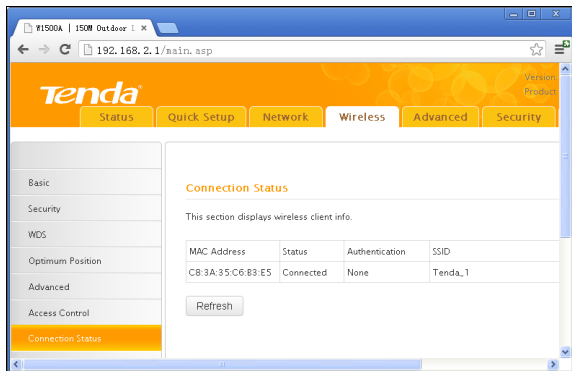


## 4.7 ConnectionStatus

This section displays the info of connected wireless clients including MAC addresses and encryption info, etc.



The screenshot shows the web interface of a Tenda wireless router. The browser address bar shows the URL `192.168.2.1/main.asp`. The interface has a navigation menu with tabs for Status, Quick Setup, Network, Wireless, Advanced, and Security. The left sidebar contains a list of configuration categories: Basic, Security, WDS, Optimum Position, Advanced, Access Control, and Connection Status (which is currently selected and highlighted in orange).

The main content area is titled "Connection Status" and contains the following text: "This section displays wireless client info."

MAC Address	Status	Authentication	SSID
CB:3A:35:C6:B3:E5	Connected	None	Tenda_1

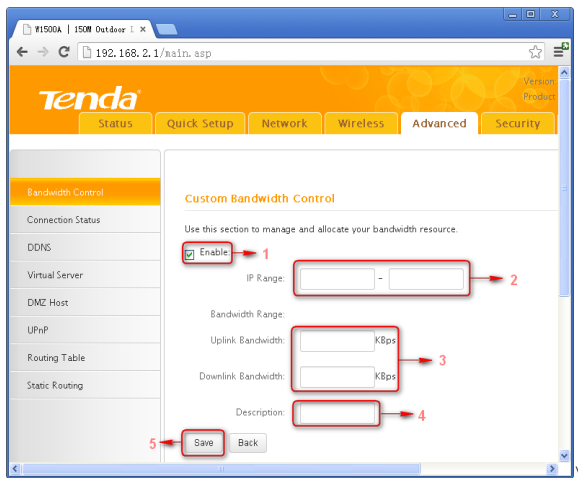
Below the table is a "Refresh" button.

## Chapter5 Advanced Applications

The **Advanced** tab only works on router mode, it has the following 7 submenus: Bandwidth Settings, Connection Status, DDNS, Virtual Server, DMZ Host, UPnP, Routing Table and Static Routing.

### 5.1 Bandwidth Settings


Bandwidth control is used for limit internal network speed. It supports IP address range configuration. Click Add and below screen will appear.



- **Enable:** Check/uncheck to enable/disable current entry.
- When disabled, corresponding entry will not take effect though existing in fact.
- **IP Range:** Enter a single IP or an IP range.
- **Uplink Bandwidth:** Max uplink traffic.
- **Downlink Bandwidth:** Max downlink traffic.
- **Description:** Briefly describe the current rule, the Max number of rule is 10.

## 5.2 Connection status

Showing the current connection information, which is client IP address, MAC address and connection mode.



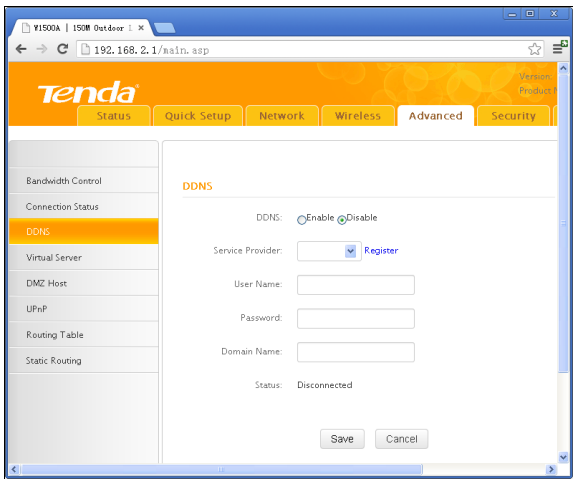
The screenshot shows a web browser window with the URL `192.168.2.1/main.asp`. The page title is "Tenda" and the navigation menu includes "Status", "Quick Setup", "Network", "Wireless", "Advanced", and "Security". The "Advanced" tab is selected, and the "Connection Status" sub-tab is active. The page content includes a description: "This section displays client info and connection status, etc." and a table with the following data:

IP Address	MAC Address	Medium Type(Wired/Wireless)
192.168.2.185	00:B0:0C:17:EC:A1	Wired
192.168.0.120	78:2B:C8:04:99:48	Wired
192.168.2.173	44:37:E6:51:FE:40	Wired
192.168.2.168	10:78:D2:F4:66:56	Wired

A "Refresh" button is located below the table.

## 5.3 DDNS

Dynamic DNS or DDNS is a method of updating, in real time, a Domain Name System (DNS) to point to a changing IP address on the Internet. This is used to provide a persistent domain name for a resource that may change location on the network.



1、 Mostly, broadband ISP (Internet service provider) only provide client with Dynamic IP address. While DDNS knows every change on IP address and Banding it with well-known name, so others users can use well-known name to communicate with the client.

2、 DDNS can help you setup virtual server in your company or home.

- Service Provider: Select the DDNS service provider you are using, [support no-ip.com](#), [dyndns.com](#)
- User Name: Enter the DDNS user name registered with your DDNS

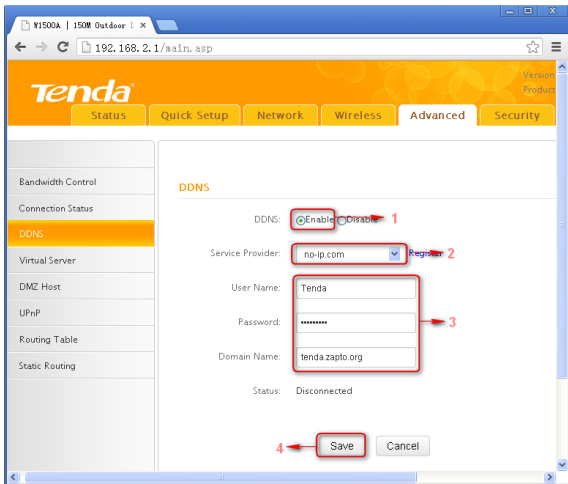
service provider.

