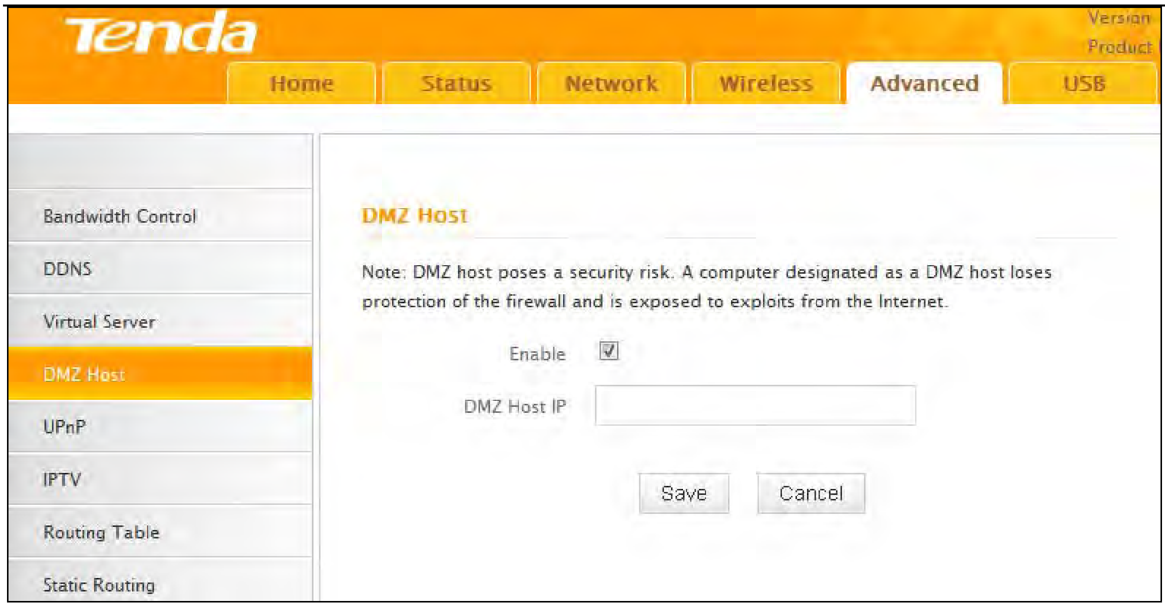


DMZ Host

Note: DMZ host poses a security risk. A computer designated as a DMZ host loses protection of the firewall and is exposed to exploits from the Internet.

Enable ☑

DMZ Host IP

Save Cancel

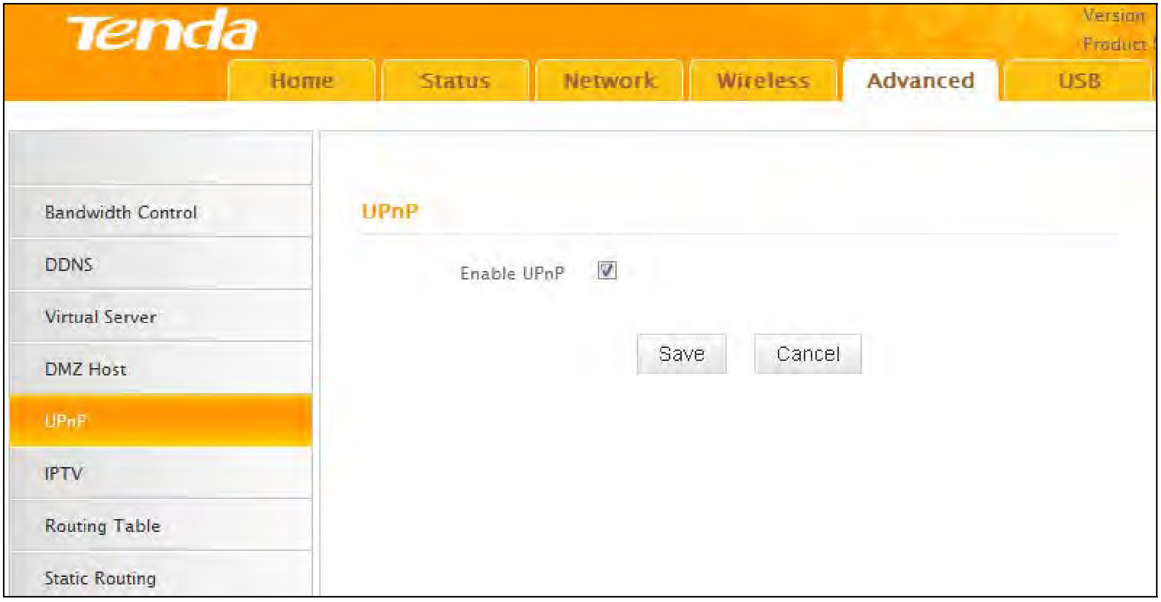
- Enable: Check/uncheck to enable/disable the DMZ host feature.
- DMZ Host IP: Enter the IP address of a computer on your LAN which you want to set as a DMZ host. The DMZ host should be connected to a LAN port on the router.

⚠**Note**

1. Once a PC is set to a DMZ host, it will be completely exposed to Internet, and thus may be vulnerable to attacks as related firewall settings become inoperative.
2. Users on the WAN can access the DMZ host through a corresponding WAN IP address.

4.5 UPnP

UPnP (Universal Plug and Play) allows a network device to discover and connect to other devices on the network. With this feature enabled, hosts in the LAN can request the device to perform special port forwarding so as to enable external hosts to access resources on internal hosts.



UPnP

Enable UPnP ☑

Save Cancel

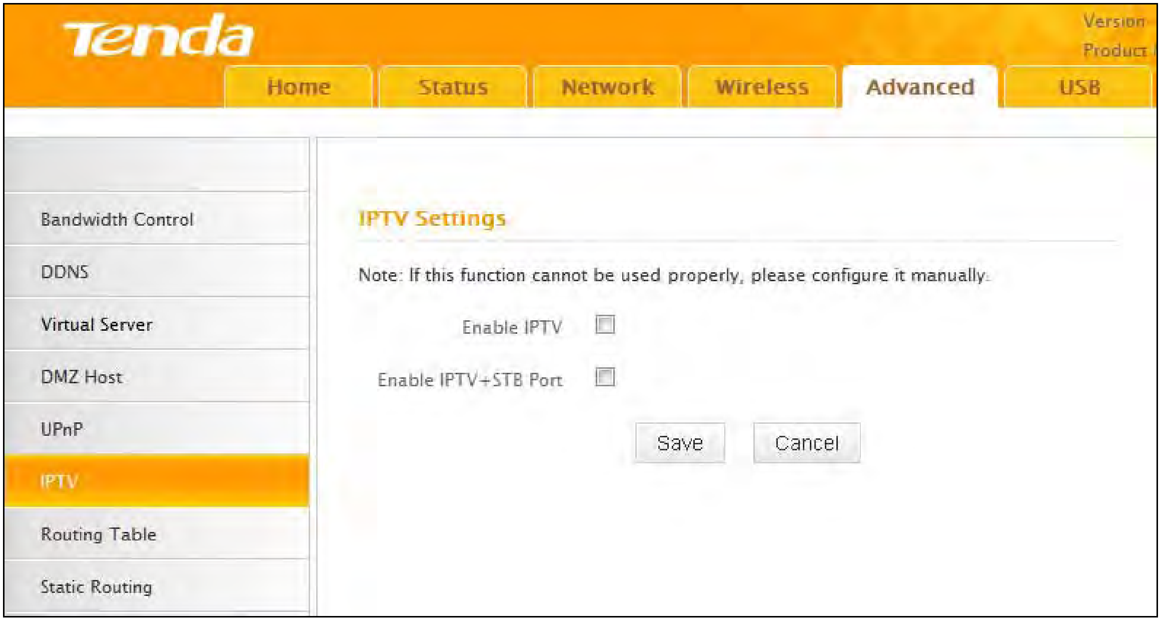
- Enable UPnP: Check/uncheck to enable/disable the UPnP feature.

⚠**Note**

UPnP works in Windows ME, Windows XP, or later, or in an environment with installed application software that supports UPnP. Operational systems needs to be integrated with or installed with Directx 9.0.

4.6 IPTV

The IPTV feature makes it possible to enjoy online videos on your TV set via a set-top box while surfing the Internet concurrently without mutual interference.



IPTV Settings

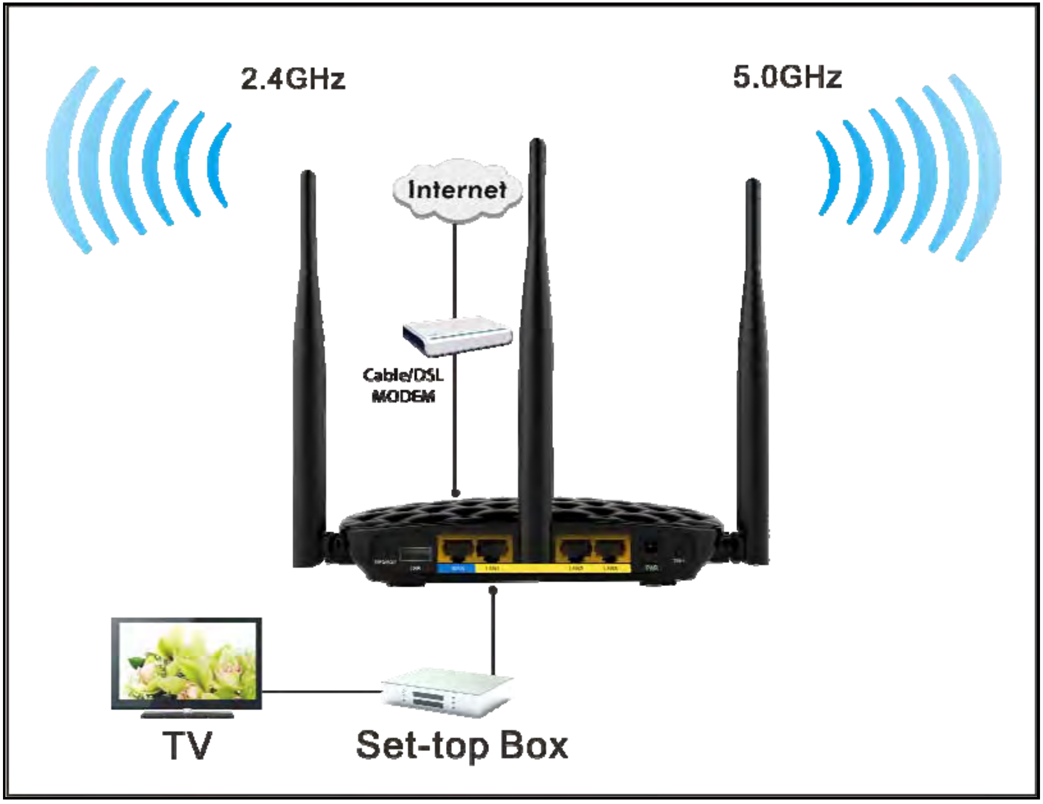
Note: If this function cannot be used properly, please configure it manually.

Enable IPTV □

Enable IPTV+STB Port □

- Enable IPTV: Check/uncheck to enable/disable the IPTV feature.
- Enable IPTV STB Port: Check/uncheck to enable/disable the IPTV-specific port.

See below for the network topology:



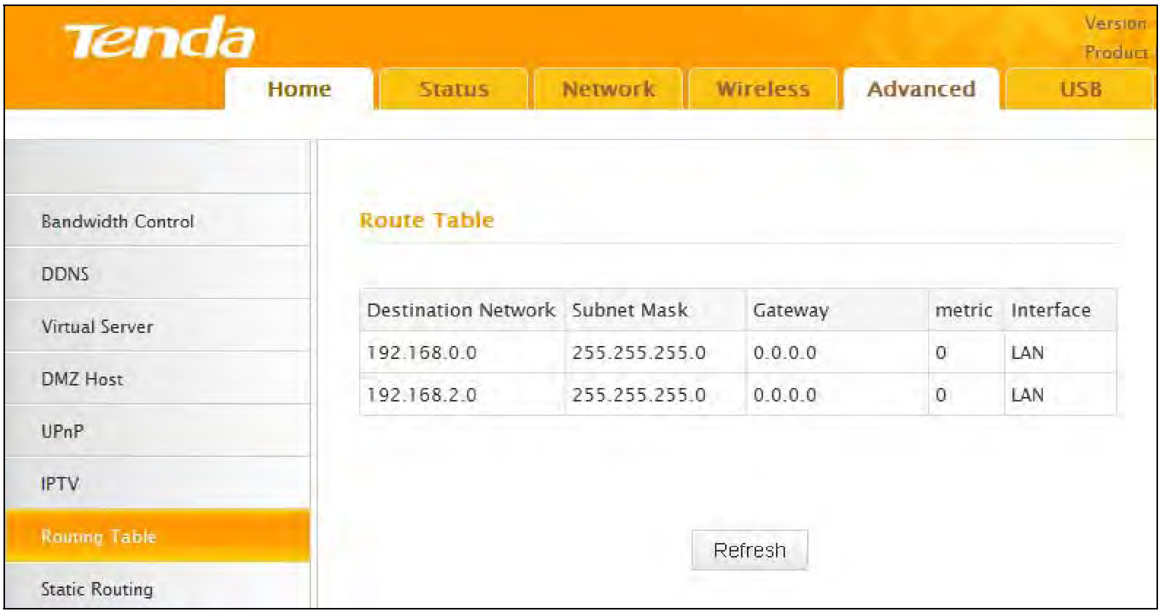
⚠**Note**

1. If you enabled both options mentioned above, then note below: (a). Set IPTV set-top box's connection type to DHCP/dynamic IP or static IP (IMPORTANT: Note that the set-top box's IP address should be on the same IP net segment as the router’s LAN IP.) if the set-top box is connected to any port of LAN ports 1-3. (b). Select the dialup mode provided by your ISP if the set-top box is connected to the IPTV-specific port.

2. After the IPTV port is set for IPTV purpose the PC that connects to such port will not be able to obtain an IP address or access Internet. Consider this situation before configuring this feature. Additionally, LAN ports1-3 can only be used as LAN ports to connect PCs instead of an IPTV set-top box.
3. The IPTV feature is currently not supported on WLAN.

4.7 Routing Table

This feature displays the routing table content.

