



# ALL-SG4816CW

Smart managed 16 Port Gigabit/Combo(TP/SFP) Switch

+ 2 SFP Slots



## User Manual

**Default-IP**  
**192.168.2.1**

**Password:**  
**admin**

### **FCC Warning**

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

### **CE Mark Warning**

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

# Content

---

<b>Introduction.....</b>	<b>4</b>
Product Overview.....	4
Web Management Features .....	4
Specifications.....	4
Mechanical .....	5
Performance .....	5
Package Contents.....	6
<b>Hardware Description .....</b>	<b>7</b>
Physical Dimensions/ Weight .....	7
Front Panel .....	7
LED Indicators.....	8
Rear Panel .....	8
Hardware Installation .....	8
<b>Software Description.....</b>	<b>9</b>
Login.....	9
Configuration.....	10
System .....	10
Ports .....	11
VLAN .....	13
Aggregation .....	14
LACP .....	15
RSTP.....	16
802.1X .....	18
IGMP Snooping.....	19
Mirroring.....	20
Quality of Service (QoS) .....	21
Filter Configuration.....	23
Rate Limit Configuration .....	24
Storm Control .....	25
Monitoring.....	26
Statistics Overview.....	26
Detailed Statistics .....	26
LACP Status.....	27
RSTP Status.....	28
IGMP Status.....	31

© ALLNET GmbH Computersysteme 2014 - Alle Rechte vorbehalten

VeriPHY .....	32
Ping .....	33
Maintenance .....	34
Warm Restart.....	34
Factory Default .....	34
Software upload .....	35
Configuration File Transfer .....	35
Logout.....	36

# Introduction

---

## Product Overview

This switch is a Management Switch equipped with 16 10/100/1000BaseT(X) UTP/SFP combo ports + 2 Gigabit SFP Open Slots. It is designed for easy installation and high performance in an environment where traffic is on the network and the number of users increased continuously. The compact rigid 19" rack-mount size is specifically designed for small to medium workgroups. It provides smooth network migration and is easy to upgrade the network capacity.

In addition, the switch features comprehensive and useful function such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP, IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

## Web Management Features

- Port Management
  - Port Mirroring
  - Bandwidth Control
  - Broadcast Storm Control
- VLAN Setting
  - Port-based/ Tag-based
- Trunking
  - Aggregation / LACP
- QoS Setting
  - 802.1p/DSCP
- Spanning tree
  - STP/RSTP
- Security Setting
  - 802.1X /IP Filter/SNMP
- IGMP Snooping

## Specifications

- Standard

© ALLNET GmbH Computersysteme 2014 - Alle Rechte vorbehalten

IEEE 802.3 10BaseT  
IEEE 802.3u 100BaseTX  
IEEE 802.ab 1000BaseT  
IEEE 802.3z 1000BaseSX/LX  
IEEE 802.3x Flow Control  
IEEE 802.1x Port-based Network Access Control  
IEEE 802.1Q VLAN Tagging  
IEEE 802.3ad Port Aggregation  
IEEE 802.1d Spanning tree protocol  
IEEE 802.1w Rapid Spanning tree protocol  
IEEE 802.1p Class of service, Priority Protocols

➤ Number of Port

16 10/100/1000BaseT(X) UTP/SFP combo ports + 2 Gigabit SFP Open Slots

## **Mechanical**

➤ LED Indicator

Per Port: LINK/ ACT, 1000

Per Unit: Power

➤ Power Input: 100~240V/AC, 50~60HZ

➤ Product Dimensions/ Weight

44 × 440 × 220 mm (H × W ×D) / 3kg

## **Performance**

➤ MAC Address: 8K

➤ Buffer Memory: 500K Bytes

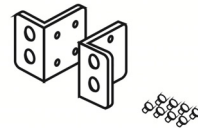
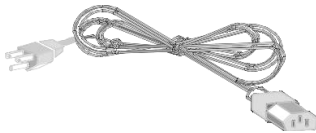
➤ Jumbo Frames: 9.6K

➤ Transmission Method: Store and Forward

## Package Contents

Before you start to install this switch, please verify your package that contains the following items:

- One Gigabit Ethernet Switch
- One Power Cord
- CD : User Manual
- Rack-mount kit



# Hardware Description

---

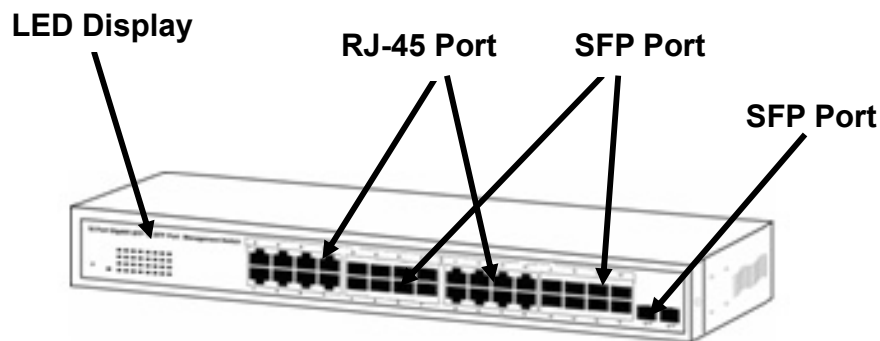
This part primarily presents hardware of the web-smart switch, physical dimensions and functional overview would be described.

