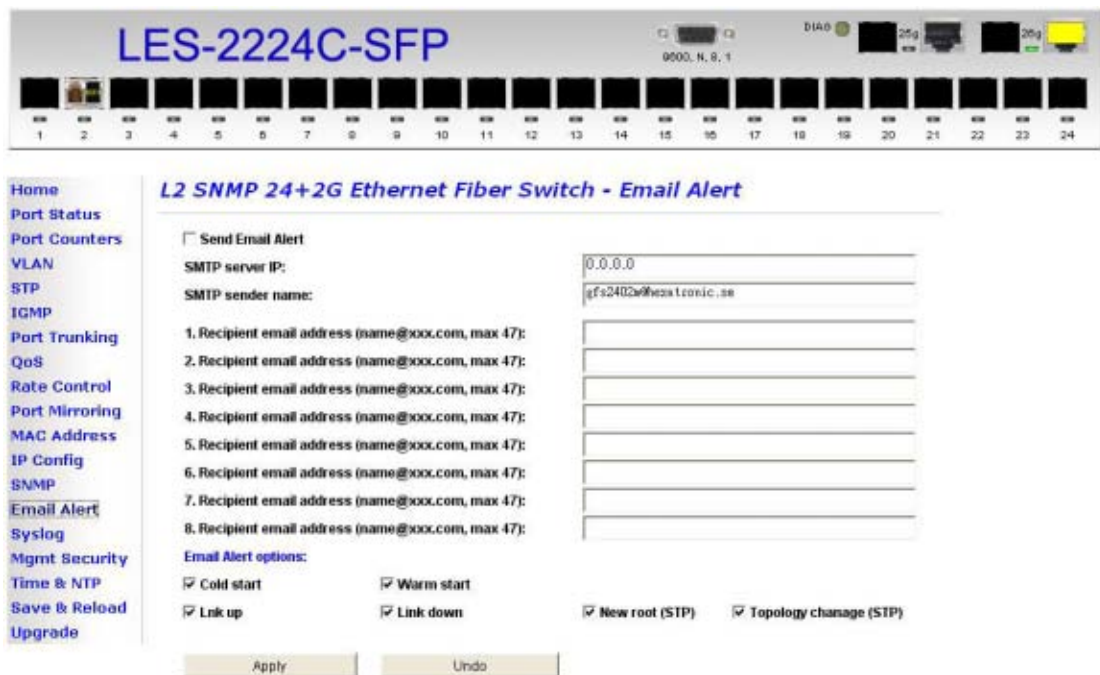
There are eight e-mail addresses can be assigned. If an event happens, an email describing the event will be sent to these addresses. This feature provides an alternate way to inform the administrator of system alarms. The user can change the "sender name" to identify which one switch sends this alert message.

Syslog

There are eight syslog servers can be assigned. Logs will be sent to these servers. The user can use this page to clear all logs, or choose to save all logs to flash. The user can also choose to export all logs to a remote TFTP server as a text file. The maximum syslog issues which can be stored are 4095.

Mgmt Security

The administrator can assign a user name and password for a maximum of eight users.

The administrator can also restrict system access so that the system can only be accessed from a group of IP addresses and forbid access from other IP addresses. There are sixteen IP addresses can be assigned. Set the Secure IP option to ON if this feature is required.

Time & NTP

NTP is a protocol for the system to synchronize time from an NTP server. Once the NTP client function is enabled, the management module gets network time using this protocol from an NTP server periodically. If there is no NTP server in the network, set the NTP client option to OFF and the user can set date and time directly.

Save & Reload

The Administrator may save the current settings to the NV-Flash of the system. When the system is running, the administrator can change the current settings and they will take effect immediately, but they will not be saved to the start up configuration unless you save running configuration to start up configuration.

The startup configuration can be up-loaded to the TFTP server in a file as a template. Downloading the template from the TFTP server is a fast way to configure, the administrator need only change options that are different.

Press the "factory default and reload" button to load the default factory setting.

Upgrade

The user can use FTP or TFTP to download the latest binary image. This SNMP switch implements an FTP server and a TFTP server. You may invoke FTP client to transfer new binary images to the Virtual file system and select the second method, specify the file name path, and then press the "upgrade" button to upgrade the firmware. If users have a TFTP server installed in the network, use the first method to specify the server address/file name path and then press the "upgrade" button to upgrade the firmware.

