Web Smart Gigabit Ethernet Media Converter

KGC-310M

HW: Ver.C
FW: RC_1.028, C1.029 up

Installation Guide

DOC.210607A

KTI Networks Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of KTI Networks Inc. to provide notification of such revision or change.

For more information, contact:
15F-7, No. 79, Sec. 1, Hsin-Tai-Wu RD
His-chih, New Taipei City, Taiwan
Fax: 886-2-26983873
E-mail: kti@ktinet.com.tw
URL: http://www.ktinet.com.tw/

TRADEMARKS

Ethernet is a registered trademark of Xerox Corp.

FCC NOTICE

This device complies with Class A Part 15 the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received including the interference that may cause.

CE NOTICE

Marking by the symbol indicates compliance of this equipment to the EMC directive of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards:

EMC Directive 2014/30/EU

EN 55032

EN 55035

LVD 2014/35/EU

IEC 62368-1

VCCI-A NOTICE

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　　ＶＣＣＩ－Ａ

Table of Contents

1. Introduction

The device is a Gigabit Ethernet media converter series that provide the following features:

Data Conversion between different Media types and Speed

The media converter supports the following conversions:

- 1000Mbps (1000BASE-T) copper to/from 1000Mbps (1000BASE-X) fiber
- 100Mbps (1000BASE-TX) copper to/from 1000Mbps (1000BASE-X) fiber
- 10Mbps (10BASE-T) copper to/from 1000Mbps (1000BASE-X) fiber
- 1000Mbps (1000BASE-T) copper to/from 100Mbps (100BASE-FX) fiber
- 100Mbps (1000BASE-TX) copper to/from 100Mbps (100BASE-FX) fiber
- 10Mbps (10BASE-T) copper to/from 100Mbps (100BASE-FX) fiber

Dual-speed Mini-GBIC (SFP) Fiber Connectivity

The mini-GBIC (SFP) port can be installed with different optional SFP optical fiber transceiver to support multimode or single mode fiber for short reach up to long reach distance. The SFP can support both 1000BASE-X and 100BASE-FX fiber connection. This feature extends a wider application range with this device.

Loop-back Test Support

The media converter provides loop-back test function which can verify the fiber link with its link partner by sending test packets to the link partner and verifying the echo packets sent back. This feature is helpful in checking connection quality of fiber link during installation.

Link Fault Pass-Through

This feature can force the link to shut down as soon as it notices that the other link has failed. It allows a link partner on one cable segment can notice a link fault occurred on the other segment and give application a chance to react.

Remote TP Port Status Monitoring

When two devices are connected with each other via fiber link the device can monitor and display the twisted-pair port status of the remote fiber link partner. The status display can be on the local LED indicators or web management interface.

802.1Q Control

With software configuration support, the device is enhanced with more 802.1Q control features for VLAN applications rather than just a typical media converter function. The optional features include:

- Filtering all untagged packets
- Filtering all tagged packets
- Filtering tagged packets with certain VID
- Egress un-tagging
- Egress tagging
- Double tagging
- 802.1ad Q-in-Q support

Web Management

The device is embedded with an Http server which provides management functions for advanced network functions including Port Control and 802.1Q and 802.1ad functions. The management can be performed via Web browser based interface over TCP/IP network.

1.1 Features

Basic functions

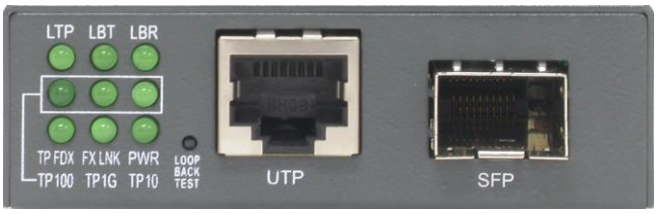
- Provides tri-speed 10/100/1000Mbps copper to 100/1000Mbps fiber conversion
- Provides SFP slot to accommodate any type of SFP fiber transceiver when needed.
- Support full wire speed Gigabit copper to Gigabit fiber conversion
- The copper port supports auto-negotiation and auto-MDI/MDI-X detection
- Copper port auto-negotiation mode, speed and duplex configuration by DIP switch settings
- Link Fault Pass Through function allows link fault status passes through between copper link and fiber link transparently.
- Far End Fault function on fiber port
- Supports 802.3x flow control for full-duplex and backpressure for half-duplex
- Supports loop-back test between two devices over fiber link
- Power saving function
- Supports remote twisted-pair status monitoring
- Diversified mounting support : desktop, wall, center rack, and optional Din-Rail support
- Center chassis installation: support installation in a center chassis rack with benefits of central software management and redundant power backup.
- Support wide range of fiber options : multimode fiber, single mode fiber (short reach up to long reach), Bi-directional single fiber, and CWDM

Management functions

- Port configuration control and status monitoring
- Supports Jumbo frame conversion
- Packet filtering
- Supports transparent forwarding
- 802.1Q Control between two ports
- Supports remote loop-back test
- Supports remote twisted-pair status monitoring
- LLDP support
- Configuration file upload and download
- In-band embedded firmware upgrade function
- Web-based browsing interface

1.2 Product Panels

The following figure illustrates the front panel and rear panel of the device:



Front

Rear

1.3 Specifications

<u>10/100/1000 Twisted-pair Copper Port (UTP, RJ-45)</u>

Compliance	IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3u 1000Base-T
Connectors	Shielded RJ-45 jacks
Pin assignments	Auto MDI/MDI-X detection
Configuration	Auto-negotiation, manual settings or software control
Transmission rate	10Mbps, 100Mbps, 1000Mbps
Duplex support	Full/Half duplex
Network cable	Cat.5 UTP

<u>Dual-speed Fiber Port (FX, SFP)</u>

Compliance	IEEE 802.3 1000Base-X, 100BASE-FX
Connectors	SFP for optional SFP type fiber transceivers
Configuration	Auto 1000Mbps Full duplex, Forced 1000Mbps Full duplex, Forced 100Mbps Full duplex
Transmission rate	1000Mbps, 100Mbps (Dual-speed support)
Network cables	MMF 50/125μm 62.5/125μm, SMF 9/125μm
Eye safety	IEC 825 compliant

<u>Loop-back Test Push Button</u>

LOOPBACK TEST	Push button to start loop-back test

LED Indicators

PWR	Power status
LTP	Local or remote TP indication on TP LEDs
LBT	Loop-back test in-progress LED
LBR	Loop-back test result LED
FXLNK	Fiber port link and activity status
TP1G	Twisted-pair copper port 1000Mbps and link status
TP100	Twisted-pair copper port 100Mbps and link status
TP10	Twisted-pair copper port 10Mbps and link status
TPFDX	Twisted-pair copper port duplex status

Configuration DIP Switches

SW1-SW3	Twisted-pair copper port configuration
SW4	Flow control setting
SW5	Remote Twisted-pair copper port monitoring
SW6	Link fault pass through function setting

Center Interface

Interface	For center chassis mounting
Connector	FutureBus

Basic Functions

MAC Addresses	Support up to 8K
Forwarding technology	Store and forward
Maximum packet length	Jumbo frame support up to 9600 bytes
Flow control	IEEE 802.3x pause frame base for full duplex operation Back pressure for half duplex operation

DC Power Input

Interfaces	DC Jack (-D 6.3mm / + D 2.0mm)
Operating Input Voltages	+5 ~ +12VDC(+/-5%)
Power consumption	3.5W max. @5V

Mechanical

Dimension (base)	108 x 72.5 x 23 mm
Housing	Enclosed metal with no fan
Mounting	Desktop mounting, wall mounting, optional Din-rail mounting

Environmental

Operating Temperature	Typical -40°C ~ +70°C (Main device)
Storage Temperature	-40°C ~ +85°C
Relative Humidity	5% ~ 90%

Electrical Approvals

FCC	Part 15 rule Class A
CE for EMC	EMC Directive 2014/30/EU
EMI standard	EN 55032
EMS standard	EN 55035
CE for Safety	LVD 2014/35/EU
Safety standard	IEC 62368-1
VCCI for EMI	VCCI-A

2. Installation

2.1 Unpacking

The product package contains:

- The media converter unit
- One power adapter
- QR code label linking to product documentation folder

2.2 Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire and damage to the product, observe the following precautions.

	Do not service any product except as explained in your system documentation.	
	Opening or removing covers may expose you to electrical shock.	
	Only a trained service technician should service components inside these compartments.	
	If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider: - The power cable, extension cable, or plug is damaged. - An object has fallen into the product. - The product has been exposed to water. - The product has been dropped or damaged. - The product does not operate correctly when you follow the operating instructions.	
	Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.	
	Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.	
		Since the surface temperature of the device may be higher than 70℃ in range of the rated operating temperatures, install and operate the product only by authorized personnel only. Install the product at a restricted area where un-authorized persons cannot reach.

2.3 Mounting the Media Converter

The media converter can be mounted on a desktop or shelf or a wall. Make sure that there is proper heat dissipation from and adequate ventilation around the device. Do not place heavy objects on the device.