- Password: Enter the DDNS Password registered with your DDNS service provider.
- Domain Name: Enter the DDNS domain name with your DDNS service provider.

For example: If you have registered a DDNS service from no-ip.com for a web server on the host at 192.168.2.10 and get below info:

User Name	Tenda
Password	123456
Domain Name	tenda.zapto.org

First set a mapping rule on Virtual Server interface (For details, see Virtual Server section) and then enter the registered user name, password and domain name as shown below:

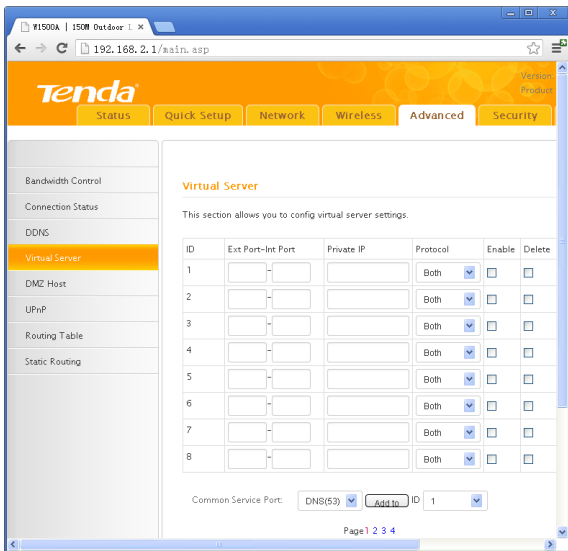


Then Click Save to save the settings.

Simply input "http://tenda.zapto.org" in a launched web browser and your web server will be accessible.

## 5.4 Virtual Server

Defines the mapping between the service port range of WAN access and LAN server, all of the WAN ports used within the scope of access will be re-positioned to the LAN network server specified by IP address.



- **Ext Port-Int Port:** WAN service port. Internal LAN PC port corresponding mapped to an external port.
- **Private IP:** The IP address of a computer used as a server in LAN.
- **Protocol:** Includes TCP, UDP and Both. Select "Both" if you are not sure about which protocol to use.
- **Enable:** The corresponding entry takes effect only if you checked this option.
- **Delete:** Clear all settings of this item.
- **Common Service Port:** The well-known protocol ports are listed

in the drop-down list. Select one and select a sequence number in the ID drop-down list and then click "Add", this port will be added automatically to the ID list. For other well-known service ports that are not listed, you can manually add them to the list.

- **Add to:** Add the selected well-known port to the policy ID.

For Example: you can build a WEB server on your computer and set the router's port range forwarding to enable your friends to access to your computer. Suppose that your WEB server or your computer's static IP address is 192.168.2.100, and you wish your friends can access the server through the default port 80 and adopts TCP protocol.

The screenshot shows the Tenda web interface for configuring Virtual Servers. The left sidebar lists various settings, with 'Virtual Server' selected. The main content area is titled 'Virtual Server' and includes a table for configuring virtual server settings. The table has columns for ID, Ext Port-Int Port, Private IP, Protocol, Enable, and Delete. Row 1 is pre-filled with ID 1, Ext Port 80, Int Port 80, Private IP 192.168.2.100, Protocol Both, and Enable checked. Below the table is a 'Common Service Port' section with a dropdown menu set to 'DNS(53)', an 'Add to' button, and an 'ID' dropdown set to '1'.

ID	Ext Port-Int Port	Private IP	Protocol	Enable	Delete
1	80 - 80	192.168.2.100	Both	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2			Both	<input type="checkbox"/>	<input type="checkbox"/>
3			Both	<input type="checkbox"/>	<input type="checkbox"/>
4			Both	<input type="checkbox"/>	<input type="checkbox"/>
5			Both	<input type="checkbox"/>	<input type="checkbox"/>
6			Both	<input type="checkbox"/>	<input type="checkbox"/>
7			Both	<input type="checkbox"/>	<input type="checkbox"/>
8			Both	<input type="checkbox"/>	<input type="checkbox"/>

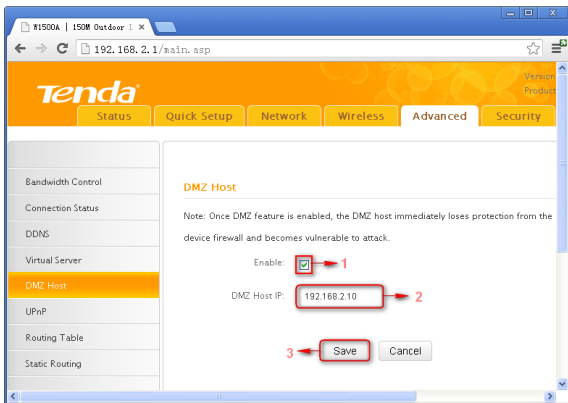
Common Service Port: DNS(53) Add to ID 1



**Notice:** If you set the service port of the virtual server as 80, you must set the Web Management port on Remote Web Management screen to be any value except 80 such as 8080. Otherwise, there will be a conflict to disable the virtual server.

## 5.5 DMZ Host

The DMZ Settings screen allows one local computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC.



- **DMZ Host IP:** The IP address of the LAN computer you want to set as DMZ host.
- **Enable:** Check to enable the DMZ host.

### For example:

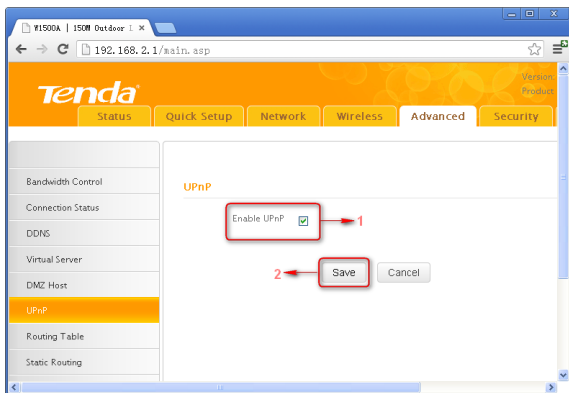
Set the computer at the IP address of 192.168.2.10 as DMZ host to connect another host on the Internet for intercommunication.

