

Table of Contents

1 Overview	4
1.1 Features.....	4
1.2 Packing List	7
2 Hardware Installation.....	8
2.1 Front Panel	8
2.2 Rear Panel.....	12
2.3 Environment Requirements	13
2.4 Hardware Installation	14
3 Configuration	17
3.1 Fast Login.....	17
3.2 Status.....	20
3.3 Port Setting.....	21
3.3.1 Port.....	22
3.3.2 Rate Limit	24
3.3.3 Storm Control.....	26
3.3.4 Statistics	27

3.4 Mirror	28
3.5 VLAN	29
3.5.1 VLAN Mode	30
3.5.2 Port VLAN.....	31
3.5.3 802.1Q VLAN	32
3.5.4 Tag VLAN Configuration	33
3.6 Trunk.....	34
3.7 QoS.....	35
3.8 MAC Address Setting.....	37
3.8.1 MAC Filter.....	37
3.8.2 Static MAC	38
3.9 802.1X Setting	39
3.9.1 802.1X	40
3.9.2 802.1X Port.....	41
3.10 RSTP Setting	42
3.10.1 RSTP	43
3.10.2 RSTP Port.....	45

3.10.3 RSTP Status	46
3.11 IGMP Snooping	46
3.11.1 Snooping Configuration	47
3.11.2 Snooping Status	49
3.12 System	50
3.12.1 SNMP	50
3.12.2 Change Password	52
3.12.3 Cable Diagnostic	53
3.12.4 Upgrade	54
3.12.5 IP Configuration	55
3.12.6 MAC Aging	56
3.12.7 Restore Factory	57
3.12.8 Backup	58
3.12.9 Restore	59
3.12.10 Logout	59

1 Overview

Thank you for purchasing the FULL GIGABIT LIGHT MANAGEMENT SWITCH full Gigabit light management switch. The FULL GIGABIT LIGHT MANAGEMENT SWITCH provides 16/24 10/100/1000M adaptive RJ45 ports and 2 shared SFP ports, supporting automatic switchover between Gigabit electrical interface and Gigabit SFP module optical interface. You can extend the network from 100 meters to over 80 km as required. The FULL GIGABIT LIGHT MANAGEMENT SWITCH supports the management in Web or SNMP mode, and provides such intelligent configurations as port management, VLAN, Trunk, QoS, static MAC address table, 802.1X authentication, Rapid Spanning Tree Protocol (RSTP), IGMP Snooping, port security and port traffic statistics. Boasting powerful functions and easy operation, it is the best choice for Internet bar, medium/small enterprises and intelligent community network.

1.1 Features

- In accordance with the IEEE802.3, IEEE802.3u, IEEE802.3ab and IEEE802.3z Ethernet standards.

- Providing 16/24 10/100/1000 Mbps adaptive RJ45 ports, and supporting automatic identifying of parallel/cross-connected lines (Auto MDI/MDIX).
- Providing 2 shared SFP interfaces, and supporting automatic switchover between Gigabit electrical interface and Gigabit SFP optical interface.
- Supporting IEEE802.3x full-duplex flow control and half-duplex backpressure flow control.
- Adopting the storage-transfer structure and integrating the 8K MAC address table, to fully cater diversified applications.
- Providing backplane bandwidth up to 32/48 Gbps, and supporting non-blocking line speed transfer.
- Supporting up to 16/24 groups of part-based VLANs; supporting up to 128 groups of Tag VLANs based on IEEE 802.1Q, with VLAN ID ranging 1 ~ 4094.
- Supporting IEEE 802.3ad port trunk function and providing 8 trunk groups, each of which can contain up to 8/12 port members.
- Supporting up to 128 static MAC address tables.

- Supporting the QoS function, and providing the mapping mode based on the port, IEEE802.1p and TOS priorities and the automatic control for the transfer queue based on 4 priorities.
- Controlling the security of the port access, and supporting the control over port MAC address filtering, binding and aging.
- Supporting intelligent control over broadcast storm, and providing setting options for broadcast type and broadcast control.
- Supporting the port mirroring function.
- Supporting the 802.1X authentication function.
- Supporting the 802.1W RSTP, and being compatible with the 802.1D Spanning Tree Protocol (STP).
- Supporting the IGMP Snooping function.
- Setting the switch IP address with the specified IP address mode or through the automatic obtainment by the DHCP client.
- Supporting the Web management.
- Supporting the SNMP management.
- Supporting the upgrade of switch software and backup and restoration of switch configuration files.
- Supporting the line diagnosis function.

- Supporting the traffic statistics function, and dynamically displaying the packet receiving-transfer at the port.
- Equipped with built-in switching power supply; adopting 1U steel chassis for standard 19-inch rack.

1.2 Packing List

Carefully open the package, and then check whether the following articles are contained:

1. Full Gigabit light management switch: 1
2. Power cable: 1
3. L-shape supports: 2; matched screws: 8
4. Rubber footpads: 4
5. User manual: 1
6. Warranty card: 1

2 Hardware Installation

2.1 Front Panel

The front panel of the FULL GIGABIT LIGHT MANAGEMENT SWITCH comprises the network ports, status indicators and Reset button, as shown below.



Front Panel of TELSEY FULL GIGABIT LIGHT MANAGEMENT SWITCH



Front Panel of FULL GIGABIT LIGHT MANAGEMENT SWITCH

Status indicators:

Each port provides 1 LINK/ACT (connection/transmission) and 1 1000 Mbps (rate) status indicators. The SFP interface shares the same indicator group (that is, 1 LINK/ACT (connection/transmission) and 1 1000 Mbps (rate) status indicators) with the Gigabit RJ45 port. In addition, there are 1 SYS status indicators and 1 POWER status indicator.

By use of such green LED indicators, you can know the working status of the switch. The following table describes the meanings of such indicators.

Indicator Name		Description
Power	Always on	After the switch is connected with the power supply, this indicator is always on.
	Off	If this indicator is off, you need to check whether the AC power supply is normally connected with the switch.
Link/Act	Always on	After a device is connected to a port of the switch, the LINK/ACT indicator of this port is on. If only the LINK/ACT indicator is on but all of the other indicators are off, the connection rate of this port is 10/100 Mbps.
	Flashing	When a port is receiving/transmitting data, the corresponding LINK/ACT indicator flashes.
	Off	There is no connection at the corresponding port.
1000 Mbps	Always on	After a device at 1000 Mbps is connected to a port of the switch, the 1000 Mbps indicator of this port is on.
	Off	If a port has no connection or its connection is not at 1000 Mbps, the 1000 Mbps indicator of this port is off.
SYS	Always on	It indicates that the switch is normally running.
	Flashing	It indicates that the switch is restoring the default settings.
	Off	It indicates that the switch is in startup and initialization process.

Status of the port indicators during power-on self-test of switch	Off – flashing for 1 s – off – corresponding port status
---	--

When the SFP optical interface is in use, the 1000 Mbps indicator and Link/Act indicator get on at the same time, and then the SFP interface indicator gets on at the end of negotiation.

Reset button: Located at the lower left corner of the front panel it is used to clear the current settings of the switch and restore the default ones.

Caution !

How to use the RESET button:

To restore the default settings, make sure the switch is normally running, and then press the RESET button until the status of the SYS indicator changes in this way: Always on – flashing – off. At this time, you can release this button, and the switch automatically restores the default settings before delivery. When the SYS indicator gets on again, the switch restarts with the default settings. Be cautious here, because this operation is to clear the current settings.