## Physical Dimensions/ Weight

44 x 440 x 220 mm (H x W x D) /3kg

## Front Panel

The front Panel of the web-smart Switch consists of 16 10/100/1000BaseT(X) UTP/SFP combo ports + 2 Gigabit SFP Open Slots. All of LED Indicators are also located on the front panel.



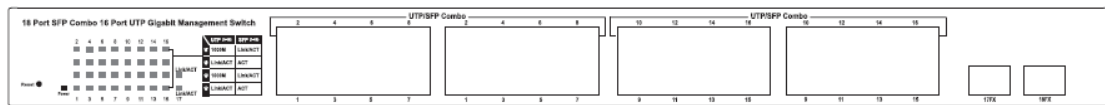


## LED Indicators

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

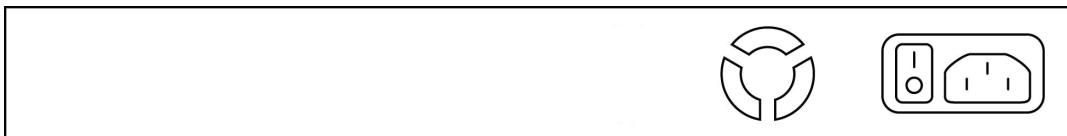
**Table 1-1 LED Indicators**

LED		Status	Description
Power		On	Power on
		off	Power off
UTP (1-16)	1000	On	Port is linked to 1000M
		Off	Port isn't linked to 1000M
	Link/ACT	On	Link
		Flashing	Data activating
SFP (1-18)	Link/ACT (1-18)	On	Link
		Flashing	Data activating
	ACT (1-16)	On	Link
		Flashing	Data activating



## Rear Panel

The 3-pronged power plug is placed at the rear panel which is on the right side of the switch shown as below.



## Hardware Installation

Set the switch on a large flat space with a power socket close by. The flat space 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. The last, use twisted pair cable to connect this switch to your PC then user could start to operate the switch.

# Software Description

---

This part instructs user how to set up and manage the switch through the web user interface. Please follow the description to understand the procedure.

At the first, open the web browser, and go to **192.168.2.1** site then the user will see the login screen. Key in the password to pass the authentication then clicks the **Apply**. The login process is completed and comes out the sign "Password successfully entered".

## Login

Password: **admin**



Figure 1-1

After the user login, the right side of website shows all functions as Fig. 1-2.

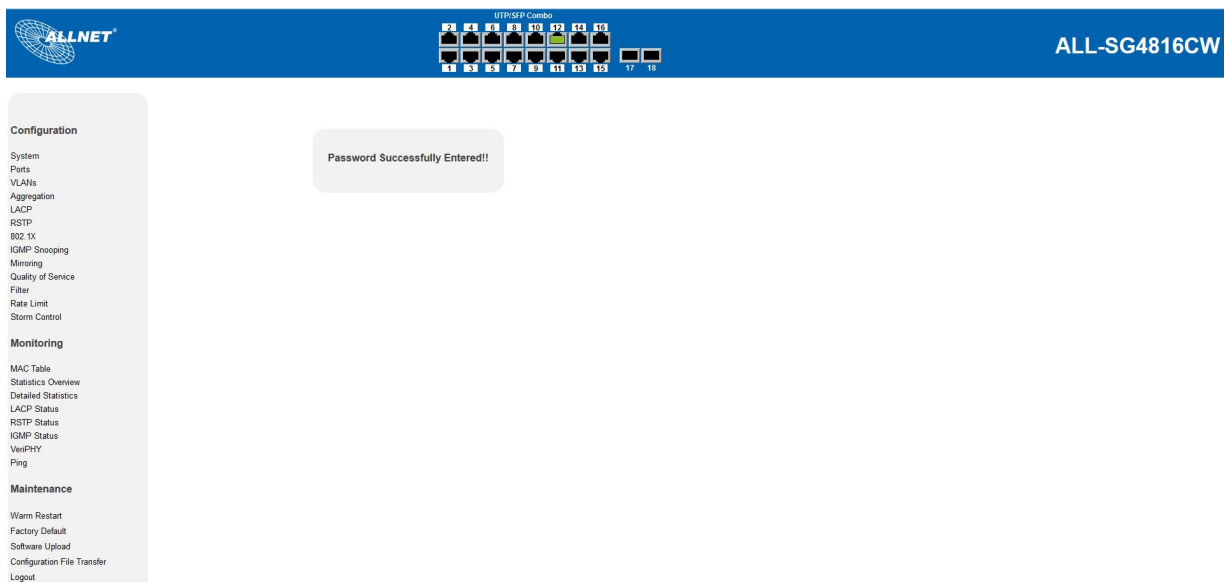


Figure 1-2

## **Configuration**

### System

#### System Configuration

This page shows system configuration information. User can configure lots of information as below:

**Configuration**  
[System](#)  
Ports  
VLANs  
Aggregation  
LACP  
RSTP  
802.1X  
IGMP Snooping  
Mirroring  
Quality of Service  
Filter  
Rate Limit  
Storm Control

**Monitoring**  
MAC Table  
Statistics Overview  
Detailed Statistics  
LACP Status  
RSTP Status  
IGMP Status  
VeriPHY  
Ping