Command line interface

1. Interfcae

- **ifclear**   **- clear rmon counters**

- **ifcounters**   **- show rmon counters (per port)**
  Usage: ifcounters port_no
  port_no=1..27 or x(all)

- **ifdisable**   **- disable interface (per port)**
  Usage: ifdisable port_no
  port_no=1..26 or x(all)

- **ifenable**   **- enable interface (per port)**
  Usage: ifenable port_no
  port_no=1..26 or x(all)

- **ifname**   **- name interface (per port)**
  Usage: ifname port_no {string|no}
  port_no=1..26 or x(all)
  The max string length is 31

- **ifshow**   **- show interface information (per port)**
  Usage: ifshow port_no
  port_no=1..27 or x(all)

- **ifduplex**   **- set interface duplex**
  Usage: ifduplex port_no {half|full}
  port_no=1..24 or x(all)

- **ifflowctrl**   **- set flow control (per port)**
  Usage: ifflowctrl port_no {0|1}
  port_no=1..26 or x(all)
  0: Flow Control disabled, 1: enabled

2. VLAN

- vlan-8021q   - set 802.1Q vlan on/off

Current 802.1Q VLAN: off

Usage: vlan_8021q {on|off}

- ifpvid   - set default VLAN ID (per port)

Usage: ifpvid port_no vlan_id

port_no=1..27 or x(all)

valn_id=1..4093

- forcepvid   - force to use default VLAN ID (ignore the tagged frame's VID)

Current Force PVID: off

Usage: forcepvid {on|off}

Force to use Default VLAN ID (the tagged frame's VID is ignored), 0: not Force

Note: If the Default VLAN ID is 5, and enable forcepvid function. The result will be as below:

VLAN 300 Packet	→ forcepvid →	VLAN 5 Packet
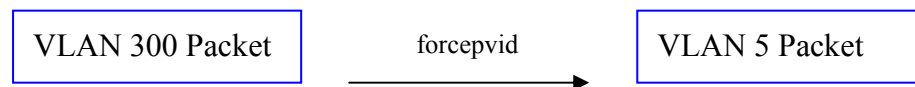
- ifprotected   - set interface protected (per port)

Usage: ifprotected port_no {0|1}

port_no=1..27 or x(all)

0: Normal operation, 1: Protected

- drop-non1q   - drop non 802.1Q frame (per port)

Usage: dropnon1q port_no {0|1}

port_no=1..26 or x(all)

1: Drop Non 802.1Q Frame, 0: not Drop

- drop-not-member   - drop a frame if ingress port is not a member

Current Drop Not Member: off

Usage: drop-not-member {on|off}

- **drop-vid-miss** - drop a frame if vid not existed in VLAN table

Current Drop VID Miss: off

Usage: drop-vid-miss {on|off}

- **addvlan** - add a 802.1Q vlan

Usage: addvlan vid [vlan_name]

vid=1..4093, the max length of vlan_name is 15

- **delvlan** - delete a 802.1Q vlan

Usage: delvlan vid

vid=1..4093

- **showvlan** - show vlan information

Vlan information will show when this command is pressed.

Example:

Current 802.1Q VLAN: Off, Force to use default VLAN ID: Off

Drop Not Member: Off, Drop VID Miss: Off

Port 1: Default VLAN ID: 1, Drop Non 1Q Frame: Off   Port Based VLAN

Table: 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,

22,23,24,25,26,27

- **addmember** - add member ports to a 802.1Q vlan

Usage: addmember vid member_ports_list

vid=1..4093

Example 1: addmember 10 1 8 (add port 1 and 8 to vlan 10)

Example 2: addmember 10 1t 8 (t: carry vlan tag when forwarded to port 1)

Example 3: addmember 10 1u 8 (u: unmodified when forwarded to port 1)

- **delmember** - delete member ports from a 802.1Q vlan

Usage: delmember vid member_ports_list

vid=1..4093

Example: delmember 10 1 2 (delete port 1 and 2 from vlan 10)

● port-base-vlan   - set port based vlan (per port)