Network ports:

- The network port part comprises totally 16/24 10/100/1000M adaptive RJ45 ports (Ports 1 ~ 16/24), which supports automatic identifying of parallel/cross-connected lines (Auto MDI/MDIX).
- Gigabit SFP optical module interfaces (shared with the Gigabit RJ45 port) supports hot-swapping of the SFP optical module and automatic switchover between Gigabit RJ45 electrical interface and Gigabit SFP optical interface.
- As an optical module interface, the SFP interface cannot support the optical connection until it is equipped with the specified SFP (Mini GBIC) optical module.
- The optical connection of the SFP module is prior to the network cable connection of the RJ45 electrical interface.
- Upon detection of the SFP optical connection, the switch immediately interrupts the connection of the RJ45 electrical interface, and automatically switches the port connection to the SFP optical interface.
- When the switch works in the SFP optical connection mode, the RJ45 electrical interface is forcedly isolated. However, upon detection of optical disconnection, the switch immediately checks the RJ45 interface, and automatically switches the established port connection to the RJ45 electrical interface.

Note: After the switch is powered, the port indicator corresponding to the optical interface may get on after a while, which is normal. The switch does not detect the optical connection until the initialization and startup of internal software system are normally completed. As a result, such port indicator turns on in about 40 s after power-on. However, if the SFP optical module is unplugged and then plugged during the normal running of the switch, detection and switchover can be completed within about 3 s, for starting optical communication.

Tip !

To extend your network to over 100 meters, you need optical connection. Please log in to our website www.tenda.com.cn, to get more information about optical fiber, SFP optical module, and optical network construction.

2.2 Rear Panel

The rear panel provides an AC input socket, as shown below. Use the delivery-attached power cable to connect the switch with the power supply. The built-in high-performance switching power supply of the FULL GIGABIT LIGHT MANAGEMENT SWITCH supports this mains input range: AC 100 V ~ 240V, 50 Hz ~ 60 HZ.



Rear Panel

2.3 Environment Requirements

- Ethernet LAN is available. Use the network cable to connect the FULL GIGABIT LIGHT MANAGEMENT SWITCH to such LAN.
- A computer supporting the TCP/IP and equipped with browser of a version higher than Microsoft IE 4.0 or Netscape Navigator4.0 is available. It is used to set the FULL GIGABIT LIGHT MANAGEMENT SWITCH switch.
- Power supply should be AC100 V ~ 240 V, 50 Hz ~ 60 Hz.
- Temperature of the working environment: 0 °C ~ 45 °C. Place the switch far away from the devices generating heat. A space of at least 10 cm should be reserved at each side around the switch, for better heat dissipation.
- Environment humidity: 5%-95%, without condensation. Do not place the switch at the extremely dirty or damp place.
- Keep the switch away from strong electric/magnetic field, and keep it free from vibration, dust and direct irradiation of hard light.

2.4 Hardware Installation

Installation on platform :

As shown below, paste 4 delivery-attached rubber footpads to 4 flutes at the switch bottom, and then horizontally place the switch on the solid platform.



Horizontal Installation of FULL GIGABIT LIGHT MANAGEMENT SWITCH
(FULL GIGABIT LIGHT MANAGEMENT SWITCH as Example)

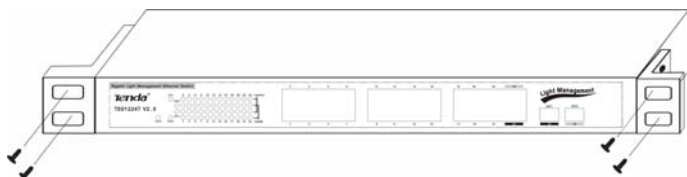
Installation in rack:

The FULL GIGABIT LIGHT MANAGEMENT SWITCH structure is suitable for the 19-inch rack. With L supports, it can be conveniently installed into a rack with dimensions specified by EIA.

As shown below, use screws to fix 2 delivery-attached L-shape supports on both sides of the switch, and horizontally insert the switch into a layer of the rack, and then use screws to fix the switch supports on the rack.



L-shape Supports of FULL GIGABIT LIGHT MANAGEMENT SWITCH
(FULL GIGABIT LIGHT MANAGEMENT SWITCH as Example)



Fixing FULL GIGABIT LIGHT MANAGEMENT SWITCH on Rack FULL
GIGABIT LIGHT MANAGEMENT SWITCH as Example)

Network connection:

The FULL GIGABIT LIGHT MANAGEMENT SWITCH supports the 10/100/1000 Mbps Ethernet, 10/100 Mbps half/full-duplex mode and 1000 Mbps full-duplex mode. All RJ45 ports support the Auto MDI/MDIX function. They can be used as ordinary ports or Uplink backbone cascading ports. You can use any RJ45 port to connect the switch with the workstation, server or network devices as switch or HUB, without separated using of cross-connected or straight-through twisted pair.

The FULL GIGABIT LIGHT MANAGEMENT SWITCH provides 2 shared SFP optical module interfaces. After the specified Gigabit SFP optical modules are inserted, these interfaces can support matched optical fibers/cables for extending the Gigabit network to over 80 km, to go beyond the limitation of 100 meters of the twisted pair network.

Network transmission media:

For the RJ45 port, you should use Category-5, super Category-5 or Category-6 unshielded twisted pair (CAT5/CAT5e/CAT6 UTP). Category-6 unshielded twisted pair is recommended to ensure stable data transmission at 1000 Mbps.

Depending on the wavelength of the SFP optical module to be used, you should select the proper optical fiber/cable for the corresponding LC interface.

Caution !

Make sure only one cascading channel exists between switches or between switch and HUB. Otherwise, loop appears and it may result in network breakdown.

3 Configuration

3.1 Fast Login

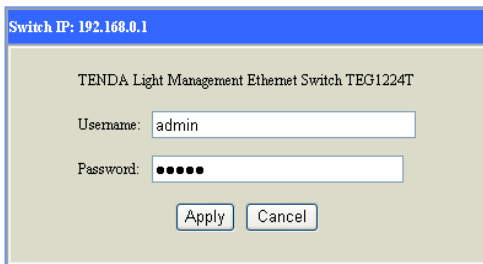
As the FULL GIGABIT LIGHT MANAGEMENT SWITCH is not equipped with internal DHCP server, you need to manually configure the IP address of the computer for login and configuration. The table below lists the default parameters of the switch.

Parameter	Default Value
Default IP address	192.168.0.1
Default user name	admin
Default password	admin

You can log in to the setting window of the switch through following steps:

- a. Connect the switch with the computer NIC interface.
- b. Power on the switch.
- c. Check whether the IP address of the computer is within this network segment: 192.168.0.xxx (“xxx” ranges 2 254), for example, 192.168.0.100. **For the IP address setting, refer to Appendix 3.**

- d. Open the browser, and enter <http://192.168.0.1> and then press “Enter”. The switch login window appears, as shown below.



Switch IP: 192.168.0.1

TENDA Light Management Ethernet Switch TEG1224T

Username: admin

Password: ●●●●●●

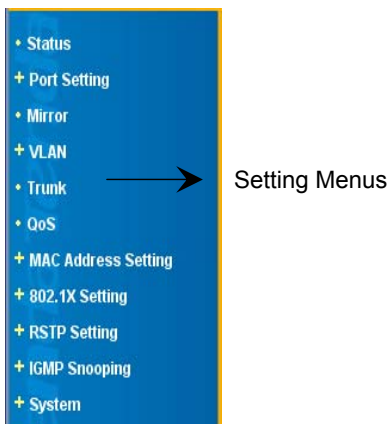
Apply Cancel

- e. Enter the user name and password (both default user name and default password are admin), and then click “Apply” to log in to the switch configuration window.