**Maintenance**  
Warm Restart  
Factory Default  
Software Upload  
Configuration File Transfer  
Logout

**System Configuration**

MAC Address	00-03-ce-14-6f-a5
S/W Version	G18 V130603
H/W Version	1.0
System Up-Time	0 days 02:49:07
Active IP Address	192.168.2.1
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.2.254
DHCP Server	0.0.0.0
Lease Time Left	0 secs

DHCP Enabled	<input type="checkbox"/>
Fallback IP Address	<input type="text" value="192.168.2.1"/>
Fallback Subnet Mask	<input type="text" value="255.255.255.0"/>
Fallback Gateway	<input type="text" value="192.168.2.254"/>
Management VLAN	<input type="text" value="1"/>
Name	<input type="text"/>
Password	<input type="password" value="•••••"/>
Inactivity Timeout (secs)	<input type="text" value="0"/>
SNMP enabled	<input checked="" type="checkbox"/>
SNMP Trap destination	<input type="text" value="0.0.0.0"/>
SNMP Read Community	<input type="text" value="public"/>
SNMP Write Community	<input type="text" value="private"/>
SNMP Trap Community	<input type="text" value="public"/>

**Figure 2-1**

- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default).
- **S/W Version:** Displays the switch's firmware version.
- **H/W Version:** Displays the switch's Hardware version.
- **DHCP Enabled:** Click the box to enable DHCP
- **Fallback IP address:** Manually assign the IP address that the network is

using. The default IP is 192.168.2.1

- Fallback Subnet Mask: Assign the subnet mask to the IP address
- Fallback Gateway: Assign the network gateway for industrial switch. The default gateway is 0.0.0.0.
- Management VLAN: ID of a configured VLAN (1-4094) through which you can manage the switch. By default, all ports on the switch are members of VLAN 1. However, if the management VLAN is changed, the management station must be attached to a port belonging to this VLAN.
- Name: Type in the new user name (The default value is 'admin').
- Password: Type in the new password (The default value is 'admin').
- SNMP Enabled: Enables or disables SNMP on the switch. Supports SNMP version 1 and 2c management clients.
- SNMP Trap Destination: IP address of the trap manager to receive notification messages from this switch. Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station.
- SNMP Read Community: A community string that acts like a password and permits access to the SNMP database on this switch.
- SNMP Trap Community: Community string sent with the notification operation.

## Ports

Port Security ensures access to a switch port based on MAC address, limits the total number of devices from using a switch port, and protects against MAC flooding attacks.

## Port Configuration

In Port Configuration, you can set and view the operation mode for each port.

- Enable Jumbo Frames: This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- Power Saving Mode: Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements.
- Mode: allow user to manually set the port speed such as Auto, 10 half, 10 Full, 100 Half, 100 Full, 1000 Full or Disabled. User may press Apply button to complete the configuration procedure.

Configuration

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

Monitoring

MAC Table
Statistics Overview
Detailed Statistics
LACP Status
RSTP Status
IGMP Status
VeriPHY
Ping

Maintenance

Warm Restart
Factory Default
Software Upload
Configuration File Transfer
Logout

Port Configuration

Enable Jumbo Frames ☐

PERFECT\_REACH/Power Saving Mode: Disable

Port	Link	Mode	Flow Control
1	Down	Auto Speed ▾	<input type="checkbox"/>
2	Down	Auto Speed ▾	<input type="checkbox"/>
3	Down	Auto Speed ▾	<input type="checkbox"/>
4	Down	Auto Speed ▾	<input type="checkbox"/>
5	Down	Auto Speed ▾	<input type="checkbox"/>
6	Down	Auto Speed ▾	<input type="checkbox"/>
7	Down	Auto Speed ▾	<input type="checkbox"/>
8	Down	Auto Speed ▾	<input type="checkbox"/>
9	Down	Auto Speed ▾	<input type="checkbox"/>
10	Down	Auto Speed ▾	<input type="checkbox"/>
11	Down	Auto Speed ▾	<input type="checkbox"/>
12	1000FDX	Auto Speed ▾	<input type="checkbox"/>
13	Down	Auto Speed ▾	<input type="checkbox"/>
14	Down	Auto Speed ▾	<input type="checkbox"/>
15	Down	Auto Speed ▾	<input type="checkbox"/>
16	Down	Auto Speed ▾	<input type="checkbox"/>
17	Down	Auto Speed ▾	<input type="checkbox"/>
18	Down	Auto Speed ▾	<input type="checkbox"/>

Drop frames after excessive collisions ☐

Apply Refresh

Figure 2-2

## VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same 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.

### Port Segmentation (VLAN) Configuration

- VLAN ID: ID of configured VLAN (1-4094, no leading zeroes).
- VLAN Configuration List: Lists all the current VLAN groups created for this system. Up to 16 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

**Configuration**

- System
- Ports
- VLANs**
- Aggregation
- LACP
- RSTP
- 802.1X
- IGMP Snooping
- Mirroring
- Quality of Service
- Filter
- Rate Limit
- Storm Control

**Monitoring**

- MAC Table
- Statistics Overview
- Detailed Statistics
- LACP Status
- RSTP Status
- IGMP Status
- VeriPHY
- Ping

**Maintenance**

- Warm Restart
- Factory Default
- Software Upload
- Configuration File Transfer
- Logout

**Port Segmentation (VLAN) Configuration**

Add a VLAN

VLAN ID

Add

**VLAN Configuration List**

1							
---	--	--	--	--	--	--	--

Modify Delete Refresh

Port Config

**Figure 2-3**

## 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. The hash algorithm automatically applies load balancing to the ports in the trunk. A port failure within the trunk group causes the network traffic to be directed to the remaining ports. Load balancing is maintained whenever a link in a trunk is lost or returned to service.

