A Network Systems Solution

UNIC⊙M™

SmartGST-2404GM

24 Port 10/100/1000Base-T
Managed Switch
with four SFP (Mini) GBIC Slots

GEP-66424T

USER'S MANUAL

Content

Introduction

The SmartGST-2404GM Switch is a multi-port Switch that can be used to build high-performance switched workgroup networks. This switch is a store-and-forward device that offers low latency for high-speed networking. The SmartGST-2404GM is targeted at workgroup, department or backbone computing environments.

The SmartGST-2404GM Switch has twenty-four auto-sensing 10/100/1000 Base-T RJ-45 ports and four mini GBIC slots for higher connection speed.

Features

- ν   Conforms to IEEE802.3 10BASE-T, IEEE802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000Base-T, IEEE 802.3z Gigabit Fiber, IEEE802.3x Flow control and Back pressure, IEEE802.1d Spanning tree protocol, IEEE 802.s Rapid Spanning Tree, IEEE 802.3ad Port trunk with LACP, IEEE802.1p Class of service, IEEE802.1Q VLAN Tagging
- ν   Store-and-Forward Switching Architecture
- ν   Auto-MDIX on all ports
- ν   48Gbps Back-Plane
- ν   8K MAC Address Table
- ν   500Kbytes memory buffer
- ν   N-Way Auto-Negotiation
- ν   True Non-Blocking Switching
- ν   10K Jumbo Frame support
- ν   Back Pressure with half duplex
- ν   Flow Control with full duplex
- ν   Support Port Based VLAN and Tag VLAN
- ν   Support IGMP Snooping

- ν Supports Class of Service
- ν Supports Port Mirror
- ν Supports Port Trunk
- ν Supports Rapid Spanning Tree
- ν Supports ingress packet filter and egress rate limit
- ν Supports IP address security to prevent unauthorized intruder
- ν Provides Web interface management and one default button for system default setting
- ν Supports Bandwidth control

Software Feature

Management	Web Management
Firmware update	TFTP firmware upgrade
Port configuration	Port enable/disable Port speed Full /half duplex Flow control
Port Trunk	IEEE802.3ad port trunk with link aggregation control protocol (LACP) The trunk group up to 8 and maximum trunk port member up to 16 ports

Port statistics	Several of counters for TX and RX packet.
VLAN	Port based VLAN Tag VLAN and GVRP protocol The VLAN entry up to 4K and VID up to 4094
Quality of Service	Port based Tag based IPv4 ToS IPv6 DSCP
Class of Service	Per port support 4 priority queues
Spanning Tree	IEEE802.1w rapid spanning tree Compatible with IEEE 802.1d
Port Mirror	RX packet mirror
IGMP	IGMP V1, V2 Multicast groups up to 8K
Broadcast Storm	Disable/5%/10%/20%
Bandwidth Control	Per port support Bandwidth control. Per level 128 Kbps.

Package Contents

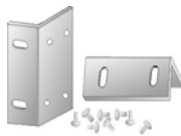Unpack the contents of the SmartGST-2404GM Switch and verify them against the checklist below:

ν   SmartGST-2404GM Switch

ν   Four Rubber Pads

ν   Rack-mounted Kit

ν   Power Cord

ν   User Manual

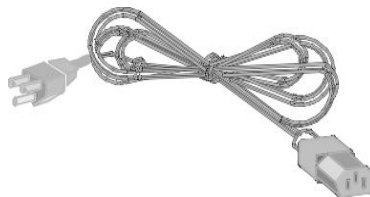**SmartGST-2404GM**   **Four Rubber Pads**

Rack-mounted Kit   **Power Cord**   **User Manual**

Compare the contents of your SmartGST-2404GM Switch package with the standard checklist above. If any item is missing or damaged, please contact the local dealer for service.

Hardware Description

This section mainly describes the hardware of the SmartGST-2404GM Switch and gives a physical and functional overview on the certain switch.

Physical Dimension

SmartGST-2404GM Switch's physical dimensions are **440mm x 161mm x 44mm (Lx W x H)**.

Front Panel

The Front Panel of the SmartGST-2404GM Switch consists of twenty-four 10/100/1000 Base-TX RJ-45 ports (Auto MDI/MDIX) and 4 Mini GBIC slots which can insert the Mini Gigabit Fiber module (optional). The LED Indicators are also located on the front panel of the switch.
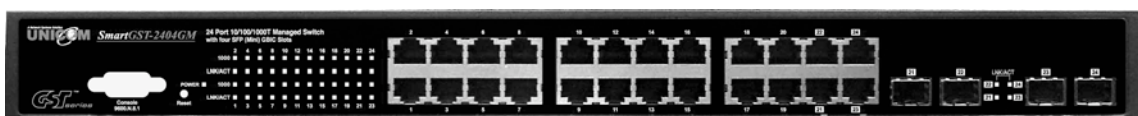
The Front panel of the SmartGST-2404GM Switch

ν   **Reset Button**: There is a reset button on the front panel. Press the reset button less than 5 seconds for warming power reset. While the time of pressing the button lasts more than 5 seconds, the machine will load the factory default value including user name, password and IP address.

ν   **RJ-45 Ports (Auto MDI/MDIX):** 24x 10/100/1000 N-way auto-sensing for 10Base-T or 100Base-TX or 1000Base-T connections.