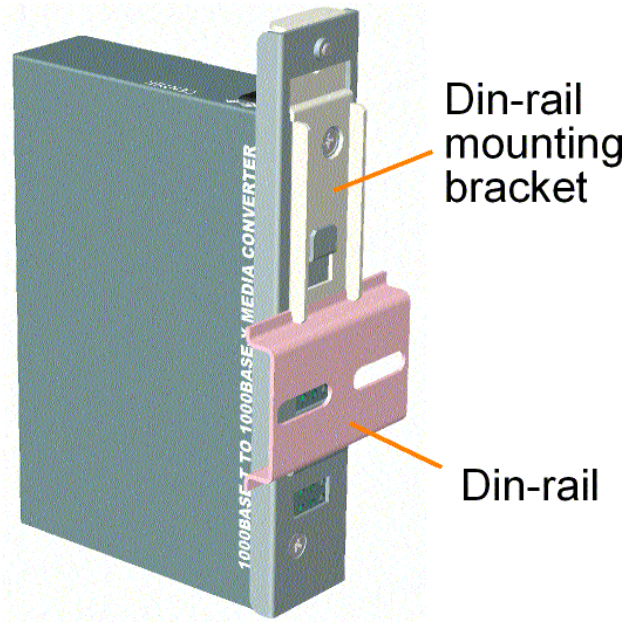
Desktop mounting

Wall mounting

The device has one mounting wall on the bottom side to support wall mounting.

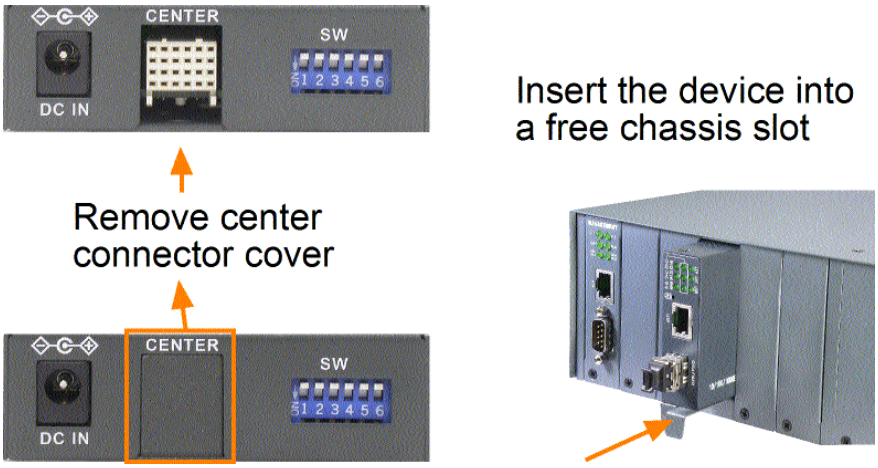
Din-Rail mounting

For a Din-Rail chassis, the device can support mounting on a Din-Rail. An optional Din-Rail bracket, KC-3DR can be purchased separately. The following figure shows an example after bracket installation:



Center rack mounting

The media converter can also be installed in KC-1300 center chassis. The center chassis provides the power supply to the converter also with optional power redundancy. Up to 16 units can be installed in one chassis. Unscrew and remove the cover of the center connector before inserting the converter into the chassis. Refer to the operation manual of center chassis KC-1300 for more information.



2.4 Applying Power

Before you begin the installation, check the AC voltage of your area. The AC power adapter which is used to supply the DC power for the unit should have the AC voltage matching the commercial power voltage in your area.

Steps to apply the power to the device are:

1. Connect power adapter DC plug to the DC input jack located on the back of the unit before connecting to the AC outlet.
2. Connect the power adapter to the AC outlet.
3. Check Power LED indication.

Note: Before you begin the installation, check the AC voltage of your area. The AC power adapter which is used to supply the DC power for the unit should have the AC voltage matching the commercial power voltage in your area.

2.5 Making UTP Connections

The 10/100/1000 twisted-pair copper (TP) port supports the following connection types and distances:

Network Cables

10BASE-T: 2-pair UTP Cat. 3,4,5 , EIA/TIA-568B 100-ohm

100BASE-TX: 2-pair UTP Cat. 5, EIA/TIA-568B 100-ohm

1000BASE-T: 4-pair UTP Cat. 5 or higher (Cat.5e is recommended), EIA/TIA-568B 100-ohm

Link distance: Up to 100 meters

Auto MDI/MDI-X Function

This function allows the port to auto-detect the twisted-pair signals and adapts itself to form a valid MDI to MDI-X connection with the remote connected device automatically. No matter a straight through cable or crossover cable is connected, the ports can sense the receiving pair automatically and configure itself to match the rule for MDI to MDI-X connection. It simplifies the cable installation.

Auto-negotiation Function

The port is featured with auto-negotiation function and full capability to support connection to any Ethernet devices. The port performs a negotiation process for the speed and duplex configuration with the connected device automatically when each time a link is being established. If the connected device is also auto-negotiation capable, both devices will come out the best configuration after negotiation process. If the connected device is incapable in auto-negotiation, the port will sense the speed and use half duplex for the connection.

Port Configuration Management

For making proper connection to an auto-negotiation INCAPABLE device, it is suggested to set port configuration to one of non-auto (forced) operating modes and specify speed and duplex mode which match the configuration used by the connected device.

Two methods for setting copper port configuration are as follows:

1. DIP SW (switches) SW1, SW2, SW3
2. Software management via web interface
   Configuration -> Ports -> TP Mode

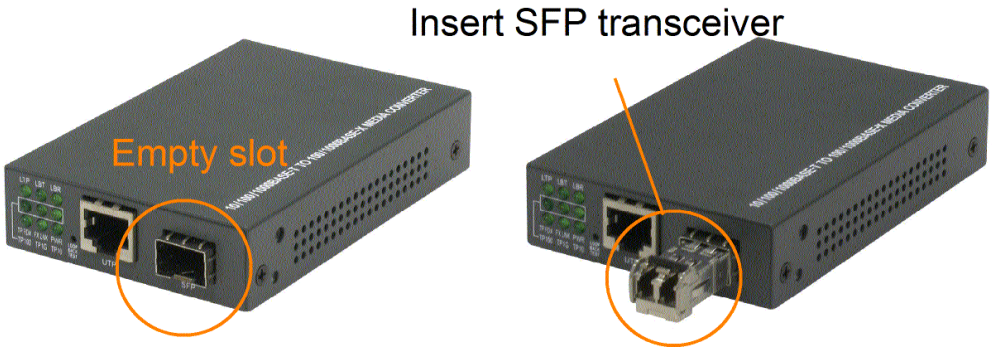
2.6 Making Fiber Connection

The mini-GBIC SFP (FX) port must be installed with an SFP fiber transceiver for making fiber connection. Your device unit may come with an SFP transceiver pre-installed when it was shipped.

Installing SFP Fiber Transceiver

To install an SFP fiber transceiver into mini-GBIC SFP port, the steps are:

1. Turn off the power to the device unit.
2. Insert the SFP fiber transceiver into the mini-GBIC port. Normally, a bail is provided for every SFP transceiver. Hold the bail and make insertion.
3. Until the SFP transceiver is seated securely in the slot, place the bail in lock position.

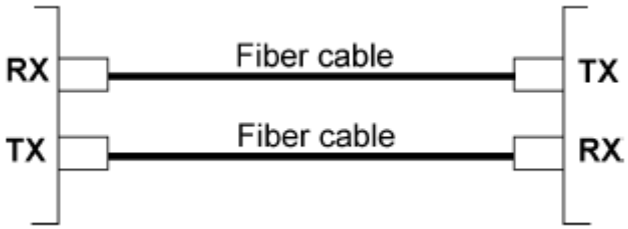


Dual Speed Support

The SFP port supports 1000BASE-X based SFP fiber transceivers and 100BASE-FX based SFP fiber transceivers. Select “Auto” for port configuration. The system will detect the type of the installed transceiver and configure the port properly and automatically during boot-up.

Connecting Fiber Cables

LC connectors are commonly equipped on most SFP transceiver modules. Identify TX and RX connector before making cable connection. The following figure illustrates a connection example between two fiber ports:



Make sure the Rx-to-Tx connection rule is followed on the both ends of the fiber cable.

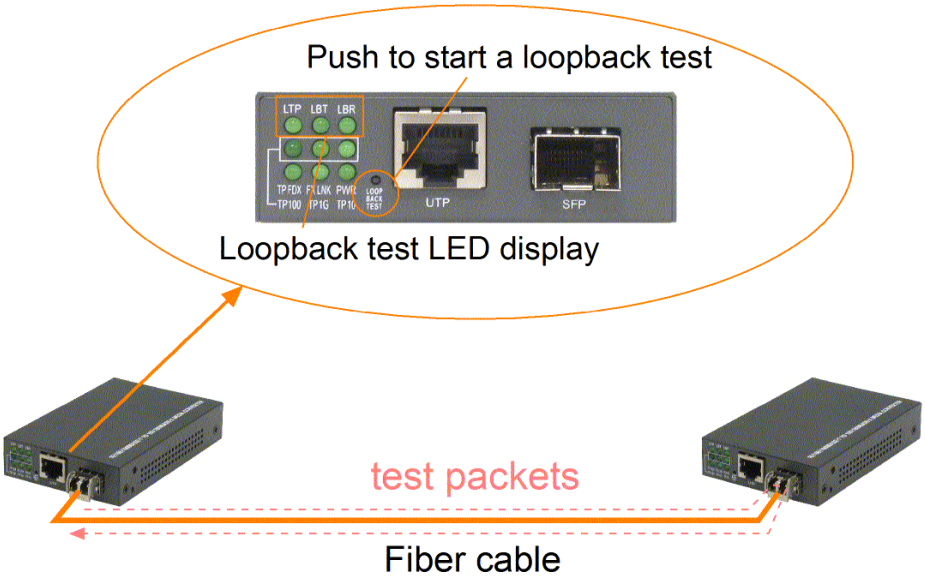
Network Cables

Multimode (MMF) - 50/125µm, 62.5/125µm

Single mode (SMF) - 9/125µm

2.7 Loop-back Test Push Button

The push button is used to perform loop-back test between two media converters connected with fiber cable as shown below:



It allows installer to perform diagnostic to the fiber link during installation and check the test result displayed on the LED indicators.