On the menu bar on the left, there are “Status”, “Port Setting”, “Mirror”, “VLAN”, “Trunk”, “QoS”, “MAC Address Setting”, “802.1X Setting”, “RSTP

Setting”, “IGMP Snooping” and “System”. Click any menu item to set the corresponding function. The detailed setting procedure is to be described later.



3.2 Status

The screenshot shows the Tenda web management interface. The top header features the Tenda logo and the URL www.tenda.cn. A left sidebar contains a menu with the following items: Status, Port Setting, Mirror, VLAN, Trunk, QoS, MAC Address Setting, 802.1X Setting, RSTP Setting, IGMP Snooping, and System. The main content area is titled 'System' and displays a table with the following information:

Hardware Version	V2.0
Firmware Version	V2.0
DHCP Client	Disable
VLAN Mode	PortVlan
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
MAC Address	00-0b-b5-00-00-16
ARP Aging Time	300

System: Displaying the current system status of the switch.

- Hardware Version: Hardware version of the switch.
- Firmware Version: Software version of the switch.
- DHCP Client: Status of the DHCP client, “Disable” by default.
- IP Address: “192.168.0.1” by default.
- Subnet Mask: “255.255.255.0” by default.
- Gateway: “0.0.0.0” by default. :
- MAC Address: MAC address of the switch.

- ARL Aging Time: Aging time of the MAC address set, 300 s by default.

3.3 Port Setting

In this part, you can set the automatic negotiation, rate, duplex and flow control modes of each port. Totally, 6 working modes are available for a port: 10 Mbps half-duplex, 10 Mbps full-duplex, 100 Mbps half-duplex, 100 Mbps full-duplex, 1000 Mbps full-duplex and automatic negotiation. By default, the automatic negotiation mode is adopted. In this mode, upon switch power-on, each port automatically communicates and negotiates with its connection object, to determine an optimal working mode. For other working modes, your manual setting is required, and they should match the working mode of the connection object or the connection object is working in the automatic negotiation mode; otherwise, communication may fail. Flow control is a mechanism in which both ends of the connection control data flow, to avoid receiver's buffer overflow. Port settings affect the port mirroring and Trunk group functions.

3.3.1 Port

The screenshot shows the Tenda web management interface. The top navigation bar includes the Tenda logo and the URL www.tenda.cn. A left sidebar contains a menu with options like Status, Port Setting, Mirror, VLAN, Trunk, QoS, MAC Address Setting, 802.1X Setting, RSIP Setting, IGMP Snooping, and System. The main content area is divided into two sections: 'Port Configuration' and 'Port Status'.

Port Configuration

Port	Admin	Auto Negotiate	Speed Duplex	Flow Control
1	Enable	Enable	10Mbps Half	Disable

Below the configuration table is an 'Apply' button.

Port Status

Port	Link Status	Speed Mode	Speed Duplex	Flow Control	Port	Link Status	Speed Mode	Speed Duplex	Flow Control
1	Down	Auto-Negotiate	Down	Disable	2	Down	Auto-Negotiate	Down	Disable
3	Down	Auto-Negotiate	Down	Disable	4	Down	Auto-Negotiate	Down	Disable
5	Down	Auto-Negotiate	Down	Disable	6	Down	Auto-Negotiate	Down	Disable

Port Configuration: Basic function configurations of the switch, including port enablement/disablement, port working mode and flow control. The following part describes the configuration details:

- **Port:** Selecting the corresponding port number for setting. 16/24 10/100/1000 Mbps Ethernet ports are available for your selection.
- **Admin:** Enabling or disabling the switch port. If “Disable” is selected, this port cannot be used. (Caution: Do not disable the ports unless necessary.)
- **Auto Negotiate:** Enabling or disabling the auto negotiation function of the port. (Caution: You must select “Disable” here before setting “Speed Duplex”.)

- **Speed Duplex:** Selecting 10 Mbps full-duplex and half-duplex mode, 100 Mbps full-duplex and half-duplex mode or 1000 Mbps full-duplex mode for the port.

- **Flow Control:** Supporting the IEEE802.3x full-duplex flow control and half-duplex backpressure flow control (the switch can automatically switch the flow control mode depending on the duplex mode of the port).

Port Status: Listing the current setting status details of all ports, as shown below.

Port	Link Status	Speed Mode	Speed Duplex	Flow Control	Port	Link Status	Speed Mode	Speed Duplex	Flow Control
1	Down	Auto-Negotiate	Down	Enable	2	Down	Auto-Negotiate	Down	Enable
3	Down	Auto-Negotiate	Down	Enable	4	Down	Auto-Negotiate	Down	Enable

3.3.2 Rate Limit


Rate Limit Configuration

Port	Policer	Shaper	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

Rate Limit Configuration: Limiting the receiving rate of each port, thus to prevent the user from occupying excessive bandwidth. In this way, the normal network using by other users and smooth network connection can be guaranteed. This function is applicable to the Internet bar and community broadband access applications.

- Port: Selecting the corresponding port number for setting. 16/24 10/100/1000 Mbps ports are available for your selection.
- Policer: Controlling the receiving rate by level. Available rates are: 128 Kbps; 256 Kbps; 384 Kbps; 512 Kbps; 640 Kbps; 768 Kbps; 896 Kbps; 1024 Kbps; 1152 Kbps; 1280 Kbps; 1408 Kbps; 1536 Kbps; 1664 Kbps; 1792 Kbps; 1920 Kbps; 2048 Kbps; 2176 Kbps; 2304 Kbps; 2432 Kbps; 2560 Kbps; 2688 Kbps; 2816 Kbps; 2944

Kbps; 3072 Kbps; 3200 Kbps; 3328 Kbps; 3456 Kbps; 3584 Kbps;
3712 Kbps; 3840 Kbps; 3968 Kbps; No Limit.

 **Caution:** If the selected rate is higher than the actual connection rate of the port, the value displayed on the window is the selected value instead of the actual one.

Shaper: Displaying the bandwidth control status of all ports, as shown below.

Port	Policer	Shaper	Port	Policer	Shaper
1	No Limit ▾	No Limit ▾	2	No Limit ▾	No Limit ▾
3	No Limit ▾	No Limit ▾	4	No Limit ▾	No Limit ▾

3.3.3 Storm Control



Storm Control: Suppressing the transfer of broadcast packets of the switch. When different types of broadcast packets reach the corresponding limit set, the switch automatically discards excessive packets, thus to ensure stable running of the switch.



Caution:

1. Broadcast means transmitting packets to all hosts in the network. Multicast means transmitting packets to a host group in the network. Unicast means transmitting packets to a specific host in the network. Unknown unicast (flood) means transmitting the unicast packets with unknown destination MAC address.

- The switch is unable to totally suppress broadcast packets. Instead, it can only limit the transmitting rate for broadcast packets.

3.3.4 Statistics

The screenshot shows the 'Statistics' page in the Tenda switch web interface. The page title is 'Statistics'. There are two buttons, 'Clear' and 'Renew', located above the data table. The table displays statistics for 10 ports. All values are currently 0.

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

Statistics: Displaying the quantities of the bytes and frames which are being received/transmitted by all ports currently and the quantities of error frames received/transmitted by all ports.

