KGS-0865

Industrial Managed

8-Port Gigabit Ethernet Switch

Installation Guide

For more information, contact:

United States   KTI Networks Inc.
P.O. BOX 631008
Houston, Texas 77263-1008

Phone: 713-2663891
Fax: 713-2663893
E-mail: kti@ktinet.com
URL: http://www.ktinet.com/

International   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 Part 15 of 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 undesired operation.

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 Class A
IEC 61000-6-4
   IEC/EN 61000-3-2
   IEC/EN 61000-3-3
IEC 61000-6-2
   IEC/EN 61000-4-2
   IEC/EN 61000-4-3
   IEC/EN 61000-4-4
   IEC/EN 61000-4-5
   IEC/EN 61000-4-6
   IEC/EN 61000-4-8
   IEC/EN 61000-4-11

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 switch provides eight 10/100/1000Mbps copper ports for connections to Ethernet, Fast Ethernet or Gigabit Ethernet devices. With the featured auto-negotiation function, the switch can detect and configure the connection speed and duplex automatically. The switch also provides auto-MDI/MDI-X function, which can detect the connected cable and switch the transmission wire pair and receiving pair automatically. This auto-crossover function can simplify the type of network cables used.

The switch is embedded with an Http server which provides management functions for advanced network functions including Port Control, Quality of Service, and Virtual LAN functions. The management can be performed via Web browser based interface over TCP/IP network.

For industrial environment, the device is designed with the following enhanced features exceeding that of commercial Ethernet switches:

- High and wide operating Temperature range
- Screw panel and DIN rail mounting support for industrial enclosure
- Industrial-rated Emission and Immunity performance

1.1 Features

- Provides 8 10/100/1000Mbps copper ports
- Auto-negotiation
- Auto-MDI/MDI-X crossover function
- Supports IEEE 802.3x flow control for full duplex
- Supports back pressure flow control for half duplex
- Fully non-blocking Gigabit full wire speed switching performance
- Jumbo frame support
- Alarm relay output for power failure event and software configured port link fault events
- 802.1Q VLAN function
- Port mirroring function
- IGMP snooping function
- LLDP support
- QoS (Quality of Service) function
- Web management
- SNMP MIB-II support and trap function
- Wide operating temperature range
- Supports Green Ethernet power saving
- Supports IEEE 802.3az Energy Efficient Ethernet
- Supports DIN-Rail mounting and panel mounting
- Industrial-rated emission and immunity performance

1.2 Product Panels

The following figure illustrates the panels of the switch:
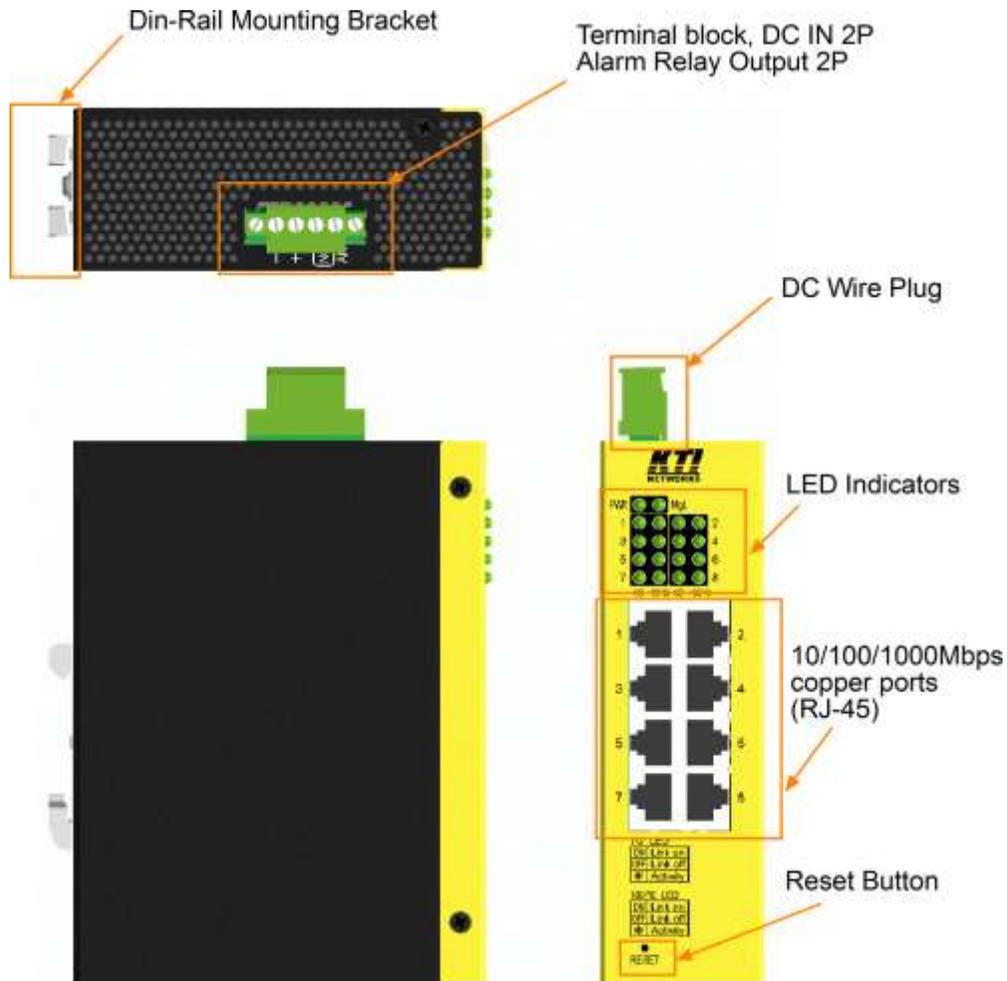
1.3 LED Indicators