### Aggregation / Trunking Configuration

To assign a port to a trunk, click the required trunk number, then click Apply.

**Configuration**  
System  
Ports  
VLANs  
Aggregation  
LACP  
RSTP  
802.1X  
IGMP Snooping  
Mirroring  
Quality of Service  
Filter  
Rate Limit  
Storm Control

**Monitoring**  
MAC Table  
Statistics Overview  
Detailed Statistics  
LACP Status  
RSTP Status  
IGMP Status  
VeriPHY  
Ping

**Maintenance**  
Warm Restart  
Factory Default  
Software Upload  
Configuration File Transfer  
Logout

**Aggregation/Trunking Configuration** 

**Figure 2-4**

## LACP

IEEE 802.3ad Link Aggregation Control Protocol (LACP) increases bandwidth by automatically aggregating several physical links together as a logical trunk and providing load balancing and fault tolerance for uplink connections.

### LACP Port Configuration

- Port: The port number.
- Enabled: Enables LACP on the associated port.
- Key Value: Configures a port's LACP administration key. The port administrative key must be set to the same value for ports that belong to the same link aggregation group (LAG). If this administrative key is not set when an LAG is formed (i.e., it has the null value of 0), this key will automatically be set to the same value as that used by the LAG.



**Configuration**  
System  
Ports  
VLANs  
Aggregation  
LACP  
RSTP  
802.1X  
IGMP Snooping  
Mirroring  
Quality of Service  
Filter  
Rate Limit  
Storm Control

**Monitoring**  
MAC Table  
Statistics Overview  
Detailed Statistics  
LACP Status  
RSTP Status  
IGMP Status  
VeriPHY  
Ping

**Maintenance**  
Warm Restart  
Factory Default  
Software Upload  
Configuration File Transfer  
Logout

**LACP Port Configuration**

Port	Protocol Enabled	Key Value
1	<input type="checkbox"/>	auto
2	<input type="checkbox"/>	auto
3	<input type="checkbox"/>	auto
4	<input type="checkbox"/>	auto
5	<input type="checkbox"/>	auto
6	<input type="checkbox"/>	auto
7	<input type="checkbox"/>	auto
8	<input type="checkbox"/>	auto
9	<input type="checkbox"/>	auto
10	<input type="checkbox"/>	auto
11	<input type="checkbox"/>	auto
12	<input type="checkbox"/>	auto
13	<input type="checkbox"/>	auto
14	<input type="checkbox"/>	auto
15	<input type="checkbox"/>	auto
16	<input type="checkbox"/>	auto
17	<input type="checkbox"/>	auto
18	<input type="checkbox"/>	auto

Apply Refresh

**Figure 2-5**



## RSTP

IEEE 802.1w Rapid Spanning tree protocol (LACP) provides a loop-free network and redundant links to the core network with rapid convergence to ensure faster recovery from failed links, enhancing overall network stability and reliability.

### RSTP System Configuration

- **System Priority:** This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Number between 0 - 61440 in increments of 4096. Therefore, there are 16 distinct values.
- **Hello Time:** Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Number between 1-10 (default is 2).
- **Max Age –** The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. That also means the maximum life time for a BPDU frame. Number between 6-40 (default is 20).
- **Forward Delay:** The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). Number between 4 – 30 (default is 15).
- **Force Version:** Set and show the RSTP protocol to use. Normal - use RSTP, Compatible - compatible with STP.

### **RSTP System Configuration**

System Priority	32768 ▾
Hello Time	2
Max Age	20
Forward Delay	15
Force version	Normal ▾

**Figure 2-6-1**

### RSTP Port Configuration

- Port: The port ID. It cannot be changed. Aggregations mean any configured trunk group.
- Enabled: Click on the tick-box to enable/disable the RSTP protocol for the port.
- Edge: Expect the port to be an edge port (linking to an end station) or a link to another STP device.
- Path Cost: This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Set the RSTP path cost on the port. Number between 0 - 200000000. 0 means auto generated path cost.

### **RSTP Port Configuration**

Port	Protocol Enabled	Edge	Path Cost
Aggregations	<input type="checkbox"/>		
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
11	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
13	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
14	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
17	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
18	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto

Apply

Refresh

**Figure 2-6-2**

## 802.1X

802.1X provides port-based authentication, which involves communications between a supplicant, authenticator, and authentication server. Port refers to a single point of attachment to the LAN infrastructure. The supplicant is often software on a client device, such as a laptop; the authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

Port-based Network access control (PNAC) ensures all users are authorized before being granted access to the network. User authentication is carried out using any standard-based RADIUS server.