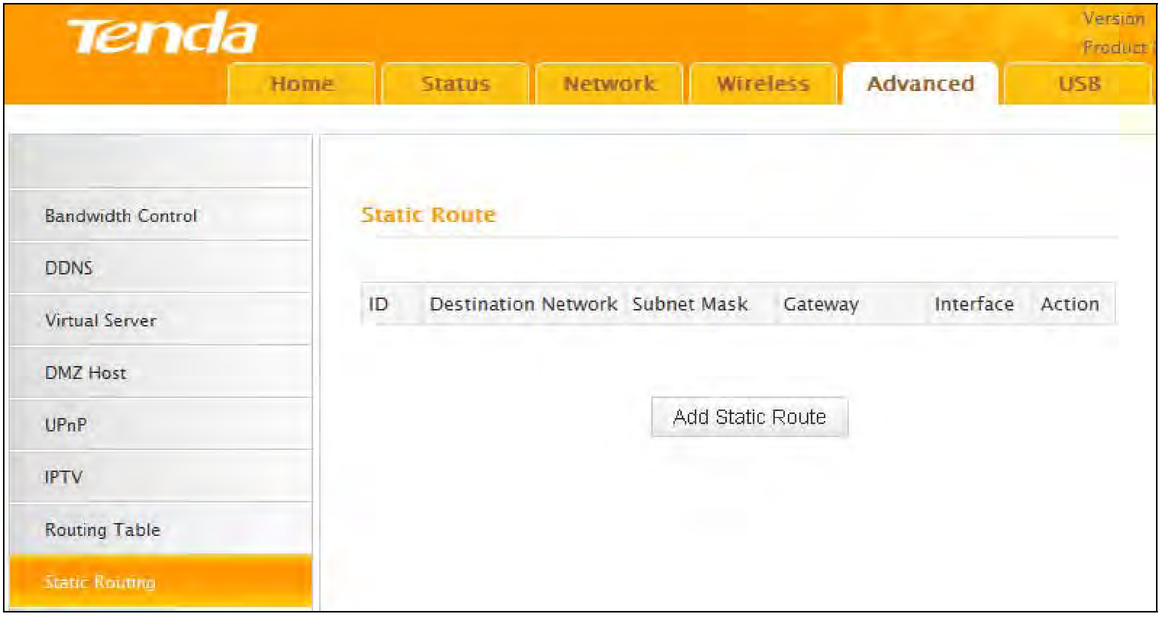


Route Table

Destination Network	Subnet Mask	Gateway	metric	Interface
192.168.0.0	255.255.255.0	0.0.0.0	0	LAN
192.168.2.0	255.255.255.0	0.0.0.0	0	LAN

4.8 Static Routing

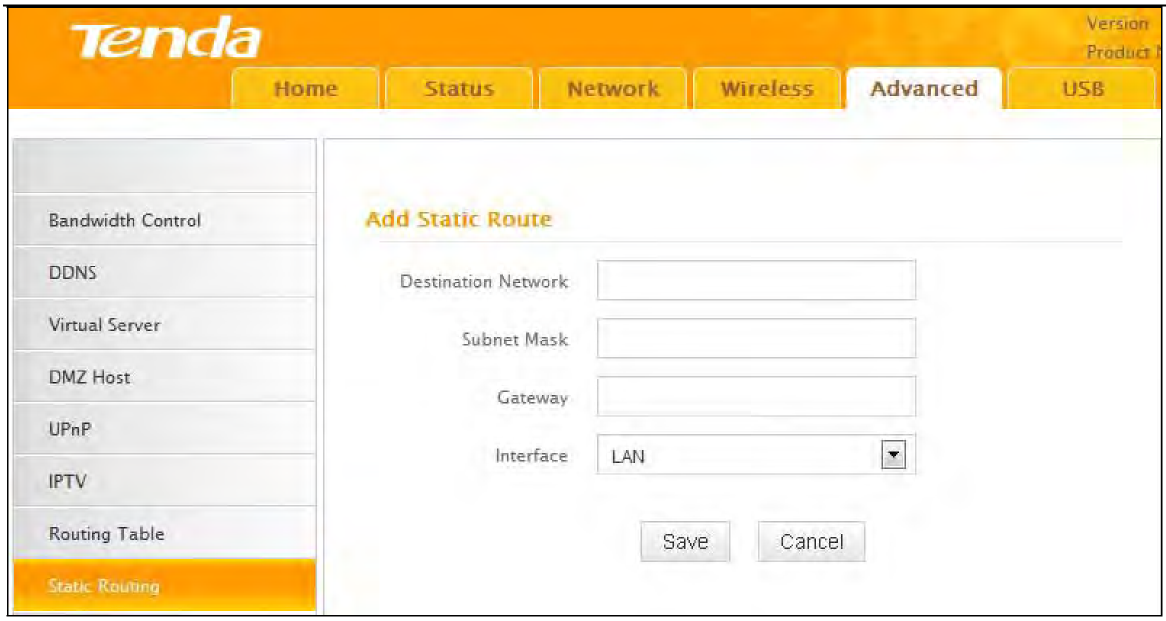
Use this section to customize static routes of data through your network.



Static Route

ID	Destination Network	Subnet Mask	Gateway	Interface	Action

Click **Add Static Route** and here comes the screen below:



Add Static Route

Destination Network

Subnet Mask

Gateway

Interface: LAN

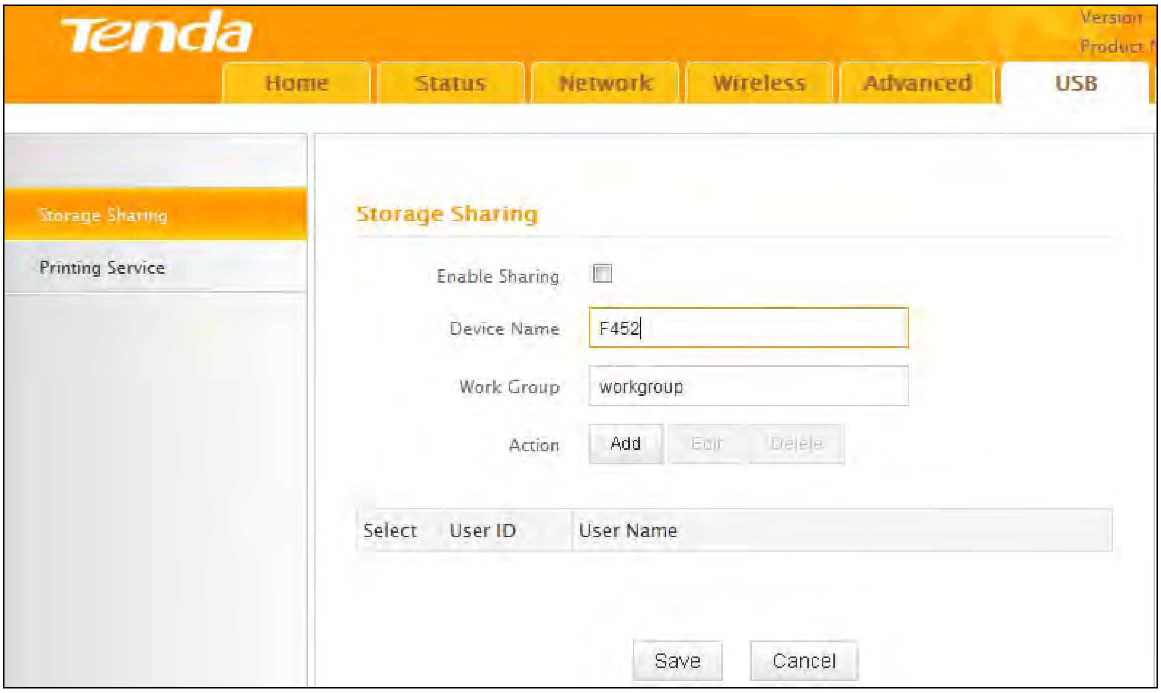
- Destination Network: The IP address of a destination network.
- Subnet Mask: The Subnet Mask that corresponds to the specified destination IP address.
- Gateway: The IP address for next hop.

5 USB

This router provides a USB interface for USB device connection. The "USB" tab includes two submenus: **Storage Sharing** and **Printing Service**.

5.1 Storage Sharing

The storage sharing feature allows you to share data files on the storage device attached to the router.



Storage Sharing

Enable Sharing □

Device Name: F452

Work Group: workgroup

Action

Select	User ID	User Name

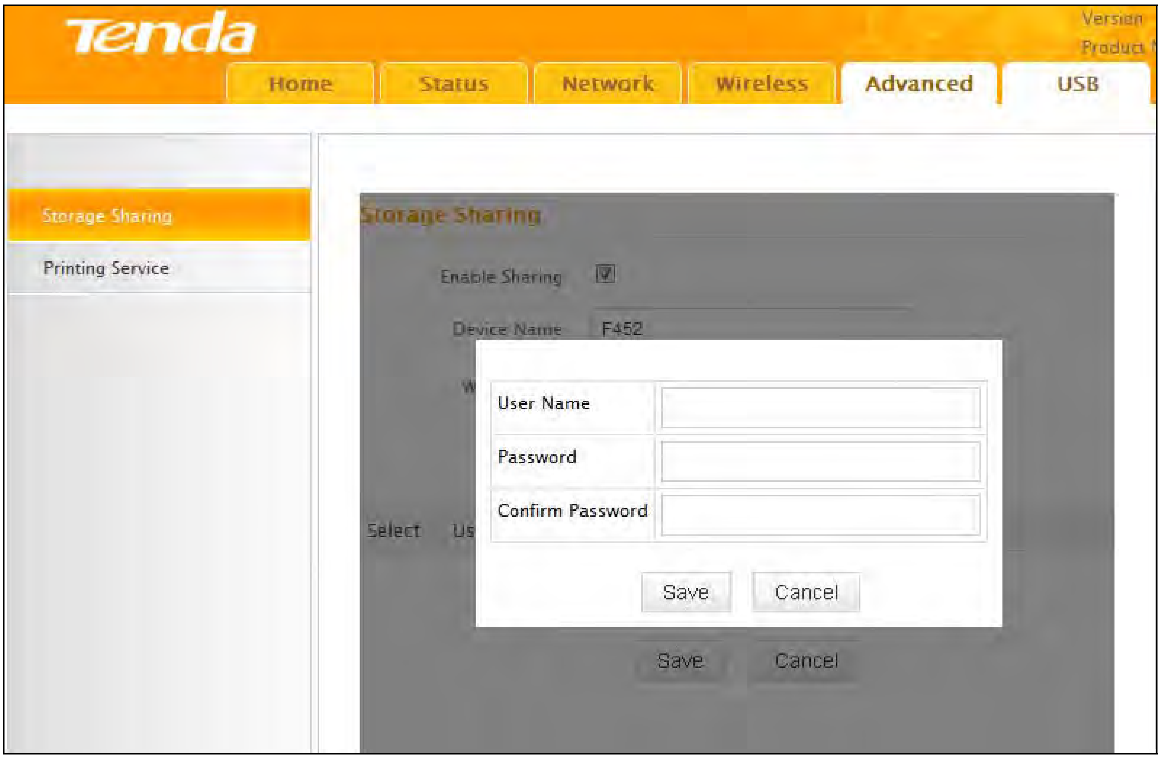
- Enable Sharing: Check/uncheck to enable/disable storage sharing feature.
- Device Name: Define a meaningful name for the device.
- Work Group: Define a work group name for the device.
- Add: Click to add a user account. Up to 5 accounts can be added.

- Edit: Click to edit an existing account.
- Delete: Click to delete an existing account.

Operation Instructions:

Before sharing files on a USB storage device, you must create a user account.

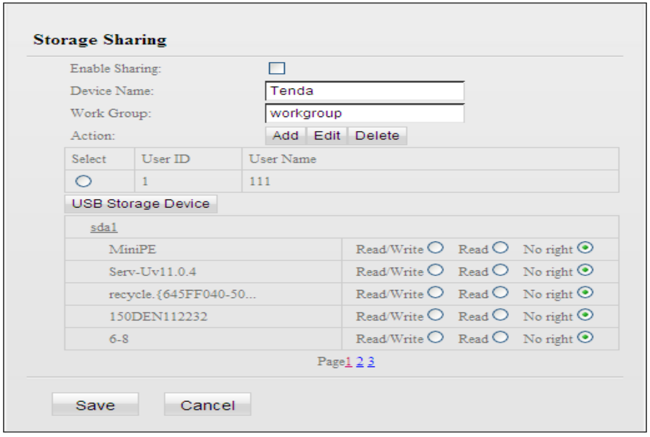
1. Create account: Click **Add** to display a dialogue box as shown below:



User Name	
Password	
Confirm Password	

2. Enter a user name and a password, which will be used to authenticate users trying to access the USB storage device for sharing files.Re-type to confirm password.

Click the **OK** button and window below will open:



Enable Sharing: □

Device Name: Tenda

Work Group: workgroup

Select	User ID	User Name
○	1	111

MiniPE	Read/Write ○	Read ○	No right ●
Serv-Uv11.0.4	Read/Write ○	Read ○	No right ●
recycle.{645FF040-50...	Read/Write ○	Read ○	No right ●
150DEN112232	Read/Write ○	Read ○	No right ●
6-8	Read/Write ○	Read ○	No right ●

3. Set Access Rights

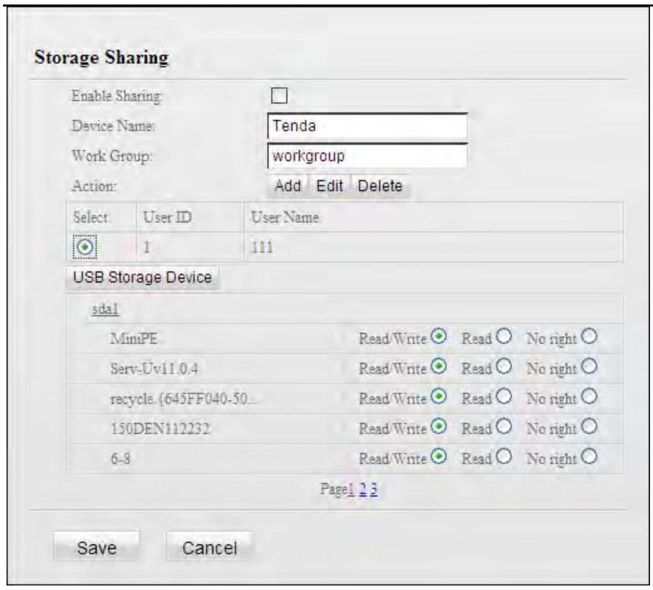
First select an account and click USB Storage Device. And then select a proper access right from below for each entry.

Read/Write：The right to read and write.

Read: The right to read only.

No right: No right to share corresponding file.

Click **Save** to apply all settings.



Storage Sharing

Enable Sharing: □

Device Name: Tenda

Work Group: workgroup

Action: Add Edit Delete

Select	User ID	User Name
●	1	111

USB Storage Device

sda1

MiniPE	Read/Write ●	Read ○	No right ○
Serv-Uv11.0.4	Read/Write ●	Read ○	No right ○
recycle.{645FF040-50...	Read/Write ●	Read ○	No right ○
150DEN112232	Read/Write ●	Read ○	No right ○
6-8	Read/Write ●	Read ○	No right ○

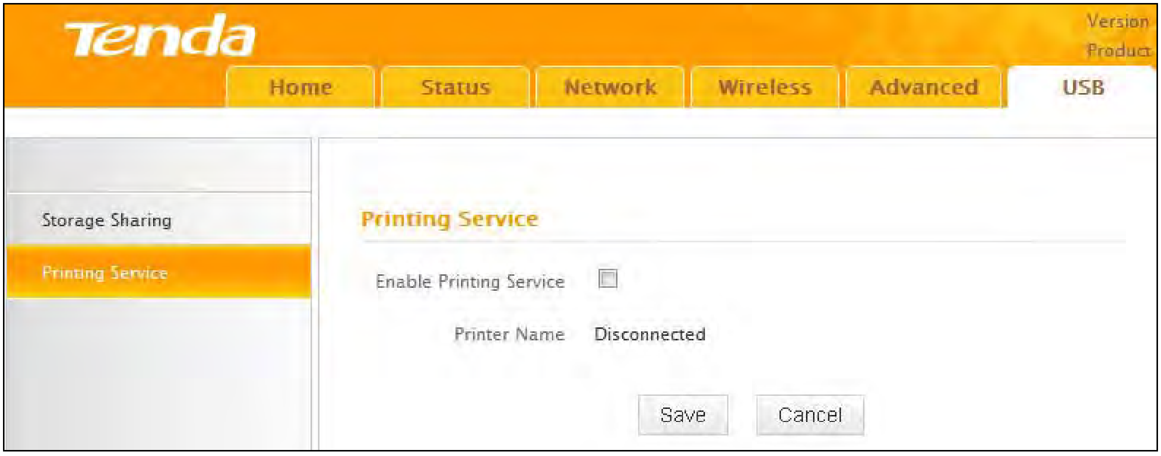
Page1 2 3

4. Access shared file

To access resources on such storage device, double click “My Computer” on your PC and enter \\192.168.0.1 into the address bar.

5.2 USB Printing Service

The USB printing service allows you to connect a USB printer to the device and allow all clients on your network to print anything they want from their PCs. The router can identify a printer automatically as long as it is successfully connected.