**Notice:** When the DMZ host is enabled, the firewall settings of the DMZ host will not function.

## 5.6 UPnP

With the UPnP (Universal Plug and Play) function, the internal host can request the router to process some special port switching so as to enable the external host to visit the resources of the internal host.

UPnP works in Windows XP, Windows ME or later (Note: Operational system needs to be integrated with or installed with DirectX 9.0) or in an environment with installed application software that supports UPnP.



**Enable UPnP:** Click the checkbox to enable the UPnP.

## 5.7 Routing Table

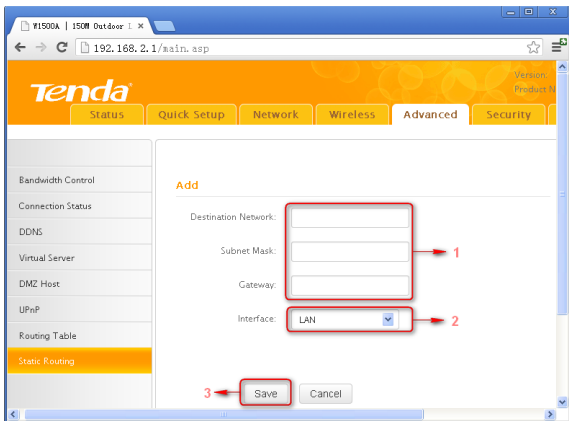
This page shows the router's core routing table.



The main duty for a router is to look for a best path for every data packet, and transfer this data packet to a destination station. In order to fulfill this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.

## 5.8 Static Routing

This page is used to set the router's static routing under router mode. Click Add, the following page you will see.



- **Destination Network:** The destination host or IP segment you visit.
- **Subnet Mask:** Enter the subnet mask, generally it is 255.255.255.0
- **Gateway:** The entry IP address of the next router.
- **Interface:** If destination need go through WAN port, then set it as WAN. Otherwise, set it as LAN.

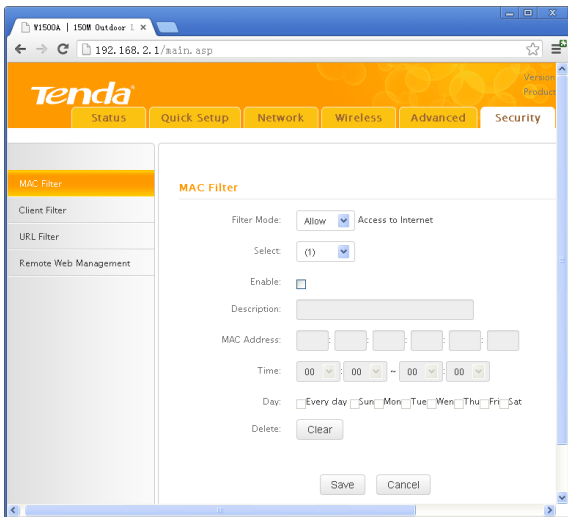
## Chapter 6. Security Settings

### 6.1 Mac Address Filter

Security Settings only fits for Wireless Router Mode.

To better manage PCs in LAN, you can use the MAC Address Filter function to allow/disallow such PCs to access to Internet. In Filter Mode, you can choose Disable, Allow Access to Internet, and Deny Access to Internet.

If you choose Allow Access to Internet, you will see the following configuration page.



**Filter Mode:** Select Deny or Allow according to your own needs.

**Deny Access to Internet:** Disallow only PCs at specified MAC addresses to access Internet. Other PCs are allowed.

**Allow Access to Internet:** Allow only PCs at specified MAC addresses to access Internet. Other PCs are denied

**Select:** Select a number (indicating a corresponding entry) from the drop-down menu. Up to 10 rules can be set.

**Enable:** Check/uncheck to enable/disable the corresponding entry.

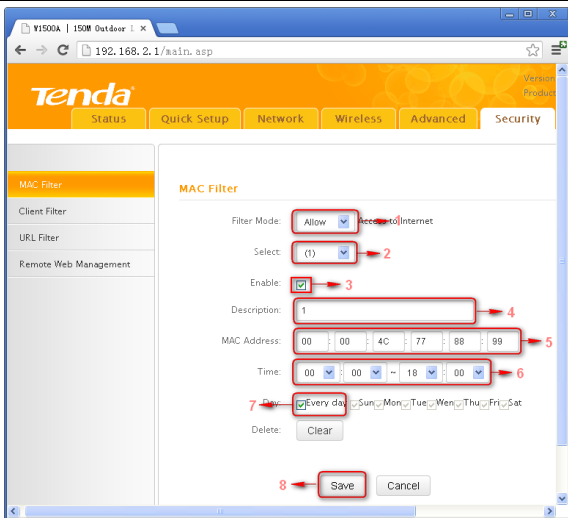
**Description:** Enter a meaningful name to you for corresponding entry.

**MAC Address:** Enter the PC's MAC address that you want to filter out.

**Time:** Select a time range for the corresponding entry to take effect, or else the default time is 00:00~00:00, which means the entry will be effective all the day.

**Day:** select a day or several days for the corresponding entry to take effect.

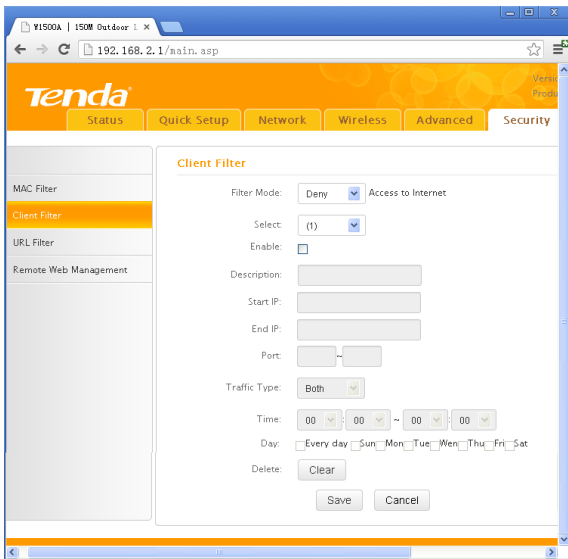
**Example :** To allow a PC at the MAC address of 00:00:4C:77:88:99 to access Internet from 00:00 to 18 : 00 everyday, configure same settings on the screenshot below on your device:



Click **Save** to save the settings.