LED	Function
PWR	Power status
Mgt.	Management status
1 - 8	Port 1 – Port 8
1G	1Gbps link and activity status (Port 1 - Port 8)
100/10	100Mbps or 10Mbps link and activity status (Port 1 - Port 8)

1.4 Specifications

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

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 or better

Switch Functions

Forwarding & filtering	Non-blocking, full wire speed
Switching technology	Store and forward
Maximum packet length	Jumbo frame support up to 9600 bytes
MAC Addresses	8K
Packet Buffer Size	4M bits
Flow control	IEEE 802.3x pause frame base for full duplex operation. Back pressure for half duplex operation
MAC Aging time	300 seconds
Storm control	Broadcast packets are dropped when more than 64 broadcast packets are received.

DC Power Input

Screwed terminal block	2P (DC+, DC-) with flange
Operating Voltages	+8 ~ +57VDC
Power Consumption	10W max.
Power Saving Mode	Total consumption 0.28W when all ports link down
Protection	Polarity Reversal

Alarm Relay Output

Screwed terminal block	2 dry contacts (NO)
Contact rating	30VDC/1A or 120VAC/0.5A
Alarm events	Power failure, software configured port link faults

Mechanical

Dimension (base)	42 x 106 x 140 mm (WxDxH)
Housing	Enclosed metal with no fan

Mounting	Din-rail mounting
	Panel mounting (with optional bracket)

Environmental

Operating Temperature	Typical -30ºC ~ +70ºC
Storage Temperature	-40ºC ~ +85ºC
Relative Humidity	5% ~ 90% non-condensing

Approvals

FCC	Part 15 rule Class A
CE	EMC Class A
VCCI	Class A
	EN 61000-6-4
	EN 61000-3-2
	IEC 61000-3-3
	IEC 61000-6-2
	IEC 61000-4-2
	IEC 61000-4-3
	IEC 61000-4-4
	IEC 61000-4-6
	IEC 61000-4-8
	IEC 61000-4-11
LVD	IEC60950-1 safety
	IEC 60068-2-64 Vibration
	IEC 60068-2-27 shock test
NEMA	TS2 environment

2. Installation

2.1 Unpacking

The product package contains:

- The switch unit for Din-rail mounting
- One product CD-ROM

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.

2.3 Mounting the Switch to a Din-Rail

In the product package, a DIN-rail bracket is provided or has been installed for mounting the switch in a industrial DIN-rail enclosure.

The steps to mount the switch onto a DIN rail are:

1. Install the mounting bracket onto the switch unit with screws as shown below:

2. Attach bracket to the lower edge of the DIN rail and push the unit upward a little bit until the bracket can clamp on the upper edge of the DIN rail.

3. Clamp the unit to the DIN rail and make sure it is mounted securely.

The final dimension is:
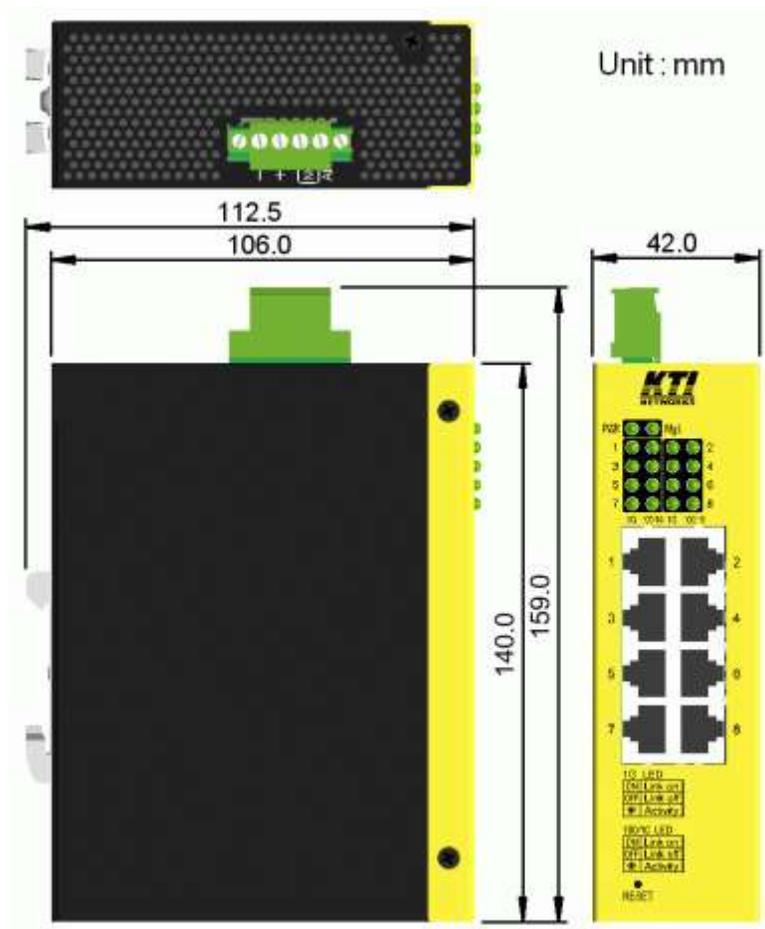
2.4 Mounting the Switch on a Panel