Printing Service

Enable Printing Service ☐

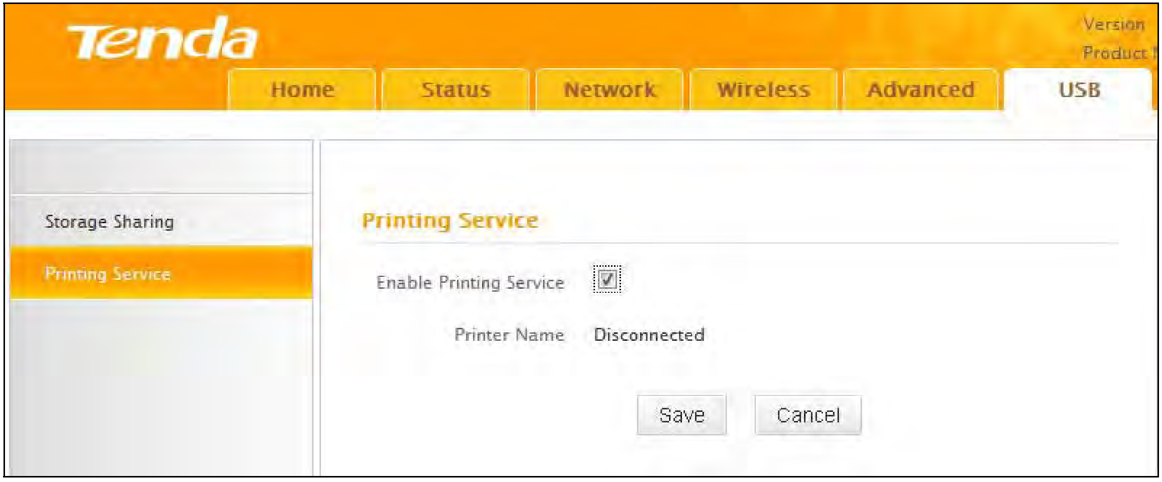
Printer Name Disconnected

- Enable Printing Service: Check/uncheck to enable/disable USB printing service.

Operation Instructions:

1. Correctly connect your USB printer to the USB port on the device.

2. Enable Printing Service

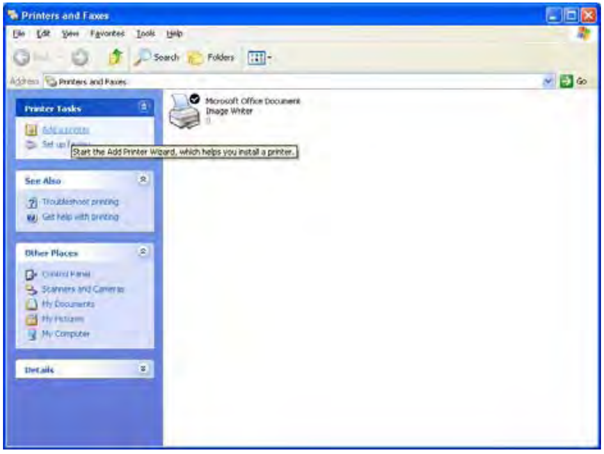


Printing Service

Enable Printing Service ☑

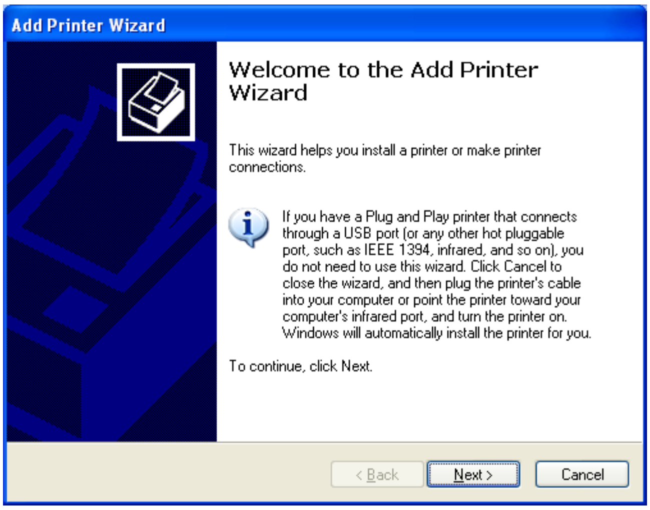
Printer Name Disconnected

3. On your PC (connected to the router), click **Start**——**Settings**——**Printers and Faxes** and select **Add a printer** on appearing window (Take Windows XP for example).



Start the Add Printer Wizard, which helps you install a printer.

4. Click **Next**.



Add Printer Wizard

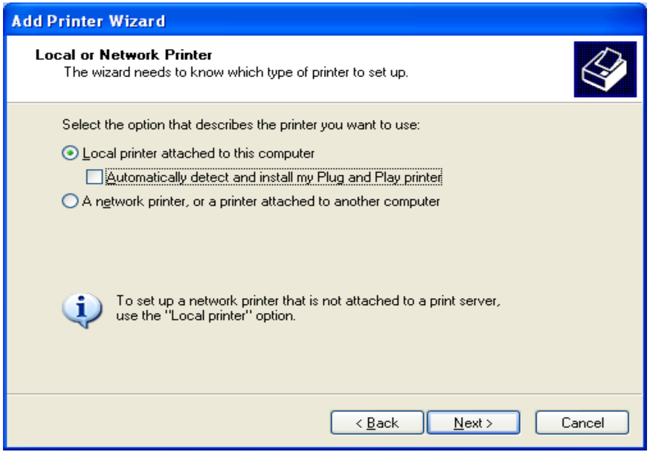
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

5. Select **Local printer attached to this computer**" and click **Next**.



Add Printer Wizard

Local or Network Printer

The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

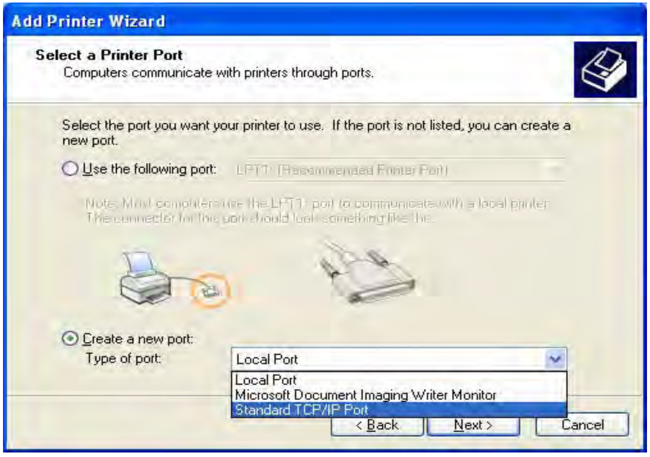
● Local printer attached to this computer

□ Automatically detect and install my Plug and Play printer

○ A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

6. Select **Create a new port**, Type of port: **Standard TCP/IP Port** and click **Next**.



Add Printer Wizard

Select a Printer Port

Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

○ Use the following port: LPT1: (Recommended Printer Port)

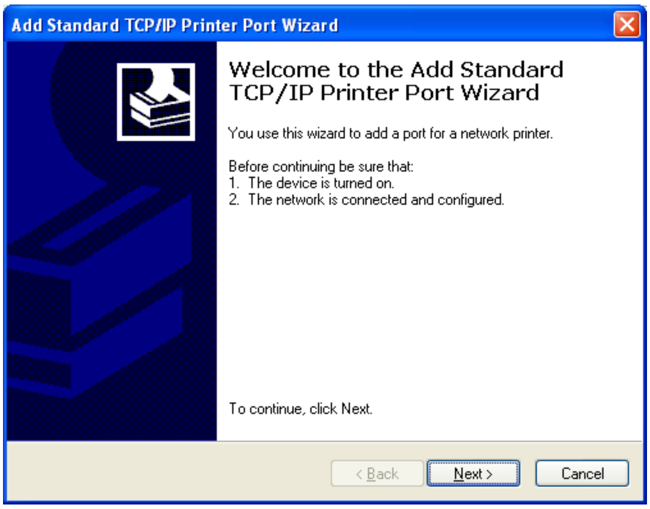
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:

● Create a new port:

Type of port: Local Port

Local Port
Microsoft Document Imaging Writer Monitor
Standard TCP/IP Port

7. Click **Next**.



Add Standard TCP/IP Printer Port Wizard

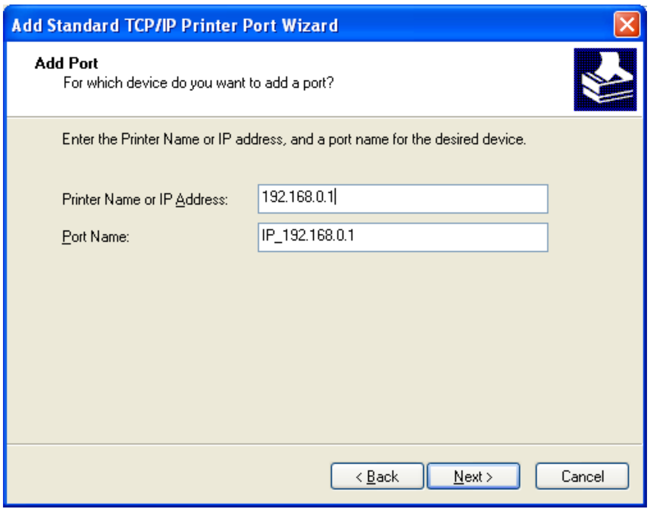
Welcome to the Add Standard TCP/IP Printer Port Wizard

You use this wizard to add a port for a network printer.

Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.

To continue, click Next.

8. Enter Router's LAN IP address and click **Next**.



Add Standard TCP/IP Printer Port Wizard

Add Port

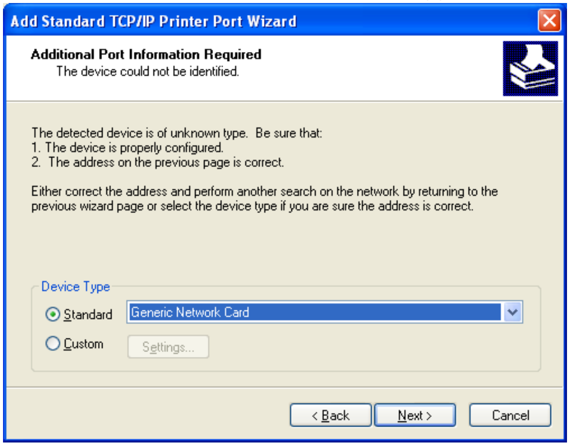
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.0.1

Port Name: IP_192.168.0.1

9. Click **Standard** under Device Type and select **Generic Network Card**, then click **Next**.



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required

The device could not be identified.

The detected device is of unknown type. Be sure that:
1. The device is properly configured.
2. The address on the previous page is correct.

Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.

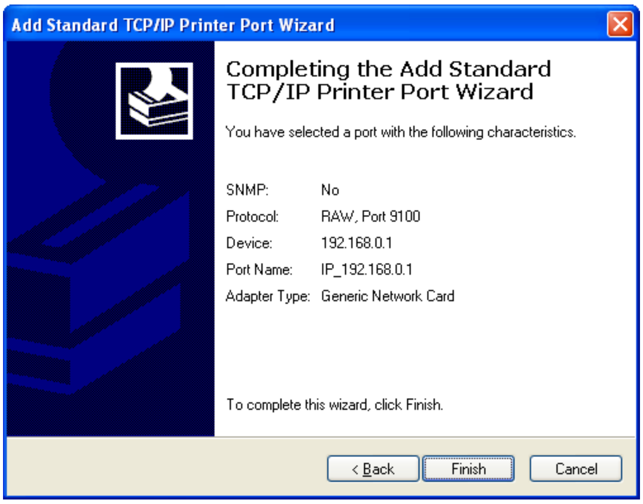
Device Type

● Standard Generic Network Card

○ Custom Settings...

< Back Next > Cancel

10. Click **Finish**.



Add Standard TCP/IP Printer Port Wizard

Completing the Add Standard TCP/IP Printer Port Wizard

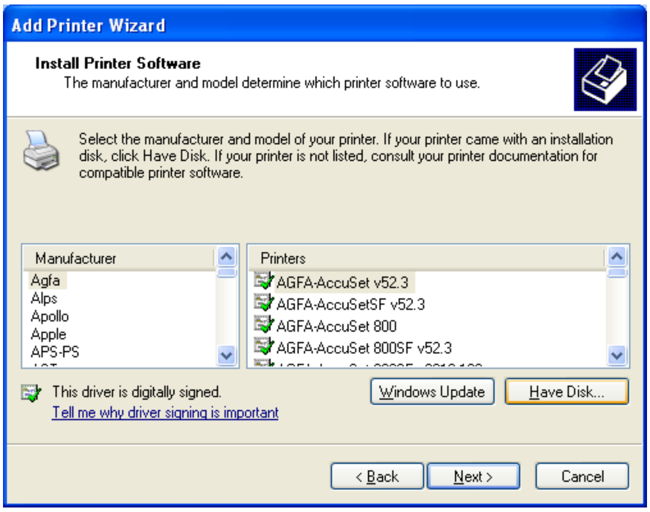
You have selected a port with the following characteristics.

SNMP: No
Protocol: RAW, Port 9100
Device: 192.168.0.1
Port Name: IP_192.168.0.1
Adapter Type: Generic Network Card

To complete this wizard, click Finish.

< Back Finish Cancel

11. Select **Have Disk**.



Add Printer Wizard

Install Printer Software

The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

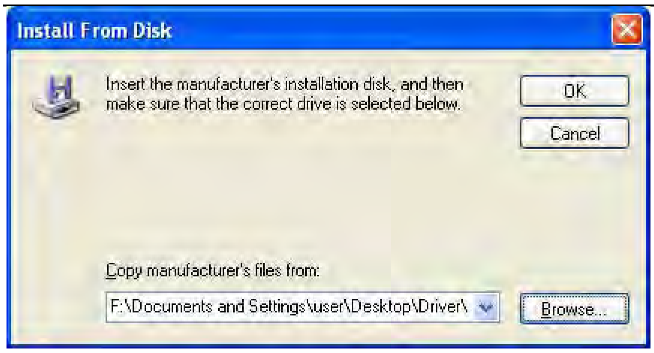
Manufacturer	Printers
Agfa	AGFA-AccuSet v52.3
Alps	AGFA-AccuSetSF v52.3
Apollo	AGFA-AccuSet 800
Apple	AGFA-AccuSet 800SF v52.3
APS-PS	

This driver is digitally signed.
Tell me why driver signing is important

Windows Update Have Disk...

< Back Next > Cancel

12. Click **Browse**, select corresponding drive file and click **Open**. At last click **OK**.



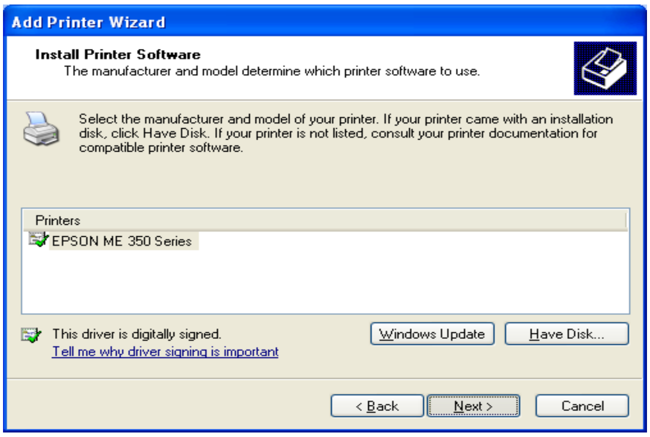
Install From Disk

Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:

F:\Documents and Settings\user\Desktop\Driver\

13. Click **Next**.



Add Printer Wizard

Install Printer Software

The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

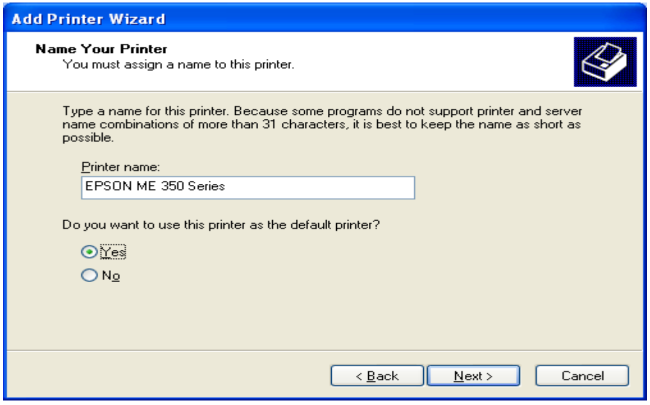
Printers

EPSON ME 350 Series

This driver is digitally signed.