In general, **MDI** means connecting to another Hub or Switch while **MDIX**

means connecting to a workstation or PC. Therefore, **Auto MDI/MDIX** would allow connecting to another Switch or workstation without changing non-crossover or crossover cabling.

ν **Four MINI GBIC slots:** 4 slots for optional Mini GBIC modules.

LED Indicators

The LED Indicators display real-time information of systematic operation status. The following table provides descriptions of LED status and their meaning.
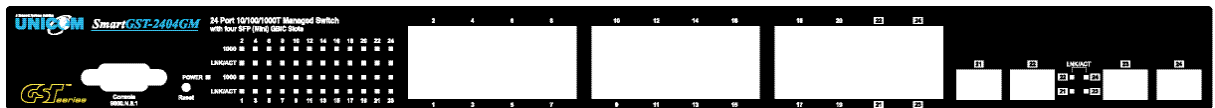
LED indicators

LED	Status	Description
Power	Green	Power On
	Off	Power is not connected
LNK/ACT	Green	The port is connecting with the device.
	Blink	The port is receiving or transmitting data.
	Off	No device attached.
1000	Green	In 1000Mbps connection speed
LNK/ACT (Mini GBIC)	Green	The port is connecting with the device.
	Blink	The port is receiving or transmitting data.
	Off	No device attached

The Description of LED Indicators

Rear Panel

The 3-pronged power plug is located at the rear Panel of the SmartGST-2404GM Switch as shown in figure. The switch will work with AC in the range of 100-240V AC, 50-60Hz.

The Rear Panel of SmartGST-2404GM Switch

Desktop Installation

Set the switch on a sufficiently large flat space with a power outlet nearby. The surface where you put the switch should be clean, smooth, level and sturdy. Make sure there is enough clearance around the switch to allow attachment of cables, power cord and allow air circulation.

Attaching Rubber Pads

A. Make sure the mounting surface on the bottom of the switch is grease and dust free.
B. Remove adhesive backing of Rubber Pads.
C. Apply the Rubber Pads to each bottom corner of the switch and these footpads will protect the switch from shock and vibration.

Rack-mounted Installation

The SmartGST-2404GM Switch come with a rack-mounted kid and can be mounted in an EIA standard size/19-inch Rack. The switch can be placed in a wiring closet with other equipment.

Perform the following steps to rack mount the switch:

1. Position one bracket to align with the holes on one side of the switch and secure it with the smaller bracket screws. Then attach the remaining bracket to the other side of the switch.
2. After attached mounting brackets, position the SmartGST-2404GM switch in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the switch to the rack with a screwdriver and the rack-mounting screws.

[NOTE] For proper ventilation, allow about at least 4 inches (10 cm) of clearance on the front and 3.4 inches (8 cm) on the back of the Switch. This is especially important for enclosed rack installation.

Power On

Connect the power cord to the power socket on the rear panel of the switch. The other side of power cord connects to the power outlet. The internal power supply of the switch works with voltage range of AC in the 100-240VAC, frequency 50~60Hz. Check the power indicator on the front panel to see if power is properly supplied.

Network Application

This section provides few samples of network topology in witch the switch is used. In general, the SmartGST-2404GM Switch is designed as a segment switch. That is, with its large address table (8K MAC address) and high performance, it is ideal for interconnecting networking segments.

PC, workstations and servers can communicate each other by directly connecting with SmartGST-2404GM Switch. The switch automatically learns nodes address, which are subsequently used to filter and forward all traffic based on the destination address.

By using Uplink port, the switch can connect with another switch or hub to interconnect other small-switched workgroups to form a larger switched network. Meanwhile, you can also use fiber ports to connect switches.

Small Workgroup

The SmartGST-2404GM Switch can be used as a standalone switch for personal computers, server and printer server which are directly connected to form a small workgroup.
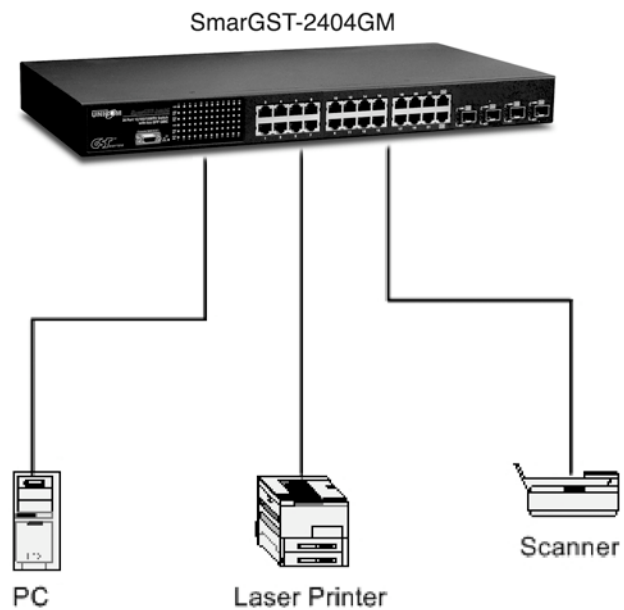
Segment Bridge

For enterprise networks where large data broadcasts are constantly processed, this switch is an ideal solution for department users to connect to the corporate backbone.