## 6.2 Client Filter

To better manage PCs in LAN, you can allow or disallow such PCs to access certain ports on Internet using the Client Filter functionality.



**Filter Mode:** Select Deny or Allow according to your own needs.

**Disable:** disable the corresponding entry.

**Deny Access to Internet:** Disallow PCs at specified IP addresses to access certain ports on Internet.

**Allow Access to Internet:** Allow only PCs at specified IP addresses to access certain ports on Internet.

**Select:** Select a number (indicating a filter rule) from the drop-down menu. Up to 10 rules can be set.



**Enable:** Check/uncheck to enable/disable the corresponding entry.

**Description:** Enter a meaningful name to yourself for a new filter rule.

**Start IP:** Enter a starting IP address.

**End IP:** Enter an ending IP address.

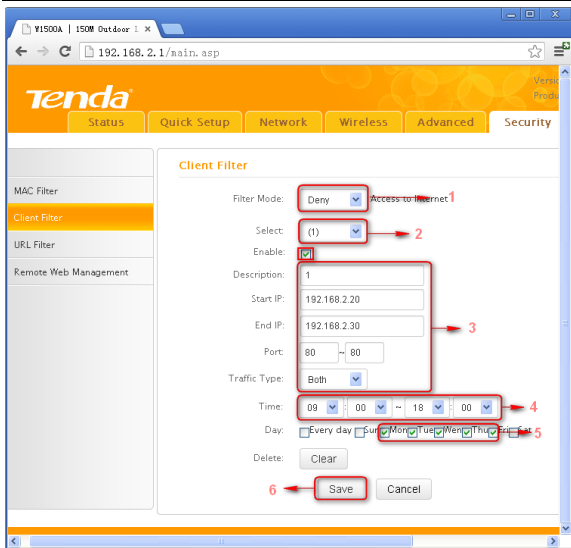
**Port:** Enter TCP/UDP protocol port number (s); it can be a range of ports or a single port from 1 to 65534.

**Traffic Type:** Select a protocol or protocols for the traffic (TCP/UDP/Both).

**Time:** Select a time range for the rule to take effect.

**Day:** Select a day or several days for the rule to take effect.

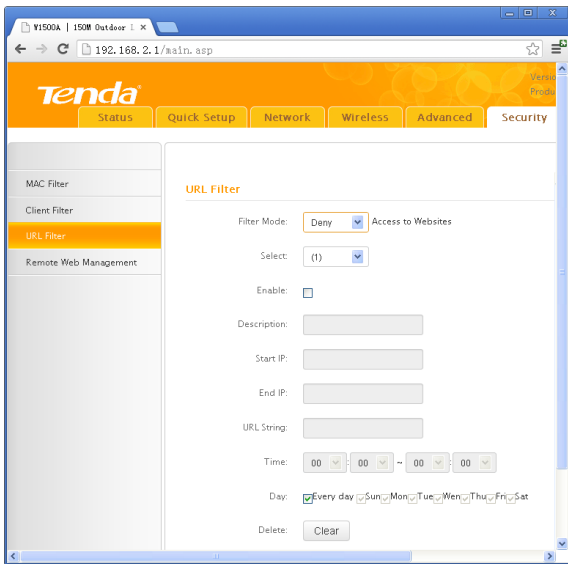
**Example:** To forbid PCs within the IP address range of 192.168.2.20--192.168.2.30 to visit websites from 9:00 to 18:00, do as follows:



Click Save to save the settings.

## 6.3 URL Filter

To better control LAN PCs, you can use the URL filter functionality to allow or disallow such PC to access certain websites within a specified time range. In Filter Mode, you can choose Disable, Allow Access to Websites, and Deny Access to Websites. You will see the page below.



**Filter Mode:** Select Deny or Allow according to your own needs.

**Deny Access to Websites:** Disallow PCs at specified IP addresses to access websites with certain URL string.

**Allow Access to Websites:** Allow PCs at specified IP addresses to access websites with certain URL string.

**Select:** Select a number (indicating a filter rule) from the drop-down menu. Up to 10 rules can be set.

**Description:** Enter a meaningful name to yourself for a new filter rule.

**Start IP:** Enter a starting IP address.

**End IP:** Enter an ending IP address.

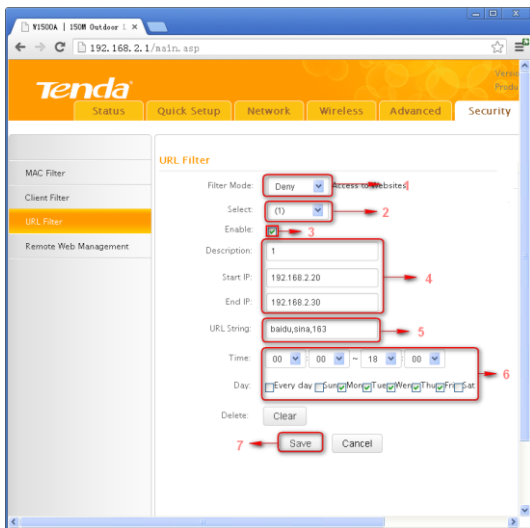
**URL String:** Enter domain names or a part of a domain name that needs to be filtered out.

**Time:** Select a time range for the corresponding entry to take effect.

**Day:** select a day or several days for the corresponding entry to take effect.

### Example:

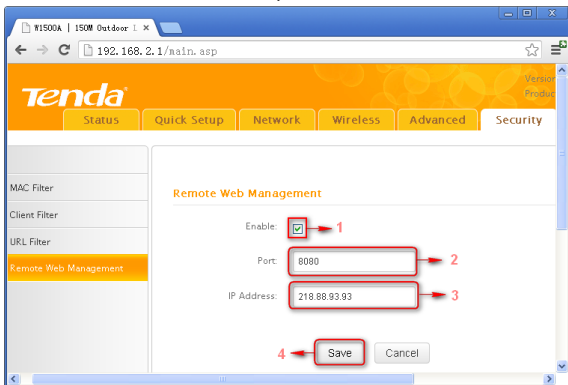
To forbid PCs within the IP addresses range of 192.168.2.20--192.168.2.30 on your LAN to visit websites whose URL contains "sina", "baidu" and "163" from 00 : 00 to 18 : 00 on working days: Monday- Friday, then do as follows:



Click Save to save the settings.