### 802.1X Configuration

- **Mode:** Enables or disables 802.1X globally for all ports on the switch. The 802.1X protocol must be enabled globally for the switch before the port settings are active. (Default: Disabled)
- **RADIUS IP:** Address of authentication server.
- **RADIUS UDP Port:** Network port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
- **RADIUS Secret:** Sets the text string used for encryption between the switch and the RADIUS server. This key is used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 48 characters).

**Configuration**

System  
Ports  
VLANs  
Aggregation  
LACP  
RSTP  
**802.1X**  
IGMP Snooping  
Mirroring  
Quality of Service  
Filter  
Rate Limit  
Storm Control

**Monitoring**

MAC Table  
Statistics Overview  
Detailed Statistics  
LACP Status  
RSTP Status  
IGMP Status  
VeniPHY  
Ping

**Maintenance**

Warm Restart  
Factory Default  
Software Upload  
Configuration File Transfer  
Logout

**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	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
2	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
3	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
4	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
5	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
6	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
7	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
8	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
9	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
10	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
11	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
12	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
13	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
14	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
15	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
16	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
17	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
18	Force Authorized ▾	802.1X Disabled	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
			<a href="#">Re-authenticate All</a>	<a href="#">Force Reinitialize All</a>	

Parameters

Apply Refresh

Figure 2-7

## IGMP Snooping

IGMP Snooping is the process of listening to IGMP network traffic. IGMP Snooping, as implied by the name, is a feature that allows a layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer3 IGMP packets sent in a multicast network.

When IGMP Snooping is enabled in a switch, it analyzes all IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. Moreover, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

Prevents flooding of IP multicast traffic, and limits bandwidth intensive video traffic to only the subscribers.

### IGMP Configuration

- IGMP Enabled: When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
- Router Ports: Set if ports are connecting to the IGMP administrative routers.
- Unregistered IPMC Flooding enabled: Set the forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled, and forward to router-ports only when disabled.
- IGMP Snooping Enabled: When enabled, the port will monitor network traffic to determine which hosts want to receive the multicast traffic.
- IGMP Querying Enabled: When enabled, the port can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic.

### IGMP Configuration

IGMP Enabled	<input type="checkbox"/>
Router Ports	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/>
Unregistered IPMC Flooding enabled	<input checked="" type="checkbox"/>

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Figure 2-8**

## Mirroring

Port Mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

### Mirroring Configuration

- Port to Mirror to: The port that will “duplicate” or “mirror” the traffic on the source port. Only incoming packets can be mirrored. Packets will be dropped when the available egress bandwidth is less than ingress bandwidth.
- Ports to Mirror: Select the ports that you want to mirror from this section of the page. A port will be mirrored when the “Mirroring Enabled” check-box is checked.

Port	Mirror Source
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>
11	<input type="checkbox"/>
12	<input type="checkbox"/>
13	<input type="checkbox"/>
14	<input type="checkbox"/>
15	<input type="checkbox"/>
16	<input type="checkbox"/>
17	<input type="checkbox"/>
18	<input type="checkbox"/>

Mirror Port: 1 ▼

Apply Refresh

Figure 2-9

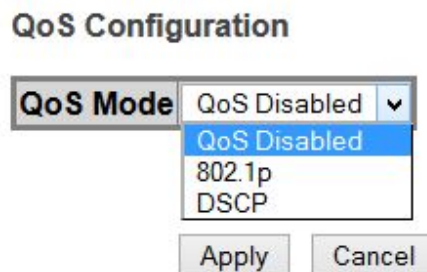
## Quality of Service (QoS)

In QoS Mode, select QoS Disabled, 802.1p, or DSCP to configure the related parameters.

### QoS Configuration

- Strict: Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- WRR: Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights with default values of 1, 2, 4, 8 for queues 0 through 7, respectively. (This is the default selection.)

※Note: WRR can only be selected if Jumbo Frame mode is disabled on the Port Configuration page



**Figure 2-10-1**

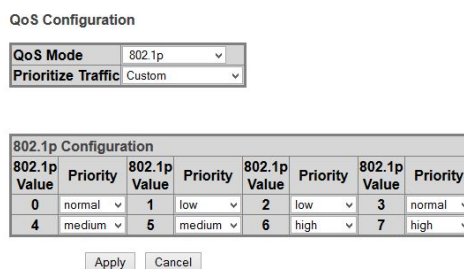
### QoS Mode: QoS Disabled

When the QoS Mode is set to QoS Disabled, the following table is displayed.

### QoS Mode: 802.1p

Packets are prioritized using the 802.1p field in the VLAN tag. This field is three bits long, representing the values 0 - 7. When the QoS Mode is set to 802.1p, the 802.1p Configuration table appears, allowing you to map each of the eight 802.1p values to a local priority queue (low, normal, medium or high). The default settings are shown below.

When the QoS Mode is set to 802.1p, the 802.1p Configuration table is displayed as shown below.



**Figure 2-10-2**

### QoS Mode: DSCP

DSCP: Packets are prioritized using the DSCP (Differentiated Services Code Point) value. The Differentiated Services Code Point (DSCP) is a six-bit field that is contained within an IP (TCP or UDP) header. The six bits allow the DSCP field to take any value in the range 0 - 63. When QoS Mode is set to DSCP, the DSCP Configuration table is displayed, allowing you to map each of the DSCP values to a hardware output queue (low, normal, medium or high). The default settings map all DSCP values to the high priority egress queue. User can use the Prioritize Traffic drop-down list to quickly set values into the DSCP Configuration table which is a common priority queue. Use Custom if you want to set each value individually.