In the illustration below, two Ethernet switches with PCs, print server, and local server attached, are both connected to the switch. All the devices in this network can communicate with each other through the switch. Connecting servers to the switch allows other users to access the data on server.
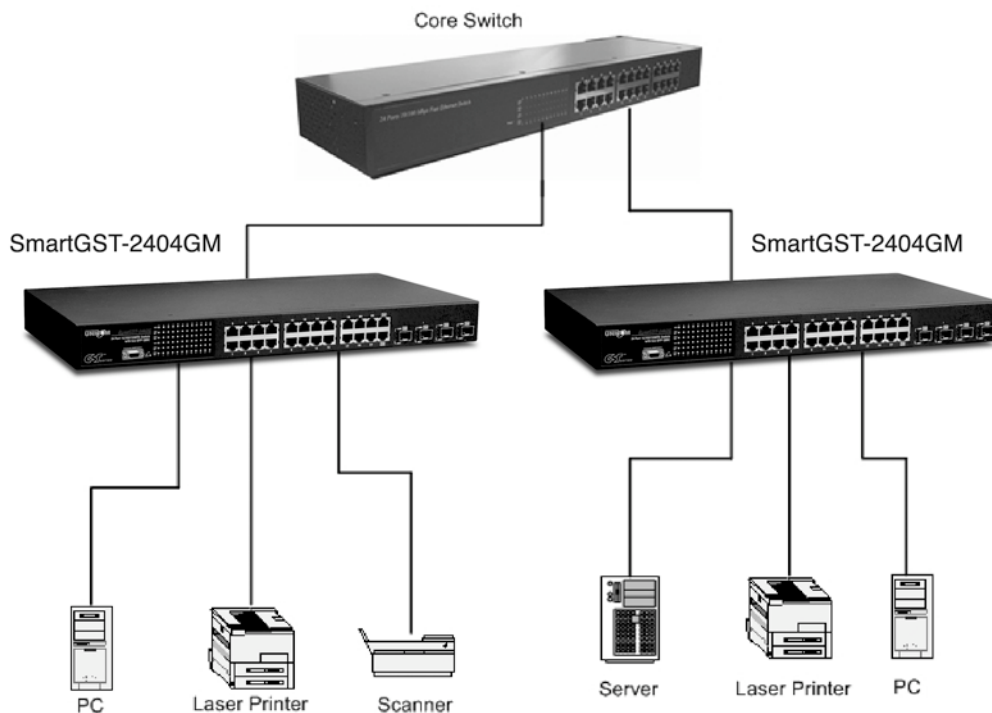
Web-Based Management

This section introduces the configuration and functionality of the Web-Based management of the certain switch.
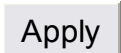
About Web-based Management

On the CPU board of the switch there is an embedded HTML web site residing in flash memory, which offers advanced management features and allow users to manage the switch from anywhere in the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0. And, it is applied with Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

System Login

The default value as listed below:
ν   IP Address: **192.168.16.1**
ν   Subnet Mask: **255.255.255.0**
ν   Default Gateway: **192.168.16.254**
ν   Password: **root**

1. Launch the Internet Explorer

2. Key in "http://" + "IP Address of the SmartGST-2404GM Switch, " and then press "**Enter**"

3. Login screen will appear right after

4. Key in the default password as "**root**"

5. Click [Apply], and then configuration is ready to be set up

24 10/100/1000TX plus 4 MINI GBIC Web Managed Switch

Configuration   Password Successfully Entered

System
Ports
VLANs
Aggregation
LACP
RSTP
802.1X
IGMP Snooping
Quality of Service
Filter
Rate Limit
Mirror

Monitoring

Statistics Overview
Detailed Statistics
LACP Status
RSTP Status
IGMP Status

Maintenance

Warm Restart
Factory Default
Software Upload
Configuration File Transfer

Main Interface

System Configuration

Display system parameters information as listed below, and the other parameters of system can be configured as well.

ν **MAC Address:** the unique hardware address assigned by manufacturer (default)

ν **S/W Version:** the Software Version of Kernel

ν **H/W Version:** the Hardware Version of Switch

ν **Active IP Address:** Current IP Address

ν **Active Subnet Mask:** Current IP Subnet Mask

ν **Active Gateway:** Current Gateway

ν **DHCP Server:** DHCP Server IP Address

ν **Lease Time Left:** DHCP lease time. After 50% of the lease time has passed, the client/switch will attempt to renew the lease with the original DHCP server that it obtained the lease from using a DHCPREQUEST message. Any time the client/switch boots and the lease is 50% or more passed, the client/switch will attempt to renew the lease. At 87.5% of the lease completion, the client/switch will attempt to contact any DHCP server for a new lease.

System Configuration

MAC Address	00-ff-38-ff-f2-34
S/W Version	v1.02
H/W Version	1.0
Active IP Address	192.168.16.1
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	192.168.16.1
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	0.0.0.0
Management VLAN (1~4095)	1
Name	
Password	
Inactivity Timeout (10~10000secs, 0secs means login forever)	0

Apply   Refresh

ν **DHCP Enable:** Enable DHCP Client Function

ν **Fallback IP Address:** Assigning the Switch IP address. The default IP is 192.168.16.1

ν **Fallback Subnet Mask:** Assigning the Switch IP Subnet Mask

ν **Fallback Gateway:** Assigning the Switch Gateway. The default value is 192.168.16.254

ν **Management VLAN:** It is used for Remote Management Security(in fact, the SNMP, and Web browser can be used to manage the switch from the remote side only when the port of VLAN group ID is equal to the Management VLAN ID)