The switches may be provided optionally with a panel mounting bracket. The bracket supports mounting the switch on a plane surface securely. The mounting steps are:

1. Install the mounting bracket on the switch unit.

2. Screw the bracket on the switch unit.

3. Screw the switch unit on a panel and the locations for screws are shown below:
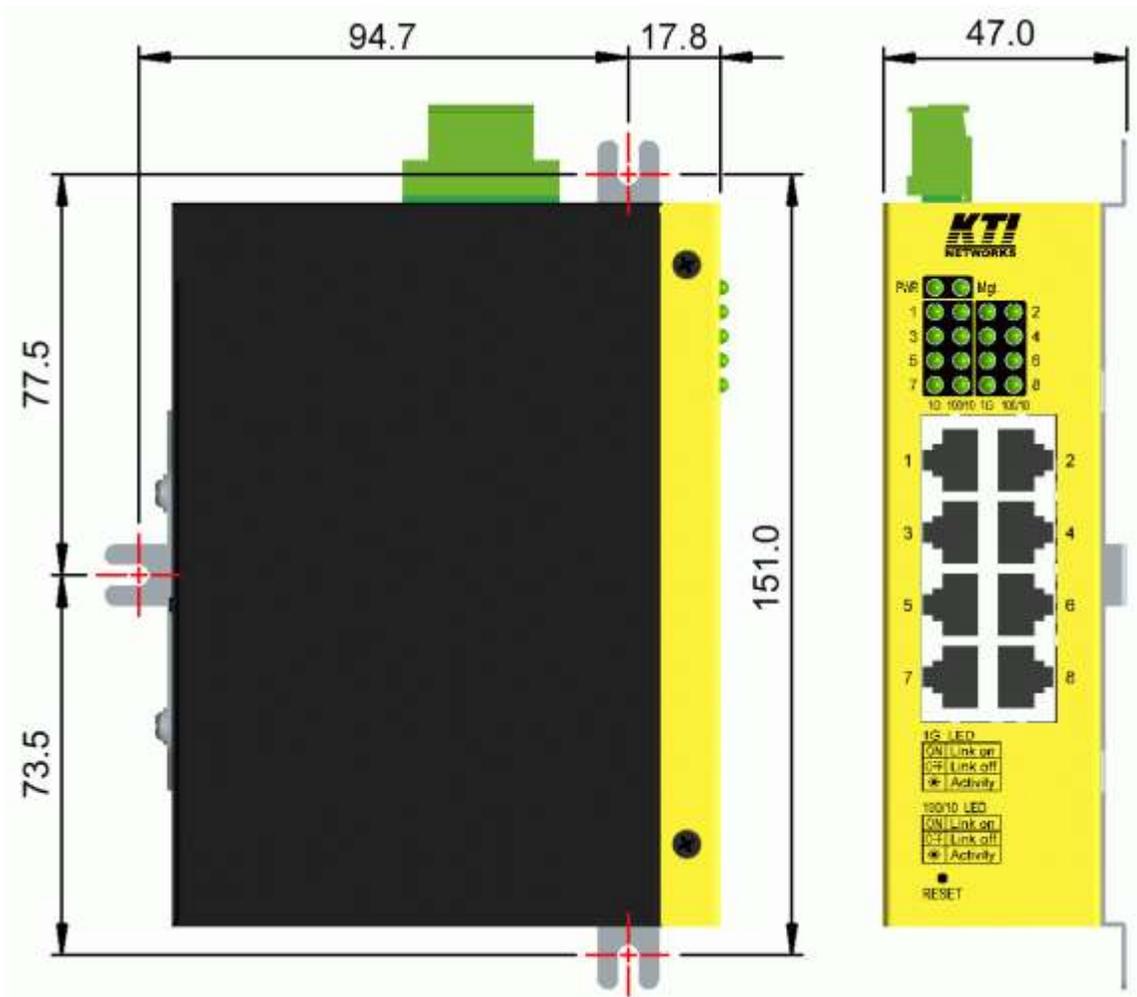
2.5 Applying Power

Power pins of the terminal block connector

Pin	1	−	DC− Positive (−) input terminal
	2	+	DC+ Negative (+) input terminal

DC+/- Input specifications

Working voltage range: +8V ~ +57VDC

WARNING: The -48VDC power supply is not supported.