Tell me why driver signing is important

14. Define a name for the printer and click **Next**.



Add Printer Wizard

Name Your Printer

You must assign a name to this printer.

Type a name for this printer. Because some programs do not support printer and server name combinations of more than 31 characters, it is best to keep the name as short as possible.

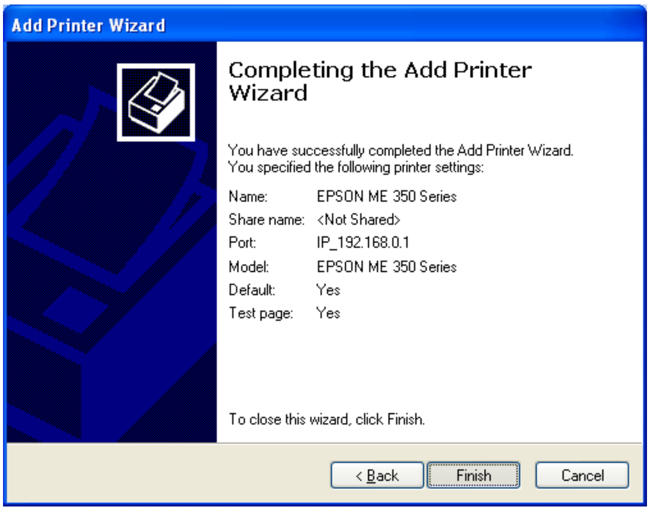
Printer name: EPSON ME 350 Series

Do you want to use this printer as the default printer?

● Yes

○ No

15. Click **Finish**.



Add Printer Wizard

Completing the Add Printer Wizard

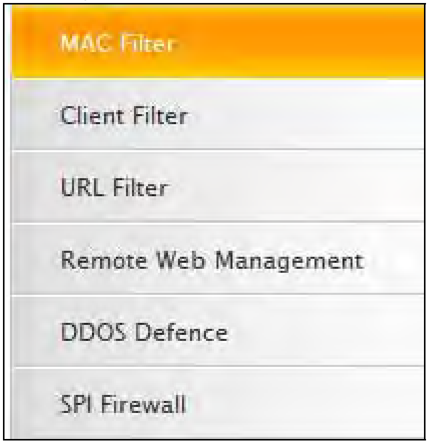
You have successfully completed the Add Printer Wizard. You specified the following printer settings:

Name:	EPSON ME 350 Series
Share name:	<Not Shared>
Port:	IP_192.168.0.1
Model:	EPSON ME 350 Series
Default:	Yes
Test page:	Yes

To close this wizard, click Finish.

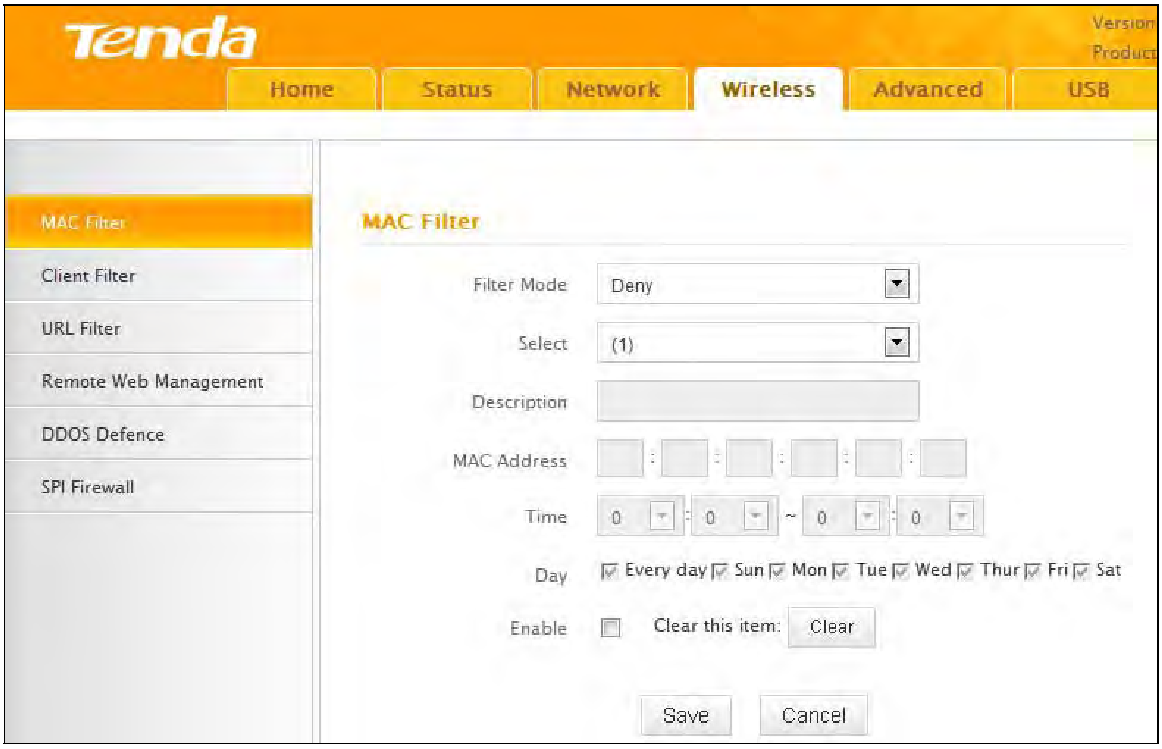
6 Security

The **Security** tab includes 6 submenus: MAC Filter, Client Filter, URL Filter, Remote Web Management, DDoS Defence and SPI Firewall. Clicking any of them enters the corresponding interface for configuration. Details are explained below:



6.1 MAC Filter

To better manage devices in the LAN, you may use the MAC Address Filter function to allow/disallow such devices to access the Internet.



MAC Filter

Filter Mode: Deny

Select: (1)

Description:

MAC Address: : : : : :

Time: 0 : 0 ~ 0 : 0

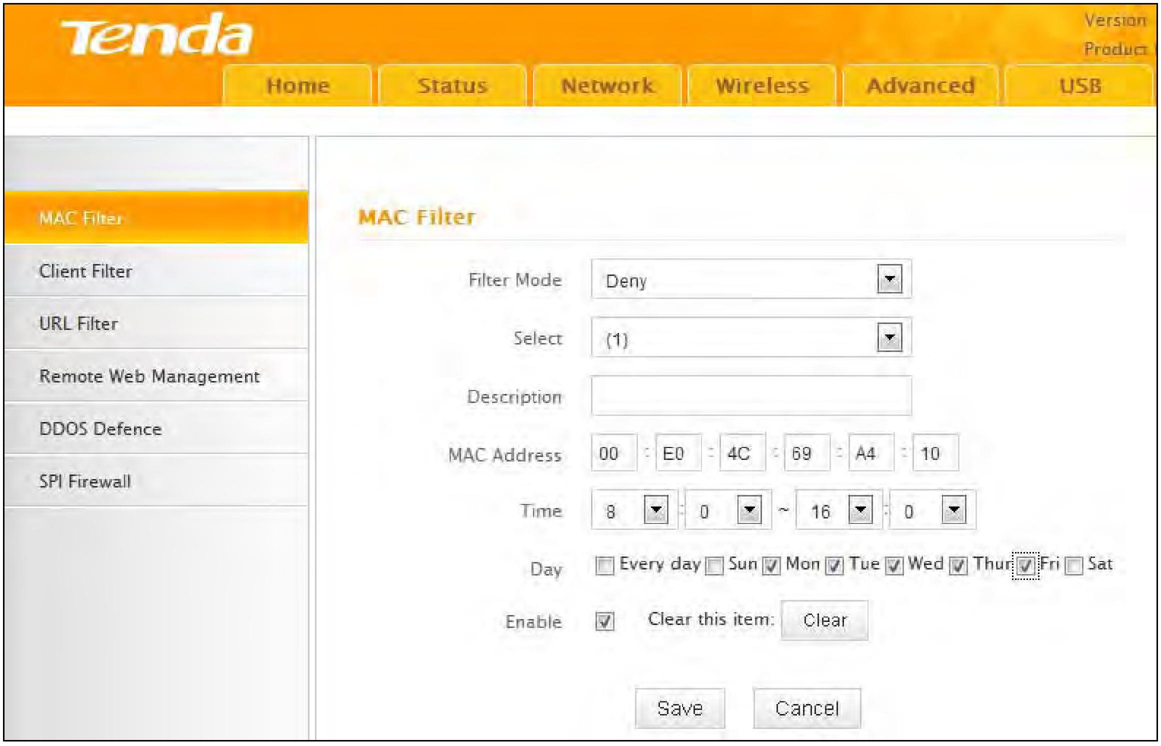
Day: ☑ Every day ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat

Enable □ Clear this item: Clear

- Filter Mode:
- Disable: Disable the MAC Filter feature.
- Deny Access to Internet: Disallow only specified devices to access Internet, other devices are not restricted.
- Allow Access to Internet: Allow only specified devices to access Internet, other devices are denied.
- Select: Select an ID for the current entry.
- Description: Briefly describe current entry.
- MAC: Specify the MAC address of the computer that you want to restrict.
- Time: Specify a time range for current entry to take effect.

- Day: select a day, or several days, for the entry to take effect.
- Enable: Select to enable/disable corresponding entry.

Example: To prevent a PC at the MAC address of 00:E0:4C:69:A4:10 from accessing Internet between 8:00 and16:00 on working days: from Monday to Friday, configure the same settings as shown in the screen below, on your device:



MAC Filter

Filter Mode: Deny

Select: (1)

Description:

MAC Address: 00 : E0 : 4C : 69 : A4 : 10

Time: 8 : 0 ~ 16 : 0

Day: □ Every day □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri □ Sat

Enable: ☑ Clear this item: Clear

Save Cancel

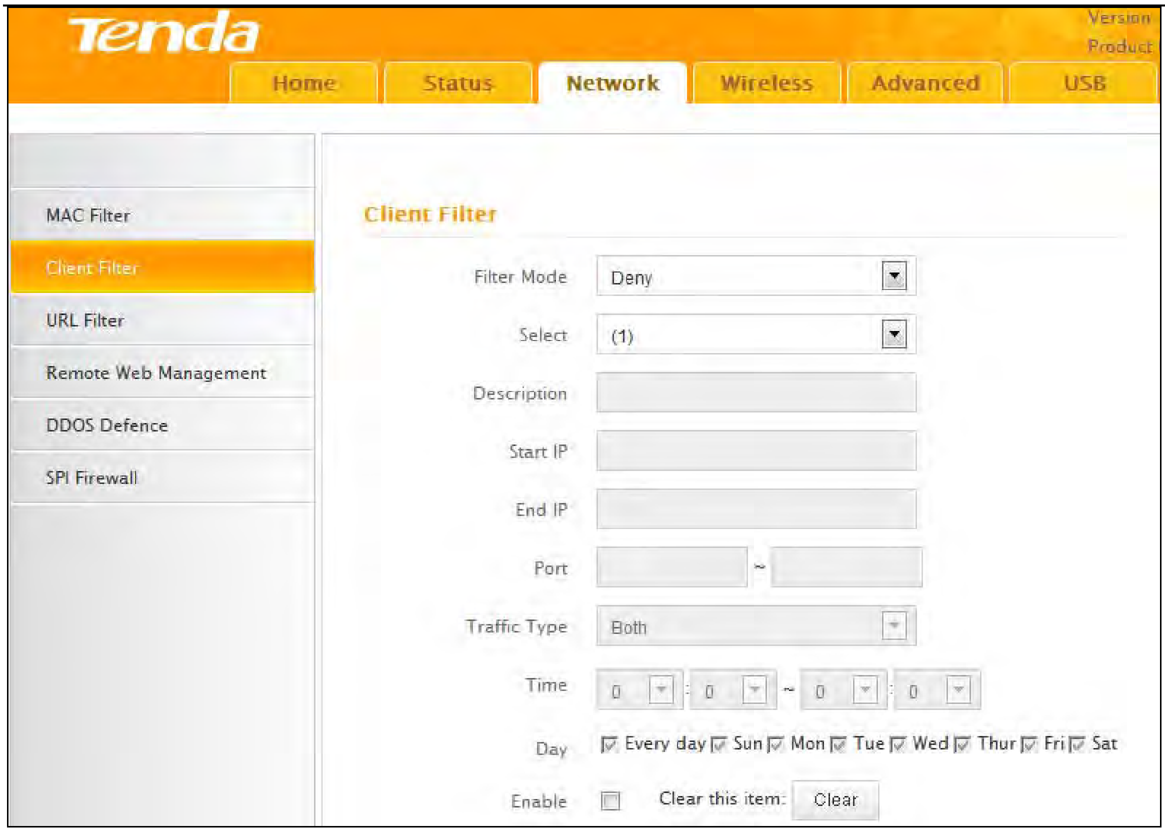
Tips ---

1. Maximum 10 entries can be configured in MAC Filter.

2. After saving your configurations, for correct time, please go to **Tools**>**Time** to configure your router's system time.

6.2 Client Filter

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

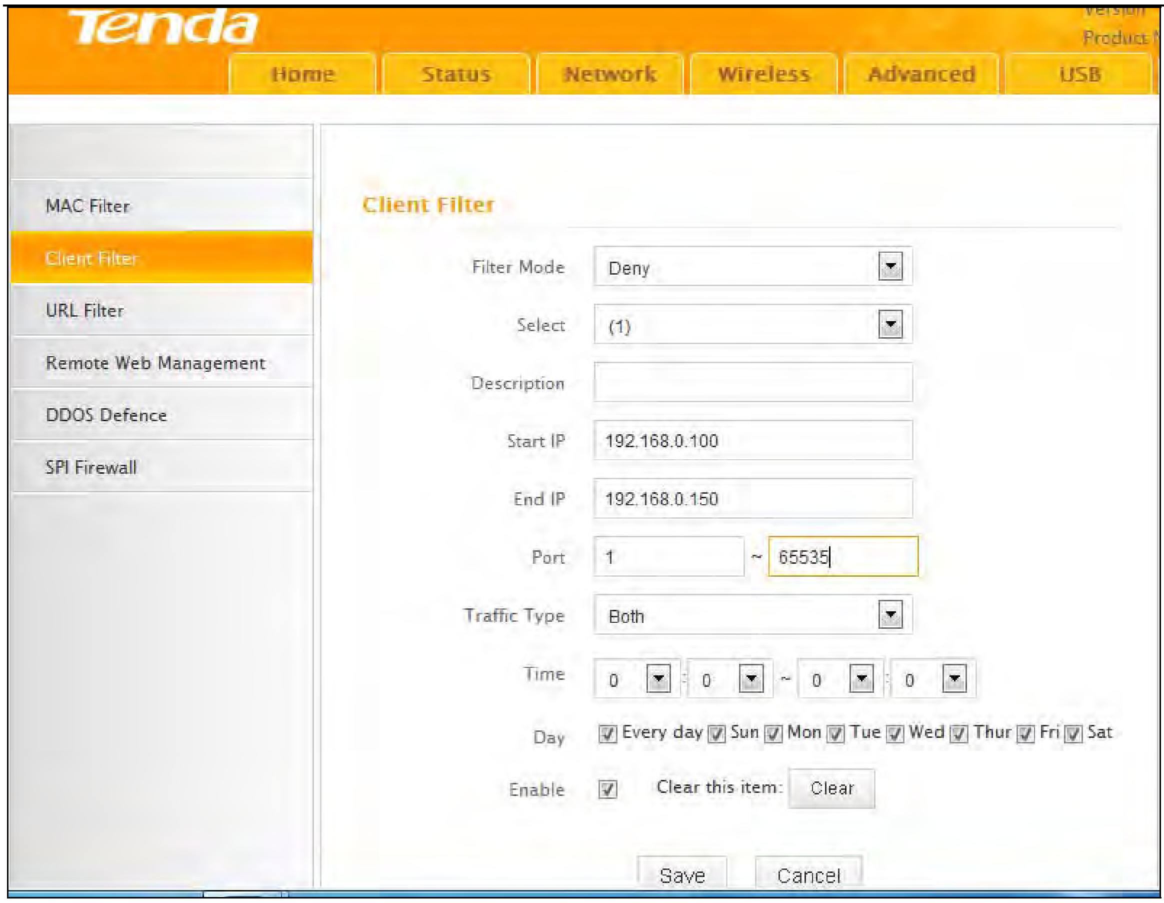


Client Filter

Filter Mode	Deny
Select	(1)
Description	
Start IP	
End IP	
Port	~
Traffic Type	Both
Time	0 : 0 ~ 0 : 0
Day	☑ Every day ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat
Enable	☐ Clear this item: Clear

- Filter Mode: Select Deny or Allow.
- Select: Select an ID for the current entry.
- Description: Briefly describe the current entry.
- Start IP: Enter a starting IP address.
- End IP: Enter an ending IP address.
- Port: Enter TCP/UDP protocol port number,   it can be a single port or a range of ports.
- Traffic Type: Select a protocol or protocols for the traffic (TCP/UDP/Both).
- Time: Specify a time range for current entry to take effect.
- Day: select a day or several days for current entry to take effect.
- Enable: Check to enable or uncheck to disable a corresponding filter rule (allow/disallow matched addresses to pass through router).