ν **Name:** The name of the switch

ν **Password:** Web GUI login password(The default password is root)

ν **Inactivity Timeout:** timeout time for the web connection

ν Click Apply to activate the configuration

ν Or, Click Refresh to reset the configuration before applying

Port Configuration

Configure the Status of Ports

ν **Link:** "Down" means "No Link". User can select the link speed or auto speed which the system will auto detects the connecting speed

ν **Mode:** Set the speed, full-duplex or half-duplex mode of the ports

ν **Flow control:** Set Flow Control Function as "enable" or "disable" in Full Duplex mode

ν **MaxFrame (1518 ~ 9600):** the Maximum Frame Size (in bytes) from frames received on the port. Tagged frames are allowed to be 4 Bytes longer than the Maximum Frame size

ν **Drop frames after excessive collisions:** When the collision packets are over the limit, then the frame will be dropped

ν   Click Apply to apply the configuration

ν   Or, click Refresh to reset the configuration before applying

Port Configuration

Port	Link	Mode	Flow Control	MaxFrame (1518~9600)
1	Down	Auto Speed	☐	1518
2	100FDX	Auto Speed	☐	1518
3	Down	Auto Speed	☐	1518
4	100FDX	Auto Speed	☐	1518
5	Down	Auto Speed	☐	1518
6	Down	Auto Speed	☐	1518
7	Down	Auto Speed	☐	1518
8	Down	Auto Speed	☐	1518
9	Down	Auto Speed	☐	1518
10	Down	Auto Speed	☐	1518
11	Down	Auto Speed	☐	1518
12	Down	Auto Speed	☐	1518
13	Down	Auto Speed	☐	1518
14	Down	Auto Speed	☐	1518
15	Down	Auto Speed	☐	1518
16	Down	Auto Speed	☐	1518
17	Down	Auto Speed	☐	1518
18	Down	Auto Speed	☐	1518
19	Down	Auto Speed	☐	1518
20	Down	Auto Speed	☐	1518
21	Down	Auto Speed	☐	1518
22	Down	Auto Speed	☐	1518
23	Down	Auto Speed	☐	1518
24	Down	Auto Speed	☐	1518

Drop frames after excessive collisions	☐

Combo Port 21 is Copper Port
Combo Port 22 is Copper Port
Combo Port 23 is Copper Port
Combo Port 24 is Copper Port

Apply   Refresh

Port Configuration interface

19

VLAN Setting

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allows user to isolate network traffic so only the members of VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

ν   Assigning the VLAN ID by inputting a number (from 1~4095) into the VID text-box

ν   Grouping the members of VLAN by checking the check-box to make the selection

ν   Click Apply   to bring up the configuration interface as below:

VLAN Setting interface

VLAN Port Setting

Click VLAN Port Setting to bring up the configuration interface for adjusting the VID Setting

- ν **PVID:** Enter the Port VLAN ID

- ν **Awareness:** Enable the awareness that ports will strip the VLAN tag from received frames and insert the tag in transmitted frames (PVID). Disable the awareness that ports will not strip the tag from received frames or insert the tag in transmitted frames

- ν **Frame Type:** To set the outgoing frame

  - ¬ **Tag:** Outgoing frames with VLAN-Tagged

  - ¬ **All:** All type of frames

- ν Click Apply to apply the configuration

- ν Or, click Refresh to reset the configuration before applying

Vlan Port Setting

Port	PVID(1~4094)	Awareness	Frame Type
1	1	Disable	All
2	1	Disable	All
3	1	Disable	All
4	1	Disable	All
5	1	Disable	All
6	1	Disable	All
7	1	Disable	All
8	1	Disable	All
9	1	Disable	All
10	1	Disable	All
11	1	Disable	All
12	1	Disable	All
13	1	Disable	All
14	1	Disable	All
15	1	Disable	All
16	1	Disable	All
17	1	Disable	All
18	1	Disable	All
19	1	Disable	All
20	1	Disable	All
21	1	Disable	All
22	1	Disable	All
23	1	Disable	All
24	1	Disable	All

PVID can be set to 'none' used for trunk links. You can leave this value to none for setting PVID to none.

Apply   Refresh

VLAN Port Setting interface

Aggregation

Port trunk allows multiple links to be bundled together and act as a single physical link for increased throughput. It provides load balancing and redundancy of links in a switched inter-network. Actually, the link does not have an inherent total bandwidth equal to the sum of its component physical links. Traffic in a trunk is distributed across an individual link within the trunk in a deterministic method

that called a hash algorithm. Traffic pattern on the network should be considered carefully before applying it. When a proper hash algorithm is used, traffic is kind of randomly decided to be transmitted across either link within the trunk and load balancing will be seen.

ν   Select the group members(Normal means the port is not the trunk port)

ν   Click   Apply   to apply the configuration

ν   Or, click   Refresh   to reset the configuration before applying

Aggregation/Trunking Configuration

Group\Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
Group 1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 2																								
Group 3																								
Group 4																								
Group 5																								
Group 6																								
Group 7																								
Group 8																								

[Apply] [Refresh]

Aggregation interface

LACP Setting

The Link Aggregation Control Protocol (LACP) provides a standardization which means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an

orderly manner. Link aggregation allows user grouping up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail information refers to IEEE 802.3ad.