- Clear: Clearing all current counting values, that is, clearing the port statistics data.
- Renew: Re-reading counted values, that is, manually refreshing current port statistics data.

3.4 Mirror

The screenshot shows the Tenda web management interface. On the left is a navigation menu with options: Status, Port Setting, Mirror, VLAN, Trunk, QoS, MAC Address Setting, 802.1X Setting, HSTP Setting, IGMP Snooping, and System. The main content area is titled 'Mirror' and contains a table for port selection.

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

Below the table is an 'Apply' button. Underneath, there are three informational notes:

1. Port mirroring allow ingress traffic to be monitored by a mirror port. Fully satisfies the public security department to the internet bar, the enterprise to the network visit monitoring demand.
2. The mirroring port's bandwidth must be exceed the mirrored's.
3. Mirrored port and mirroring port can not be the same one and can across VLAN.

- The port mirroring function means transfer the packets of one or more monitored ports to the monitoring port, thus to support the public security department to monitor the Internet access by the Internet bar or enterprise.
- The bandwidth of the monitoring port cannot be smaller than that of the monitored port.
- If the monitoring port is just the monitored port, the system automatically ignores this monitored port.

- This function supports cross-VLAN monitoring. In other words, if the monitored port and the monitoring part belong to different VLAN groups, monitoring is allowed.

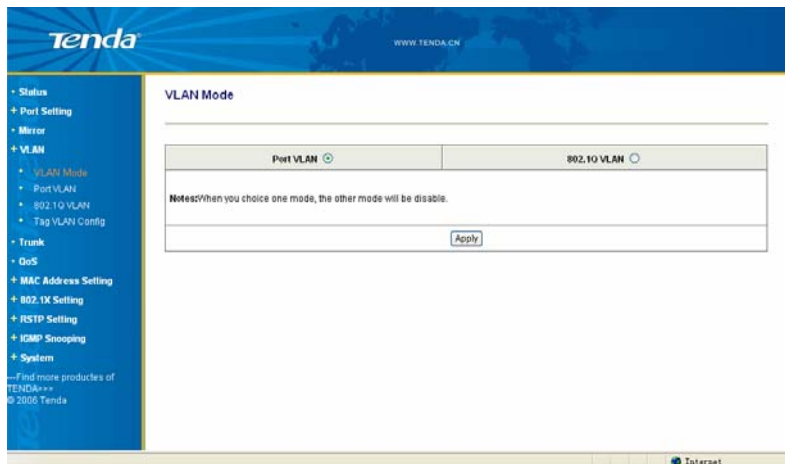
Mirror:

- Mirror Port: Selecting a port to serve as the monitoring port.
- Mirrored Port: Selecting one or more ports to be monitored.

3.5 VLAN

To establish secure autonomous broadcast/multicast domains, you can make switch ports form VLANs. The VLAN technology can be used to divide a network into multiple network segments, to shrink broadcast domains. All Ethernet packets, such as unicast, multicast, broadcast and unknown unicast packets, are to be transferred only within the VLAN. In addition, VLAN can be used to change the topological structure of the network, without any movement of network workstations or change of network connections. You can modify the VLAN setting of a workstation, to “move” this workstation from a VLAN (VLAN of the Sales Dept.) to another VLAN (for example, VLAN of the Market Dept.). In this way, the network nodes can be moved, changed or added in an extremely flexible and easy way.

3.5.1 VLAN Mode



Two VLAN modes are available: Port VLAN and 802.1Q VLAN.

- Port VLAN: Clicking this option and then clicking “Apply”, to set the port VLAN mode.
- 802.1Q VLAN: Clicking this option and then clicking “Apply”, to set the 802.1Q VLAN mode.

**Note:**

After a VLAN mode is selected, the other mode will be disabled.

3.5.2 Port VLAN

The screenshot shows the Tenda web interface for configuring Port VLAN. On the left is a navigation menu with options like Status, Port Setting, Mirror, VLAN, Trunk, QoS, MAC Address Setting, 802.1X Setting, RSTP Setting, IGMP Snooping, and System. The main content area is titled 'Port VLAN' and contains two tables.

Port VLAN Configuration:

VLAN Group	1											
VLAN Member	1	2	3	4	5	6	7	8	9	10	11	12
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Below the table is an 'Apply' button.

VLAN Group Configuration:

VLAN Group	VLAN Member																								
1	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Description of Port VLAN configuration: Port VLAN uses the physical ports of the switch to distinguish VLANs.

- VLAN Group: Including all 16/24 ports, 1 by default.
- VLAN Member: Adding the physical ports of the switch to be included in this VLAN.

3.5.3 802.1Q VLAN

802.1Q VLAN

VLAN ID: (1-4094)

Port	1	2	3	4	5	6	7	8	9	10	11	12
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Each incoming frame must be assigned a VLAN membership and forwarded according to the assigned VID.
 1. Frames that are not discarded are then subject to the VLAN classification.
 2. Untagged and priority tagged frames are classified to a Port VLAN Identifier.
 3. Tagged frames are classified to the VID given in the frame's tag.

VLAN Group

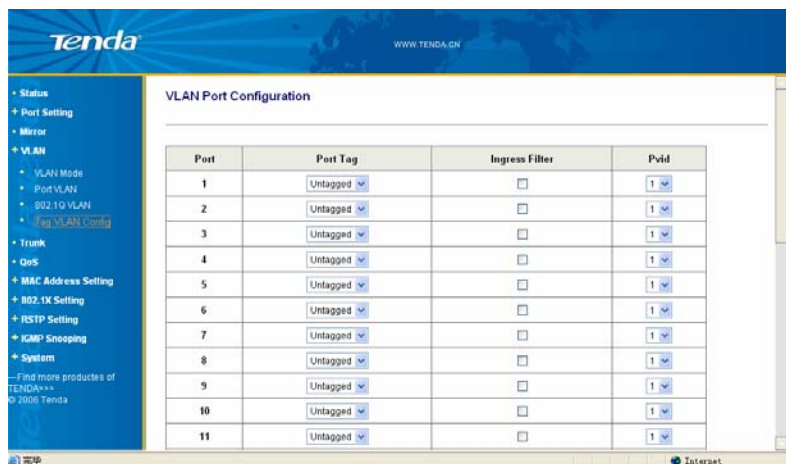
NO.	Vlan ID	VLAN Port Member	Operation

Description of 802.1Q VLAN configuration:

In Tag VLAN mode, port VID is used to distinguish VLANs. When data frames pass the switch, the VID information in their tag header indicates different VLANs corresponding to them, so the switch determines the destination ports of such frames according to the current VLAN settings.

- VLAN ID: Including all 16/24 ports, 1 by default. Modification to attributes of VLAN ID 1 is not allowed.
- Port: Adding the numbers of the ports to be included in this VLAN ID.