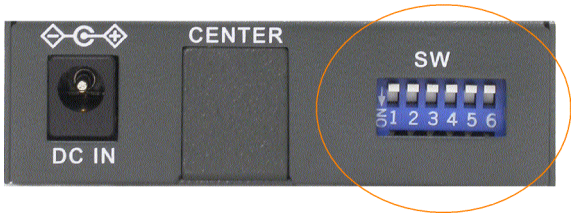
The button may also be used to restore the software configuration settings to factory default values.

The operations are:

Operations	**Functions**
Press the button and release in normal operation	Perform loop-back test over fiber cable
Press the button about 5 seconds when power up	Restore all factory default settings

2.8 Configuration DIP SW

The configuration DIP SW (setting switches) is used for setting operation configuration manually.



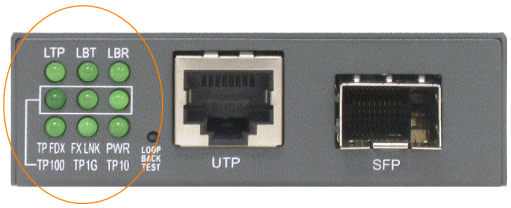
The functions of each DIP SW states are:

SW1	SW2	SW3	SW4	SW5	SW6	Function
OFF	OFF	OFF	------	------	------	Ignore DIP SW6 SW5 SW4 settings (Use software configuration for managed model)
ON	OFF	OFF	------	------	------	Set TP Port in non-auto, 10Mbps, Full duplex mode
OFF	ON	OFF	------	------	------	Set TP Port in non-auto, 10Mbps, Half duplex mode
ON	ON	OFF	------	------	------	Set TP Port in non-auto, 100Mbps, Full duplex mode
OFF	OFF	ON	------	------	------	Set TP Port in non-auto, 100Mbps, Half duplex mode
ON	OFF	ON	------	------	------	Set TP Port in auto, 1000Mbps, Full duplex mode
OFF	ON	ON	------	------	------	Disable TP Port function
ON	ON	ON	------	------	------	Set TP Port in auto, 10/100/1000Mbps, Half/Full duplex
------	------	------	OFF	------	------	Enable flow control
------	------	------	ON	------	------	Disable flow control
------	------	------	------	OFF	------	Disable remote TP status auto-report function
------	------	------	------	ON	------	Enable remote TP status auto-report on TP LEDs
------	------	------	------	------	OFF	Disable Link Fault Pass Through function
------	------	------	------	------	ON	Enable Link Fault Pass Through function

<u>Important Note:</u>

Any change of DIP SW setting will not take effect until next boot-up.

2.9 LED Indication



LED	Function	State	Interpretation
PWR	Power status	ON	The power is supplied to the unit.
		OFF	The power is not supplied to the unit.
LTP	Local TP status	ON	Local TP port status displayed on TPxxx LEDs
		OFF	Remote TP port status displayed on TPxxx LEDs
		Blink	Fail to display remote TP port status
Remark:	*1. LTP is always ON if remote TP status auto-report function is disabled.*		
	2. When remote TP status auto-report function is enabled, LTP is ON and OFF for ten seconds respectively.		
LBT	Loop-back Test	Blink	Loop-back Test in operation
		ON	Loop-back Test Result is displayed on LBR LED.
		OFF	Loop-back Test stops
Remark:	*1. LBT blinks to indicate loop-back test in operation.*		
	2. LBT is ON for 10 seconds to indicate a test result is displayed on LBR.		
LBR	Loop-back Test Result	ON	Loop-back Test OK
		Blink	Loop-back Test failed
Remark:	*1. LBR display is valid only when LBT is ON.*		
	2. LBR is displayed for 10 seconds to indicate a loop-back test result.		
FXLNK	FX port link status	ON	Link is established on FX port. (No traffic)
		Blink	Port link is up and there is traffic.
		OFF	FX port link is down.
TP1G	TP 1000M link status	ON	1000M link is established on the TP port.
		Blink	Port link is up and there is traffic.
		OFF	TP port link is down.
TP100	TP 100M link status	ON	100M link is established on the TP port.
		Blink	Port link is up and there is traffic.
		OFF	TP port link is down.
TP10	TP 10M link status	ON	10M link is established on the TP port.
		Blink	Port link is up and there is traffic.
		OFF	TP port link is down.
TPFDX	TP duplex status	ON	Full duplex on TP port
		OFF	Half duplex on TP port

2.10 Configuring IP Address and Password for the Device

For managed model, the device unit is shipped with the following factory default settings for software management:

Default IP address of the device: ***192.168.0.2 / 255.255.255.0***

The IP Address is an identification of the device unit in a TCP/IP network. Each unit should be designated a new and unique IP address in the network. Refer to Web management interface for System Configuration.

The managed device is shipped with factory default password ***123*** for software management. The password is used for authentication in accessing to the device via web-based interface. For security reason, it is recommended to change the default settings for the device unit before deploying it to your network. Refer to Web management interface for System Configuration.

3. Functions

To help a better understanding about the software management interfaces, this chapter describes some advanced functions provided by the media converter.

3.1 Abbreviation

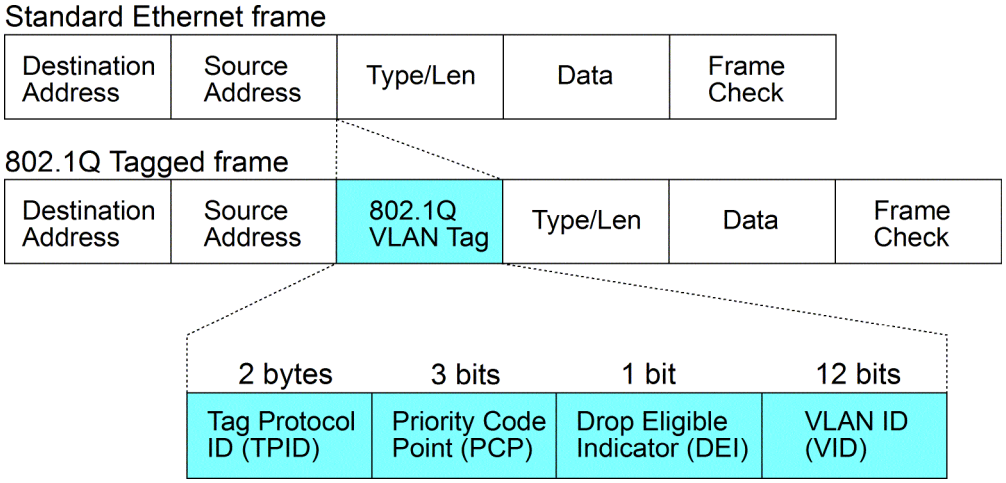
TP Port: The twisted-pair copper port of the media converter device.

FX Port: The optical fiber port of the media converter device.

Ingress Port: Ingress port is the input port on which a packet is received.

Egress Port: Egress port is the output port from which a packet is sent out.

IEEE 802.1Q Packets: A packet which is embedded with a VLAN Tag field



VLAN Tag: In IEEE 802.1Q packet format, 4-byte tag field is inserted in the original Ethernet frame between the Source Address and Type/Length fields.

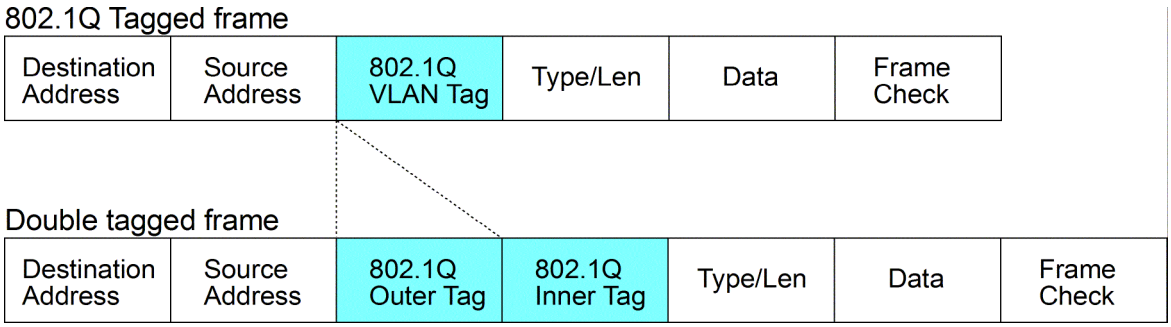
VID: VLAN identifier, 12-bit field identifies the VLAN to which the frame belongs to.

Untagged frame: A standard Ethernet frame with no VLAN Tag field

Priority-tagged frame: An IEEE 802.1Q frame which VID field value is zero (VID=0)

VLAN-Tagged frame: An IEEE 802.1Q frame which VID field value is not zero (VID>0)

Double tagging, Double Tags: With the IEEE standard 802.1ad, double-tagging can be useful for Internet service providers, allowing them to use VLANs internally while mixing traffic from clients that are already VLAN-tagged. The outer (next to source MAC and representing ISP VLAN) S-TAG (service tag) comes first, followed by the inner C-TAG (customer tag). In such cases, 802.1ad specifies a TPID of 0x88a8 for service-provider outer S-TAG.