## 6.4 Remote Web Management

The Remote Web management allows the Router to be configured from the Internet by a web browser.



- **Enable:** Select whether to enable the Remote Web-based Management feature.
- **Port:** Remote admin port; the port used by trusted hosts from Internet or other external networks to access and manage the device remotely via a web browser.
- **IP address :** Enter a trusted IP address of a PC from Internet or other external networks which you want to authorize to manage the device remotely via a web browser.

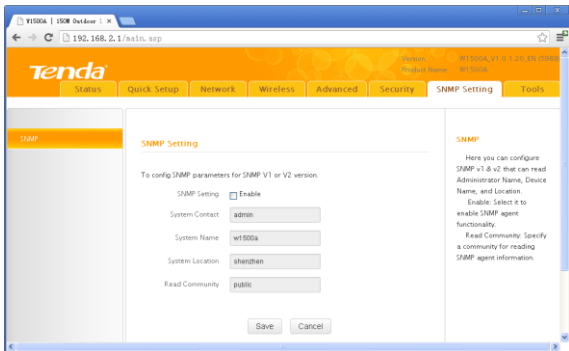
### Notice:

1. To access the device via port 8080, enter `http://x.x.x.x:8080` where "x.x.x.x" represents the the device's Internet IP address and 8080 is the remote admin port. Assuming the device's Internet IP address is 220.135.211.56, then, simply replace the "x.x.x.x" with "220.135.211.56" (namely, `http://220.135.211.56:8080`).
2. Leaving the IP address field at "0.0.0.0" makes the device remotely accessible to all the PCs on Internet or other external networks; populating it

with a specific IP address, say, 218.88.93.33, makes the device only remotely accessible to the PC at the specified IP address.

## Chapter 7 SNMP

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is widely used in local area networks (LAN) for collecting information, and managing and monitoring, network devices. For using this function, please enable it and provide the information which the following page need.



- **System contact** : Set the name to access the AP. Usually set the administrator's name.
- **Device Name** : Set the AP's name, such as Tenda\_W1500A.
- **Location** : Set the AP's network location.
- **Read Community** :Indicates the community read access string to permit reading this AP's SNMP information. The default is Public.

## Chapter 8 System tools

This section focuses on how to maintain AP, including Syslog, Statistics, Time & Date, Change Password, Backup, Restore, Firmware Update, Restore to Factory Default, Reboot.

### 8.1 Syslog

The section is to view the system log. You can view the various statuses after system startup and check whether there's network attack. If the log is over 200 records, it will clear them automatically.

The screenshot shows the Tenda web management interface for the N150 Outdoor device. The 'Syslog' tab is selected in the left sidebar. The main content area shows the Syslog configuration and a table of log entries.

**Syslog**

This section allows you to view all events that occur upon system startup.

View Log Levels:

Index	Time	Type	Log Contents
1	2011-05-01 00:00:06	wan	Broadcasting Dhcp_discover
2	2011-05-01 00:00:06	wan	Dhcp_offer Received from (192.168.0.2)
3	2011-05-01 00:00:06	wan	Broadcasting Dhcp_request for (192.168.0.100)
4	2011-05-01 00:00:06	wan	Dhcp_ack received from (192.168.0.2)
5	2011-05-01 00:00:06	wan	Get Client IP Address (192.168.0.100)
6	2011-05-01 00:00:06	system	DHCP Server Start
7	2011-05-01 00:00:10	system	wan up

Refresh Clear

**Syslog**

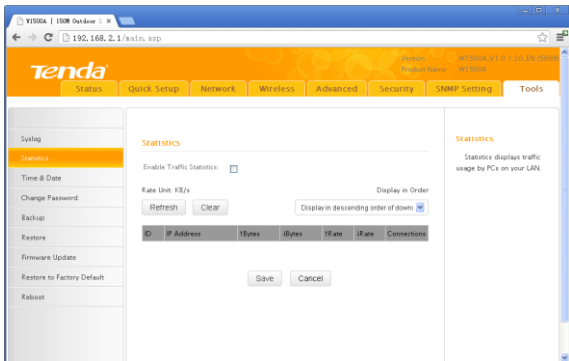
This section allows you to view all events that occur upon system startup. The device records a maximum of 200 log entries.  
Note: Logs will be cleared automatically when reaching the limit of 200 entries (25 pages).

- **Refresh:** Click this button to update the log.
- **Clear:** Click this button to clear the current log.



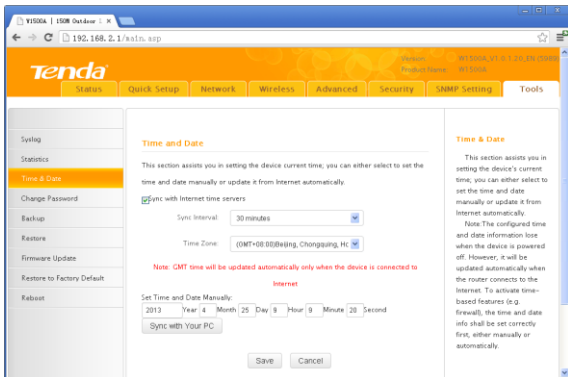
## 8.2 Statistics

Statistics is only for routing mode. This section will display the LAN IP addresses and the corresponding packet traffic status of the local network.



- **Enable Traffic Statistics:** Tick this box to enable the network user traffic statistics. If there is no need to, we suggest turn off this function.
- **Refresh:** Click this button to update the statistic list.

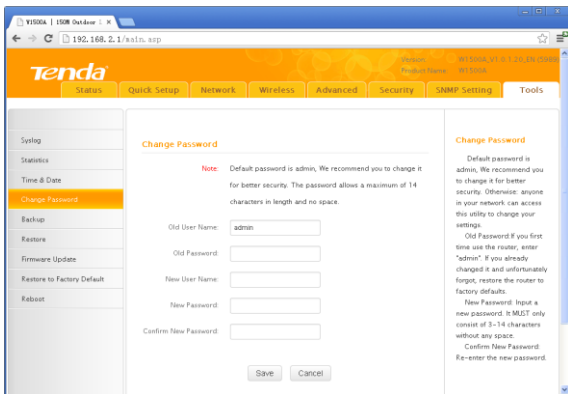
## 8.3 Time & Date



This section is to select the time zone for your location. You can select your own time or obtain the standard GMT time from Internet.