Example: To prohibit PCs within the IP address range of 192.168.0.100--192.168.0.150 from accessing the Internet, use the following example:



Client Filter

Filter Mode: Deny

Select: (1)

Description:

Start IP: 192.168.0.100

End IP: 192.168.0.150

Port: 1 ~ 65535

Traffic Type: Both

Time: 0 : 0 ~ 0 : 0

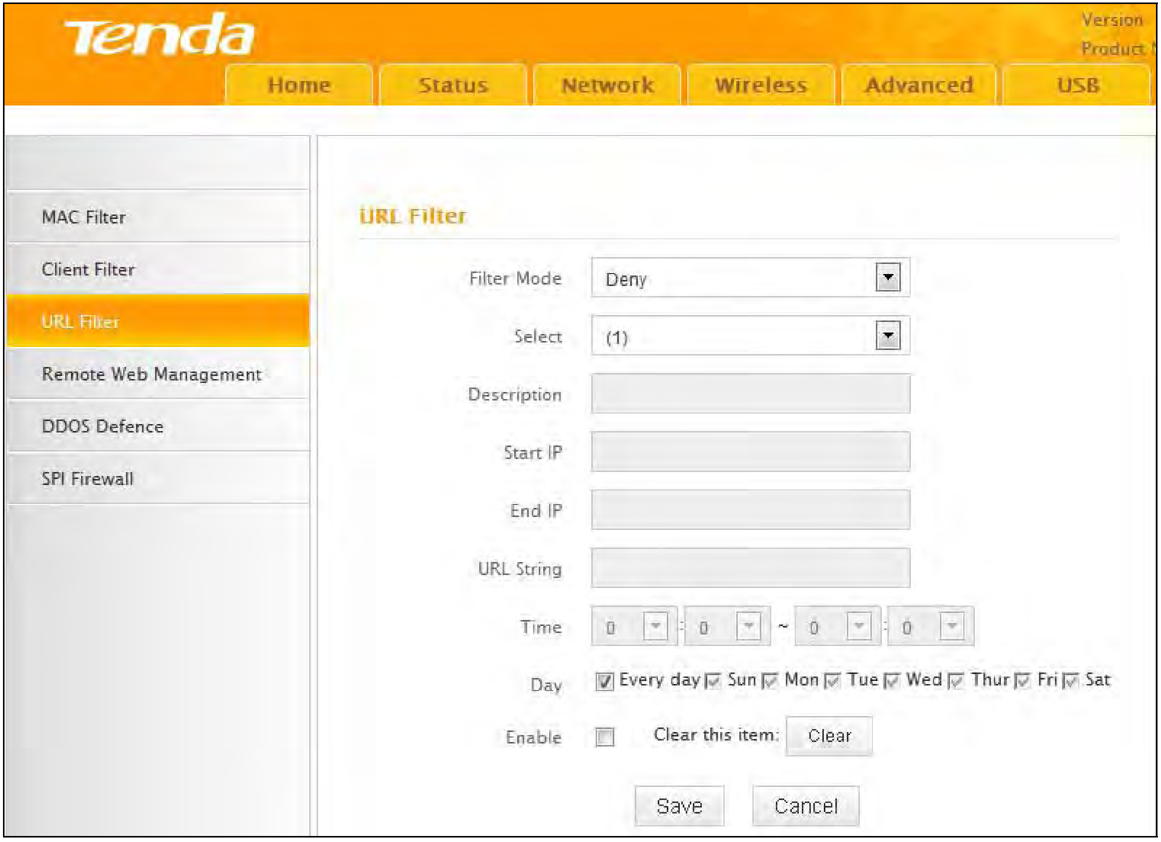
Day: ☑ Every day ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat

Enable: ☑ Clear this item: Clear

Save Cancel

6.3 URL Filter

To better control LAN devices, you can use the URL filter function to allow or disallow PC's to access certain websites within a specified time range.



Filter Mode: Deny

Select: (1)

Description:

Start IP:

End IP:

URL String:

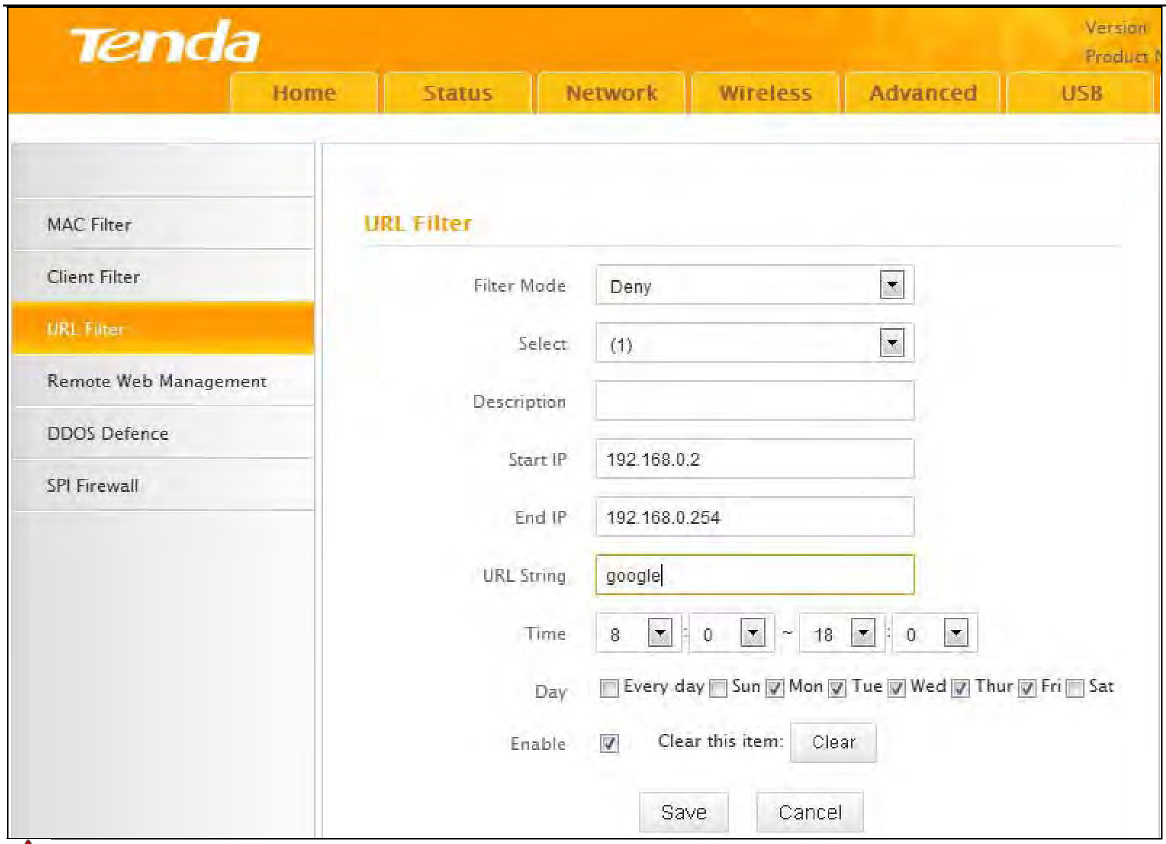
Time: 0 : 0 ~ 0 : 0

Day: ☑ Every day ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat

Enable: □

- Filter Mode: Select Deny or Allow.
- Select: Select an ID for current entry.
- Enable: Check to enable or uncheck to disable a corresponding filter rule (allow/disallow matched addresses to pass through router).
- Description: Briefly describe the current entry.
- Start IP: Enter a starting IP address.
- Start IP: Enter a starting IP address.
- URL String: Enter domain names or a part of a domain name to be filtered out.
- Time: Specify a time range for current entry to take effect.
- Day: select a day or several days for current entry to take effect.

If you want to disallow all computers on your LAN to access Google.com from 8:00 to 18:00 on working days: Monday- Friday, then use the following example:



URL Filter

Filter Mode: Deny

Select: (1)

Description:

Start IP: 192.168.0.2

End IP: 192.168.0.254

URL String: google

Time: 8 : 0 ~ 18 : 0

Day: □ Every day □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri □ Sat

Enable: ☑ Clear this item: Clear

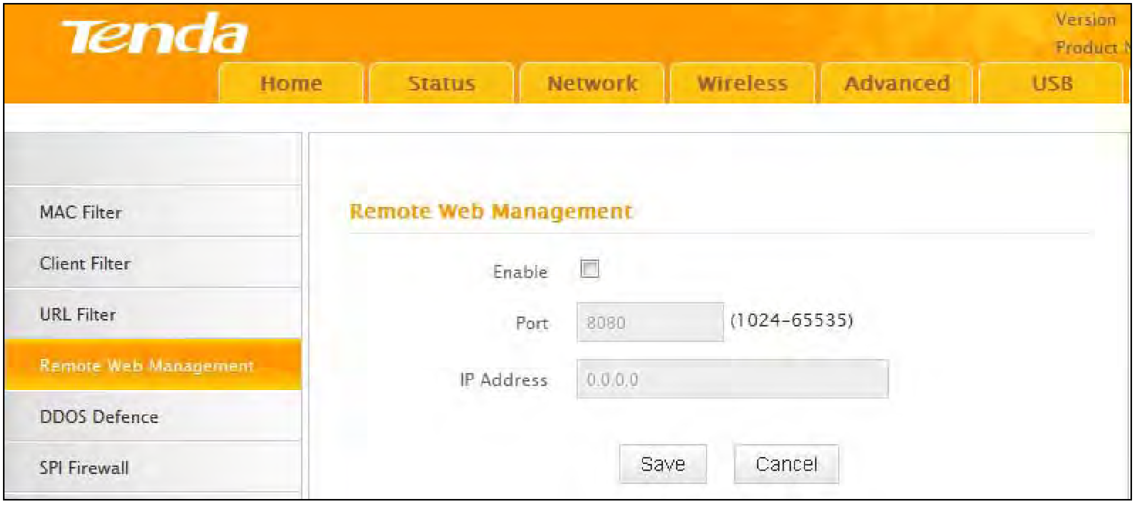
Save Cancel

Note

Each entry can include up to 16 domain names, each of which must be separated with the quotation symbols " ".

6.4 Remote Web Management

The Remote management allows the router to be configured from the Internet via a web browser.



Remote Web Management

Enable: □

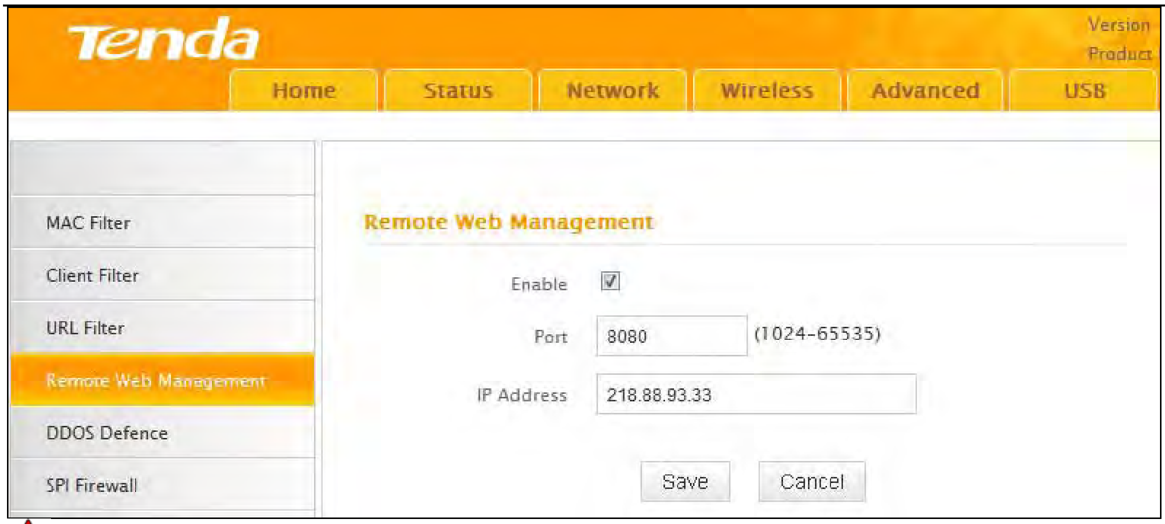
Port: 8080 (1024-65535)

IP Address: 0.0.0.0

Save Cancel

- Enable: Select to enable the Remote Web-based Management feature.
- Port: Remote admin port is the port number used to access the router from Internet.
- IP Address: Enter the IP address of the PC on the Internet authorized to manage your router remotely.

For example: If you want to allow only the PC at the IP address of 218.88.93.33 from the Internet to access the router’s web-based utility via port 8080, then configure the same settings as shown below on your router.



Remote Web Management

Enable ☑

Port 8080 (1024-65535)

IP Address 218.88.93.33

Note

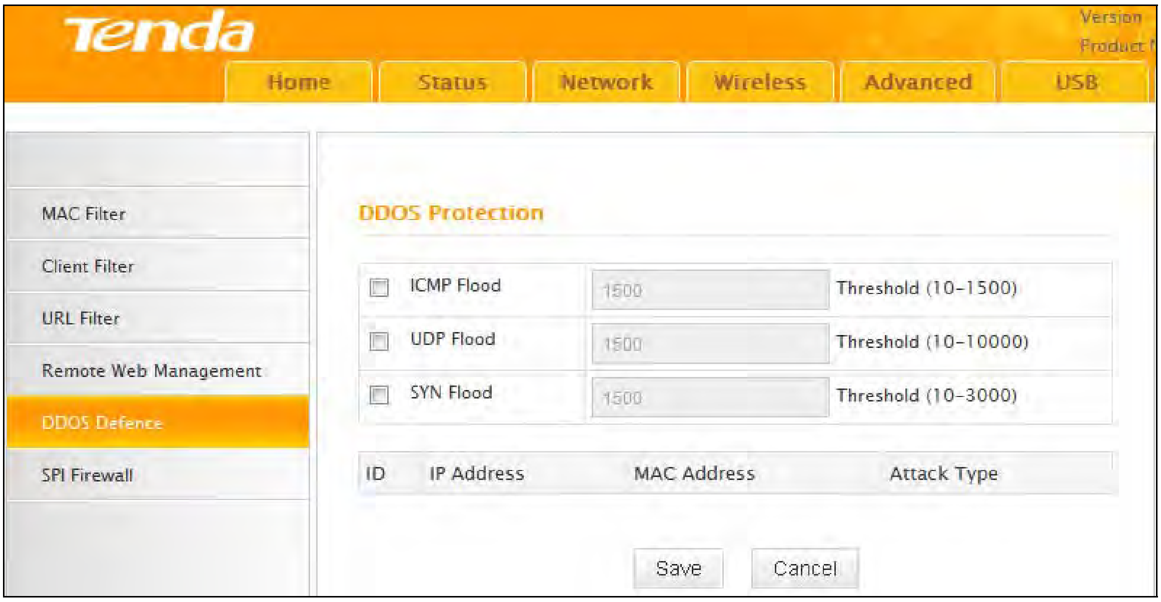
1. The default port is 8080. Do not change it.