LACP Port Configuration

Port	Protocol Enabled	Key Value
1	☐	auto
2	☐	auto
3	☐	auto
4	☐	auto
5	☐	auto
6	☐	auto
7	☐	auto
8	☐	auto
9	☐	auto
10	☐	auto
11	☐	auto
12	☐	auto
13	☐	auto
14	☐	auto
15	☐	auto
16	☐	auto
17	☐	auto
18	☐	auto
19	☐	auto
20	☐	auto
21	☐	auto
22	☐	auto
23	☐	auto
24	☐	auto

[Apply] [Refresh]

LACP Setting interface

ν **Protocol Enable:** To enable the LACP protocol of the port

ν **Key Value:** The LACP key determines which ports potentially can be

aggregated together

ν   Click Apply   to apply the configuration

ν   Or, click Refresh   to reset the configuration before applying

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides the faster spanning tree convergence after the topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

System Configuration

ν   **System Priority:** The bridge with the lowest value has the highest priority and is selected as the root whenever the value is changed, the system must be rebooted for assigning the priority number of paths. The value must be multiple of 4096 according to the protocol standard rule.

ν   **Hello Time (1-10):** The scale of 1~10 sec will be set as a period of time that how often the switch broadcasts hello messages to other switches

ν   **Max Age (6-40):** The number of seconds (from 6~ 40) which determines the amount of time that protocol information received on a port is stored by the switch.

ν   **Forward Delay Time (4-30):** The number of seconds (from 4 ~ 30) which determines how long each of the listening and learning states will last before the port begins forwarding.

ν   **Force version:** Select the RSTP default protocol. "Normal" means RSTP protocol. "Compat" means compatible with STP protocol.

RSTP System Configuration

System Priority	32768
Hello Time (1~10)	2
Max Age (6~40)	20
Forward Delay (4~30)	15
Force version	Normal

RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost(auto|1-200000000)
Aggregations	☐		
1	☐	☑	auto
2	☐	☑	auto
3	☐	☑	auto
4	☐	☑	auto
5	☐	☑	auto
6	☐	☑	auto
7	☐	☑	auto
8	☐	☑	auto
9	☐	☑	auto
10	☐	☑	auto
11	☐	☑	auto
12	☐	☑	auto
13	☐	☑	auto
14	☐	☑	auto
15	☐	☑	auto
16	☐	☑	auto
17	☐	☑	auto
18	☐	☑	auto
19	☐	☑	auto
20	☐	☑	auto
21	☐	☑	auto
22	☐	☑	auto
23	☐	☑	auto
24	☐	☑	auto

Apply   Refresh

RSTP Configuration interface

Port Configuration

ν   **Protocol Enable:** To Enable or disable the port protocol

ν **Edge:** The port directly connected to end stations cannot create bridging loop in the network. To configure the port as an edge port, mark the port

ν **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000

ν Click Apply to apply the configuration

ν Or, click Refresh to reset the configuration before applying

802.1X Configuration

802.1x is an IEEE authentication feature which allows a client connecting to a wireless access point or wired switch, however, prevents the client from gaining access to the Internet until it provides credentials, like a user name and password that are verified by a separated server.

ν **Mode:** To disable or enable 802.1x protocol
ν **RADIUS IP:** Set the Radius Server IP address
ν **RADIUS UDP Port:** Set the UDP destination port for authentication requests to the specified Radius Server
ν **RADIUS Secret:** Set an encryption key for use during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server
ν **Admin State:** Select the state of port
    ¬ **Force Authorized:** The specified port is required to be held in the unauthorized state
    ¬ **Force Unauthorized:** The specified port is required to be held in the authorized state
    ¬ **Auto:** The specified port is set to the authorized or unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server

802.1X Configuration

Mode:	Disabled				
RADIUS IP	0.0.0.0				
RADIUS UDP Port	1812				
RADIUS Secret					

Port	Admin State	Port State			
1	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
2	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
3	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
4	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
5	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
6	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
7	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
8	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
9	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
10	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
11	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
12	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
13	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
14	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
15	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
16	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
17	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
18	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
19	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
20	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
21	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
22	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
23	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
24	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
			Re-authenticate All	Force Reinitialize All	

[Parameters]

[Apply] [Refresh]

802.1X Configuration interface

- ν **Re-authenticate:** Restart authentication process for the port
- ν **Force Reinitialize:** Restart authentication process for the port
- ν **Statistics:** Click to view each port statistic

ν   **Re-authenticate All:** Restart authentication process for all the port

ν   **Force reinitialize All:** Restart authentication process for all the port

ν   Click   Apply   to apply the configuration

ν   Or, click   Refresh   to reset the configuration before applying

Parameters Configuration

ν   **Reauthentication Enable:** Enable the re-authentication mode

ν   **Reauthentication period (1~3600 seconds):** Set the period of time after which clients connected must be re-authenticated

ν   **EPA Timeout (1~255 seconds:** Set the period of time the switch waits for a supplicant response to an EAP request

ν   Click   Apply   to apply the configuration

ν   Or, click   Refresh   to reset the configuration before applying

802.1X Parameters

Reauthentication Enabled	☐ Enabled
Reauthentication Period [1-3600 seconds]	3600
EAP timeout [1 - 255 seconds]	30
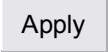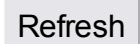
Apply   Refresh

IGMP Snooping

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect

IGMP queries and report packets and manage IP multicast traffic through the switch.