- **Sync with Internet time servers** : Obtain the standard GMT time from Internet automatically.
- **Sync Interval** : System time synchronization interval. Please choose according to your need, the system default cycle time is half an hour.
- **Time Zone** : Select your time zone from the drop-down menu.
- **Sync with Your PC** : Customize the time of the device the same with your PC.

## 8.4 Change Password

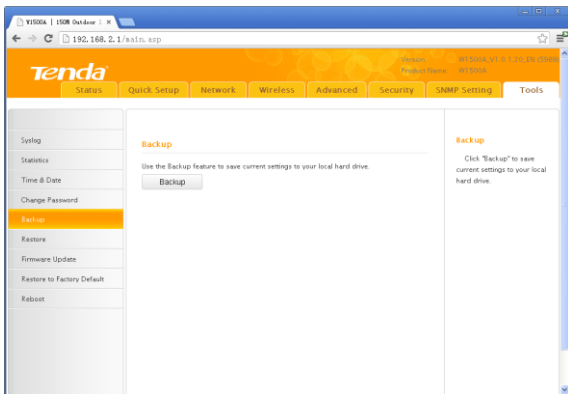


This section is to set a new user name and password to better secure your device and network. Type in correct parameters in the blank and click **save** to finish the username and password settings.

- **Old User Name:** Enter the old username.
- **Old Password:** Enter the old password.
- **New Username:** Enter a new user name for the device.
- **New Password:** Enter a new password for the device.
- **Confirm New Password:** Re-enter to confirm the new password.

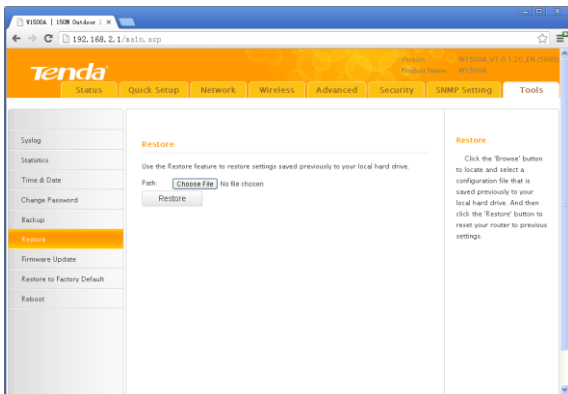
 **Note** : It is highly recommended to change the password to secure your network and the device.

## 8.5 Backup



**Backup:** Click this button to back up the device's configurations.

## 8.6 Restore

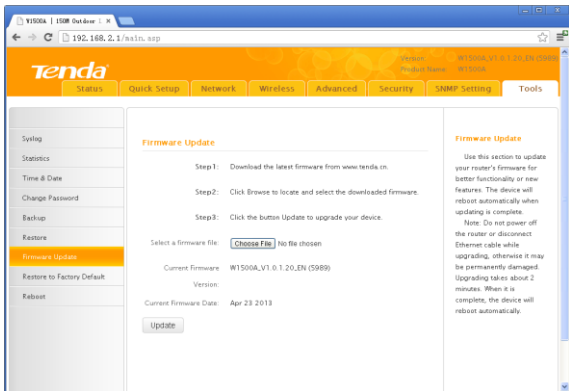


**Choose File:** Click this button to browse the directory where you backup or save the device's settings.

**Restore:** Click this button to restore the device's configurations.

## 8.7 Firmware Update

By upgrading the router's software, you will get more stable version and appreciation of the routing function.



### Firmware Update Steps :

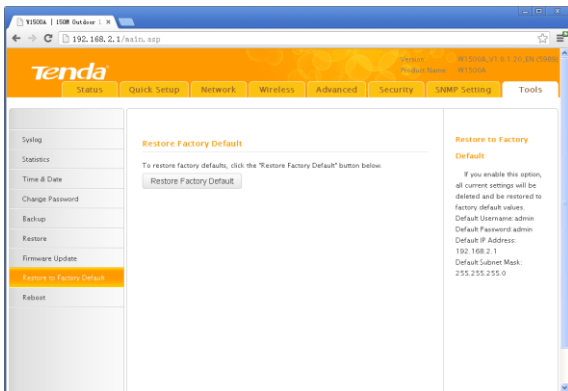
On the Firmware Upgrade screen, click the **Choose File** button and find the new firmware file.

Click **Update** button, and follow the on-screen instructions.

After the upgrade is completed, the device will reboot automatically.

**⚠️ Note:** Do not power off the system during the firmware upgrade to avoid damaging the device. The upgrade process will take a few minutes, please wait patiently.

## 8.8 Restore to Factory Default



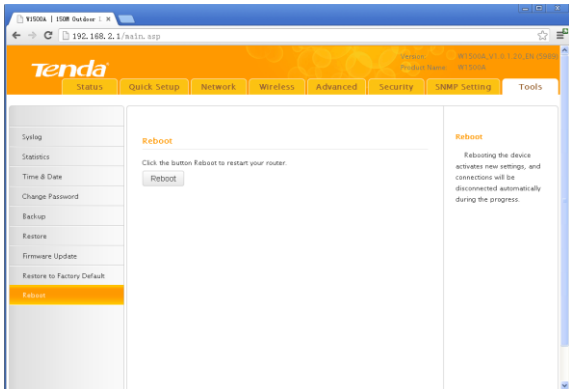
Restore to Factory Default: Click this button is to reset all configurations to the default values. It means the device will lose all the settings you have set.

### Factory Default Settings:

- **User Name:** admin
- **Password:** admin
- **IP Address:** 192.168.2.1
- **Subnet Mask:** 255.255.255.0

## 8.9 Reboot

This page is used to reboot the device. Rebooting the device makes the settings configured go into effect. This process will take about one minute.