C-tag: Tag with TPID 0x8100

S-tag: Tag with TPID 0x88A8

Priority C-tagged frame: Priority tagged frame with C-tag (TPID=0x8100, VID=0)

Priority S-tagged frame: Priority tagged frame with S-tag (TPID=0x88A8, VID=0)

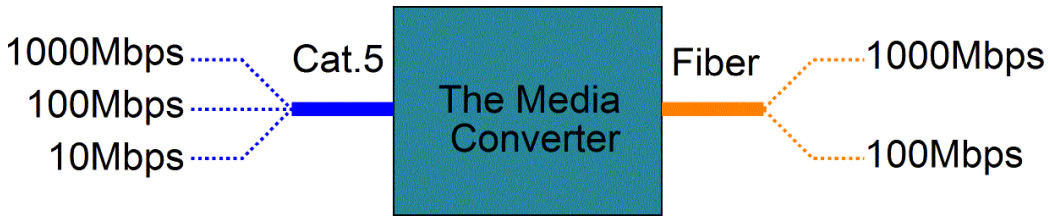
VLAN C-tagged frame: Tagged frame with C-tag (TPID=0x8100, VID>0)

VLAN S-tagged frame: Tagged frame with S-tag (TPID=0x88A8, VID>0)

PVID (Port VID): PVID is the default VID of an ingress port. It is used in 802.1Q filtering for untagged packets. It is also often used as [Default Tag - VID] for egress tagging operation.

3.2 Converter Function

The device supports the following data conversions between fiber cable and twisted-pair Cat.5 (copper) cable:

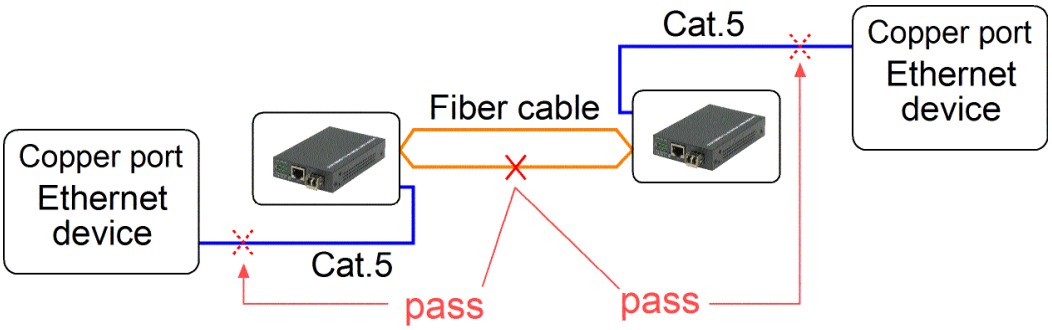


The data rate on twisted-pair segment depends on the link speed finally established with the link partner.

3.3 Link Fault Pass Through Function

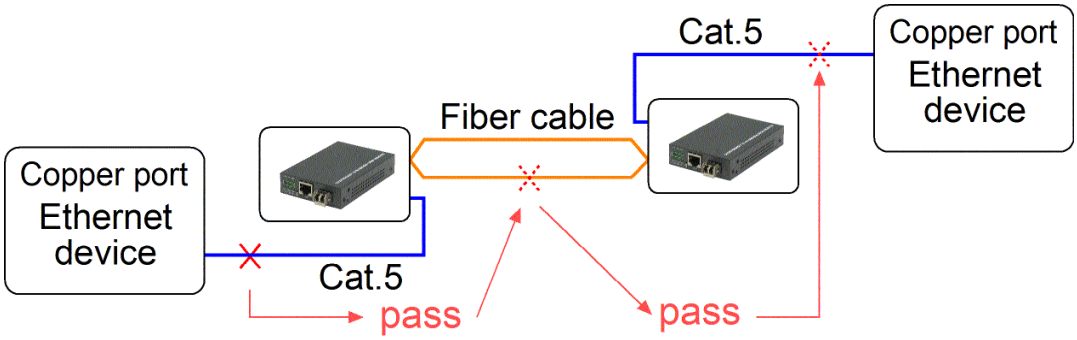
When the Link Fault Pass Through (LFPT) function is enabled and the media converter detects a link fault on one port segment, it will force the other port segment link down. It looks like that a link fault is passed from one port to the other.

The following example illustrates a link fault occurs on the fiber cable (any one cable in a duplex fiber connection). The link fault is forwarded to both copper link partners finally by LFPT operation of two media converters.



Both Ethernet devices will also detect a link fault on each Cat.5 connection, although the real fault occurs on the fiber connection exactly.

The following example illustrates a real link fault occurs on one Cat.5 and the link fault is passed to the other Cat.5 over two converters and the fiber cable by LFPT operation. Finally, the other link partner also detects a link fault.



Advantage

The function allows two remote link partners of the media converters detect the link fault finally no matter where the exact fault occurs. It allows the upper application takes necessary action in case a real link fault occurs in any cable segment.

Methods to enable the function

The LFPT function can be enabled by:

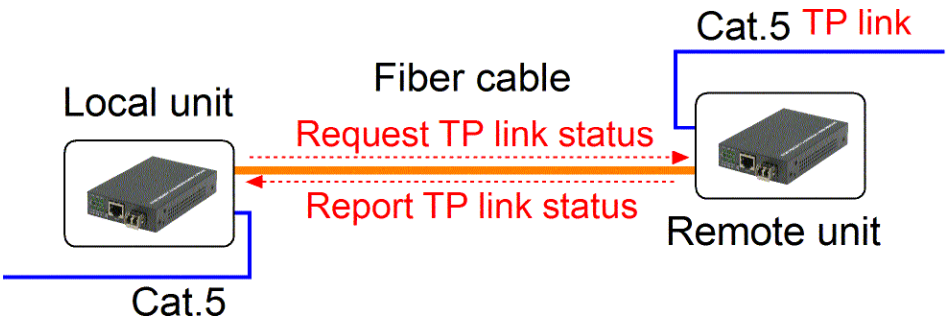
Hardware setting: DIP SW6 is set to ON position

Software setting: Web management ->

Configuration -> System -> [Link fault pass through]

3.4 Remote TP Status Monitoring Function

The local media converter can monitor the TP port link status of its remote link partner connected on the fiber cable. The status is displayed on the local LED indicators as follows:



Methods to enable the function

Hardware setting: DIP SW5 is set to ON position

Software setting: Web management ->

Configuration -> System -> [Remote TP auto report]

Remote TP Status Display

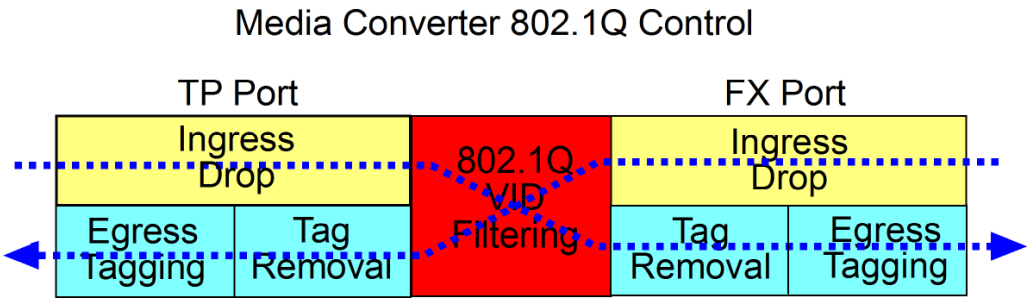
1. The status is displayed on local LEDs - TP1G, TP100, TP10 and TPFDX when LTP is OFF.

LED	State	Status
LTP	**OFF**	**Remote TP status is valid on the following LEDs**
TP1G	ON	Remote TP link in 1000Mbps
	OFF	Remote TP link down
TP100	ON	Remote TP link in 100Mbps
	OFF	Remote TP link down
TP10	ON	Remote TP link in 10Mbps
	OFF	Remote TP link down
TPFDX	ON	Remote TP link in full duplex
	OFF	Remote TP link in half duplex

2. Web management -> Monitoring -> Statistics -> Remote TP [Link]

3.5 802.1Q Control Function

802.1Q Control function allows perform 802.1Q VLAN related operation to the packets passing through the media converter according packet contents as follows:



[Ingress Drop] setting

The setting is the first filtering mechanism to filter incoming packets based on frame types. The options are:

Disable - disable port ingress drop and admit all packet types

Drop Untag - drop all untagged frames

Drop C-tag - drop frame with outer tag TPID 0x8100

Drop S-tag - drop frame with outer tag TPID 0x88A8

Drop All taggged - drop frames with outer tag TPID 0x8100 or 0x88A8

802.1Q VID Filtering

802.1Q VID Filtering function allows to admit or reject certain VID tagged packets. Up to 16 "*allowed*" (positive list) or "*rejected*" (negative list) VIDs can be configured. This function allows limit certain frames to pass from one link segment to another one. Disabling 802.1Q filtering function also sets VLAN to "Port-based" mode. Enabling the function sets VLAN to "VLAN aware" mode.

[VID Table]

Disable - 802.1Q VID filtering is disabled.

Allowed VID - Only the frames with classified VIDs in VID table are admitted.

Rejected VID - The frames with classified VIDs in VID table are rejected and dropped.

Each ingress frame is classified via VLAN classification and gets one Classified Tag. The Classification Tag is bundled to the frame in passing through VLAN operation until egress. Refer to next section for more information.

[Tag Removal] setting

This setting is used to remove tags of the incoming frames if available. The options are:

Keep All tags - disable tag removal

Pop up 1 tag - remove up to 1 tag (outer tag if available)

Pop up 2 tag - remove up to 2 tags (outer and inner tag if available)

Egress Tagging – [Egress Tagging Rule] setting

Tag is inserted into the outgoing frame in egress operation.

Type 0 – Port Egress Tagging disabled

Type 1 – Tag all frames

Type 2 – Tag all frames, except priority-tagged frames (VID=0) and frame with VID= Exceptional VID

Type 3 – Tag all frames, except priority-tagged frames (VID=0)

Egress Tagging - [Tagging Exceptional VID (Type 2)] setting

Type 2 exceptional VID in Tagging rule, *1 ~ 4095* - decimal 12-bit VID value

3.5.1 VLAN Operation

This section describes the operation relations between different configuration settings.