The switch support IP multicast that IGMP protocol can be enabled on switch then displays the IGMP snooping information. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

ν   **IGMP Enable:** To enable or disable IGMP function

ν   **Router Ports:** A static router port. It is a port that has a multicast router, which has a connection to the internet, attached to it. Selecting a router port will allow multicast packets coming from the router to be propagated through the network, as well as allowing multicast messages (IGMP) coming from the network to be propagated to the router. All IGMP Report packets will be forwarded to the router port, and IGMP queries (from the router port) will be flooded to all ports. All UDP multicast packets will be forwarded to the router port because routers do not send IGMP reports or implement IGMP snooping.

ν   **Unregistered IPMC Flooding Enable: To** enable unregistered IP multicast flooding

ν   **IGMP Snooping Enabled:** To enable or disable the IGMP protocol of VLAN group

ν   **Quick Search VLAN Entry, VLAN ID:** Enter the VLAN ID number to quick search the VLAN group.

ν   Click [Apply] to apply the configuration

ν   Or, click [Refresh] to reset the configuration before applying

IGMP Snooping interface

QoS Setting

Configuring QoS mode of the port, per port priority, TOS and COS priority setting.

ν **Mode:** Select the QoS mode – port, DSCP or vlantag

ν **Port Priority:** select the priority level – low, normal, medium or high

ν Click   Apply   to apply the configuration

ν Click   Refresh   to reset the configuration before applying

QoS Configuration

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

Vlan tag Mapping

DSCP Mapping

Priority Queue Service

Apply   Refresh

QoS Configuration interface

ν   Click VLAN tag Mapping to enter VLAN tag priority configuration interface.

Select the VLAN tap priority level 0~7

ν   Click Apply to apply the configuration

ν   Or, click Refresh to reset the configuration before applying

32

QoS Vlan Tag Priority Mapping

Port	ValnTag=0	ValnTag=1	ValnTag=2	ValnTag=3	ValnTag=4	ValnTag=5	ValnTag=6	ValnTag=7
1	normal	low	low	normal	medium	medium	high	high
2	normal	low	low	normal	medium	medium	high	high
3	normal	low	low	normal	medium	medium	high	high
4	normal	low	low	normal	medium	medium	high	high
5	normal	low	low	normal	medium	medium	high	high
6	normal	low	low	normal	medium	medium	high	high
7	normal	low	low	normal	medium	medium	high	high
8	normal	low	low	normal	medium	medium	high	high
9	normal	low	low	normal	medium	medium	high	high
10	normal	low	low	normal	medium	medium	high	high
11	normal	low	low	normal	medium	medium	high	high
12	normal	low	low	normal	medium	medium	high	high
13	normal	low	low	normal	medium	medium	high	high
14	normal	low	low	normal	medium	medium	high	high
15	normal	low	low	normal	medium	medium	high	high
16	normal	low	low	normal	medium	medium	high	high
17	normal	low	low	normal	medium	medium	high	high
18	normal	low	low	normal	medium	medium	high	high
19	normal	low	low	normal	medium	medium	high	high
20	normal	low	low	normal	medium	medium	high	high
21	normal	low	low	normal	medium	medium	high	high
22	normal	low	low	normal	medium	medium	high	high
23	normal	low	low	normal	medium	medium	high	high
24	normal	low	low	normal	medium	medium	high	high

Apply   Refresh

QoS VLAN Tag Priority Mapping interface

ν Click DSCP Mapping to enter TOS priority configuration interface

¬ **DSCP [0- 63]:** the system provides 0~63 TOS priority level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example: user set the TOS level 25 is high. The port 1 is following the TOS priority policy. When the packet received by port 1, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), and then the packet priority will have highest priority

¬ **Priority:** select the priority level – high, medium, low or normal

ν Click Apply to apply the configuration

ν Or, press Refresh to reset the configuration before applying

QoS DSCP Mapping

DSCP [0-63]	Priority
	high
	high
	high
	high
	high
	high
	high
All others	high

Apply   Refresh

QoS DSCP Mapping interface

Filter Configuration

Filter the specific IP address on port that it can ensure the network security.

■ **Mode:** Select the mode – DHCP or Static

〕 **DHCP:** If the port is DHCP client enabling, the IP Address will automatically display in IP Address column

〕 **Static:** Key in a specific IP Address and IP Mask for filtering

■ **IP Address:** Key in the specific IP Address to filter

■ **IP Mask:** Key in the IP Mask of the IP Address

- **DHCP Server Allowed:** Allowing DHCP server packet to pass through this port

- Click Apply to apply the configuration

- Or, press Refresh to reset the configuration before applying

Filter Configuration

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled			☑
2	Disabled			☑
3	Disabled			☑
4	Disabled			☑
5	Disabled			☑
6	Disabled			☑
7	Disabled			☑
8	Disabled			☑
9	Disabled			☑
10	Disabled			☑
11	Disabled			☑
12	Disabled			☑
13	Disabled			☑
14	Disabled			☑
15	Disabled			☑
16	Disabled			☑
17	Disabled			☑
18	Disabled			☑
19	Disabled			☑
20	Disabled			☑
21	Disabled			☑
22	Disabled			☑
23	Disabled			☑
24	Disabled			☑

Apply Refresh

Filter Configuration interface

Rate Limiting

- **Storm Control:** The traffic storm control prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical

interfaces.