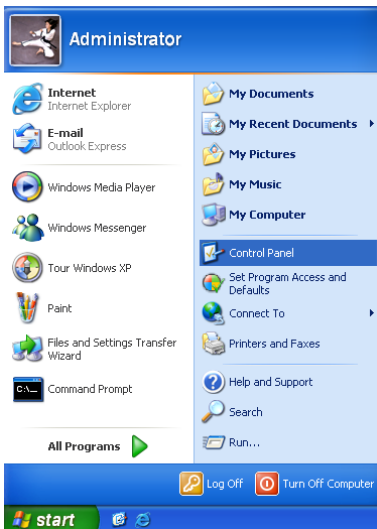
**Reboot:** Click this button to reboot the device.

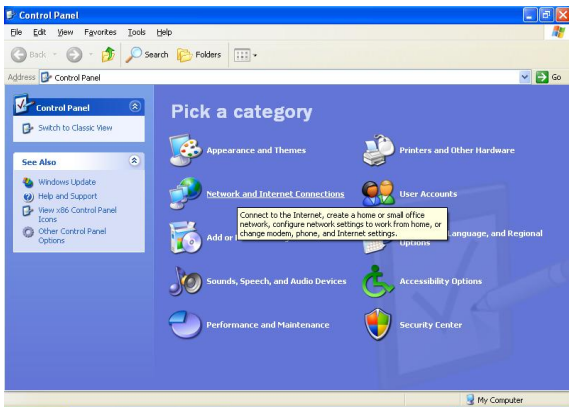


## Appendix 1 TCP/IP Settings

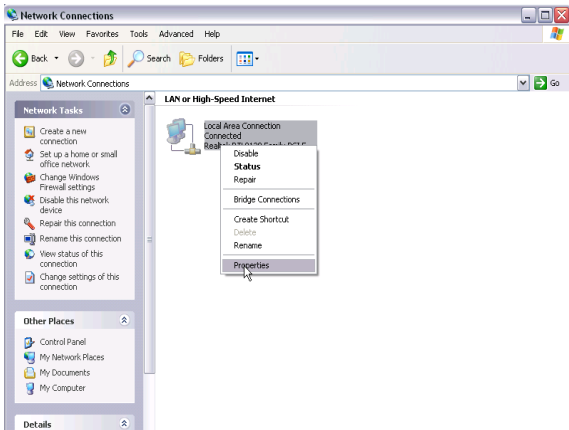
If you are using Windows XP, do as follows:

1. From the desktop, click **Start > Control Panel > Network and Internet Connections**.

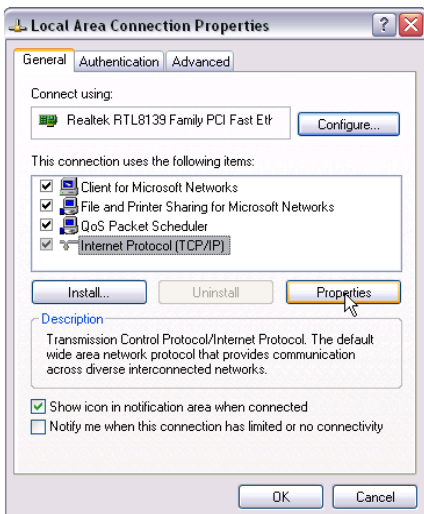




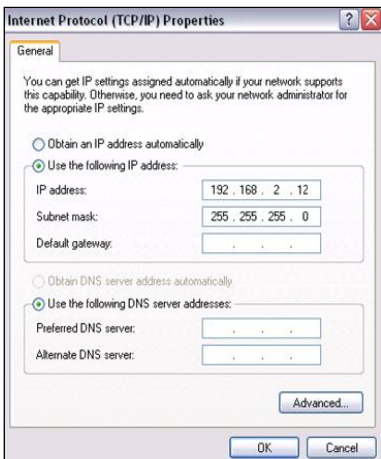
2. Right-click on the **Local Area Connection** and select **Properties**.



3. Select **Internet Protocol (TCP/IP)** and click **Properties**.



4. Select **Use the following IP address**.



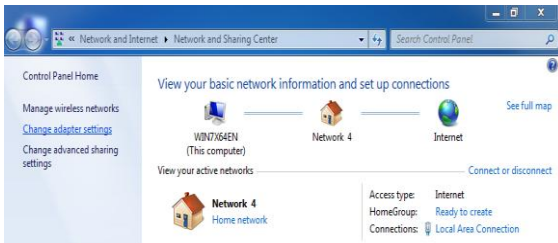
**IP address:** Enter 192.168.2.xxx where xxx can be any number between 2 and 253).

**Subnet mask:** Enter 255.255.255.0.

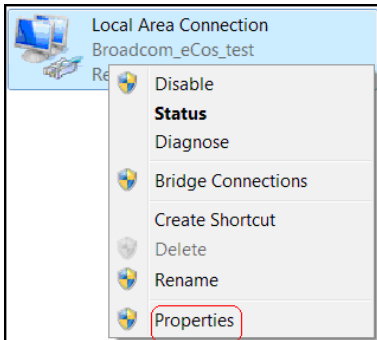
Click **OK** twice to save your settings.

If you are using Windows 7, do as follows:

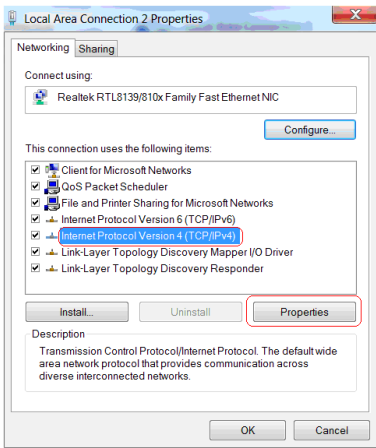
1. Click on **Start**-> **Control Panel** -> **Network and Internet**-> **Network and Sharing Center**. Click **Change adapter settings**.



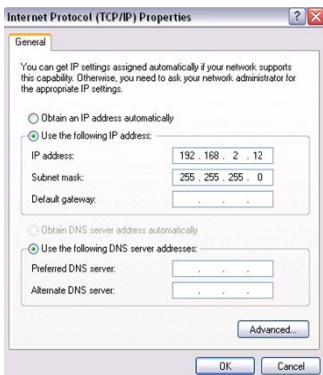
2. Right-click on the **Local Area Connection** and select **Properties**.



3. Select **Internet Protocol Version 4 (TCP/IPv4)** and **click Properties** or **directly** double-click on **Internet Protocol Version 4 (TCP/IPv4)**.