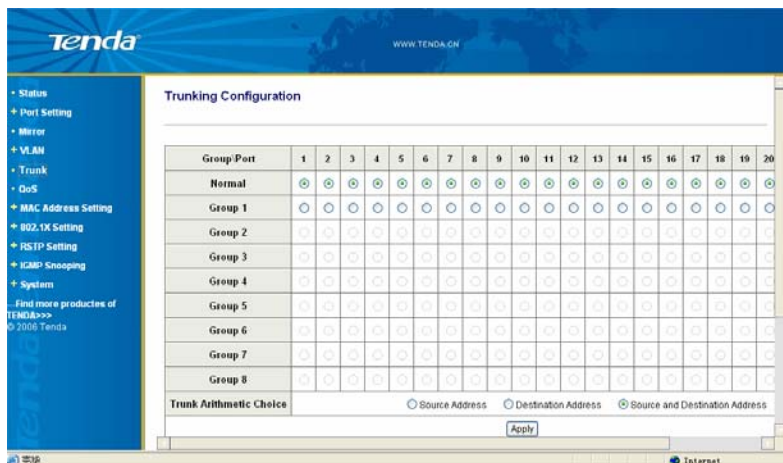
3.5.4 Tag VLAN Configuration



Description of 802.1Q VLAN port configuration:

- Port Tag: Setting the Tag attribute for the this port The port Tag rule specifies the changes to be made upon frame output, that is, egress rule. The available rules are adding Tag for frame and removing Tag of frame.
- Ingress Filter: Specifying the ingress filtering rule, which determines to receive or not receive the Tag messages inconsistent with the port Pvid.
- Pvid: Setting the VLAN ID of this port.

3.6 Trunk



- Trunk is used to expand the bandwidth, hot backup and error tolerance of the inter-switch cascading (Uplink) channel.
- All ports which are set as the trunk group members can be used by the trunk group only and cannot be used for other purposes, even when they are not being used by the trunk group.
- Cross-VLAN trunk group is not supported. In other words, all members of a trunk group must be within the same VLAN; otherwise, the trunk function cannot work.
- When the trunk group is used for the inter-switch cascading, you should make sure the cascading port used for connecting with the

opposite switch is set by the opposite switch into the same trunk group. In other words, the cascading of multiple ports (trunk members) must be achieved in the mode of trunk group to trunk group.

- Never connect two trunk groups of a switch together or cascade two switches through two groups of trunk channels, because such operations result in network loop, which may cause broadcast storm or even breakdown of the entire network.

3.7 QoS

The screenshot shows the Tenda switch web interface. The left sidebar contains a navigation menu with items: Status, Port Setting, Mirror, VLAN, Trunk, QoS, MAC Address Setting, 802.1X Setting, RSTP Setting, IGMP Snooping, and System. The main content area is titled 'QoS' and features a configuration table with the following data:

Port ID	Port Priority	802.1P Tag Priority	802.1P Default Priority	ToS Priority
1	low	Disable	0	Disable

Below the table is an 'Apply' button. An 'Explain' section follows, containing two points:

1. The QoS (Quality Of Service) feature provides four internal queues to support four different classifications of traffic. High priority packet streams experience less delay inside the switch.
2. The switch can classify the packets as one of the four priorities according to Port ID, 802.1P priority tag and IP ToS.

At the bottom of the main area is a 'QoS Status Table' with the following data:

Port ID	Port Priority	802.1P tag priority	802.1P default priority	ToS priority
1	high	Disable	0	Disable

- Simple QoS functions can be implemented through the combination of priority mode settings and priority control

operations. This switch supports packet mapping by 4 priority levels (low, medium, common, and high) and 3 priority setting modes.

- If “Port Priority” is enabled and high priority is assigned to a physical port, all packets passing this port are mapped into high priority. As a result, the switch processes the packets received/transmitted by this port first.
- If “802.1Q tag Priority” is enabled, the switch automatically reads 3-bit priority tag from the packet with VLAN tag. And if such priority tag indicates a high priority, this packet is mapped into high priority. In this way, if a port is set with high priority, when the switch gets faulty, it processes the packets transmitted by this port first.
- If “ToS Priority” is enabled, the switch automatically reads 8-bit ToS tag from the IPv6/IPv4 packet. And if such priority tag indicates a high priority, this packet is mapped into high priority for prior processing.

Description of QoS configuration:

- Port ID: Selecting the port to be set.
- Port Priority: Selecting “low”, “common”, “medium” or “high”.
- 802.1P tag priority: Enabled or disabled.

- ToS priority: Enabled or disabled.

QoS Status Table: Displaying the status of all ports.

Port ID	Port Priority	802.1P tag priority	802.1P default priority	ToS priority
1	high	Disable	0	Disable
2	high	Disable	0	Disable

3.8 MAC Address Setting

3.8.1 MAC Filter

The screenshot shows the Tenda web management interface. The top header features the Tenda logo and the website URL www.tenda.cn. A left-hand navigation menu lists various system settings, with 'MAC Address Setting' expanded to show 'MAC Filter' and 'Static MAC'. The main content area is titled 'MAC Filter' and contains a form for adding MAC addresses. The form has a 'MAC Address' label followed by six input boxes for the hexadecimal digits. Below the input boxes is an 'Add Address' button. A note states: 'To forbid certain network equipment accessing this device, just add their MAC to the filter list'. Below this is a 'MAC Filter Table' section containing a table with columns for 'NO.', 'Source MAC', and 'Operation'. The table is currently empty, and there is a 'Delete All' button below it.

MAC Filter: The filtered MAC address is to be added into “blacklist” of the switch. As a result, when this MAC address tries to connect with any port of the switch, network communication cannot be achieved.

MAC Address: Entering the MAC address to be filtered.

MAC Filter Table: Listing the MAC addresses filtered, as shown below. You can click “Delete” on the right to delete the corresponding MAC address filtered.

NO.	Source MAC	Operation
1	00-11-22-33-44-55	Delete
Delete All		

3.8.2 Static MAC

The screenshot shows the Tenda web management interface. The left sidebar contains a navigation menu with options like Status, Port Setting, Mirror, VLAN, Trunk, QoS, MAC Address Setting, MAC Filter, Static MAC, 802.1X Setting, RSTP Setting, IGMP Snooping, and System. The main content area is titled "Static MAC Address" and contains a form with fields for "MAC Address" and "Port ID" (set to 1). Below the form is an "Add Address" button and a list of instructions. At the bottom, there is a "Static MAC Address Table" with columns for NO., Source MAC, Port ID, and Operation, and a "Delete All" button.

Static MAC Address: Adding an MAC address to the specified port. The data transmission of the bound MAC address can be implemented only through the corresponding port.

- MAC Address: Entering the MAC address.
- Port ID: Selecting the port to bound with an MAC address.

Static MAC Address Table: Listing the MAC addresses bound, as shown below. You can click “Delete” on the right to delete the corresponding MAC address bound.

NO.	Source MAC	Port ID	Operation
1	00-11-22-33-44-55	1	<input type="button" value="Delete"/>
2	12-34-56-78-9a-bc	4	<input type="button" value="Delete"/>
<input type="button" value="Delete All"/>			

3.9 802.1X Setting

As an authentication protocol, 802.1X provides methods and policies for authenticating users. It is the port-based authentication policy, for the final purpose of judging availability of a port. For a port, it “enables” this port upon successful authentication to allow transmission of all messages; or “disables” this port upon failed authentication to only allow transmission of 802.1X authentication messages.

3.9.1 802.1X

The screenshot shows the Tenda web interface for 802.1X Configuration. The left sidebar contains a navigation menu with the following items: Status, Port Setting, Mirror, VLAN, Trunk, QoS, MAC Address Setting, 802.1X Setting (selected), 802.1X Port, RSTP Setting, IGMP Snooping, and System. Below the menu is a search bar and copyright information: "Find more products of TENDA*** © 2009 Tenda".