- ⌐ **ICMP Rate:** Select the ICMP traffic storm control rate
- ⌐ **Learn Frames Rate:** The learn frame rate is that the packet rate is learned and unicast. Learn Frames Rate is to find the Ethernet transfer rate but for the un-learn and flooding packets rate are no effect.
- ⌐ **Broadcast Rate:** Select the broadcast traffic storm control rate
- ⌐ **Multicast Rate:** Select the multicast traffic storm control rate
- ⌐ **Flooded unicast Rate:** Select the unicast traffic rate

■ **Policer:** Enter the port effective egress rate

■ **Sharper:** Enter the port effective ingress rate

■ Click ⬚ Apply to apply the configuration

■ Or, press ⬚ Refresh to reset the configuration before applying

Rate Limit Configuration

Storm Control Number of frames per second	
ICMP Rate	No Limit
Learn Frames Rate	No Limit
Broadcast Rate	No Limit
Multicast Rate	No Limit
Flooded unicast Rate	No Limit

Port	Policer	Shaper
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit
8	No Limit	No Limit
9	No Limit	No Limit
10	No Limit	No Limit
11	No Limit	No Limit
12	No Limit	No Limit
13	No Limit	No Limit
14	No Limit	No Limit
15	No Limit	No Limit
16	No Limit	No Limit
17	No Limit	No Limit
18	No Limit	No Limit
19	No Limit	No Limit
20	No Limit	No Limit
21	No Limit	No Limit
22	No Limit	No Limit
23	No Limit	No Limit
24	No Limit	No Limit

Apply   Refresh

Rate Limit Configuration interface

Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic goes in or out monitored ports will be duplicated into analysis port.

- **Analysis Port:** It means mirror port can be used to see all monitor port traffic. (Mirror port can be connected to LAN analyzer or Netxray)
- **Monitor Port:** the ports which wants to be monitored. All monitor port traffic will be copied to analysis port. Maximum 23 monitor ports can be selected.
- Click Apply to apply the configuration
- Or, press Refresh to reset the configuration before applying

Port Mirroring

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

Apply   Refresh

Port Mirroring Configuration interface

Statistics Overview

The following information provides the current port statistic information

Press Clear button to clean all counts, and then click Refresh to get the new setting information as below:

Statistics Overview for all ports

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	0	0	0	0	0	0
2	1459648	14996	80806389	692872	0	0
3	0	0	0	0	0	0
4	20566778	59671	1138597	14660	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
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	0	0	0	0	0	0
23	0	0	0	0	0	0
24	0	0	0	0	0	0

Clear   Refresh

Statistics Overview interface

Statistics Detail

The following information provides statistic detail information of statistic on each port, and simply selecting the port to viewing the statistic information.

Press Clear button to clean all counts, and then click Refresh to get the new setting information as below:

Statistics for Port 1

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

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	-	Tx Broadcast	-
Rx Multicast	-	Tx Multicast	-
Rx Broad- and Multicast	0	Tx Broad- and Multicast	0
Rx Error Packets	0	Tx Error Packets	0

Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	-	Tx 64 Bytes	-
Rx 65-127 Bytes	-	Tx 65-127 Bytes	-
Rx 128-255 Bytes	-	Tx 128-255 Bytes	-
Rx 256-511 Bytes	-	Tx 256-511 Bytes	-
Rx 512-1023 Bytes	-	Tx 512-1023 Bytes	-
Rx 1024- Bytes	-	Tx 1024- Bytes	-

Receive Error Counters		Transmit Error Counters	
Rx CRC/Aligment	-	Tx Collisions	-
Rx Undersize	-	Tx Drops	-
Rx Oversize	-	Tx Overflow	-
Rx Fragments	-		
Rx Jabber	-		
Rx Drops	-		

Clear   Refresh

Statistics Detail interface

LACP Status

When the LACP aggregator is setup, the related information will be shown as below:

LACP Aggregation Overview

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

Legend

	Down	Port link down
0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0	Learning	Port Learning by RSTP
	Forwarding	Port link up and forwarding frames
0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

LACP Port Status

Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		
4	no		
5	no		
6	no		
7	no		
8	no		
9	no		
10	no		
11	no		
12	no		
13	no		
14	no		
15	no		
16	no		
17	no		
18	no		
19	no		
20	no		
21	no		
22	no		
23	no		
24	no		

Refresh

LACP Status interface

Spanning Tree Status

Click Refresh to get the newest configuration information. The Rapid Spanning Tree Protocol information will display as below:

RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-ff-38-ff-f2-f2	2	20	15	Steady	This switch is Root!

RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP
Port 9						Non-STP
Port 10						Non-STP
Port 11						Non-STP
Port 12						Non-STP
Port 13						Non-STP
Port 14						Non-STP
Port 15						Non-STP
Port 16						Non-STP
Port 17						Non-STP
Port 18						Non-STP
Port 19						Non-STP
Port 20						Non-STP
Port 21						Non-STP
Port 22						Non-STP
Port 23						Non-STP
Port 24						Non-STP

[Refresh]

RSTP Status interface

IGMP Status

IGMP Snooping information will be shown as below:

IGMP Status

Current Page:1   Total Page:1

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

Quick Search Vlan Entry, Vlan ID: [ ] Search

Refresh   FirstPage   PrePage   NextPage   EndPage

IGMP Status interface

Warm Restart

Reboot the switch in software reset. All the configurations will be reminded

Click Yes to restart the system

Warm Restart

Are you sure you want to perform a Warm Restart? Yes No

System Restart interface

Factory Default

Reset switch to default configuration

Click [Yes] to reset the all configuration to the default value

Factory Default

Are you sure you want to perform a Factory Default and Warm Restart? [Yes] [No]