2. To access the router via port 8080, enter "http://x.x.x.x:8080" where "x.x.x.x" represents the Internet IP address of the router and 8080 is the port used for the Web-Management interface. Assuming the router'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).

Leaving the IP address field at "0.0.0.0" makes the router remotely accessible to all the PCs on the Internet. Entering a specific IP address, such as 218.88.93.33, makes the router only remotely accessible to the PC at the specified IP address.

6.5 DDOS Defence

The DDOS Defence feature effectively blocks ICMP, UDP, and SYN flooding attacks. When the number of ICMP, UDP, or SYN packets received exceeds the defined threshold, the router will record its IP and MAC addresses in the "DDOS Defence List".



DDOS Protection

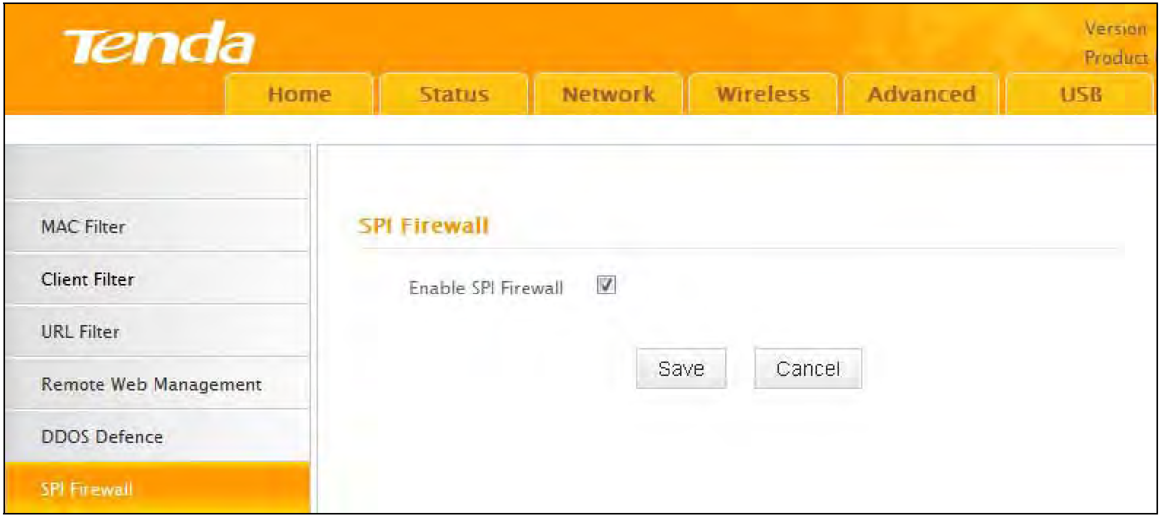
□ ICMP Flood	1500	Threshold (10-1500)
□ UDP Flood	1500	Threshold (10-10000)
□ SYN Flood	1500	Threshold (10-3000)

ID	IP Address	MAC Address	Attack Type

- ICMP Flood: If an IP receives the number of ICMP request packets that exceeds the defined limit continuously from the same sender within one second, then such IP is considered to encounter an ICMP Flood attack.
- UDP Flood：If an IP receives, on an identical port, UDP packets exceeding the defined limit continuously from the same sender within a second, then the port is suffering a UDP Flood attack.
- SYN Flood: If an IP receives, on an identical port, TCP SYN packets exceeding defined limit continuously from the same sender within a second, then the port is suffering a SYN Flood attack.

6.6 SPI Firewall

Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.



Enable SPI Firewall ☑

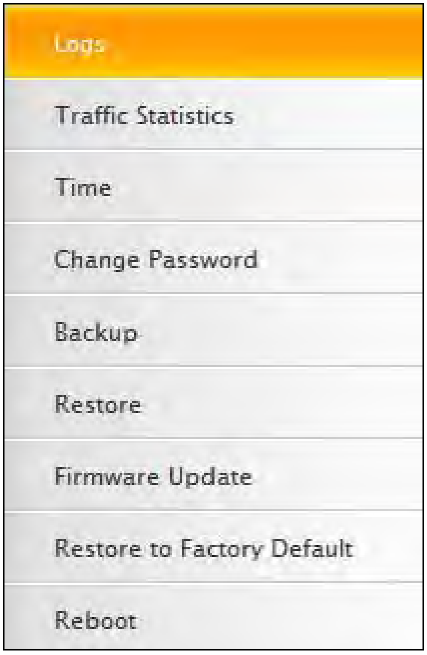
Tips --

Once SPI enabled, DMZ and remote web management will be invalid.

----

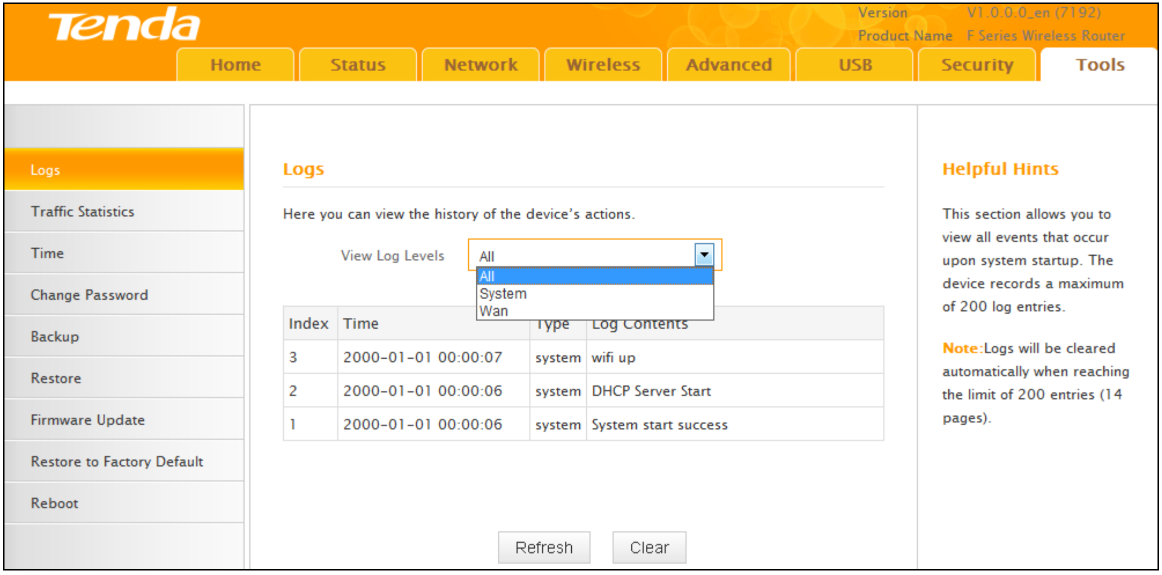
7 Tools

The "Tools" tab includes 9 submenus: Logs, Traffic Statistics, Time, Change Password, Backup, Restore, Firmware Update, Restore to Factory Default, and Reboot. Clicking any of them enters the corresponding interface for configuration. Details are explained below:



7.1 Logs

The Syslog option allows you to view all events that occur on system startup and checks whether there is an attack present in your network. The logs are classified into 3 types: All, System, and WAN.



Logs

Here you can view the history of the device's actions.

View Log Levels: All

Index	Time	Type	Log Contents
3	2000-01-01 00:00:07	system	wifi up
2	2000-01-01 00:00:06	system	DHCP Server Start
1	2000-01-01 00:00:06	system	System start success

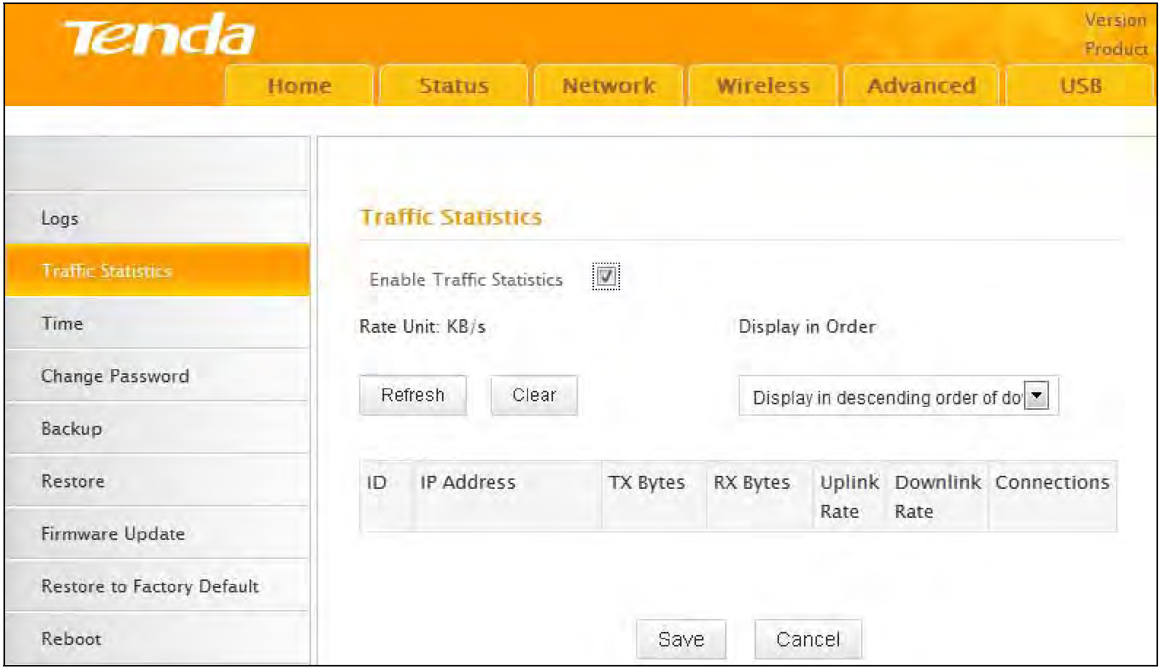
Helpful Hints

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 (14 pages).

7.2 Traffic Statistics

Traffic Statistics displays current traffic of clients on your LAN.



Traffic Statistics

Enable Traffic Statistics ☑

Rate Unit: KB/s

Display in Order: Display in descending order of do

ID	IP Address	TX Bytes	RX Bytes	Uplink Rate	Downlink Rate	Connections

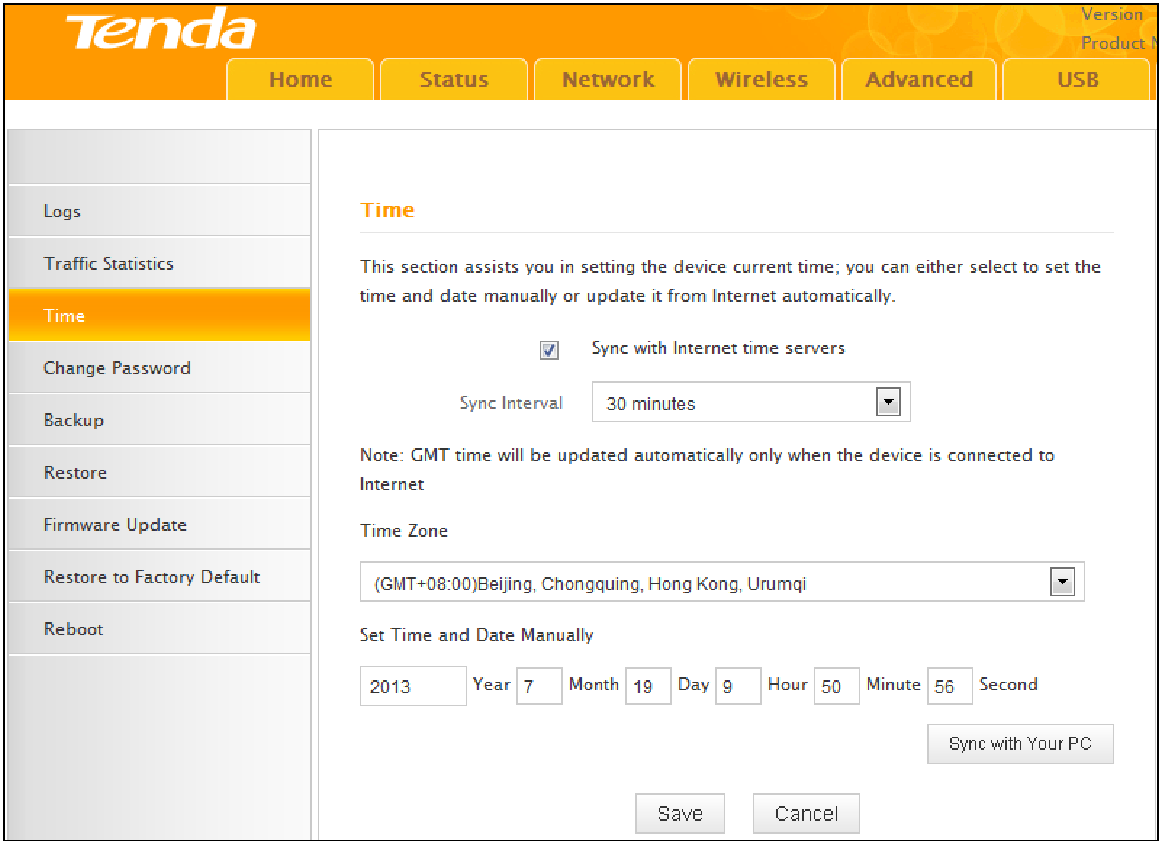
- Enable Traffic Statistics: Determine whether to enable the Traffic Statistics feature on internal users.
- Refresh: Click it to update statistic data.
- Clear: Click it to remove statistic data.

⚠**Note**

Enabling the Traffic Statistics feature may degrade the router’s performance. Do not enable it unless necessary.

7.3 Time

This section lets you configure, update, and maintain the correct time on the internal system clock. You can either select to set the time and date manually or automatically obtain the GMT time from Internet. Note that the GMT time is obtained only when the router is connected to the Internet.



Time

This section assists you in setting the device current time; you can either select to set the time and date manually or update it from Internet automatically.