Usage: port-base-vlan input_port output_ports_list

input_port=1..27

Example: port-base-vlan 1 2 8 (packets from port 1 forward to port 2 and 8 only. Other ports will not get packets.
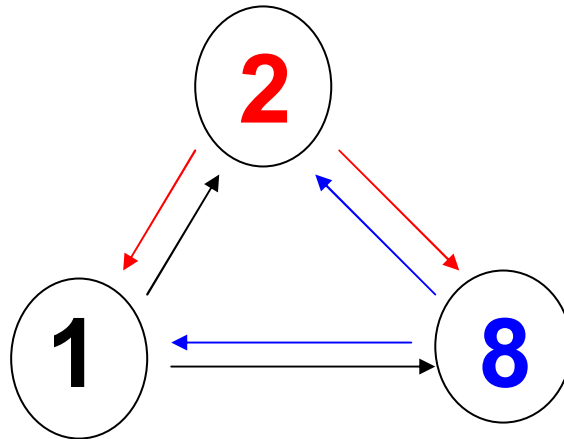
Port Base VLAN example

3. QoS

IEEE 802.1P frame

7	1	6	6	2	2	2	42-1496 bytes	4 bytes
Preamble	SFD	DA	SA	TPID	TCI	Type Length	Data	CRC

3	1	12 bits
User Priority	CFI	Bits of VLAN ID (VIDI) to identify possible VLANs

IP packet frame

Version (4)	Internet Header Length (4)	Type of Service (8)	Total Length (16)
Identification (16)		Flags (3)	Fragment Offset (13)
Time To Live (8)		Protocol (8)	Header checksum (16)
Source Address (32)			
Destination Address (32)			
Options (Variable)		Padding (0-24)	
Data			

- qos   - set Quality of Service on/off

Current Quality of Service: off

Usage: qos {on|off}

- ifdefpri   - set default priority (per port)

Usage: ifdefpri port_no priority

port_no=1..26 or x(all)

priority=0..7

- forcepri   - force to use default 802.p priority (ignore the tagged frame's priority)

Current Force 802.1p Priority: off

Usage: forcepri {on|off}

- highest-priority - set port to highest priority (per port)

Usage: highest_priority port_no {0|1}

port_no=1..26 or x(all)

1: Set port to highest priority, 0: not

- use-tos-diff   - use IP TOS/Diff fields for priority mapping
  (per port)

Usage: use_tos_diff port_no {0|1}

port_no=1..26 or x(all)

1: Use IP TOS/Diff fields for priority data, 0: Ignore IP TOS/Diff fields

- use-8021p   - use 802.1p tag fields for priority
  mapping (per port)

Usage: use_8021p port_no {0|1}

port_no=1..26 or x(all)

1: Use 802.1p tag for priority mapping if the frame is tagged, 0: Ignore
802.1p tag fields

- cos-mapping   - 802.1p priority to 4-level priority queues
  mapping

Usage: cos-mapping {default|priority queue}

priority=0..7, queue=0 (lowest queue) to 3 (highest queue)

Example: cos-mapping 7 3 (tagged priority 7 mapping to queue 3)

The default 802.1p priority to queue mapping: 1..2 to queue 0, 0 and 3 to
queue 1, 4..5 to queue 2, 6..7 to queue 3
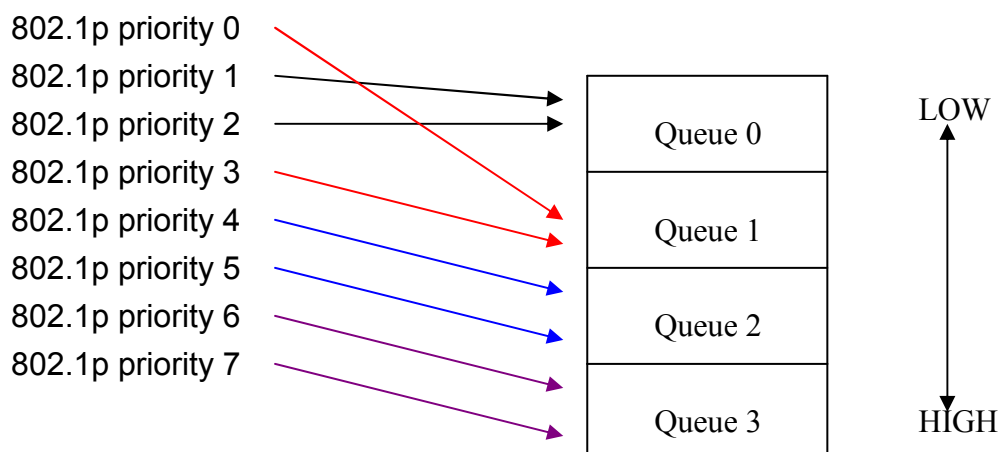
Default 802.1p priority mapping