When the QoS Mode is set to DSCP, the DSCP Configuration table is displayed as shown below.

**QoS Configuration**

<b>QoS Mode</b>	DSCP ▼
<b>Prioritize Traffic</b>	All High Priority ▼ Custom All Low Priority All Normal Priority All Medium Priority All High Priority
<b>DSCP Configuration</b>	
<b>DSCP Value(0..63)</b>	<b>Priority</b>
	high ▼
	high ▼
	high ▼
	high ▼
	high ▼
	high ▼
	high ▼
	high ▼
All others	high ▼

Apply Cancel

**Figure 2-10-3**



## Filter Configuration

To let administrators easily set management source IP addresses to the ports on the switch. Press <Apply> button to make change take effect.

Figure 2-11

Source IP Filter:

- Mode: There are three types of mode in this drop-down menu. Default is disabled.

Disabled: Allow all IP network addresses to login to this switch and manage it.

Static: Only the configured IP network address (IP with IP mask) is allowed to login to this switch and manage it. And, only those received IP packets containing the configured source network address are not filtered and can be forwarded by the switch.

**Note: In this mode, the received packets are filtered except the IP packets with configured source network address.**

**For examples:**

**1. IP Address: 192.168.3.2, IP Mask: 255.255.255.0 Network address 192.168.3.x ( 254 IP Addresses) can be forwarded on the port.**

**2. IP Address: 192.168.3.2, IP Mask: 255.255.255.255 Only IP 192.168.3.2 can be forwarded on the port.**

DHCP: Allow the IP Address got from DHCP server can login to this switch and manage it. And only the IP packets contained the source IP are allowed to forward through the switch.

- IP Address: Setting up the IP Address, it can be one IP Address or a LAN.
- IP Mask: Setting up the IP Subnet Mask related with the IP Address.

Filter Configuration

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled ▾			<input checked="" type="checkbox"/>
2	Disabled ▾			<input checked="" type="checkbox"/>
3	Disabled ▾			<input checked="" type="checkbox"/>
4	Disabled ▾			<input checked="" type="checkbox"/>
5	Disabled ▾			<input checked="" type="checkbox"/>
6	Disabled ▾			<input checked="" type="checkbox"/>
7	Disabled ▾			<input checked="" type="checkbox"/>
8	Disabled ▾			<input checked="" type="checkbox"/>
9	Disabled ▾			<input checked="" type="checkbox"/>
10	Disabled ▾			<input checked="" type="checkbox"/>
11	Disabled ▾			<input checked="" type="checkbox"/>
12	Disabled ▾			<input checked="" type="checkbox"/>
13	Disabled ▾			<input checked="" type="checkbox"/>
14	Disabled ▾			<input checked="" type="checkbox"/>
15	Disabled ▾			<input checked="" type="checkbox"/>
16	Disabled ▾			<input checked="" type="checkbox"/>
17	Disabled ▾			<input checked="" type="checkbox"/>
18	Disabled ▾			<input checked="" type="checkbox"/>

Apply Refresh



- DHCP Server Allowed: Just tick the check box under the port x to allow the DHCP Server on this port and valid port is Port 1~18.

## Rate Limit Configuration

Select the "Port no." which you want to configure the mode of the speed.

**Policer :** Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~18 ranges is from 128~3968 kbps. Default: No Limit

**Shaper:** Set up the limit of Egress bandwidth for the port you choose. Outgoing traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~18 ranges is from 128~3968 kbps. Default: No Limit

Rate Limit Configuration

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 ▾

Apply Refresh

Figure 2-12

## Storm Control

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

### Storm Control Configuration

Storm Control is used to block unnecessary multicast and broadcast frames that reduce switch's performance. When the function is enabled and Storm Control rate settings are detected as exceeded, the unnecessary frames would be dropped. There are five types of traffic which can be rate limited, including ICMP Rate, Learn Frames Rate, Broadcast Rate, Multicast Rate and Flooded unicast Rate. The setting range is 1k~32768k per second. Default of four Rates is No Limit.

#### Storm Control 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 ▾

1k  
2k  
4k  
8k  
16k  
32k  
64k  
128k  
256k  
512k  
1024k  
2048k  
4096k  
8192k  
16384k  
32768k  
No Limit

**Figure 2-13**

After completing the function’s setting, press **<Apply>** button to have this function taken effect.

**Monitoring**

**MAC Table**

Statistic Overview for MAC addresses.

MAC Table

MAC address	Type	Port
	Dynamic	12
	Dynamic	12
	Dynamic	12
	Dynamic	12
	Dynamic	12
	Dynamic	12
	Dynamic	12

**Statistics Overview**

Statistic Overview for all ports

User can mirror traffic from any source port to a target port for real-time analysis the following figures shows clearly the statistics overview.

Statistics Overview for all ports

Clear Refresh

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	0	0	0	0	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
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	1558937	14359	9535694	87330	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

Figure 3-1

**Detailed Statistics**

Display the detailed counting number of each port’s traffic. In the list, the window can show all counter information each port at one time.