☑ Sync with Internet time servers

Sync Interval: 30 minutes

Note: GMT time will be updated automatically only when the device is connected to Internet

Time Zone

(GMT+08:00)Beijing, Chongquing, Hong Kong, Urumqi

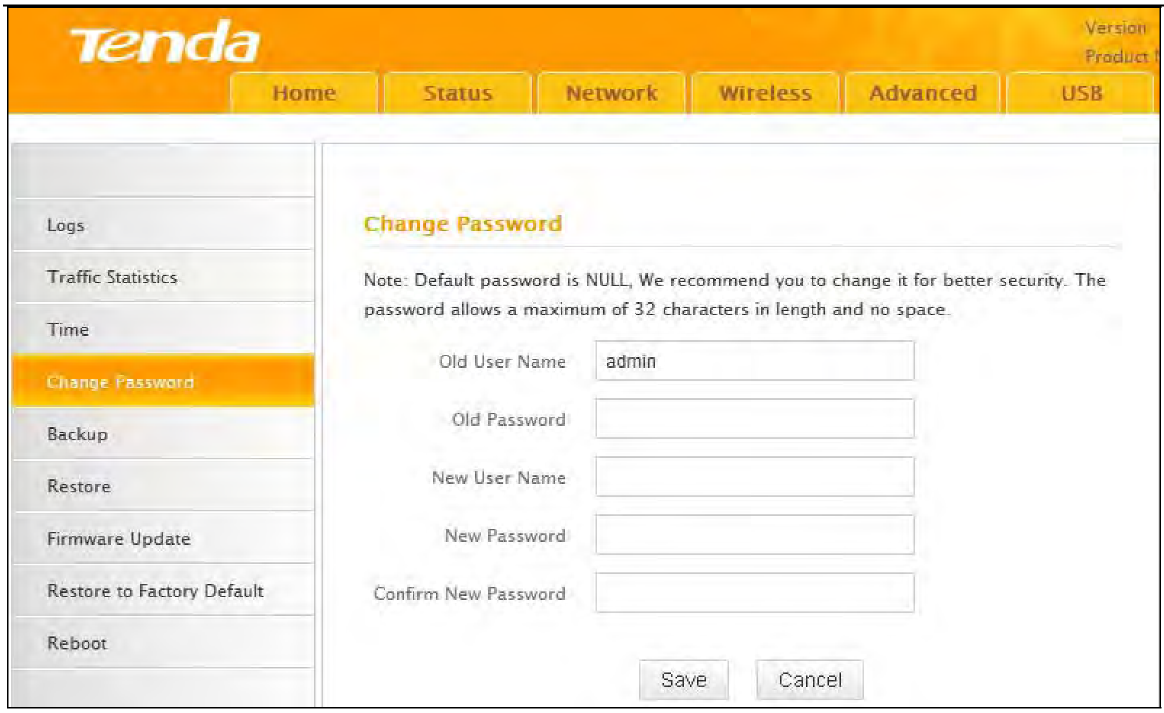
Set Time and Date Manually

2013 Year 7 Month 19 Day 9 Hour 50 Minute 56 Second

- Sync with Internet time servers: Time and date will be updated automatically from the Internet.
- Sync Interval: Specify a time interval for periodic update of time and date information from the Internet.
- Time Zone: Select your current time zone.
- Sync with Your PC: Click it to copy your PC’s time to the router.

7.4 Change Password

This section allows you to change login password and user name for accessing the router’s Web-based management interface.



Change Password

Note: Default password is NULL, We recommend you to change it for better security. The password allows a maximum of 32 characters in length and no space.

Old User Name: admin

Old Password:

New User Name:

New Password:

Confirm New Password:

Both login password and user name are preset to “admin” by default. To change either or both, do the following:

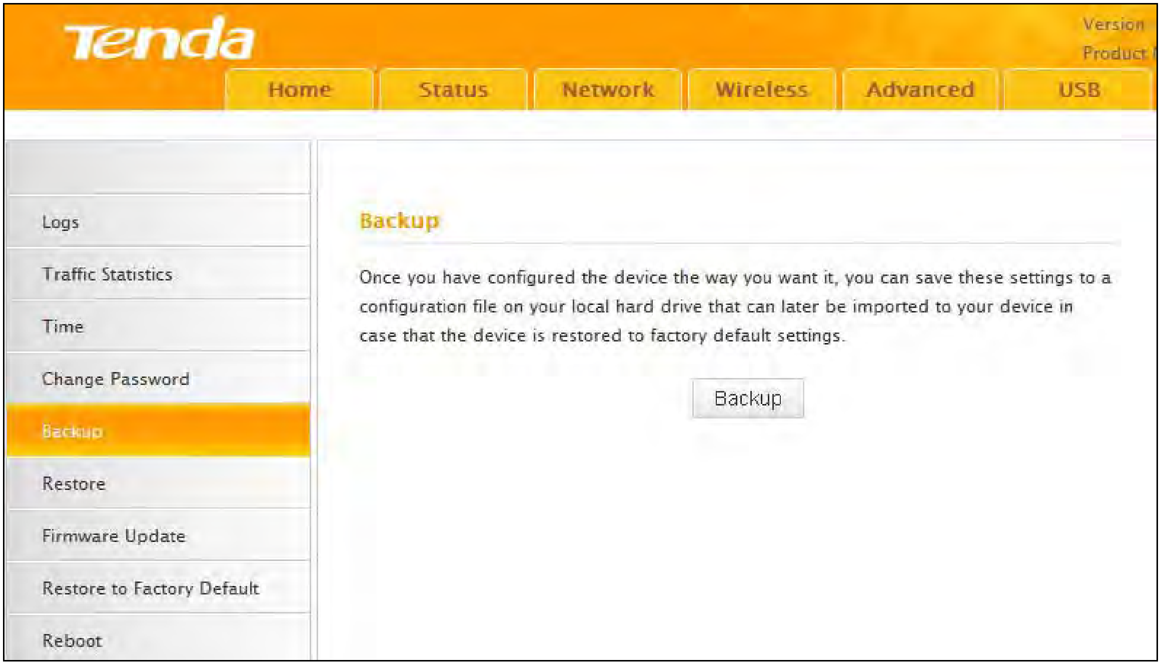
1. Enter your current user name and password in **Old User Name** and **Old Password fields**.
2. Enter a new user name and a new password in **New User Name** and **New Password** fields.
3. Click **Save**.

⚠**Note**

For security purpose, it is highly recommended that you change the default login password and user name as part of the initial configuration of your router.

7.5 Backup

This feature allows you to backup current settings. Once you have configured the router, you can save these settings to a configuration file on your local hard drive. The configuration file can later be imported to your router in case the router is reset to factory default settings.



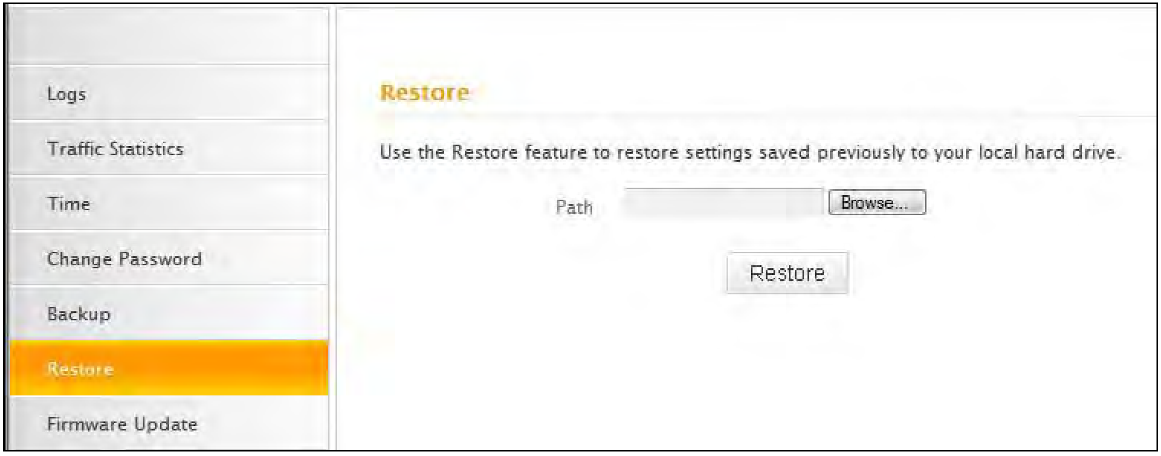
Backup

Once you have configured the device the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your device in case that the device is restored to factory default settings.

- Backup: To backup settings, click the Backup button and specify a directory to save settings to your local hardware.

7.6 Restore

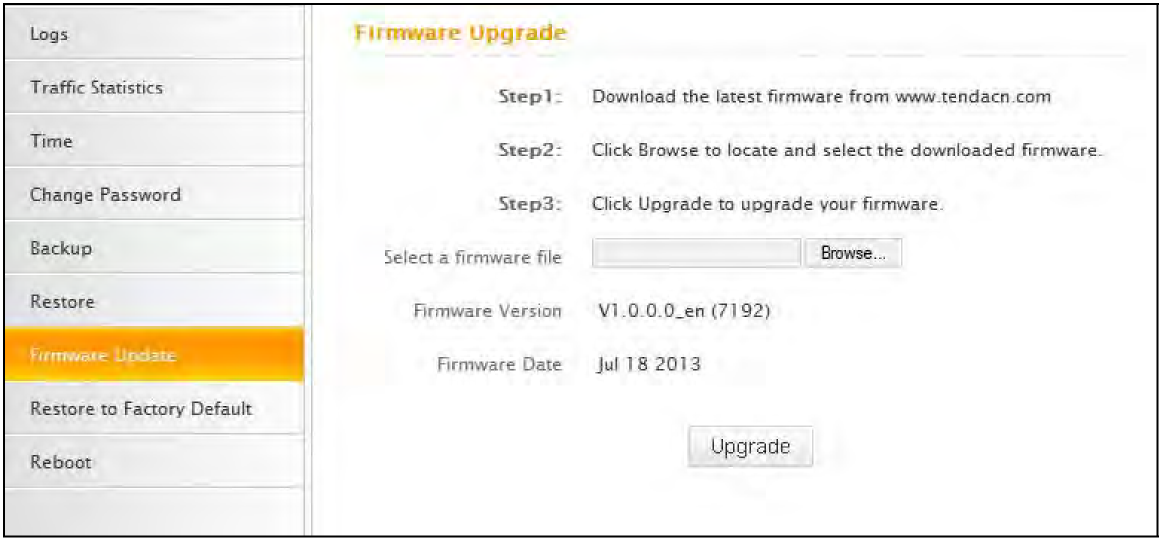
This section allows you to restore settings previously configured and saved to your local hard drive.



Use the Restore feature to restore settings saved previously to your local hard drive.

7.7 Firmware Update

Firmware upgrade is released periodically to improve the functionality of your router, and also to add any new features. If you run into a problem with a specific feature of the router you could log on to our website (www.tendacn.com) to download the latest firmware to update your device.



Firmware Upgrade

Step1: Download the latest firmware from www.tendacn.com

Step2: Click Browse to locate and select the downloaded firmware.

Step3: Click Upgrade to upgrade your firmware.

Select a firmware file

Firmware Version V1.0.0.0_en (7192)

Firmware Date Jul 18 2013

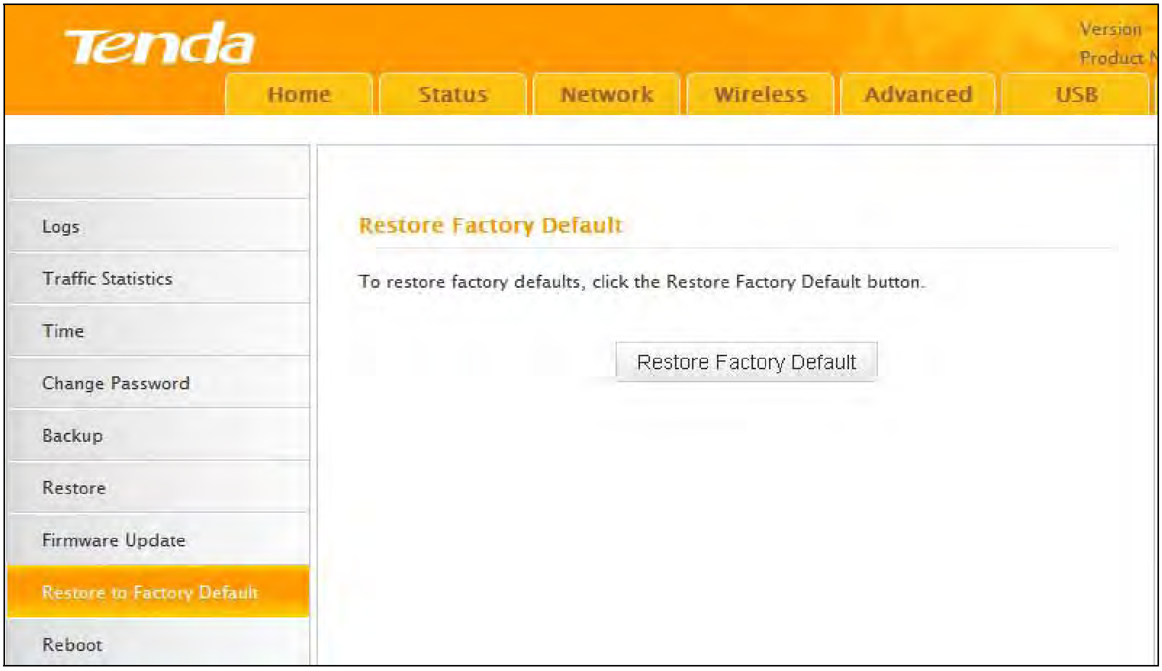
To update firmware, do the following:

1. Click **Browse** to locate and select the firmware file and **Upgrade** to update your router.
2. Device restarts automatically when the upgrade process is completed.

⚠**Note**

DO NOT power off the router when the upgrade is in process otherwise the router may be permanently damaged. When the upgrade is completed, the router will automatically reboot. The firmware upgrade may take a few minutes to complete so please wait for the process to finish.

7.8 Restore to Factory Default



Restore Factory Default

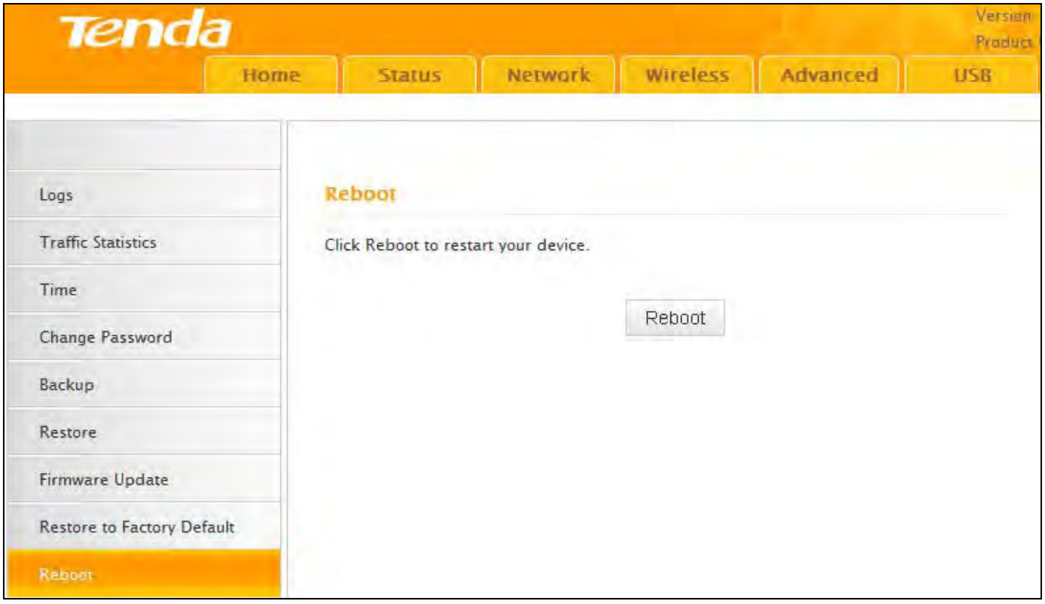
To restore factory defaults, click the Restore Factory Default button.

Click the **Restore Factory Default** button to reset the router to its factory default settings.

- Default IP Address: 192.168.0.1
- Default Subnet Mask: 255.255.255.0
- Default User Name: admin
- Default Password: admin

7.9 Reboot

This section allows you to reboot the router.