- dscp-mapping - DiffServ value (0..63) of IP header to 4-level priority queues mapping

Usage: dscp-mapping {default|dscp queue}

dscp=0..63, queue=0 (lowest queue) to 3 (highest queue)

Example: dscp-mapping 63 3 (frames with DSCP field 63 mapping to queue 3)

The default DSCP to queue mapping: 0..15 to queue 0, 16..31 to queue 1, 32..47 to queue 2, 48..63 to queue 3

- schedule-policy - set the scheduling policy

Current schedule policy: 0

Usage: schedule-policy {0|1}

0 (default): use an 8, 4, 2, 1 (4 queues) weighted round robin queuing scheme,

1: use a strict priority scheme (packets in highest queue always transmit first

- showqos - show qos information

4. MAC

- **aging-time**   - set aging time

Current aging time: 300 (sec)

Usage: aging-time time

time=0..1048575 (sec), default is 300 (5 minutes). If time is 0, the aging function is disabled, and all learned addresses will remain in the database for ever.

- **fast-aging**   - aging out dynamic mac address (per port)

Usage: fast-aging port_no

port_no=1..27 or x(all)

- **showmactbl**   - show all mac address table

Example:

***** MAC Address ***** VLAN ID * Ports **** Type *

Mac=00-30-DA-03-DD-CC, vid=0000, Ports=[26], Dynamic, Age=1

Mac=00-00-22-30-12-34, vid=0000, Ports=[27], Dynamic, Age=1

Mac=00-30-48-81-14-C8, vid=0000, Ports=[26], Dynamic, Age=1

Total entries = 3

- **showstatic**   - show static mac address table

- **showfilter**   - show forbidden mac address table

- **addstatic**   - add static mac address

Usage: addstatic mac_addr vlan_id ports_list

mac_addr=xx-xx-xx-xx-xx-xx, vlan_id=1..4093

Example 1: addstatic 00-11-22-33-44-55 100 3

Example 2: addstatic 01-11-22-33-44-55 100 2 3 5

- **addfilter**   - add forbidden mac address

Usage: addfilter mac_addr vlan_id

mac_addr=xx-xx-xx-xx-xx-xx, vlan_id=1..4093

- **delmac**   - delete a mac address

Usage: delmac mac_addr vlan_id

mac_addr=xx-xx-xx-xx-xx-xx, vlan_id=1..4093

- clearallmac   - aging out all dynamic mac address

- clearallstatic   - clear all static mac address

- clearallfilter   - clear all forbidden mac address

- max-mac-count   - set maximum number of dynamic mac address that can be learned (per port)

 Usage: max-mac-count port_no count

port_no=1..24 or x(all)

count=0..8191

5. Sniffer

●   sniff-capture-port - set sniffer off/on, if on, assign a capture port

Usage: sniff-capture-port {off|on capture_port

Example 1: sniff-capture-port off (disable sniffer)

Example 2: sniff-capture-port on 10 (enable sniffer, copy ingress/egress traffic
  to port 10)

●   sniff-ingress-ports - duplicate the ingress traffic of some ports to
    capture port

Usage: sniff-ingress-ports monitored_ports_list

Example: sniff-ingress-ports 1 4(copy ingress traffic of port 1 to port 4)

1	2	3	4	5	6	7	8

Duplicate packet(The same with port 1)

Input Packet
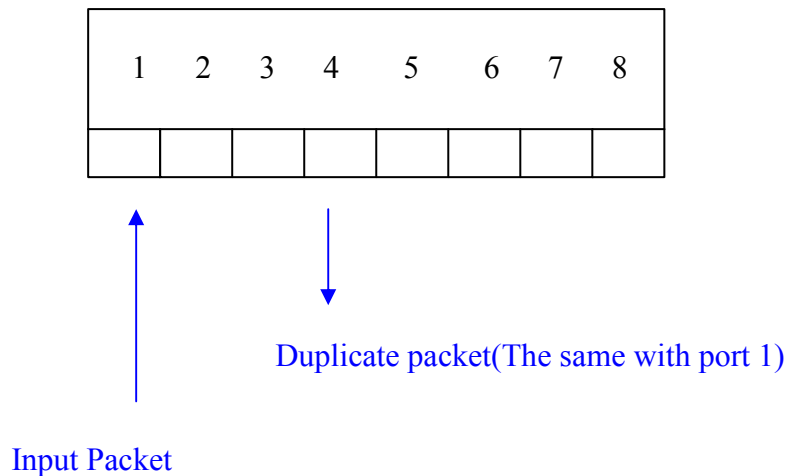
●   sniff-egress-ports - duplicate the egress traffic of some ports to
    capture port