<table>
<tr><td colspan="2">[802.1Q Filtering] setting options</td><td>Disable</td><td>Allowed VIDs
Rejected VIDs</td></tr>
<tr><td colspan="2">VLAN operation for TP port and FX port</td><td>Port-based mode</td><td>VLAN aware mode</td></tr>
<tr><td rowspan="3">Each ingress frame is classified with one Classified Tag:
(outer tag is classified if double tagged)</td><td rowspan="3">Classified Tag – VID, PCP, DEI, TPID</td><td rowspan="3">For all types of ingress frames
Classified Tag =>
VID= [Default Tag – VID]
PCP= [Default Tag – PCP]
DEI= [Default Tag – DEI]
TPID=0x8100</td><td>For untagged frames
Classified Tag =>
VID= [Default Tag – VID]
PCP= [Default Tag – PCP]
DEI= [Default Tag – DEI]
TPID=0x8100</td></tr>
<tr><td>For priority tagged frame
Classified Tag =>
VID= [Default Tag – VID]
PCP= Frame outer tag – PCP
DEI= Frame outer tag – DEI
TPID= Frame outer tag – TPID</td></tr>
<tr><td>For all tagged frame
Classified Tag =>
VID= Frame outer tag – VID
PCP= Frame outer tag – PCP</td></tr>
</table>

			DEI= Frame outer tag – DEI *TPID= Frame outer tag – TPID*
VID Filtering		*No filtering*	*For untagged frames =>* *No filtering*
			For other types of frames => *Filtering based on VID table configuration and the classified Tag – VID*
			Note: *[Management VLAN] – VID,* *TP port PVID and FX port PVID are always permitted.*
[Egress Tagging Rule] options		*Type 0, Type 1*	*Type 0, Type 1,Type 2,Type 3*
[Egress Tag TPID] options		*0x8100(C-tag)* *0x88A8(S-tag)* *s-customer-tag 1*	*0x8100(C-tag)* *0x88A8(S-tag)* *s-custom-tag 1* *s-custom-tag 2*
Egress tagging operation	**Inserted Tag - VID, PCP, DEI**	*Use Classified Tag - VID, PCP, DEI*	*Use Classified Tag - VID, PCP, DEI*
	Inserted Tag - TPID	*[Egress Tag TPID] = 0x8100(C-tag) or 0x88A8(S-tag) => Use the setting value*	*[Egress Tag TPID] = 0x8100(C-tag) or 0x88A8(S-tag) => Use the setting value*
		[Egress Tag TPID] = s-custom-tag 1 => *Use [Custom TPID] setting*	*[Egress Tag TPID] = s-custom-tag 1 =>* *Use [Custom TPID] setting*
			[Egress Tag TPID] = s-custom-tag 2 => *Use [Custom TPID] setting if Classified Tag TPID = 0x88A8* *All other cases, use 0x8100(C-tag)*

3.6 SNMP Trap Function

SNMP trap function allows the device to send trap message to an SNMP trap host over SNMP protocol when the associated trap event occurs.

SNMP Trap settings

The settings are used to configure a trap host who can receive the SNMP trap message issued from a media converter device unit.

[SNNP Trap destination]

The IP address of the target SNMP trap host who is allowed to receive the traps.

[SNMP Trap community]

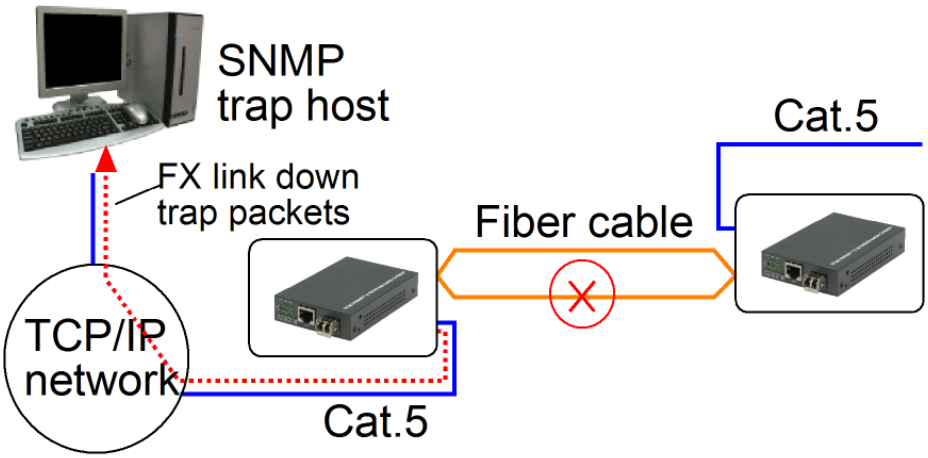
The community string bound in a trap message

SNMP Trap events

The following events are defined for generating a trap message when the event occurs on the unit.

- The device boot up.
- TP copper port link down
- TP copper port link up (link recovery).
- FX fiber port link down
- FX fiber port link up (link recovery).

The following example illustrates an event of FX port link down occurs and is detected by the device. Then, it generates a trap message to the SNMP trap host PC.



4. Web Management

The media converter features an http server which can serve the management requests coming from any web browser software over TCP/IP network.

Set IP Address for the System Unit

Before the device unit can be managed from a web browser software, make sure a unique IP address is configured for the unit.

4.1 Start Browser Software and Making Connection

Start your browser software and enter the IP address of the unit to which you want to connect. The IP address is used as URL for the browser software to search the device.

```
URL: http://xxx.xxx.xxx.xxx/
```

Factory default IP address: 192.168.0.2

Factory default password: 123↵

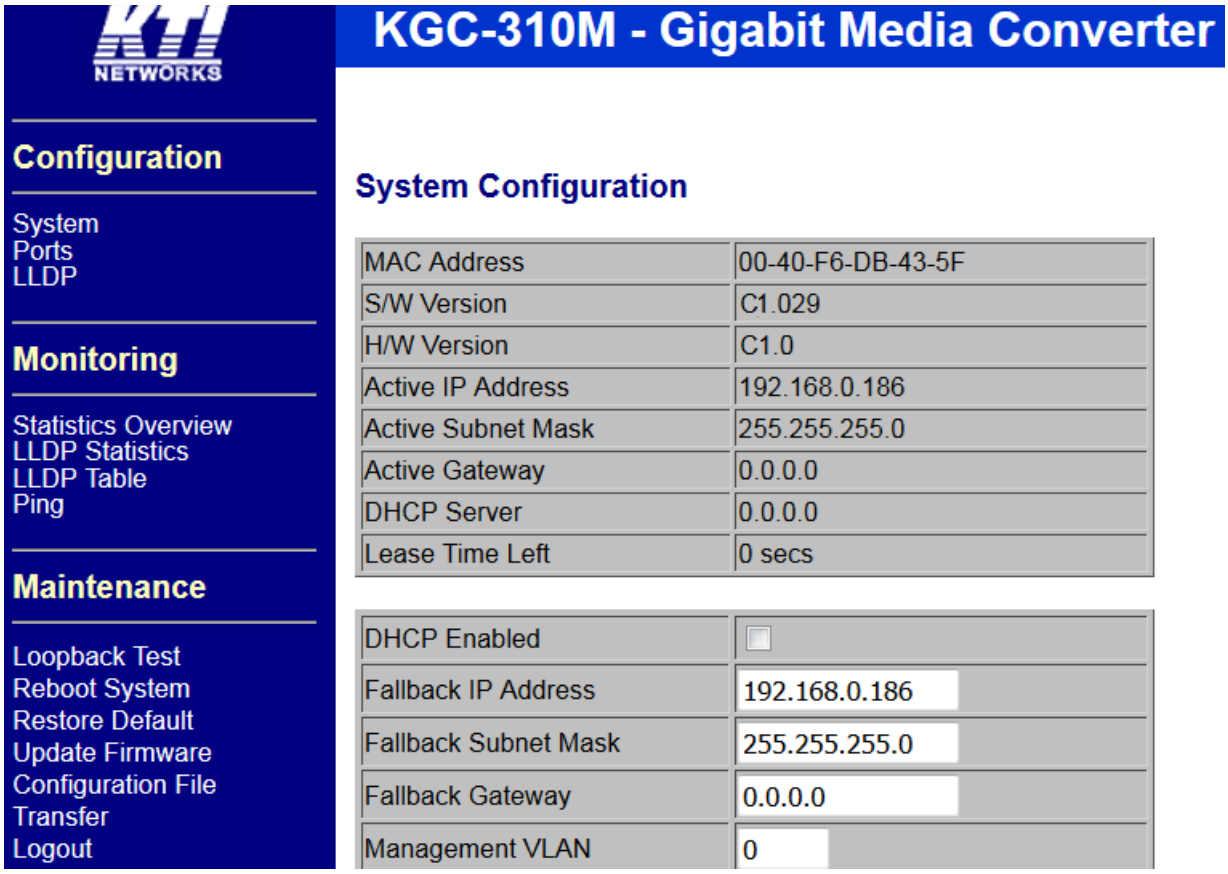
4.2 Login to the Device Unit

When browser software connects to the device unit successfully, a Login screen is provided for you to login to the device as follows:

The device will accept only one successful management connection at the same time. The other connection attempts will be prompted with a warning message.

A new connection will be accepted when the current user logout successfully or auto logout by the device due to no access for time out of 5 minutes. *System Configuration* is displayed after a successful login.

4.3 Main Management Menu



The following information describes the basic functions of the main menu.