The main content area is titled "802.1X Configuration" and contains the following configuration table:

802.1X Enabled	Enable <input type="checkbox"/>
RADIUS IP	<input type="text" value="0.0.0.0"/>
RADIUS UDP Port	<input type="text" value="1812"/>
RADIUS Secret	<input type="text"/>
Reauthentication Enabled	Enable <input type="checkbox"/>
Reauthentication Period	<input type="text" value="3600"/> (1 - 3600 seconds)
EAP timeout	<input type="text" value="30"/> (1 - 255 seconds)
<input type="button" value="Apply"/>	

At the bottom of the interface, there is a status bar with the Tenda logo on the left and an "Internet" icon on the right.

802.1X Configuration:

- 802.1X Enabled: Enabling or disabling the 802.1X authentication function.
- RADIUS IP: Setting the IP address of the RADIUS.
- RADIUS UDP Port: Setting the RADIUS UDP port of the switch, 1812 by default.
- RADIUS Secret: Setting this value according to the secret key corresponding to the RADIUS.
- Reauthentication Enabled: Enabling or disabling the reauthentication function.

- Reauthentication Period: Setting the cycle of reauthentication, 3600 s by default (that is, reauthentication is performed every hour).
- EAP timeout: Setting the timeout time of EAP response, 30 s by default.

3.9.2 802.1X Port

802.1X Port Configuration

Port	Admin State	Port State	Force Re-authenticate
1	Force Authorized	802.1X disabled	Force Re-authenticate
2	Force Authorized	802.1X disabled	Force Re-authenticate
3	Force Authorized	802.1X disabled	Force Re-authenticate
4	Force Authorized	802.1X disabled	Force Re-authenticate
5	Force Authorized	802.1X disabled	Force Re-authenticate
6	Force Authorized	802.1X disabled	Force Re-authenticate
7	Force Authorized	802.1X disabled	Force Re-authenticate
8	Force Authorized	802.1X disabled	Force Re-authenticate
9	Force Authorized	802.1X disabled	Force Re-authenticate
10	Force Authorized	802.1X disabled	Force Re-authenticate
11	Force Authorized	802.1X disabled	Force Re-authenticate
12	Force Authorized	802.1X disabled	Force Re-authenticate

802.1X Port Configuration

- Admin State: Force Authorized; Force Unauthorized; Auto. In “Forced Authorized” state, the port allows transmission of any message. In “Forced Unauthorized” state, the port only allows transmission of authentication messages. In “Auto” state, the port

allows transmission of certain messages according to authentication result.

- Port State: 802.1X disabled; Link interrupted; Authorized; Unauthorized.
- Force Re-authenticate: Clicking the corresponding port to perform forced reauthentication.

3.10 RSTP Setting

RSTP can be used to create connection links for redundancy backup. You can change the RST parameters at bridge level. In view of the high complexity of RSTP algorithm, it is recommended to accept the default values. RST automatically assigns root bridge or root port, to avoid loop. However, if modification to RST parameters is necessary, you should carefully read the related RSTP contents to understand them in advance.

3.10.1 RSTP



RSTP Configuration:

- **System Priority:** Setting the system priority of the switch in the RSTP. The switch with lower system priority is easier to become the root bridge. If the switch is used in a large-scale workgroup-class network, it is recommended to skip this setting.
- **Hello Time:** Setting a value ranging 1 s ~ 10 s. It means the time interval for the root bridge transmitting BPDUs to all of other switches, so that they can know which switch is serving as the root bridge. When the switch not serving as the root bridge is set with a specific value, this value does not take effect. However, once this switch turns into the root bridge, this value takes effect.

- **Max Age:** Setting a value ranging 6 s ~ 40 s. If the current switch does not receive the BPDU packet transmitted by the root bridge when this maximum aging time is up, this switch can serve as the root bridge and transmit the BPDU packets to all other switches, if conditions permit (If this switch has the lowest bridge tag level, it then turns into the root bridge). Therefore, you should select a big value, to avoid unnecessary repeated resetting of root bridge.
- **Forward Delay:** Setting a value ranging 4 s ~ 30 s. It means the monitoring time for the switch port changing from the blocking status into forwarding status. A greater value means greater delay.
- **Version:** Selecting RSTP based on 802.1W (default value) or STP based on 802.1D.

3.10.2 RSTP Port



RSTP Port Configuration:

- Protocol Enabled: Enabling or disabling the RSTP function. By default, this function is disabled for all ports.
- Edge: If a port is directly connected with the terminal, you can set this port to an edge port. The edge port features faster status transition, and it takes a time shorter than 2 times of forwarding delay to directly change from the blocking status into the forwarding status.
- Path Cost: Setting a value ranging 0 - 200000000. "0" indicates automatically determining the port path cost depending on the port rate.

3.10.3 RSTP Status

The screenshot shows the Tenda web management interface. On the left is a navigation menu with options like Status, Port Setting, Mirror, VLAN, Trunk, QoS, MAC Address Setting, 802.1X Setting, RSTP Setting, IGMP Snooping, and System. The main content area is divided into two sections:

RSTP Bridge Overview

Bridge ID	Hello Time	Max Age	Forward Delay	Topology	Root ID
32768:00:00-b5:00:00-16	2	20	15	Steady	This switch is Root

Below the table is a "Refresh" button.

RSTP Port Status

Port	Path Cost	Edge Port	P2P Port	Protocol	Port State
1					Non-STP
2					Non-STP
3					Non-STP
4					Non-STP
5					Non-STP
6					Non-STP
7					Non-STP

RSTP status:

- RSTP Bridge Overview: Displaying the bridge ID, topology and root bridge ID specified by the system and Hello time, maximum aging time and forwarding delay set.
- RSTP Port Status: Displaying the P2P port, protocol and port state specified by the system and path cost and edge port set.

3.11 IGMP Snooping

IGMP Snooping is used to implement dynamic registration of L2 multicast on the switch. To achieve L2 multicast through the IGMP Snooping function, you need to make sure IGMP is achieved on the host and router.

The switch only snoops into different types of IGMP messages transmitted by the host and router, to dynamically maintain the L2 multicast group. Usually, multicast registration on this switch does not affect the setting of other switches. The switch transmits the IGMP query message and receives the IGMP response from the host. Based on the receiving port, VLAN ID and multicast of such IGMP packets, the switch maintains a multicast group. After that, it forwards such IGMP packets. Only the ports included into a multicast group can receive the multicast data stream. In this way, the network traffic is reduced and network bandwidth is saved.

3.11.1 Snooping Configuration

The screenshot shows the Tenda web management interface. The left sidebar contains a navigation menu with the following items: Status, Port Setting, Mirror, VLAN, Trunk, QoS, MAC Address Setting, 802.1X Setting, HSTP Setting, IGMP Snooping (selected), and System. The main content area is titled "IGMP Configuration" and includes a table for enabling IGMP and Router Ports, and a table for the IGMP Configuration List.

IGMP Configuration

IGMP	Enable <input type="checkbox"/>
Router Ports	<input type="checkbox"/> 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"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24

IGMP Configuration List

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

IGMP Configuration:

- **IGMP:** Enabling or disabling L2 multicast snooping function of the switch. By default, this option is unchecked.
- **Router Ports:** Selecting the IGMP routing ports for the multicast snooping.

IGMP Configuration List:

- **IGMP Snooping Enabled:** Enabling or disabling the L2 multicast snooping function of the switch of the corresponding VLAN.
- **IGMP Query Enabled:** Enabling or disabling the IGMP query. Once this function is enabled, you can view the multicast snooping status of the corresponding VLAN in Snooping status.