Usage: sniff-egress-ports monitored_ports_list

Example: sniff-egress 1 4(copy egress traffic of port 1 to port 4)

1	2	3	4	5	6	7	8

Output Packet   Duplicate packet(The same with port 1)
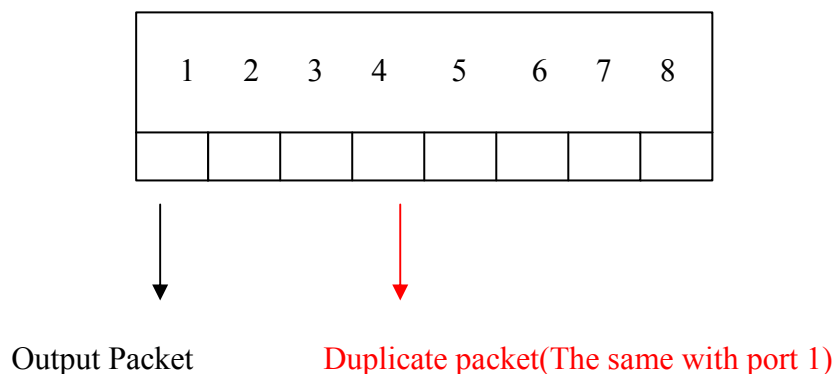
●   showsniffer   - show sniffer information

6. Rate-control

- count-ifg-pre - count interframe gap (IFG, 12 bytes per frame) and preamble (8 bytes per frame) bytes or not

Current Count IFG and Preamble: off

Usage: count-ifg-pre {on|off}

- drop-over-rate - drop or flow control if rate limit is exceeded

Current Drop Over Rate (on:drop, off:flow control): off

Usage: drop-over-rate {on|off}

- ingress-rate-control - set ingress rate control enabled/disabled (per port)

Usage: ingress-rate-control port_no {0|1}

port_no=1..24 or x(all)

1:enable ingress rate control, 0:disable

- egress-rate-control - set egress rate control enabled/disabled (per port)

Usage: egress-rate-control port_no {0|1}

port_no=1..24 or x(all)

1:enable egress rate control, 0:disable

- ingress-data-rate - set ingress data rate (per port)

Usage: ingress-data-rate port_no
{64K|128K|192K|..|1792K|2M|3M|4M|..|99M|100M}

port_no=1..24 or x(all)

the resolution from 64K (bits) to 1792K is 64K, the resolution from 2M (bits) to 100M is 1M

- egress-data-rate - set egress data rate (per port)

Usage: egress-data-rate port_no
{64K|128K|192K|..|1792K|2M|3M|4M|..|99M|100M}

port_no=1..24 or x(all)

the resolution from 64K (bits) to 1792K is 64K, the resolution from 2M (bits) to 100M is 1M

- show-rate-control - show rate control information

7. Trunking

- trunking   - set trunking (link aggregation) on/off

Current Trunking (Link Aggregation): off

Usage: trunking {on|off}

- iftrunking   - set port trunking (link aggregation, per port)

Usage: trunking port_no {off|{on|lacp_active|lacp_passive} [group_id]}

port_no=1..26 or x(all)   group_id=0..3 (default is 0)

- showtrunking   - show trunking (link aggregation)