4. Select **Use the following IP address**.



**IP address:** Enter 192.168.2.xxx where xxx can be any number between 2 and 253).

**Subnet mask:** Enter 255.255.255.0.

Click **OK** twice to save your settings.

## Appendix 2: Glossary

### Channel

A communication channel, also known as channel, refers either to a physical transmission medium such as a wire or to a logical connection over a multiplexed medium such as a radio channel. It is used to transfer an information signal, such as a digital bit stream, from one or more transmitters to one or more receivers. If there is only one AP in the range, select any channel you like. The default is Auto.

If there are several APs coexisting in the same area, it is advisable that you select a different channel for each AP to operate on, minimizing the interference between neighboring APs. For example, if 3 American- standard APs coexist in one area, you can set their channels respectively to 1, 6 and 11 to avoid mutual interference.

### SSID

Service set identifier (SSID) is used to identify a particular 802.11 wireless LAN. It is the name of a specific wireless network. To let your wireless network adapter roam among different APs, you must set all Aps' SSID to the same name.

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks with the intention to provide data confidentiality comparable to that of a traditional wired network .WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use. WEP uses the stream cipher RC4 for confidentiality,[5] and the CRC-32 checksum for integrity. Standard 64-bit WEP uses a 40-bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key. The extended 128-bit WEP protocol uses a 104-bit key size (WEP-104). A 152-bit WEP is available from some vendors. Static WEP encryption allows to include 4 WEP



Keys while dynamic WEP encryption changes WEP key dynamically.

### WPA/WPA2

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only authorized network users can access the wireless network.

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA. Currently, WPA is supported by Windows XP SP1.

## Appendix 3 FAQs

This section provides solutions to problems that may occur during installation and operation of the device. Read the following if you are running into problems. If your problem is not covered here, please go to our website of [www.tendacn.com](http://www.tendacn.com) or e-mail to [support@tenda.cn](mailto:support@tenda.cn) for help.

### **1. Q: I entered the device's LAN IP address in the web browser but cannot access the utility. What should I do?**

A: 1) Verify physical connectivity by checking whether a corresponding port's link LED lights up. If not, try a different cable. Note that an illuminated light does NOT ALWAYS indicate successful connectivity.

2). In **Router Mode**, you must use a wireless network adapter to connect to the device, as the **LAN/WAN** Ethernet port works as a **WAN** port for Internet connection; while in **AP Mode, Universal Repeater Mode**, you must specify an IP address (192.168.2.2~192.168.2.253) on your PC to connect to the device. 3) Click **Start-->Run**, enter **cmd** and then input **ping 192.168.2.1** to check the connectivity status between your PC and device. If ping succeeds, then check whether the Proxy Server feature is enabled on your browser. If enabled, disable it immediately. In case that ping fails, press and hold the "RESET" button on your device for 7 seconds to restore factory default settings, and then run "ping192.168.2.1" again. Contact our technical support for help if the problem still exists after you tried all the above.

### **2. Q: What should I do if I forget the login password to my device?**

A: Reset your device by pressing the Reset button on the PoE injector for 8~10 seconds. Note: All settings will be deleted and restored to factory defaults once you pressed the Reset button.

### **3. Q: My computer shows an IP address conflict error after having connected to the device. What should I do?**

A: 1) Check if there are other DHCP servers present in your LAN. If there are other DHCP servers except your router, disable them immediately.

2) The default IP address of the device is 192.168.2.1; make sure this

address is not used by another PC or device. In case that two computers or devices share the same IP addresses, change either to a different address.

**4. Q: My computer can neither log in to the device nor access Internet, and there is a yellow triangle with an exclamation mark shown in the network adapter icon on the right bottom corner of my computer desktop; how am I supposed to deal with it?**

A: This problem occurs because your network card has not been assigned with an IP address. If your computer is set to obtain an IP address automatically, please ensure that the router's DHCP function is enabled. DHCP can automatically assign an IP address to your computer. If there is no DHCP server available on your network, please set a static IP address and fill in gateway and DNS, otherwise you cannot access Internet.

**5. Q: How do I share resources on my computer with users on Internet through the device?**

A: To let Internet users access internal servers on your LAN such as e-mail server, Web, FTP, via the device, use the "Virtual Server" feature. To do so, follow steps below:

Step 1: Create your internal server, make sure the LAN users can access these servers and you need to know related service ports, for example, port for Web server is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: Click "Virtual Server" and select "Port Range Forwarding" (also known as Port Forwarding on some devices) on device's web interface.

Step 3: Input the Start Port/External Port, say, 80.

Step 4: Input the End Port/Internal Port, say, 80.

Input the internal server's IP address. For example, assuming that your Web server's IP address is 192.168. 2.10, then simply input it.

Step 6: Select a communication protocol used by your internal host: TCP, UDP or ICMP and enable the rule.

Step 7: Save your settings.

For your reference, we collected a list of some well-known service ports as follows:

For your reference, we collected a list of some well-known service ports as follows:

Server	Protocol	Service Port
Web Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
NetMeeting	TCP	1503、1720
SKype	TCP/UDP	File Send:6891-6900(TCP) Voice:1863、6901(TCP) Voice:1863、5190(UDP)
PPTP VPN	TCP	1723
Iphone5.0	TCP	22555
SMTP	TCP	25
POP3	TCP	110

If your problems are not covered here, please feel free to go to [www.tendacn.com](http://www.tendacn.com) to find solutions or email your problems to: [support@tenda.com.cn](mailto:support@tenda.com.cn) or [support02@tenda.com.cn](mailto:support02@tenda.com.cn). We will be more than happy to help you out as soon as possible.

Website: [www.tendacn.com](http://www.tendacn.com)

Technical Support: [support@tenda.com.cn](mailto:support@tenda.com.cn)

Shenzhen Tenda Technology Co., Ltd

[www.tendacn.com](http://www.tendacn.com)

## Appendix 4 Safety and Emission Statement



### **CE Mark Warning**

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures. This device complies with EU 1999/5/EC.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.



### **FCC Statement**

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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radiofrequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Caution: Any changes or modifications not expressly approved by the

party responsible for compliance could void the user's authority to operate this equipment.

This device complies with part 15 of the FCC Rules.

Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and(2) this device must accept any interference received, including interference that may cause undesired operation. The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

NOTE:(1)The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.(2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable

#### FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.