3.11.2 Snooping Status



IGMP Status: Displaying the multicast snooping function options of the corresponding VLAN. When the multicast table is not established, “Querier” displays “Idle”. When the switch snoops into a multicast message, “Querier” displays “Active”, and the value in “Queries transmitted” or “Queries received” may change at the same time. By change of the values in “V1 Reports”, “V2 Reports” and “V3 Reports”, you can know the corresponding version of the multicast messages received. If a message is of V2 and a device in the multicast table requires for leaving the multicast group, the leave message is transmitted.

- Refresh: Re-reading counting values, that is, manually refreshing current port status information.

3.12 System

3.12.1 SNMP



- All management information and counters are stored in the Management Information Base (MIB) of the switch. Usually, the switch adopts standard MIB-II module, supporting read by any SNMP-based NMS software. MIB data may be of either read-only or read-write mode.
- You can change the default SNMP community names of the switch and set access right for such community names.
- Trap means some message used for notifying you of certain events on the switch. Such event may be serious (for example,

switch reboot) or ordinary (for example, status change of a switch port). The switch can generate trap and send it to the NMS.

SNMP Configuration:

- **SNMP enabled:** Enabling or disabling the SNMP management function.
- **SNMP Trap destination:** Setting the destination IP address of the Trap message of the switch.
- **SNMP Read Community:** Setting the read-only community name of the SNMP information of the switch. To read the SNMP information of the switch, the SNMP management software must contain the consistent read-only community name.
- **SNMP Write Community:** Setting the writable community name of the SNMP information of the switch. To modify the SNMP information of the switch, the SNMP management software must contain the consistent writable community name.
- **SNMP Trap Community:** Used by the SNMP management software to identify the specific switch sending the Trap message.

3.12.2 Change Password

Configuration	Content
Old Password	<input type="text"/> (length<=15)
New Password	<input type="text"/> (length<=15)
Confirm New Password	<input type="text"/> (length<=15)

Configuration: Modifying the password for switch login.

- Old Password: Entering the default password (admin).
- New Password: Entering a new password.
- Confirm New Password: Entering the new password again.



Caution: A password consists of 15 characters at most.

3.12.3 Cable Diagnostic

Cable Diagnostic

Port: 1

Diagnose Mode: Full

Diagnose

Notes:

1. Full refers to both the diagnosis cable status and the diagnosis cable length;
2. Anomaly refers to the diagnosis cable status only;
3. Anomaly who X-pair refers to the diagnosis cable length only;

Cable Status

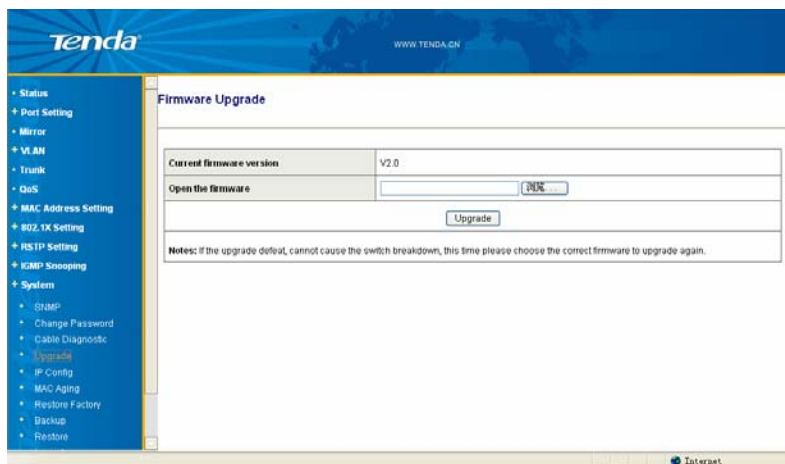
cable pair	length [m]	status
A	-	-
B	-	-

Cable Status: Displaying the number, status and length of cable pairs.

⚠ Caution:

The cable length value detected by the switch is only a reference, because cable interference difference hugely affects the detection result.

3.12.4 Upgrade



Please visit our website to obtain upgrade package and detailed upgrade guide. Be cautious during the upgrade. It is recommended to interrupt all network connections except the network connection of the computer used for upgrade. Do not power off the system during the upgrade, to avoid computer down or other abnormalities.

Firmware upgrade:

1. Log in to our website (www.tenda.com.cn) and download the software of a higher version.
2. Click “Browse” to locate the upgrade program.
3. Click “Upgrade” to upgrade the software.

⚠ Caution: Do not power off the switch during the upgrade; otherwise, the switch may be damaged.

3.12.5 IP Configuration

The screenshot shows the Tenda web management interface. The main content area is titled 'Configure IP Address'. It contains a table with the following fields:

DHCP Client	Enable <input type="checkbox"/>
IP Address	192 168 0 1
Subnet mask	255 255 255 0
Gateway	0 0 0 0
Management VLAN	1

Below the table, there is a 'Notes' section:

Notes:
If enable DHCP client, you should login the web management interface by the IP address obtained from DHCP server.

An 'Apply' button is located at the bottom right of the configuration area.

DHCP Client: Enabling or disabling the DHCP client.

IP Address: Setting the IP address, subnet mask and gateway of the switch.

- IP Address: Modifying the login IP address (192.168.0.1 by default) of the switch.
- Subnet mask: Modifying the subnet mask (255.255.255.0 by default) of the switch.

- Gateway: Modifying the gateway (0.0.0.0 by default) of the switch.
- Management VLAN: Selecting the VLAN where the management computer is located.

⚠ Caution: After enabling the DHCP client, you need to check the IP address obtained from the DHCP server and then connect with the switch again. It is not recommended to use this function, unless you are very sure about the IP address allocated by the DHCP server.

3.12.6 MAC Aging



- The default MAC address aging time is 300 s. The set value should be within 10 s ~ 65535 s; otherwise, the system reports error. If

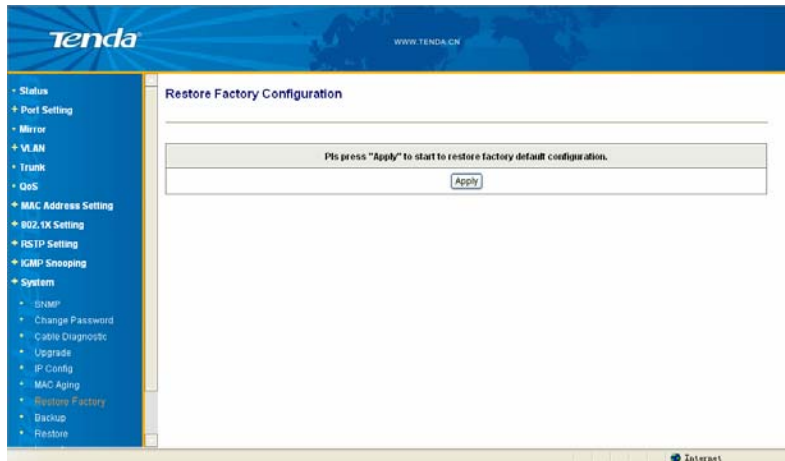
“ARL Aging” is unchecked, the system terminates MAC address aging.

ARL Aging Configuration:

- ARL Aging: Checking it to enable this function or unchecking it to disable this function (terminating the aging).
- Aging Time: Entering the aging time, 300 s by default.

⚠ Caution: Once “ARL Aging” is unchecked, the switch stops learning new MAC address and the address information in the MAC address table turns into static MAC. The MAC address learnt is free from aging.