Configuration

System	Device information, system and IP related settings
Ports	Port link status, operation mode configuration and other per port settings
LLDP	Settings for LLDP support

Monitoring

Statistics Overview	List statistics for the local ports and remote TP port link status
LLDP Statistics	Statistics counters of LLDP operation
LLDP Tables	LLDP information received
Ping	Ping utility command

Maintenance

Loopback Test	Command to perform loop-back test on fiber link
Reboot System	Command to reboot the device unit
Restore Default	Command to restore the device unit with factory default settings

Update Firmware	Command to update the device's firmware
Configuration File Transfer	Configuration file download & upload
Logout	Command to logout from current web management

4.4 Configuration

4.4.1 System

System Configuration

MAC Address	00-40-F6-DB-43-5F
S/W Version	C1.029
H/W Version	C1.0
Active IP Address	192.168.0.186
Active Subnet Mask	255.255.255.0
Active Gateway	0.0.0.0
DHCP Server	0.0.0.0
Lease Time Left	0 secs

DHCP Enabled	☐
Fallback IP Address	192.168.0.186
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	0.0.0.0
Management VLAN	0
Name	
Password	●●●
Inactivity Timeout (secs)	300 (0 or 60~10000)
SNMP enabled	☑
SNMP Trap destination	0.0.0.0
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Community	public

802.1Q Control	○ Enable ◉ Disable
Jumbo Mode	○ Enable ◉ Disable
Link fault pass through	○ Enable ◉ Disable
Remote TP auto report	○ Enable ◉ Disable
Power Saving Mode	○ Enable ◉ Disable
Drop frames after excessive collisions	○ Enable ◉ Disable
BPDU Transparent	◉ Enable ○ Disable

Apply Refresh

Configuration	Description
MAC Address	The MAC address factory configured for the switch. It can not be changed in any cases.
S/W Version	Firmware version currently running
H/W Version	Hardware version currently operating
Active IP Address	Current IP address for the switch management
Active Subnet Mask	Current subnet mask for IP address for the switch management
Active Gateway	Current gateway IP address for the switch management
DHCP Server	Current IP address of the DHCP server
Lease Time Left	The time left for the lease IP address currently used
DHCP Enabled *[2]	Use DHCP to get dynamic IP address configuration for the switch
Fallback IP Address	IP address used when DHCP mode is disabled
Fallback Subnet Mask	Subnet mask for IP address used when DHCP mode is not enabled
Fallback Gateway	Default gateway IP address used when DHCP mode is not enabled
Management VLAN	Set management VLAN ID
Name *[1]	Set the system name for this switch unit
Password	Set new password
Inactivity Timeout	No user interaction timeout for web disconnection (Auto logout). Options: 0 - no timeout 60 ~ 10000 seconds
SNMP enabled	Enable SNMP agent
SNMP Trap destination	The IP address of the SNMP trap manager
SNMP Read community	SNMP community allowed for the SNMP [get] message
SNMP Write community	SNMP community allowed for the SNMP [set] message
SNMP Trap community	SNMP community used for the SNMP trap messages sent by the switch
802.1Q Control	802.1Q Control function main configuration *Disable* - all packets are allowed to pass with no 802.1Q control. *Enable* - 802.1Q control mechanism is activated for the conversion.
Jumbo Mode	Enable / disable Jumbo mode to support jumbo packets *Disable* - support maximum packet size up to 1526 bytes *Enable* - support maximum packet size up to 9600 bytes
Link fault pass through	Enable / disable link fault pass through function
Remote TP auto report	Enable / disable remote TP port link status function
Power Saving Mode	Enable / disable port link down power saving mode
Drop frame after excessive collision	

	Enable - A frame is discarded and counted as an excessive collision if 16 collisions occur for this frame. *Disable* – Not discarded
BPDU_Transparent *[3]	Enable / disable BPDU & LLDP packet transparent forwarding
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

Note:

1. *It is suggested to give each switch unit a system name as an alternative unique identification beside IP address.*
2. *Setting change of DHCP mode takes effective in next boot-up.*
3. *Enabling [BPDU_Transparent] allows BPDU and LLDP packets are forwarded between UTP port and FX port transparently and LLDP support is forced to disable.*

4.4.1.1 Management VLAN

Management VLAN settings allow administrator to access the device and perform the management over a dedicated VLAN.

The following rules are applied with the Management VLAN:

1. If [Management VLAN] setting is VID=0, no limitation is applied in accessing the web management interface, but password authentication.
2. If [Management VLAN] setting is VID>0, the web (http) server only replies to the management hosts through the tagged packets with the embedded VID same as the configured [Management VLAN] setting.
3. The web (http) server can accept untagged or tagged management accessing packets. Reply to the web access host based on the following rule:

Incoming web access packets	**Reply packets (Outgoing to the management host)**
Untagged packets	None
Tagged packets	Packets tagged with configured management VLAN VID

4. The configured VID is always included in permitted VID list under "802.1Q VID Filtering" function.

Notes:

No matter how management VLAN is configured, login password authentication is still required.

4.4.2 Ports

Port Configuration

Port	TP	FX
Link	1000FDX	Down
Mode	Auto	Auto
Flow Control	☑	☑

Apply Refresh

Port Configuration	Function
Port	TP - Twisted-Pair copper port (also specified Port #1 in other pages) FX - Fiber port (also specified Port #2 in other pages)
Link	Port link status *Speed and duplex status with green background* - port is link on *Down with red background* - port is link down
Mode	Select port operating mode *Disabled* - disable the port operation

TP Mode	*Auto-negotiation*	*Speed capability*	*Duplex*
Auto	*Enable*	*10, 100, 1000M*	*Full, Half*
Forced 10 Half	*Disable*	*10M*	*Half*
Forced 10 Full	*Disable*	*10M*	*Full*
Forced 100 Half	*Disable*	*100M*	*Half*
Forced 100 Full	*Disable*	*100M*	*Full*
1000 Full	*Enable*	*1000M*	*Full*

FX Mode	*Auto-negotiation*	*Speed capability*	*Duplex capability*
Auto: auto-detection for transceiver type and speed			
1000 Full	*Enable*	*1000M*	*Full*
Forced 1000 Full	*Disable*	*1000M*	*Full*
Forced 100 Full	*Disable*	*100M*	*Full*
Disable: Disable port operation			

Flow Control	Set port flow control function *V* - set to enable 802.3x pause flow control for ingress and egress
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

802.1Q Control Page when [802.1Q Filtering] function is disabled

802.1Q Control

Port	TP	FX
Default Tag - VID(PVID)	1	1
Default Tag - DEI	0	0
Default Tag - PCP	0	0
Ingress Drop	Disable	Disable
Tag Removal	Keep All tags	Keep All tags

Port	TP	FX
Egress Tagging Rule	Type 0	Type 0
Egress Tag TPID	0x8100(c-tag)	0x8100(c-tag)
Custom TPID	0x8100	

802.1Q Filtering	Disable (Port-base)
	Setting

Apply Refresh

802.1Q Control Page when [802.1Q Filtering] function is enabled. The setting is "*Allowed VID*" or "*Rejected VID*"

802.1Q Control

Port	TP	FX
Default Tag - VID(PVID)	1	1
Default Tag - DEI	0	0
Default Tag - PCP	0	0
Ingress Drop	Disable	Disable
Tag Removal	Keep All tags	Keep All tags

Port	TP	FX
Egress Tagging Rule	Type 0	Type 0
Tagging Exceptional VID (Type 2)	1	1
Egress Tag TPID	0x8100(c-tag)	0x8100(c-tag)
Custom TPID	0x8100	

802.1Q Filtering	Rejected (VLAN-aware)
	Setting

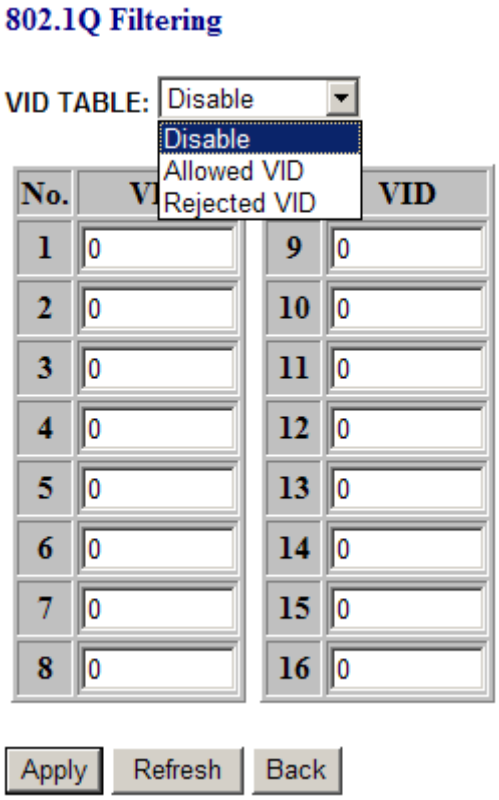
Apply Refresh

802.1Q Control	Function
Default Tag – VID (PVID)	Port VID, VID for Ingress Default Tag, also called "PVID" *1 ~ 4095* - decimal 12-bit VID value
Default Tag - DEI	CFI for Ingress Default Tag *0, 1* - 1-bit CFI value
Default Tag -PCP	User priority for Ingress Default Tag *0 ~ 7* - decimal 3-bit value
Ingress Drop	*Disable* - disable port ingress drop and admit all packet types *Drop Untag* – drop all untagged frames *Drop C-tag* – drop frame with outer tag TPID 0x8100 *Drop S-tag* – drop frame with outer tag TPID 0x88A8 *Drop All taggged* – drop frames with outer tag TPID 0x8100 or 0x88A8
Tag Removal	*Keep All tags* - disable tag removal for VLAN-tagged packets

	Pop up 1 tag – remove up to 1 tag (outer tag if available) *Pop up 2 tag* – remove up to 2 tags (outer and inner tag if available)
Egress Tagging Rule	Tag is inserted into the outgoing packet in egress operation. *Type 0* – Port Egress Tagging disabled *Type 1* – Tag all frames *Type 2* – Tag all frames, except priority-tagged frames (VID=0) and frame with VID= Exceptional VID *Type 3* – Tag all frames, except priority-tagged frames (VID=0) ** "Type 2" and "Type 3" are available only when 802.1Q Filtering is enabled.*
Tagging Exceptional VID (Type 2)	
	Type 1 exceptional VID in Tagging rule *1 ~ 4095* - decimal 12-bit VID value ** This configuration is available only when 802.1Q Filtering is enabled.*
Egress Tag TPID	Tag TPID for Egress Tagging *0x8100(c-tag)* *0x88A8(s-tag)* s-*custom_tag 1* – Use value configured in [Custom TPID] s-*custom_tag 2* - Use value configured in [Custom TPID] if ingress tag was s-tag (TPID = 0x88A8) ** "s-custom-tag 2" is available only when 802.1Q Filtering is enabled.*
Custom TPID	Specify a user-defined TPID value.
[802.1Q Filtering]	Click to set VID filtering table

Note:
Refer to Section 3.5 and 3.5.1 for more information about:
802.1Q Control, VLAN operation, Ingress VLAN Classification, Classified Tag after VLAN classification and What tag is inserted for egress tagging. Section 3.5.1 also describes the VLAN mode under different [802.1Q Filtering] settings.