Statistics for Port 12

Clear

Refresh

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

Receive Total				Transmit Total			
Rx Packets	87658			Tx Packets	14447		
Rx Octets	9570793			Tx Octets	1574596		
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	66034			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/Alignment	-			Tx Collisions	-		
Rx Undersize	-			Tx Drops	-		
Rx Oversize	-			Tx Overflow	-		
Rx Fragments	-						
Rx Jabber	-						
Rx Drops	-						

## LACP Status

[illegible]

### Figure 3-3-1

## LACP Port Status

### 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		

**Figure 3-3-2**

## **RSTP Status**

### RSTP VLAN Bridge Overview

#### RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-03-ce-07-3a-5d	2	20	15	Steady	This switch is Root!

Refresh

**Figure 3-4-1**

- Bridge Id: Show this switch's current bridge priority setting and bridge ID which stands for the MAC address of this switch.
- Hello Time: Interval (in seconds) at which the root device transmits a configuration message.
- Max Age: The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that age out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.
- Fwd Delay: The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- Topology: Indicates if spanning tree topology is steady or undergoing reconfiguration. (The time required for reconfiguration is extremely short, so no values other than "steady" state are likely to be seen in this field.)
- Root ID: The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device. Each port has been connected to the root device.

## RSTP Port Status

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

**Figure 3-4-2**

- Port/Group: The number of a port or the ID of a static trunk.
- Path Cost: The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- Edge Port: Shows if this port is functioning as an edge port, either through
  - manual selection (see the RSTP Port Configuration table) or auto-detection. Note that if the switch detects another bridge connected to this port, the manual setting for Edge Port will be overridden and the port will be instead of function as a point-to-point connection.
- P2P Port: Shows if this port is functioning as a Point-to-Point connection to exactly one other bridge. The switch can automatically determine if the interface is attached to a point-to-point link or to shared media. If shared media is detected, the switch will assume that it is connected to two or more bridges.
- Protocol: Shows the spanning tree protocol functioning on this port, either RSTP or STP (that is, STP-compatible mode).

## IGMP Status

### IGMP Status

IGMP Status shows the IGMP Snooping statistics for the whole switch.

- VLAN ID: VLAN ID number.
- Querier: Show whether Querying is enabled.
- Queries transmitted: Show the number of transmitted Query packets.
- Queries received: Show the number of received Query packets.
- v1 Reports: Show the number of received v1 Report packets.
- v2 Reports: Show the number of received v2 Report packets.
- v3 Reports: Show the number of received v2 Report packets.
- v3 Leave: Show the number of v3 leave packets received.

**IGMP Status**

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

Refresh

**Figure 3-5**



## VeriPHY

### VeriPHY Cable Diagnostics

User can perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open etc..) and feedback a distance to the fault.

- Cable Diagnostics: Cable diagnostics is performed on a per-port basis. Select the port number from the drop-down list.
- Cable Status: Shows the cable length, operating conditions and isolates a variety of common faults that can occur on Category 5 twisted pair cabling.

#### VeriPHY Cable Diagnostics

The interface shows a 'Port' dropdown menu with 'Port 1' selected and a 'Mode' dropdown menu with 'Full' selected. An 'Apply' button is located below the 'Port' dropdown. The 'Mode' dropdown menu is open, showing three options: 'Full', 'Anomaly', and 'Anomaly w/o X-pair'.

Cable Status		
Pair	Length [m]	Status
A	-	-
B	-	-
C	-	-
D	-	-

**Figure 3-6**

## Ping

This command sends ICMP echo request packets to another node on the network.

### Ping Parameters

- Target IP Address: IP address of the host
- Count: Number of packets to send. Four type of number can choose (1, 5, 10 and 20). Default : 1
- Time Out: setting the time period of host will be Ping. Four type of number can choose (1, 5, 10 and 20). Default : 1

Use the ping command to see if another site on the network can be reached.

The following are some results of the **ping** command:

- Normal response: The normal response occurs in one to ten seconds, depending on network traffic.
- Destination does not respond: If the host does not respond, a "timeout" appears in ten seconds.
- Destination unreachable: The gateway for this destination indicates that the destination is unreachable.
- Network or host unreachable: The gateway found no corresponding entry in the route table.

Press <Esc> to stop pinging.

### Ping Parameters

Target IP address	<input type="text"/>
Count	1 ▼
Time Out (in secs)	1 ▼
<input type="button" value="Apply"/>	

1

5

10

30

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

**Figure 3-7**

## **Maintenance**

The switch offers many approaches to reboot your switch, such as: power up, hardware reset and software reset. You can press RESET button in the front panel of your switch to reset the device and to retrieve default settings. After upgrading software, you have to reboot the device to have new configuration take effect. The function being discussed here is software reset.

### **Warm Restart**

Press “Yes” button to restart the switch, the reset will be complete when the power lights stop blinking.

#### **Warm Restart**

**Are you sure you want to perform a Warm Restart?**

Yes

No

**Figure 4-1**

### **Factory Default**

Factory Default provides the function to retrieve default settings and replace current configuration. Except the IP address setting, all settings will be restored to the factory default values when “Factory Default” function is performed. If you want to restore all configurations including the IP address setting to the factory default, please press the “RESET” button on the front panel.