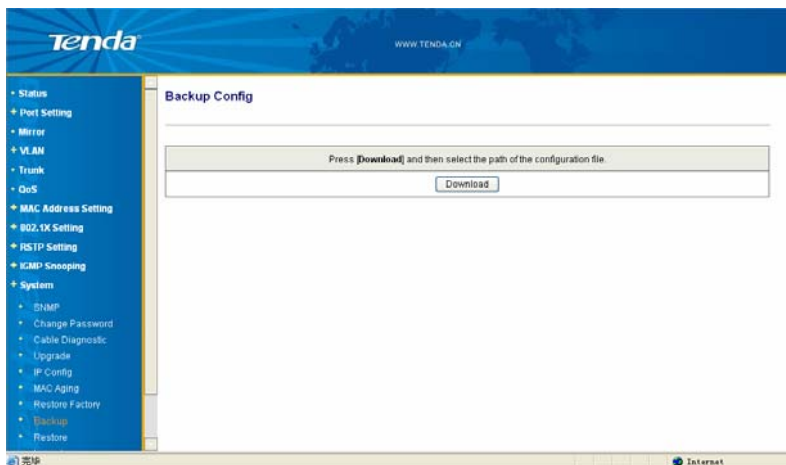
3.12.7 Restore Factory



Restore Factory Configuration: Clicking “Apply” to restore the default configuration before delivery.

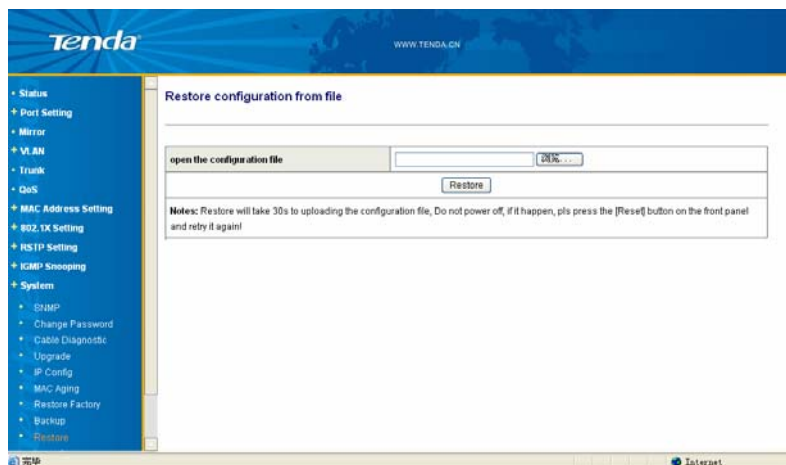
⚠ Caution: After restoring the default configuration, you need to re-log in to the setting window. If the default IP address of the switch had been changed, you should use the default IP address (192.168.0.1) for re-login at this time (Both default user name and default password are admin).

3.12.8 Backup



Backup Config: Backing up the current switch configuration. Click “Download” and select the saving path.

3.12.9 Restore



Restore configuration from file: Restoring the backup switch configuration. Click “Browse” and select the backup file, and then click “Restore”.

⚠ Caution: It takes 30 s to complete such restoration operation. During the restoration, do not power off the system to avoid computer down or other abnormalities. At the end of restoration, restart the switch.

3.12.10 Logout

This function is used to exit the setting window, to ensure system security.

Appendix 1 Online Technical Support

For any problem occurring during the installation, log in to **www.tenda.cn** for help.

The downloading center of the technical support part provides the latest driver and upgrade package for downloading.

Appendix 2 Common Commands

Common Commands	Description
cmd	Quickly entering the command line mode of Windows system (applicable to Windows2000 and higher).
ipconfig	Displaying the IP address of the current computer, for example, ipconfig /all.
ping	It is most frequently used in the network test. It is used to send a packet to the target host, asking for response. If the system can receive the response from the target host, the system can know the network response time and connection status between the local device and target host.
netstat	Displaying the details of the current active network connections, including network connections, routing table and network interface information. It can also be used to count the network connections running.
tracert	Displaying the path passed by the packet before reaching the target host and the specific time when it reaching each node. It is similar to the Ping command, but it provides far detailed information than the Ping command. It displays the entire path, IP address of each involved node and total time used.
net stop	Terminating the Windows NT network service, for example, net stop dnscache.
net send	Sending messages to other users, computers or communication names in the network. To receive messages, the system must enable the messenger service.

Appendix 3 TCP/IP Address Setting (Windows XP as Example)

Select “Start → Control Panel” to display the “Control Panel” window (see Figure 1).

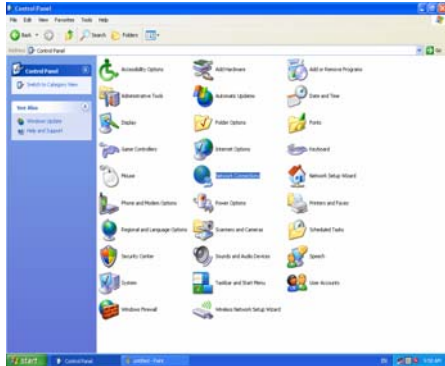


Figure 1

Click “Network Connection” to display the “Network Connections” window (see Figure 2).

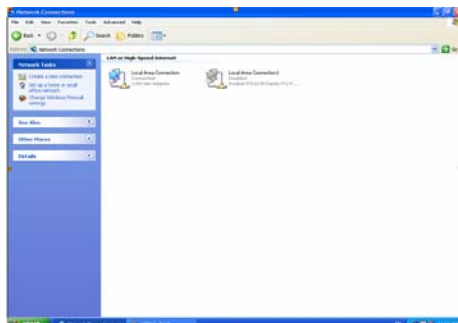


Figure 2

Right-click “Local Area Connection” and then select “Properties” in the shortcut menu, to display the “Local Area Connection Properties” dialog box. Select “Internet Protocol (TCP/IP)” in “This connection uses the following items”, and then click “Properties” (see Figure 3).

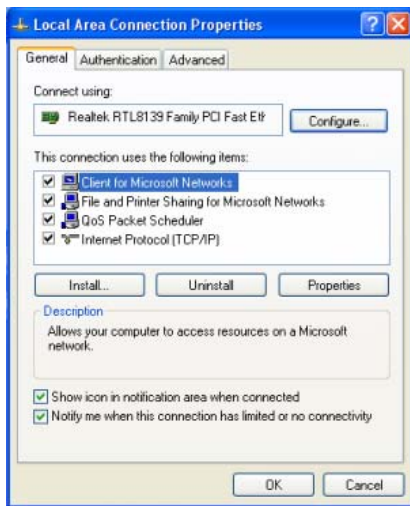


Figure 3

In “Use the following IP address”, enter “192.168.0.xxx” (“xxx” ranges 2 ~ 254) for IP address and 255.255.255.0 for subnet mask (see Figure 4).

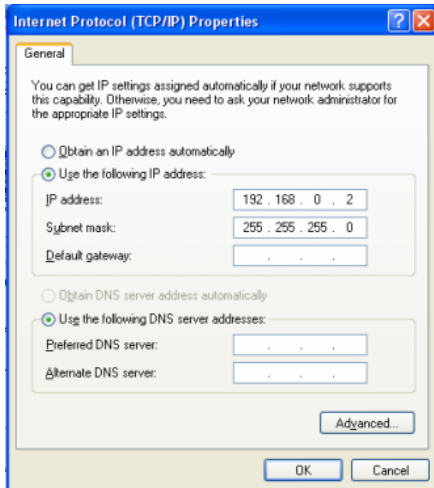


Figure 4

Click "OK" to return to the "Local Area Connection Properties" dialog box.

Click "OK" to exit the setting window.