Terminal Plug & Power Wire

A 4P terminal plugs are provided together with the switch as shown below:
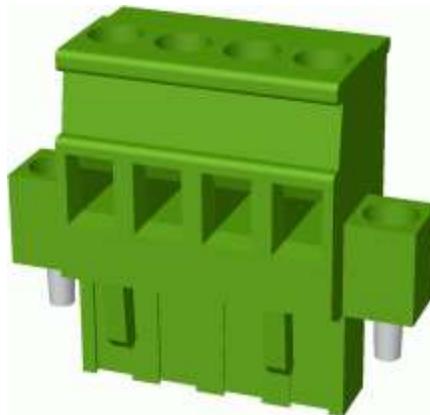
Power wires: 24 ~ 12AWG (IEC 0.5~2.5mm²)

Wire length: 1 meter max.

2.6 Alarm Relay Output

Alarm relay output is provided for reporting failure events to a remote alarm relay monitoring system. The replay output is provided with two contacts on the terminal block connector next DC power interface.

Alarm Relay output pins and logic:

Pin	3	4	Alarm relay output, NO (Normal Open) contacts
	NO		Open: normal, Shorted: Alarm

The relay output can connect relay monitoring system.

Use the provided 4P terminal plug for signal wiring and plug into the contacts.

Alarm Events

● Input power failure

● Software configured port link faults.

(The ports can be configured via web management.)

Note:

Be sure the voltage applied on the contacts is within the specification of 30VDC/1A max. or 120VAC/0.5A max.

2.7 Reset Button

The reset button is used to perform a reset to the switch. It is not used in normal cases and can be used for diagnostic purpose. If any network hanging problem is suspected, it is useful to push the button to reset the switch without turning off the power. Check whether the network is recovered.
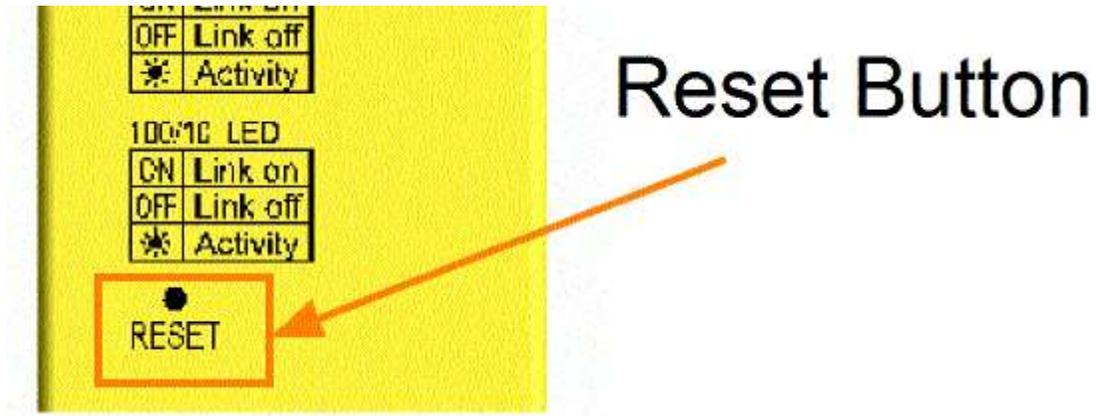
The button can also be used to restore the software configuration settings to factory default values.

The operations are:

Operation	Function
Press the button and release during switch operation	Reset & boot up the switch. The behavior is same as power boot procedure.
Press the button when boot-up until all LEDs blink.	Boot & restore all factory default settings

3. Making LAN Connections

3.1 10/100/1000 Copper Ports

The 10/100/1000 RJ-45 copper ports support 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 for all above

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 are connected, the ports can sense the receiving pair automatically and configure themselves to match the rule for MDI to MDI-X connection. It simplifies the cable installation.

Auto-negotiation Function

The ports are 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 switch will sense the speed and use half duplex for the connection.