Factory Default interface

Firmware Upload

The system provides the Web GUI firmware update function which would allow the user to update the switch firmware

Click [Browse] to locate the firmware and press [Upload] to update the firmware

Software Upload
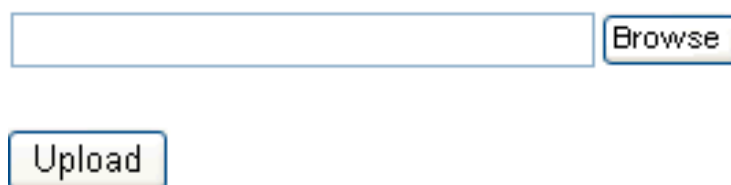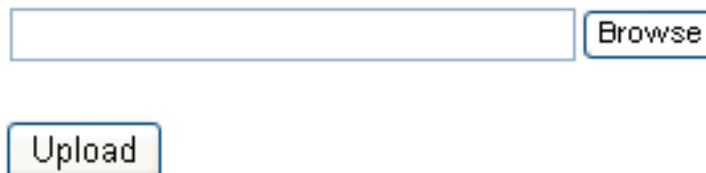
[   ] [Browse]

[Upload]

Firmware Upload interface

Configuration File Transfer

User can restore configuration value through the WEB GUI

ν   Click Browse to locate the configuration value file

ν   And then, press Upload to restore the configuration value

Configuration Upload

Browse

Upload

Configuration Download

Download

Configuration File Transfer interface

To backup the configuration value

ν   Click Download , and then follow the system instruction which will guide

user to complete the configuration value download

Troubleshooting

This section is intended to help user to solve the most common problems on the SmartGST-2404GM Switch.

Incorrect connections

The switch port can auto detect straight or crossover cable when the switch link with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps port use 2 pair twisted cable and Gigabit 1000T port use 4 pair twisted cable. If the RJ-45 connector is not correct pin on right position then the link will fail.   For fiber connection, please notice that fiber cable mode and fiber module should be the same.

Faulty or loose cables

Look for loose or obvious faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.

Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problems, and can seriously impair network performance. A category-5 cable tester is a recommended tool for every 100Base-T network installation.

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100 Ω Category 3, 4 or 5 cable for 10Mbps

connections or 100Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5 or cat-5e cable for 1000Mbps connections. The length does not exceed 100 meters.

Improper Network Topologies

It is important to make sure that user had a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, user should make sure that network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact network performance.

Diagnosing LED Indicators

The switch can be easily monitored through panel indicators to assist in identifying problems, which describes common problems you may encounter and where user can find possible solutions.

If the power indicator does turn on when the power cord is plugged in, user may have a problem with power outlet, or power cord. However, if the switch powers off after running for a while check for loose power connections, power losses or surges at power outlet. If the problem still cannot be resolved, contact the local dealer for assistance.

Technical Specification

This section provides the specifications of SmartGST-2404GM Switch and the following table lists these specifications.

Standard	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000Base-T IEEE 802.3z Gigabit Fiber IEEE 802.3x Flow Control and Back-pressure IEEE 802.1d Spanning Tree IEEE 802.w Rapid Spanning Tree IEEE 802.3ad Port trunk with LACP IEEE 802.1p Class of Service IEEE 802.1Q VLAN Tag
Network Cable	10BASE-T: 2-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m) 100BASE-TX: 2-pair UTP/STP CAT. 5 cable EIA/TIA-568 100-ohm (100m) Gigabit Copper: 4 pair UTP/STP CAT. 5 cable EIA/TIA 568 100-ohm (100M)
LED Indicators	Per RJ-45 port: 1000 (green), Link/Activity (green) Per MINI GBIC: Link/Activity (Green) Per unit: Power

Connector	Gigabit copper: 24 x RJ-45 with Auto-MDIX MINI GBIC: 4 x MINI GBIC socket (3.3v); shared with last 4-port RJ-45
Switch architecture	Store and forward switch architecture
Jumbo packet	Support 10Kbytes jumbo packet size
Back-plane	48Gbps, 71.42Mpps throughput @64bytes
MAC address	8K Mac with Auto Learning
Memory Buffer	500Kbytes
Power Supply	AC 100~240V, 50/60Hz
Power Consumption (DC)	AC: 65Watt (maximum)　DC:19W(maximum)
Dimensions	440mm x 161mm x 44mm (L x W x H)
Operation Temperature	0℃ to 45℃ (32℉ to 113℉)
Operation Humidity	10% to 90% (Non-condensing)
EMI	FCC Class A, CE
Safety	UL, cUL

Appendix

Cables

The RJ-45 ports on the switch support automatic MDI/MDI-X operation, so you can use standard straight-through twisted-pair cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

ν   **Cable Types and Specifications**

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	100 m (328 ft)	RJ-45
100BASE-FX	50/125 or 62.5/125 micron core multimode fiber (MMF)	2 km (1.24 miles)	SC or ST

Cable specification table

100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

ν   **RJ-45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

[NOTE] "+" and "-" signs represent the polarity of the wires that make up each

wire pair.

All ports on this switch support automatic MDI/MDI-X operation, you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

Pin MDI-X	Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)