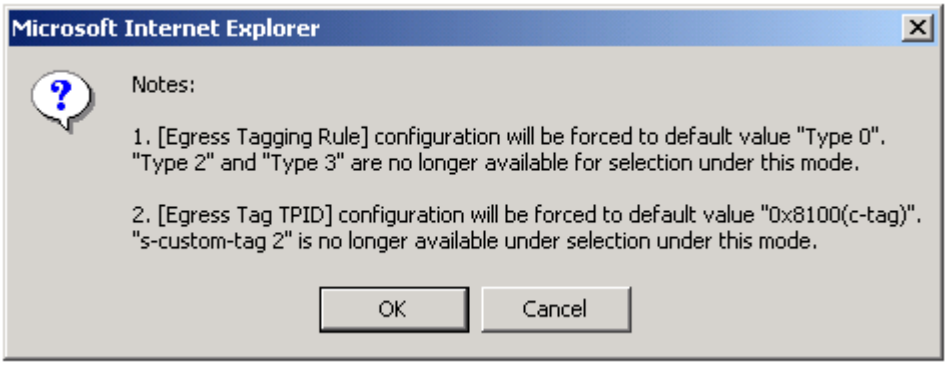
4.4.2.1 802.1Q Filtering



Configuration	Description
VID TABLE	Specify the characteristic of the VID table. *Disable* - set to disable 802.1Q filtering function. *Allowed VID* - the VID table specifies the allowed VIDs *rejected VID* - the VID table specifies the rejected VIDs * *Both Allowed VID and rejected VID are used to "Enable" 802.1Q filtering.*
No.	Entry of VID table - up to 16 VIDs can be configured in VID table
VID	*1 ~ 4095* - decimal 12-bit VID value
[Apply]	Click to apply the configuration change.
[Refresh]	Click to refresh current configuration.
[Back]	Click to previous window.

As VID TABLE setting is changed from "*Disable*" to enabled state. That is a setting of either "*Allowed VID*" or "*Rejected VID*". The following message is prompt for notices and confirmation.

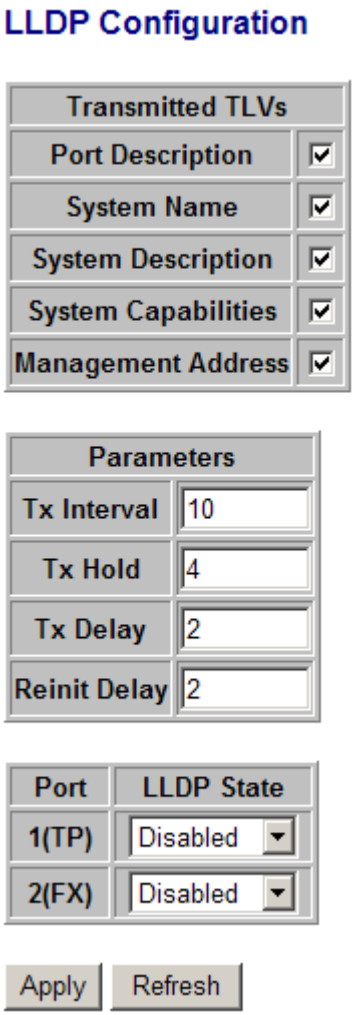
When VID TABLE setting is changed from either "*Allowed VID*" or "*Rejected VID*" to "*Disable*", the following message is also prompt for notices and confirmation.



Notes:

1. *VID table is referred for filtering VLAN-tagged frames according to the classified VID of each ingress frame. Refer to Section 3.5.1 for more information about "classified VID" and VLAN operation.*
2. *[Allowed VID] setting is useful when only certain VIDs are permitted to pass the device.*
3. *[Rejected VID] setting is useful when only certain VIDs are not allowed to pass the device.*
4. *The VID value in [Management VLAN] setting and [Default Tag – VID (PVID)] for TP port and FX port are always permitted to pass and not be filtered.*

4.4.3 LLDP



Transmitted TLVs	Description
Port Description	When checked the “port description” is included in LLDP information transmitted.
System Name	When checked the “system name” is included in LLDP information transmitted.
System Description	When checked the “system description” is included in LLDP information transmitted.
System Capability	When checked the “system capability” is included in LLDP information transmitted.
Management Address	When checked the “management address” is included in LLDP information transmitted.

Parameters	Description
Tx Interval	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between

	each LLDP frame is determined by the Tx Interval value. Valid values: ***5 – 32768*** *seconds*
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values: ***2 – 10 times***
Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values: ***1 – 8192 seconds***
Reinit Delay	When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Reinit Delay** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values: ***1 – 10 seconds***

Port Configuration	**Description**
Port	Local port number (Port #1: TP port, Port #2: FX port)
LLDP State	Set port LLDP mode: *Disabled:* The device will not send out LLDP information, and will drop LLDP information received from neighbors. BPDU and LLDP packets will be filtered and dropped. *Tx and Rx:* The device will send out LLDP information, and will analyze LLDP information received from neighbors. *Tx only:* The switch will drop LLDP information received from neighbors, but will send out LLDP information. *Rx only:* The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
[Apply]	Click to apply the configuration change.
[Refresh]	Click to refresh current configuration.

*The **Link Layer Discovery Protocol (LLDP)** is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet.*

4.5 Monitoring

4.5.1 Statistics Overview

Statistics for all ports

Clear Refresh

Port	TP	FX	Remote TP
Link	1000FDX	Down	Down
Tx Bytes	1294693	0	-
Tx Frames	13780	0	-
Rx Bytes	138578540	0	-
Rx Frames	781206	0	-
Tx Errors	0	0	-
Rx Errors	0	0	-

Statistics	**Description**
Port	TP - Twisted-Pair copper port on local unit FX - Fiber port on local unit Remote TP - TP port of the remote unit connected on the fiber link
Link	Port link status Speed and duplex status with green background - port is link on Down with red background - port is link down
Tx Bytes	Total of bytes transmitted on the port
Tx Frames	Total of packet frames transmitted on the port
Rx Bytes	Total of bytes received on the port
Rx Frames	Total of packet frames received on the port
Tx Errors	Total of error packet frames transmitted on the port
Rx Errors	Total of error packet frames received on the port
[Clear]	Click to reset all statistic counters
[Refresh]	Click to refresh all statistic counters

4.5.2 LLDP Statistics

LLDP Statistics

Port	Tx Frames	Rx Frames	Rx Error Frames	Discarde Frames	TLVs discarded	TLVs unrecognized	Org. TLVs discarded	Ageouts
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0

Refresh

Counters	**Description**
Port	The port on which LLDP frames are received or transmitted. (Port #1: TP port, Port #2: FX port)
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Error Frames	The number of received LLDP frames containing error.
Discarde Frames	If an LLDP frame is received on a port, and the device's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. TLVs discarded	The number of organizationally received TLVs.
Ageouts	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Ageout counter is incremented.
[Refresh]	Click to refresh all statistic counters

4.5.3 LLDP Table

LLDP Neighbour Table

Local Port	Chassis Id	Remote Port ID	System Name	Port description	System Capabilities	Management Address
No entries in table						

Refresh

Status	Description
Local Port	The port on which the LLDP frame was received. (Port #1: TP port, Port #2: FX port)
Chassis Id	The Chassis Id is the identification of the neighbor's LLDP frames.
Remote Port ID	Port ID of the neighbor port
System Name	System Name advertised by the neighbor unit
Port Description	The port description advertised by the neighbor unit
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. *Other* 2. *Repeater* 3. *Bridge* 4. *WLAN Access Point* 5. *Router* 6. *Telephone* 7. *DOCSIS cable device* 8. *Station only* 9. *Reserved* When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.
[Refresh]	Click to refresh all statistic counters

4.5.4 Ping

Ping Parameters

Target IP address	
Count	1
Time Out (in secs)	1

Apply

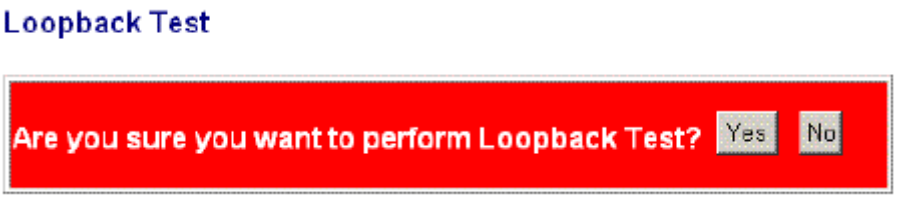
Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Ping	**Description**
Target IP Address	The target IP address to which the ping command issues
Count	The number of ping commands generated
Time Out (in secs)	The time out for a reply (in seconds)
[Apply]	Start the ping command
Results	**Description**
Target IP Address	The target IP address to which the ping command issues
Status	The command status
Received replies	The number of replies received by the system
Request time-outs	The number of requests time out
Average Response Time	The average response time of a ping request (in mini-seconds)
[Refresh]	Click to refresh all statistic counters