3.2 LED Indication
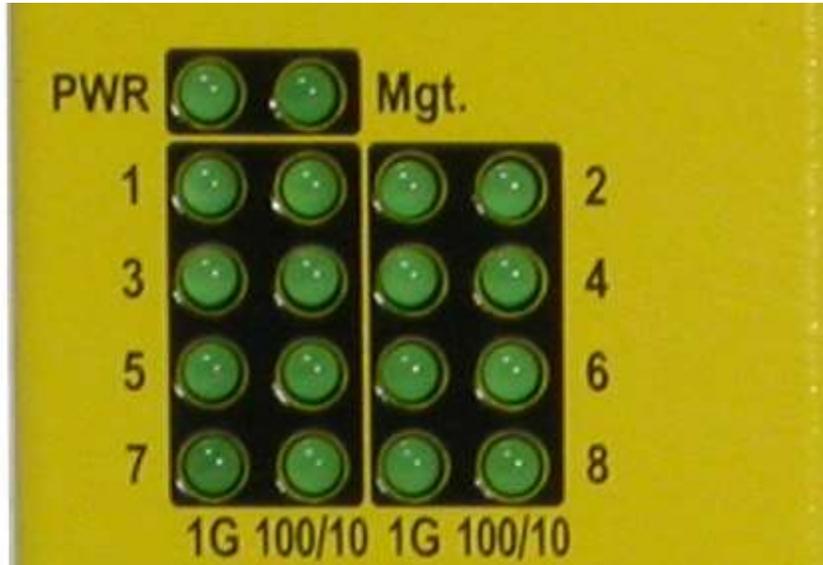
LED	Function	State	Interpretation
PWR	Power status	ON	The power is supplied to the switch.
		OFF	The power is not supplied to the switch.
Mgt.	Management status	ON	During initialization (about 15 minutes)
		ON	Error report after initialization
		OFF	Initialization and diagnostics finished with no error
		ON	Relay alarm event occurred during normal operation and LED OFF after the event is recovered.
1G	Port 1Gbps link status	ON	A 1Gbps (1000Mbps) link is established on the port. (No traffic)
		BLINK	Port link is up and there is traffic.
		OFF	Port link is down.
100/10	Port 100/10M link status	ON	A 100Mbps or 10Mbps link is established on the port.
		BLINK	Port link is up and there is traffic.
		OFF	Port link is down.

Note: LED 1G and 100/10 are per port basis.

3.3 Configuring IP Address and Password for the Device

The device unit was 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.

4. Web Management

4.1 Abbreviation

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

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

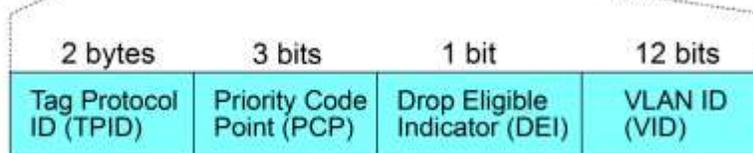**Egress Port**: Egress port is the output port from which a packet is sent out.

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

Standard Ethernet frame

Destination Address	Source Address	Type/Len	Data	Frame Check

802.1Q Tagged frame

Destination Address	Source Address	802.1Q VLAN Tag	Type/Len	Data	Frame Check

2 bytes	3 bits	1 bit	12 bits
Tag Protocol ID (TPID)	Priority Code Point (PCP)	Drop Eligible Indicator (DEI)	VLAN ID (VID)

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. It is composed of four fields including TPID, PCP, DEI and VID.

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

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

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

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

PVID (Port VID): PVID is the default VID of VLAN unaware ingress port.

4.2 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↵

4.3 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.

4.4 Main Management Menu

KGS-0865 Gigabit Switch

Configuration

System
Ports
VLANs
IGMP Snooping
Mirroring
LLDP
Quality of Service

Monitoring

Statistics Overview
IGMP Status
LLDP Statistics
LLDP Table
Ping

Maintenance

Reboot System
Restore Default
Update Firmware
Configuration File Transfer
Logout

System Configuration

MAC Address	00-40-F6-DE-00-00
S/W Version	v1.011
H/W Version	1.0
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 (seconds)	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

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
VLANs	802.1Q VLAN settings
IGMP Snooping	Configuration for IGMP snooping function
Mirroring	Mirroring function settings
LLDP	Settings for LLDP support
Quality of Service	QoS configuration

Monitoring

Statistics Overview	List statistics for the local ports and remote TP port link status
IGMP Status	Show current status of IGMP snooping
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

4.5 Configuration

4.5.1 System

System Configuration

MAC Address	00-40-F6-DE-00-00
S/W Version	v1.011_beta_2014110710
H/W Version	1.0
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 (seconds)	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

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	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
[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 immediately.*

4.5.1.1 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	Untagged packets
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.

4.5.2 Ports

Port Configuration

Power Saving Mode	Disable ▼
Enable Jumbo Frames	☐
Drop frames after excessive collisions	☐
Enable 802.3az EEE mode	☐

Port	Link	Mode	Flow Control	Relay Alarm
1	100FDX	Auto Speed ▼	☐	☐
2	Down	Auto Speed ▼	☐	☐
3	Down	Auto Speed ▼	☐	☐
4	Down	Auto Speed ▼	☐	☐
5	Down	Auto Speed ▼	☐	☐
6	Down	Auto Speed ▼	☐	☐
7	Down	Auto Speed ▼	☐	☐
8	Down	Auto Speed ▼	☐	☐