8. STP

- **spanning-tree** - set spanning tree protocol on/off

Current spanning tree protocol: off

Usage: spanning-tree {on|off}

- **showstp** - show spanning tree protocol information

- **hello-time** - set bridge hello time

Current bridge hello time: 2

Usage: hello-time value

value=1..10, default is 2

- **forward-delay** - set bridge forward delay

Current bridge forward delay: 15

Usage: forward-delay value

value=4..200, default is 15

- **max-age** - set bridge maximum age

Current bridge maximum age: 20

Usage: max-age value

value=6..200, default is 20

- **bridge-priority** - set bridge priority

Current bridge priority: 32768

Usage: bridge-priority value

value=0..65535, default is 32768

- **port-priority** - set port priority

Usage: port-priority port_no value

port_no=1..26,

value=0..255, default is 128

- **port-path-cost** - set port path cost

Usage: port-path-cost port_no value

port_no=1..26,

value=1..255, 1000 Mbps: 4, 100 Mbps: 19, 10 Mbps: 100

9. IGMP

- igmp-snooping   - set igmp snooping on/off

Current igmp snooping: off

Usage: igmp-snooping {on|off}

- igmp-auto-aging   - set igmp auto aging on/off

Current igmp auto aging: on

Usage: igmp-auto-aging {on|off}

- igmp-leave-time   - set igmp leave (aging) time

Current igmp leave (aging) time: 60

Usage: igmp-leave-time value

value=10..255 seconds, default is 60

- showigmp   - show igmp information

CDP Function Setting

There are two commands for CDP function.

(1) LES-2224C-SFP>cdp

This command is use to set CDP function on/off.

Current CDP: on

Usage: cdp {on|off}

Example : cdp on

(2) LES-2224C-SFP>showcdp

This function will display all devices which support CDP function.

Current CDP (version 2): on

Sendind CDP packets every 60 seconds

Sendind a hold time value of 180 seconds

Example for CDP neighborhood information:

Current Neighbors:

    Port 5:

        Device ID: CISCO

        Hold Time: 168

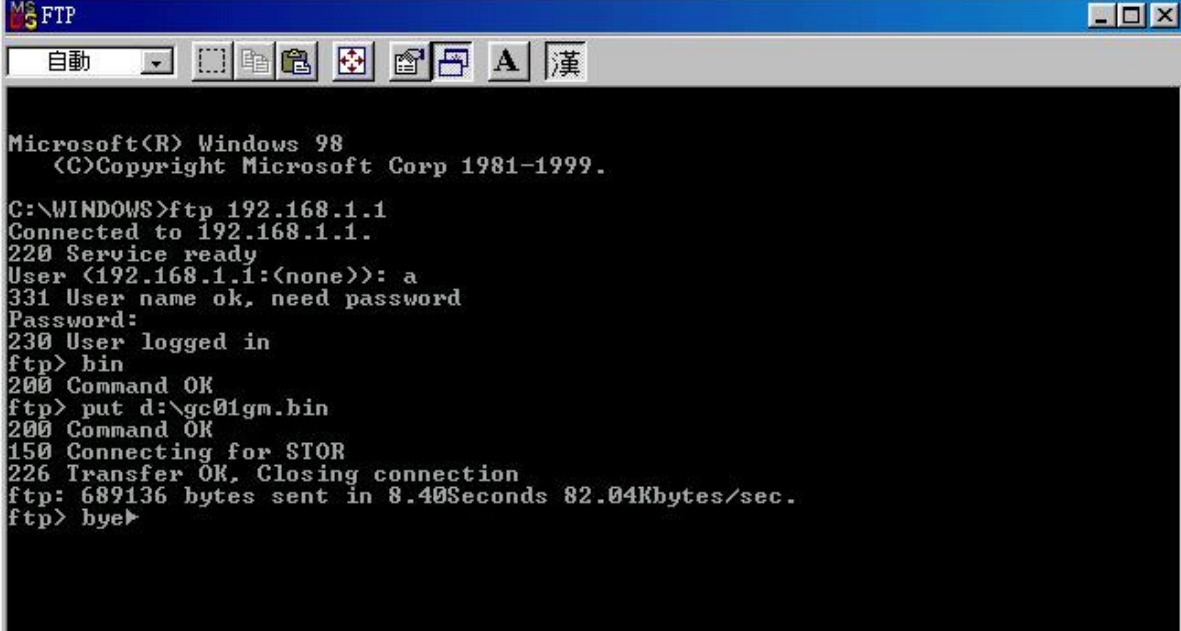   Port ID: FastEthernet0/3

        Capabilities: 0x00000028

        Platform: cisco WS-C2950-24

S/W Upgrade Procedure

This example will show how to upgrade the code by web interface.

Target box IP : 192.168.1.1

(1)Open one command box :

Key-in commands as above to transfer new code into the target box. The BIN code name is file name which you want to upgrade.

(2)Open the upgrade web page as below :

Press Upgrade key, then wait for system re-boot. The procedures are ready.