#### **Factory Default**

**Are you sure you want to perform a Factory Default?**

Yes

No

**Figure 4-2**

## Software upload

Select "Upgrade Firmware" from the Tools drop-down list then click on the "Browse" button to select the firmware file. Click the "APPLY" button to upgrade the selected switch firmware file. User can download firmware files for user's switch from the Support section of your local supplier.



Figure 4-3

## Configuration File Transfer

Configuration file transfer allows you to save the current configuration of the switch or restore a previously saved configuration back to the device. Configuration files can be saved to any location on the web management station. To upload the configuration file to save a configuration or click "Download" to restore a configuration. Use the Browse button to choose a file location on the web management station, or to find a saved configuration file.

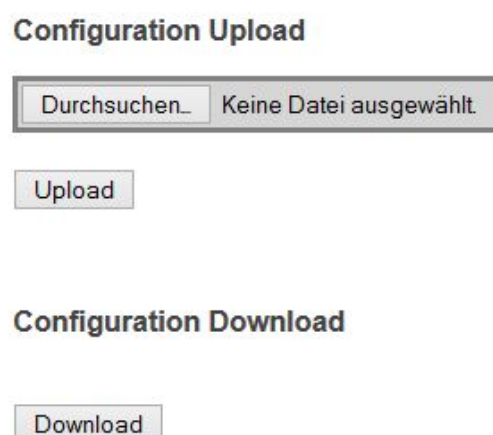
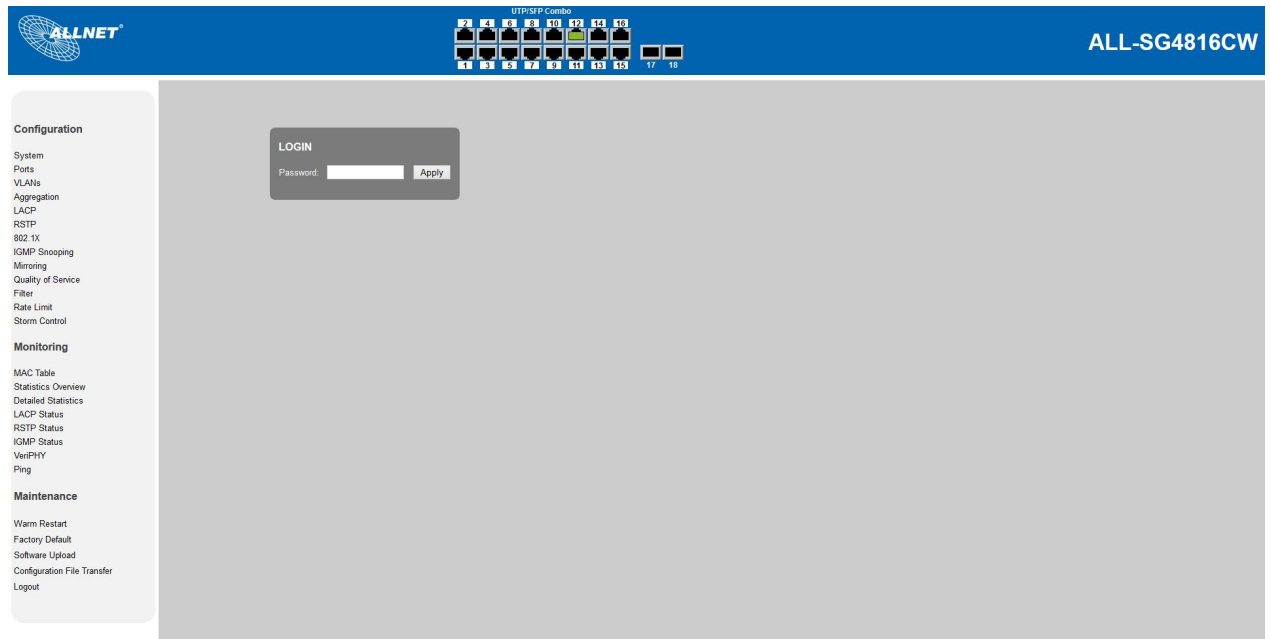


Figure4-4

## Logout

The administrator has the authority to write and access for all parameters governing the onboard agent. User should therefore assign a new administrator password as soon as possible, and store it in a safe place.



**Figure 4-5**



## CE-Declaration of Conformity

For the following equipment:

Germering, 1st of June, 2014

### Smart managed 16 Port Gigabit/Combo + 2x SFP Switch

## ALL-SG4816CW



The safety advice in the documentation accompanying the products shall be obeyed.

The conformity to the above directive is indicated by the CE sign on the device.

The ALLNET ALL-SG4816CW conforms to the Council Directives of 2004/108/EC.

This equipment meets the following conformance standards:

*EN55022:2010: Class A*

*IEC61000-3-2:2005+A1:2008+A2:2009*

*IEC61000-3-3:2008*

*EN55024:2010*

*IEC61000-4-2:2008*

*IEC61000-4-3:2006+A1:2007+A2:2010*

*IEC61000-4-4:2004+A1:2010 IEC61000-4-5:2005*

*IEC61000-4-6:2008*

*IEC61000-4-8:2009*

*IEC61000-4-11:2004*

This equipment is intended to be operated in all countries.

This declaration is made by

ALLNET GmbH Computersysteme

Maistraße 2

82110 Germering

Germany

Germering, 01.06.2014

  
\_\_\_\_\_  
Wolfgang Marcus Bauer  
CEO