Apply   Refresh

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

Configuration	Function
Power Saving Mode	*Full* - all the time
	Link-up - power saving only when link up
	Link-down - power saving only when link down
	Disable - disable port power saving
Enable Jumbo Frames	Set to enable jumbo frame support
Drop frame after excessive collision	
	v - set to enable the function

Enable 802.3az EEE mode

v - set to enable the function

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

Mode

Auto Speed ▼

| Auto Speed |
| 10 Half |
| 10 Full |
| 100 Half |
| 100 Full |
| 1000 Full |
| Disabled |

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*

Flow Control	Set port flow control function
	v - set to enable 802.3x pause flow control for ingress and egress
Relay Alarm	Set port link down alarm
	v - set to enable port link down monitoring for failure relay output
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

4.5.3 VLANs

Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID	

Add

VLAN Configuration List

1 ⦿							

Modify   Delete   Refresh

VLAN Member List

VID	Member Ports
1	1,2,3,4,5,6,7,8

Port Config

4.5.3.1 Add a VLAN

Add a VLAN

VLAN ID	2

Add

Configuration	Function
VLAN ID	Specify the VLAN to be added.
[Add]	Click to add one new VLAN.

VLAN Setup

VLAN ID: 2			
Port	Member	Port	Member
Port 1	☐	Port 5	☐
Port 2	☐	Port 6	☐
Port 3	☐	Port 7	☐
Port 4	☐	Port 8	☐

VLAN Member List

VID	Member Ports
1	1,2,3,4,5,6,7,8

[Apply]   [Refresh]   [Back]

Configuration	Function
Member Port	Check to select the port as a member of the VLAN
VLAN Member List	List current configured VLANs – VID and member ports
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go to previous page

Note:

1. *VLAN 1 with all port members is pre-configured as default.*

2. *Up to 8 VLANs are supported.*

4.5.3.2 Modify VLAN Configuration

VLAN Configuration List

1 ⊙							

[Modify] [Delete] [Refresh]

Configuration	Function
VLAN group	Select the VLAN to be modified for the member ports or deleted.
[Modify]	Click to modify the members of the selected VLAN.
[Delete]	Click to delete the selected VLAN.
[Refresh]	Click to refresh current configuration

4.5.3.3 VLAN Port Configuration

Port Config

Button	Function
[Port Config]	Click to set port configuration

VLAN Per Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Pvid	Engress Insert Rule
1	unaware ▼	☐	All ▼	1 ▼	No_PVID ▼
2	unaware ▼	☐	All ▼	1 ▼	No_PVID ▼
3	unaware ▼	☐	All ▼	1 ▼	No_PVID ▼
4	unaware ▼	☐	All ▼	1 ▼	No_PVID ▼
5	unaware ▼	☐	All ▼	1 ▼	No_PVID ▼
6	unaware ▼	☐	All ▼	1 ▼	No_PVID ▼
7	unaware ▼	☐	All ▼	1 ▼	No_PVID ▼
8	unaware ▼	☐	All ▼	1 ▼	No_PVID ▼

VLAN Member List

VID	Member Ports
1	1,2,3,4,5,6,7,8

Apply   Cancel   Back

Configuration	Function
Port	The switch port
Port Type	Specify VLAN mode for the port

Port Type

unaware ▼
unaware
c-port

unaware – Unaware to VLAN tagged packets

c-port – VLAN aware for received C-tagged & S-tagged packets.

Each received packet is classified to a classified tag and VLAN ID (VID) depending

on the Ingress port's port type. The outer tag is referred if exists.

The rule is:

Received packet type	Classified Tag	
	Unaware	C-port
Untagged	Default Tag	Default Tag
Priority tagged (VID=0)	Default Tag	Default Tag
C-tagged & S-tagged	Default Tag	Packet's Tag
Other tagged	Default Tag	Default Tag

Default Tag = TPID 0x8100 + PVID

Received packet type	Classified VID	
	Unaware	C-port
Untagged	PVID	PVID
Priority tagged (VID=0)	PVID	PVID
C-tagged & S-tagged	PVID	Packet's VID
Other tagged	PVID	PVID

The classified VID is used as index for VLAN table look up.

Received packet type	Tag Removal	
	Unaware	C-port
Untagged	No	No
Priority tagged (VID=0)	No	No
C-tagged & S-tagged	No	Tag removed
Other tagged	No	No

The outer tag is removed if two VLAN tags exist in the frame.

Ingress Filtering   Check to enable VLAN member checking for the ingress port.

The received packet is dropped if the ingress port is not in the members of the classified VLAN.

Frame Type   The accepted packet type; others are dropped.

Frame Type

```
All        ▼
All
Tagged
Untagged
```
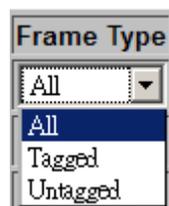
All – all types are accepted.

Tagged – C-tagged & S-tagged packets are accepted.

Untagged – all are accepted except c-tagged and S-tagged packets.