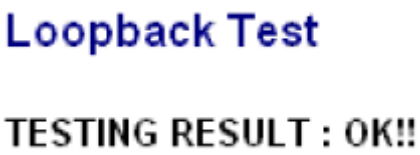
4.6 Maintenance

4.6.1 Loop-back Test



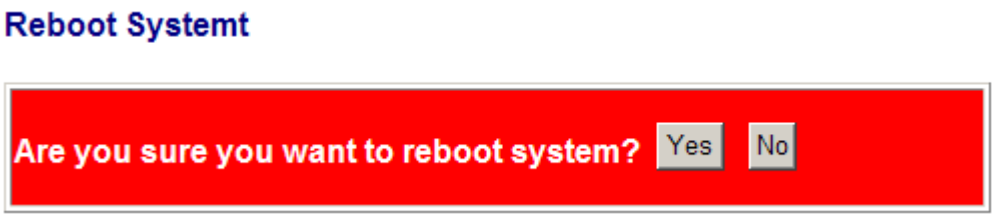
This menu is used to start a loop-back test operation with the link partner unit over the fiber link. The message displayed during test is:

The result message displayed after a test finished is:



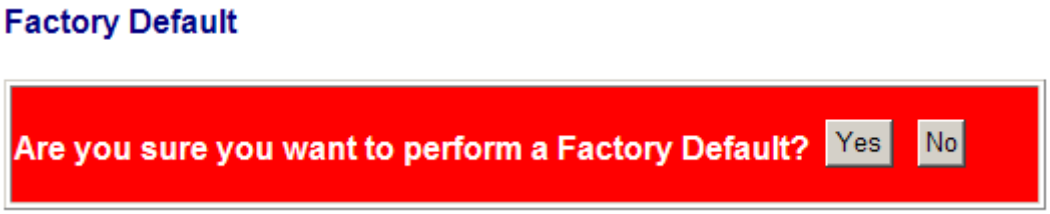
The test result is also displayed on LEDs - LBT and LBR.

4.6.2 Reboot System



This menu is used to reboot the device unit remotely with current configuration. Starting this menu will make your current http connection lost. You must rebuild the connection to perform any management operation to the unit.

4.6.3 Restore Default



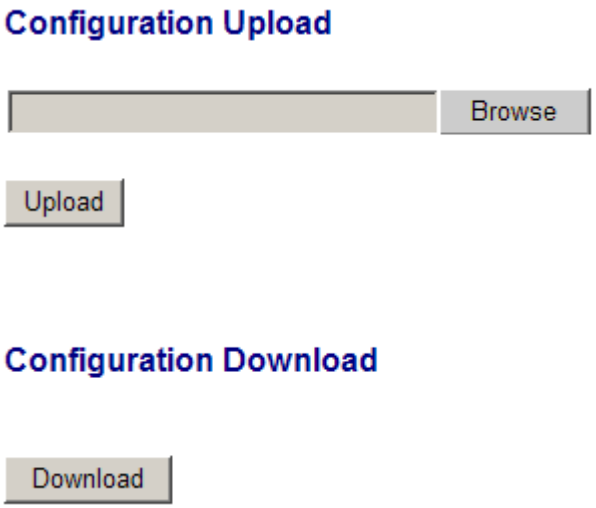
This menu is used to restore all settings of the device unit with factory default values except current IP configuration and Management VLAN configuration.

4.6.4 Update Firmware

This menu is used to perform in-band firmware (software) upgrade. Enter the path and file name of new firmware image file for uploading.

Configuration	Description
Filename	Path and filename (warp format)
[Browse]	Click to browse your computer file system for the firmware image file
[Upload]	Click to start upload

4.6.5 Configuration File Transfer



This [download] command can be used to backup current device configuration and download it to the connected management PC. The default filename is “cfgdownload”.

Configuration	Description
Filename	Path and filename of a backup configuration file to be uploaded
[Browse]	Click to browse your computer file system for the configuration file
[Upload]	Click to start upload operation from the connected PC to the switch
[Download]	Click to start download operation from the switch to the connected PC

4.6.6 Logout

This menu is used to perform a logout from the web management immediately and return a login prompt. If current user does not perform any management operation over 3 minutes, the device will execute an auto logout and abort the current connection.

5. SNMP Support

SNMP version support	Snmp v1, v2c management	
Managed Objects	MIB-II	
	system	OBJECT IDENTIFIER ::= { mib-2 1 }
	interfaces	OBJECT IDENTIFIER ::= { mib-2 2 }
	ip	OBJECT IDENTIFIER ::= { mib-2 4 }
	snmp	OBJECT IDENTIFIER ::= { mib-2 11 }
	ifMIB	OBJECT IDENTIFIER ::= { mib-2 31 }
RFC	RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)	
	RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets:MIB-II	
	RFC 1158 - Management Information Base for network management of TCP/IP-based internets: MIB-II	
SNMP Trap Support	TRAP_COLDSTART - the device boot up trap	
	TRAP_LINKUP - the port link recovery trap	
	TRAP_LINKDOWN - port link down trap	

Appendix A. Factory Default Settings

System Configuration

DHCP Enabled	*Disable*
Fallback IP Address	*192.168.0.2*
Fallback Subnet Mask	*255.255.255.0*
Fallback Gateway	*0.0.0.0*
Management VLAN	*0*
Name	*Null*
Password	*123*
Inactivity Timeout (secs)	*300*
SNMP enabled	*Disable*
SNMP Trap destination	*0.0.0.0*
SNMP Read Community	*public*
SNMP Write Community	*private*
SNMP Trap Community	*public*

802.1Q Control	*Disable*
Jumbo Mode	*Disable*
Link fault pass through	*Disable*
Remote TP auto report	*Disable*
Power Saving Mode	*Disable*
Drop frames after excessive collisions	*Disable*
BPDU_Transparent	*Enable*

Ports Configuration

Mode	*Auto* for TP port, *1000 Full* for FX port
Flow Control	*v: Enable*
Default Tag - VID(PVID)	*1*
Default Tag – DEI	*0*
Default Tag – PCP	*0*
Ingress Drop	*Disable*
Tag Removal	*Keep All Tags*

Egress Tagging Rule	*Type 0*
Tagging Exceptional VID	*1*
Egress Tag TPID	*0x8100(c-tag)*
Custom TPID	*0x8100*

802.1Q Filtering

VID TABLE	*Disable*
VID n (n=1-16)	0

LLDP Configuration

Transmitted TLVs

Port Description	*Enable*
System Name	*Enable*
System Description	*Enable*
System Capabilities	*Enable*
Management Address	*Enable*

LLDP Parameters

Tx Interval	*10*
Tx Hold	*4*
Tx Delay	*2*
Reinit Delay	*2*

LLDP Port Configuration

LLDP State	*Disable*

Appendix B. Models & Optical Specifications

Model Definition

KGC-310M-C	Managed model with no pre-installed SFP transceiver
KGC-310M-C-xxxx	Managed model with pre-installed SFP transceiver

SFP with 1000BASE-X fiber transceiver

Model Ext.	FiberCon.	Reference Fiber Distance (Typ.)
-SX	1000M LC	Duplex MMF 500m
-LX	1000M LC	Duplex MMF 550m, SMF 10km
-LX20	1000M LC	Duplex SMF 20km
-LX30	1000M LC	Duplex SMF 30km
-LX50	1000M LC	Duplex SMF 50km
-LX70	1000M LC	Duplex SMF 70km
Bi-directional WDM over single SMF		
-W3510	1000M LC	Simplex SMF 10km
-W5310	1000M LC	Simplex SMF 10km
-W3520	1000M LC	Simplex SMF 20km
-W5320	1000M LC	Simplex SMF 20km
-W3410	1000M LC	Simplex SMF 10km
-W4310	1000M LC	Simplex SMF 10km
-W3410S	1000M SC	Simplex SMF 10km
-W4310S	1000M SC	Simplex SMF 10km

Optical Specifications

Model Ext.	Wavelength	Tx Power*1	Rx Sen.*2	Max.Rx*3
-SX	850nm	-9.5~ -4	-18	0
-LX	1310nm	-9.5~ -3	-20	-3
-LX20	1310nm	-8~ -2	-23	-1
-LX30	1310nm	-4~ +1	-24	-3
-LX50	1550nm	-4~ +1	-24	-3
-LX70	1550nm	0~ +5	-24	-3
Bi-Direction WDM over single SMF				
-W3510	T1310/R1550	-9~ -3	-21	-1
-W5310	T1550/R1310	-9~ -3	-21	-1
-W3520	T1310/R1550	-8~ -2	-23	-1
-W5320	T1550/R1310	-8~ -2	-23	-1
-W3410	T1310/R1550	-9~ -3	-21	-1
-W4310	T1550/R1310	-9~ -3	-21	-1

-W3410S	T1310/R1550	-9~ -3	-21	-1
-W4310S	T1550/R1310	-9~ -3	-21	-1

*[1] *Tx Power : Transmitter power (min. ~ max., unit: dBm)*

*[2] *Rx Sen. : Receiver sensitivity (unit :dBm)*

*[3] *Max.Rx. : Maximal Received power (unit : dBm)*

Note:

The converter also can support typical 100M SFP transceivers.