PVID	The default classified VID for the port
Egress Tag Insert Rule	Classified Tag insertion rule in egress operation

Engress Insert Rule

No_PVID ▼
No_PVID
Yes
No
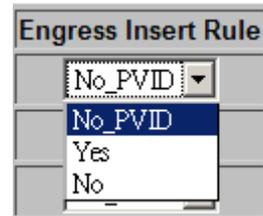
No_PVID – The classified tag is not inserted if the classified VID matches egress port's PVID.

Yes – Insert the classified tag to the outgoing packet

No – No insertion

[Apply]	Click to apply the configuration change
[Cancel]	Click to cancel the configuration change
[Back]	Click to go to previous page

4.5.4 IGMP Snooping

IGMP Configuration

IGMP Enabled	☐
Router Ports	1☐ 2☐ 3☐ 4☐ 5☐ 6☐ 7☐ 8☐
Unregistered IPMC Flooding enabled	☑

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	☑	☑

Apply   Refresh

Configuration	Description
IGMP Enabled	Check to enable global IGMP snooping.
Router Ports	Specify which ports have multicast router connected and require being forwarding IPMC packets unconditionally.

-36-

Unregistered IPMC Flooding enabled

                        Check to enable flooding un-registered IPMC packets.

VLAN ID	List of current existing VLANs
IGMP Snooping Enabled	Check to enable IGMP snooping on the associated VLAN.
IGMP Querying Enabled	Check to enable IGMP querying on the associated VLAN.

[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

4.5.5 Mirroring

Mirroring Configuration

Port	Mirror Source
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐

Mirror Port	1 ▼

Apply   Refresh

Configuration	Description
Mirror Port	The port for being forwarded all packets received on the mirrored source ports
Mirror Source	Select the ports which will be mirrored all received packets to the mirror port.

[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

4.5.6 LLDP

LLDP Configuration

Transmitted TLVs	
Port Description	☑
System Name	☑
System Description	☑
System Capabilities	☑
Management Address	☑

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

Port	LLDP State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

Apply   Refresh

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 switch will not send out LLDP information, and will drop LLDP information received from neighbors. *Tx and Rx:* The switch 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.*

4.5.7 Quality of Service

The device includes a number of QoS features related to providing low-latency guaranteed services to critical network traffic such as voice and video in contrast to best-effort traffic such as web traffic and file transfers. All incoming frames are classified to a QoS class, which is used in the queue system when assigning resources, in the arbitration from ingress to egress queues and in the egress scheduler when selecting the next frame for transmission.

The QoS class is assigned based on the class of service information, Priority Code Points (PCP, also known as IEEE 802.1p) in the frame's VLAN tags and/or the Differentiated Service Code Points (DSCP) values from the IP header. Both IPv4 and IPv6 are supported. If the frame is non-IP or untagged, the default QoS class is used.

Four QoS classes, *Low/ Normal/ Medium/ High* are defined in this device. The QoS class is used by the queue system when enqueuing frames and when evaluating resource consumptions in packet switching operation.

The mapping table from PCP value to QoS class is configured globally for all ports.
The mapping table from DSCP to QoS class is also configured globally for all ports.

QoS Configuration
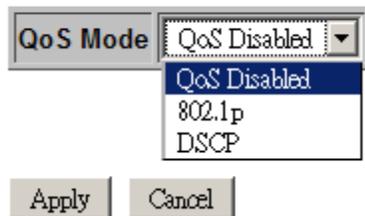
QoS Mode [QoS Disabled ▼]
            QoS Disabled
            802.1p
            DSCP

[Apply] [Cancel]

Configuration	Description
QoS Mode	*Disable* – Disable QoS function
	802.1p - Enable 802.1p priority classification for VLAN tagged packets
	DSCP - Enable DSCP priority classification for IP packets
[Apply]	Click to apply the configuration change
[Cancel]	Click to cancel the configuration change

4.5.7.1 802.1p Configuration

QoS Configuration

QoS Mode	802.1p ▾
Prioritize Traffic	Custom ▾

802.1p Configuration

802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal ▾	1	low ▾	2	low ▾	3	normal ▾
4	medium ▾	5	medium ▾	6	high ▾	7	high ▾

Apply   Cancel

Configuration	Description
QoS Mode	*802.1p, DSCP*
Priority Traffic	Preset the 802.1p mapping table
	Prioritize Traffic Custom ▾ Custom All Low Priority All Normal Priority All Medium Priority All High Priority
	Custom – set priority for each PCP value
	All Low Priority – set whole table to low priority
	All Normal Priority - set whole table to normal priority
	All Medium Priority - set whole table to medium priority
	All High Priority - set whole table to high priority
802.1p Value	PCP value entry 0 ~ 7
Priority	QoS class to which the associated PCP value maps
	normal, low, medium, high
[Apply]	Click to apply the configuration change
[Cancel]	Click to cancel the configuration change
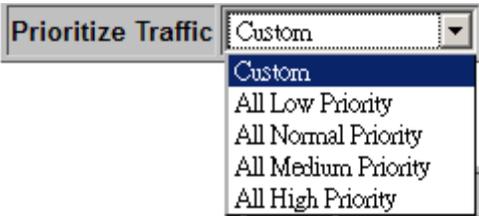
Note:

1. *QoS priority classification is applied to Priority-tagged frames, C-tagged and S-tagged frames.*

2. *Untagged frames are classified to high priority.*

4.5.7.2 DSCP Configuration

QoS Configuration

QoS Mode	DSCP
Prioritize Traffic	All High Priority

DSCP Configuration

DSCP Value(0..63)	Priority
	high
	high
	high
	high
	high
	high
	high
All others	high

[Apply] [Cancel]

Configuration	Description
QoS Mode	*802.1p, DSCP*
Priority Traffic	Preset the DSCP mapping table

Prioritize Traffic	Custom
	Custom
	All Low Priority
	All Normal Priority
	All Medium Priority
	All High Priority

Custom – set priority for each PCP value

All Low Priority – set whole table to low priority

All Normal Priority - set whole table to normal priority

All Medium Priority - set whole table to medium priority

All High Priority - set whole table to high priority

DSCP Values(0..63)	Map one DSCP value to one QoS priority class, *normal, low, medium, high.*
	Each of seven configured DSCP values can be mapped to one priority.

The rest values are mapped to single one priority.

[Apply]	Click to apply the configuration change
[Cancel]	Click to cancel the configuration change

Note:

1. *DSCP classification is applied to IPv4 and IPv6 frames.*

2. *Non-IP frames are given 0 for DSCP.*

4.6 Monitoring

4.6.1 Statistics Overview

Statistics Overview for all ports

Clear | Refresh

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	2185206	24134	82006668	602701	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	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

4.6.2 IGMP Status

IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Idle	0	0	0	0	0	0

Refresh

Member Groups

VLAN ID	Groups	Port Members
No IGMP groups		

Status	Description
VLAN ID	The VLAN ID of the entry.
Querier Status	Show the Querier status is "Active" or "Idle".
Queries transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports	The number of Received V1 Reports.
V2 Reports	The number of Received V2 Reports.
V3 Reports	The number of Received V3 Reports.
V2 Leave	The number of Received V2 Leave.
[Refresh]	Click to refresh the page.

Group Member Status	Description
VLAN ID	The VLAN where the groups found
Groups	IPMC group (IP) found on the VLAN
Port Members	Port members found of the group

4.6.3 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
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	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

4.6.4 LLDP Table

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
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Refresh

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

4.6.5 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	Number of ping commands generated
Time Out (in secs)	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	Number of replies received by the system
Request time-outs	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

4.7 Maintenance
4.7.1 Reboot System

Reboot Systemt

Are you sure you want to reboot system? Yes No
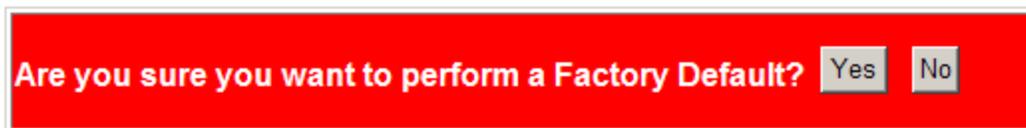
This menu is used to reboot the device unit remotely with current configuration. Starting this menu will make your current http connection lost. You must rebuild the connection to perform any management operation to the unit.

4.7.2 Restore Default

Factory Default

Are you sure you want to perform a Factory Default? Yes No

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

4.7.3 Update Firmware

Software Upload

Browse

Upload

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

4.7.4 Configuration File Transfer

Configuration Upload

[   ] Browse

Upload

Configuration Download

Download

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

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

4.7.5 Logout

Please enter password to login

Password: [   ]

Apply

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*
Power Saving Mode	disabled
Enable Jumbo Frames	disable
Drop frames after excessive collisions	disable
Enable 802.3az EEE mode	disable
Port Mode	"Auto Speed" for all ports
Flow Control	disable for all ports
Relay Alarm	disable for all ports
VLANs	VLAN1 VID=1 members=all ports
VLAN Port Type	"unaware" for all ports
VLAN Ingress Filtering	disable for all ports
VLAN Frame Type	"All" for all ports
VLAN Pvid	"1" for all ports
Egress Tag Insert Rule	"No_PVID" for all ports
IGMP Enabled	no
Router Ports	none

Unregistered IPMC Flooding enabled

yes

VLAN1 IGMP Snooping Enabled	yes
VLAN1 IGMP Querying Enabled	yes
Mirror Source	none
Mirror Port	1
TLV Port Description	yes
TLV System Name	yes
TLV System Description	yes
TLV System Capabilities	yes
TLV Management Address	yes
LLDP Tx Interval	10
LLDP Tx Hold	4
LLDP Tx Delay	2
LLDP Reinit Delay	2
LLDP State	disabled
QoS Mode	QoS Disabled