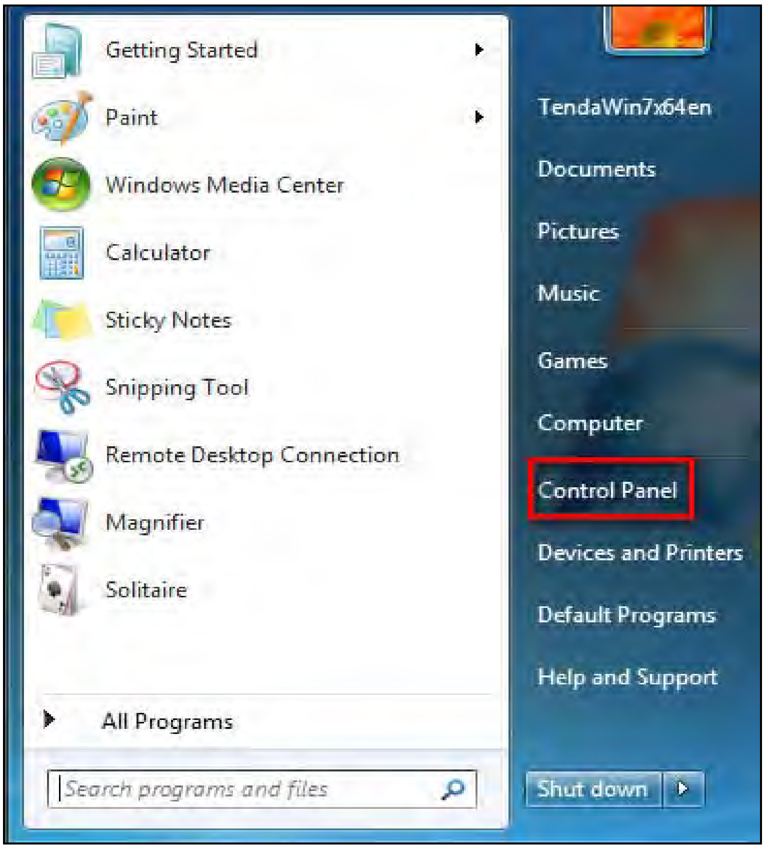
Click Reboot to restart your device.

Appendix 1 Configure PC

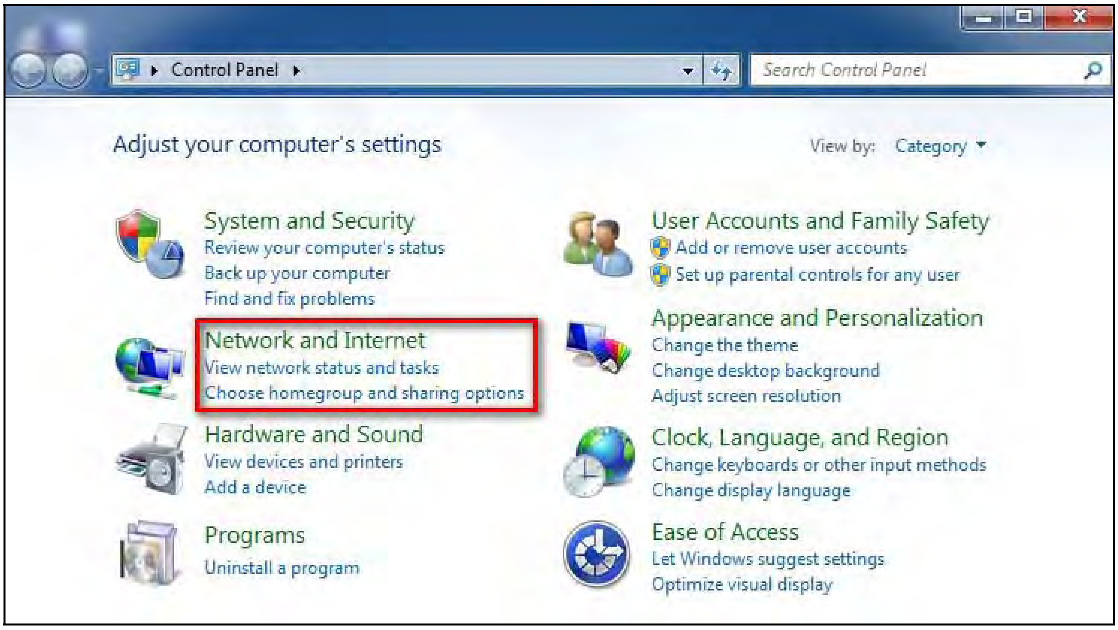
In this section we explain how to configure your PC's TCP/IP settings.

WIN7 OS

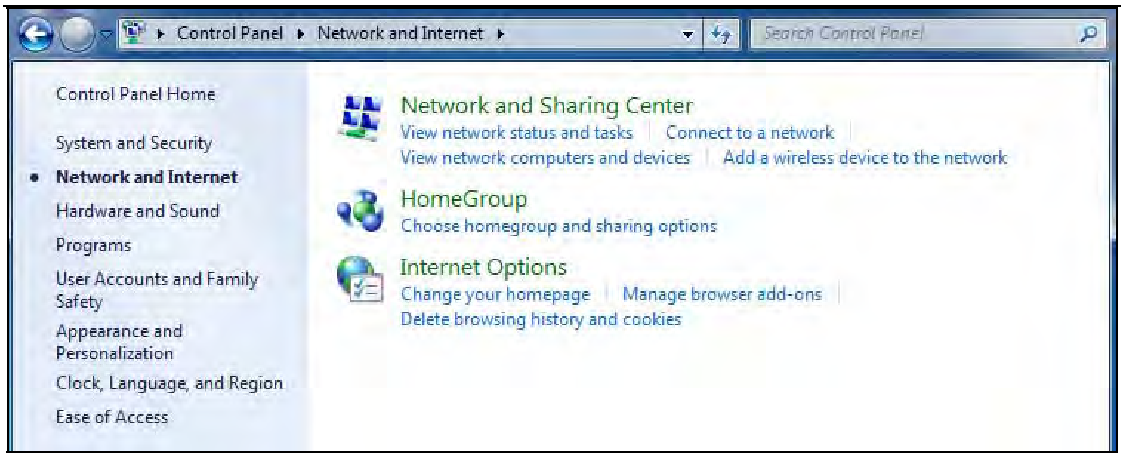
1. Click **Start>Control Panel;**



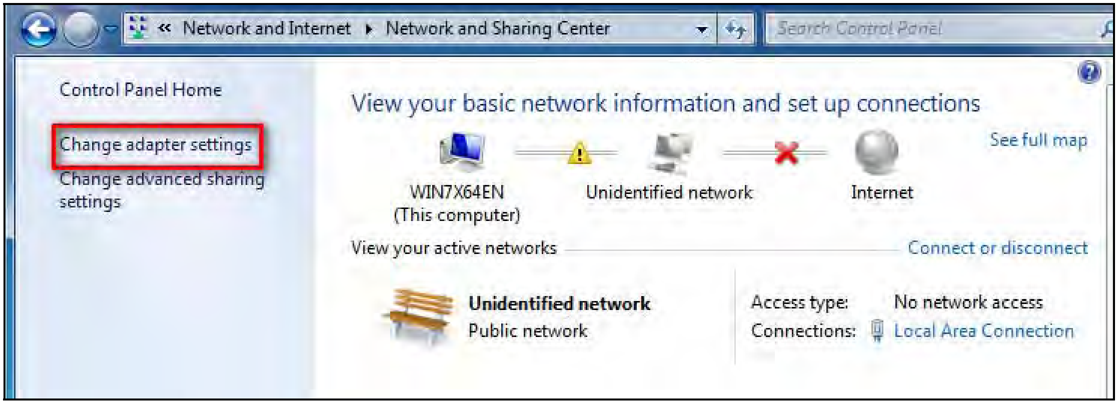
2. Enter **Control Panel** and click **Network and Internet;**


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3. Click **Network and Sharing Center**;


Control Panel ▸ Network and Internet ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Add a wireless device to the network
HomeGroup
Choose homegroup and sharing options
Internet Options
Change your homepage
Manage browser add-ons
Delete browsing history and cookies

4. Click **Change adapter settings**;



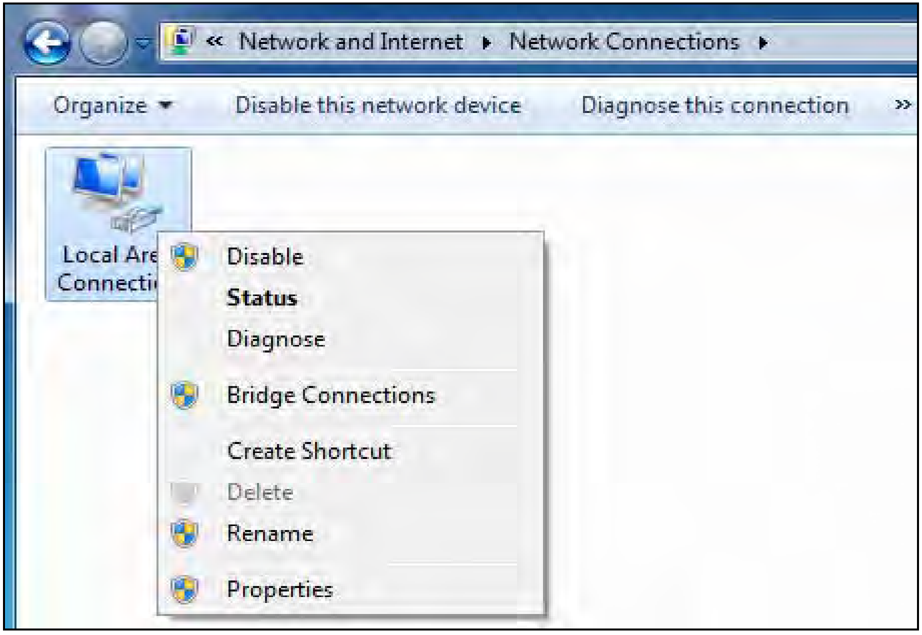
View your basic network information and set up connections

View your active networks

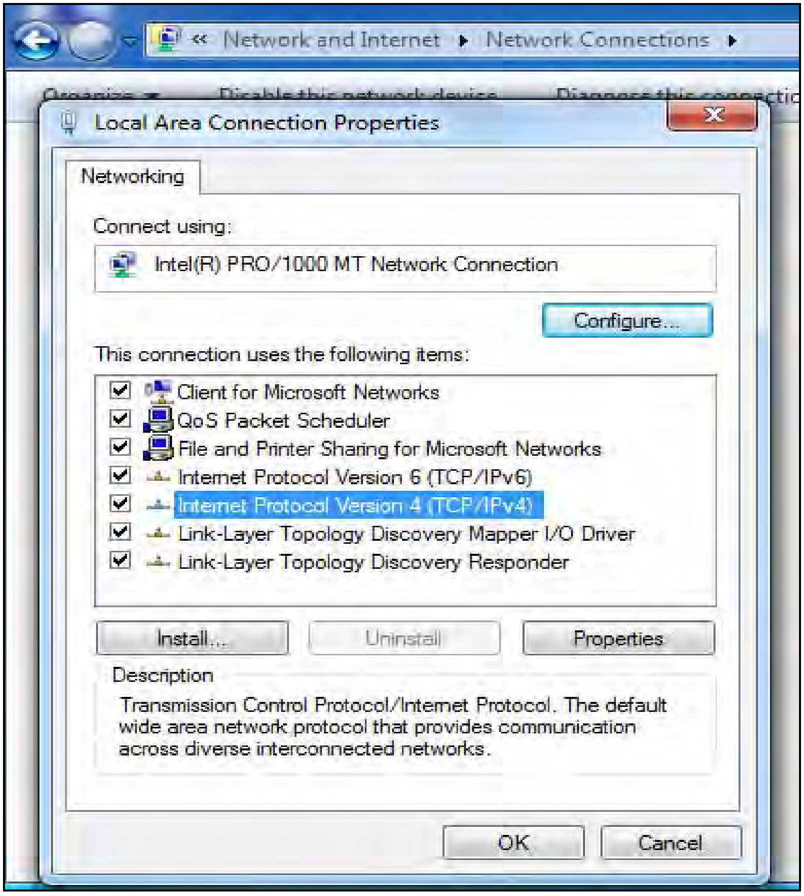
Access type: No network access

Connections: Local Area Connection

5. Right click **Local Area Connection** and select **Properties**;



6. Select **Internet Protocol Version 4(TCP/IPv4)** and click **Properties**;


« Network and Internet ▸ Network Connections ▸
Organize ▾
Disable this network device
Diagnose this connectio

Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

Configure...

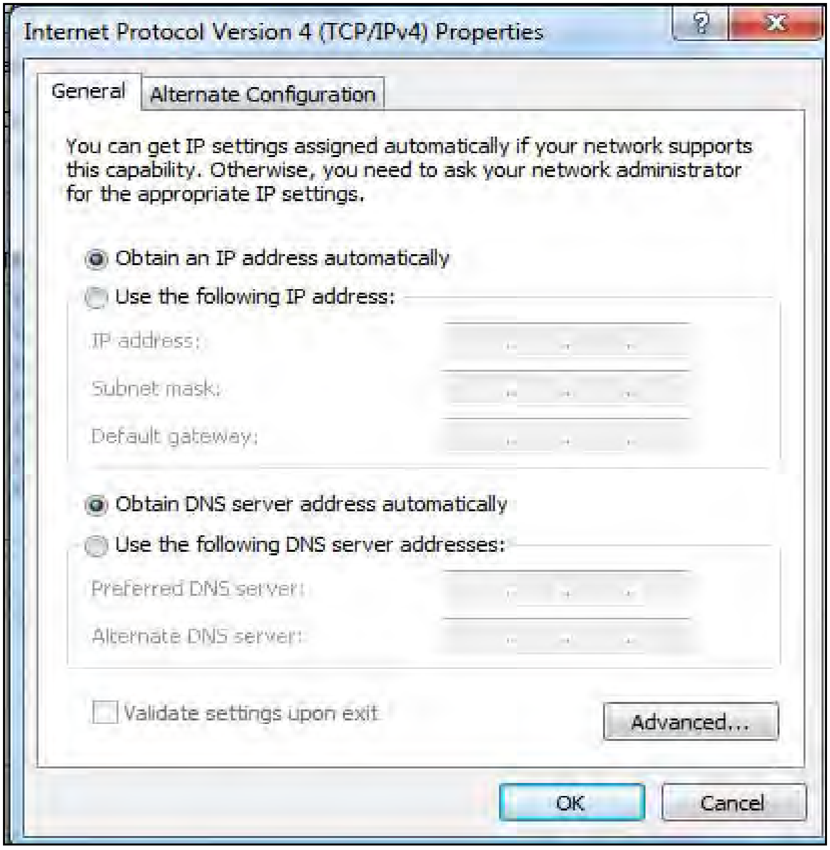
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

7. Select **Obtain an IP address automatically** and click **OK** to save the configurations.


Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

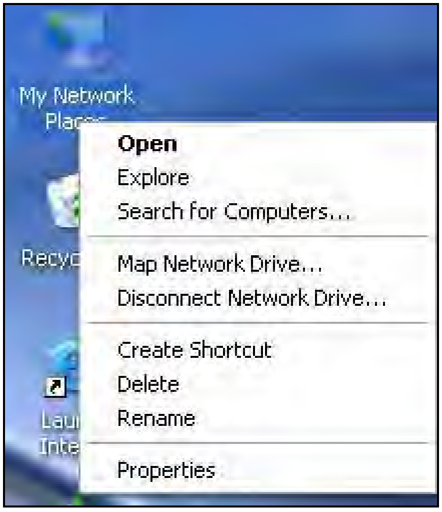
Alternate DNS server: . . .

□ Validate settings upon exit

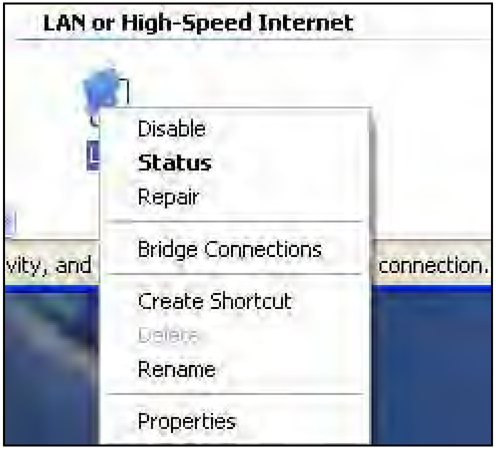
Back to Configure Router

Windows XP OS

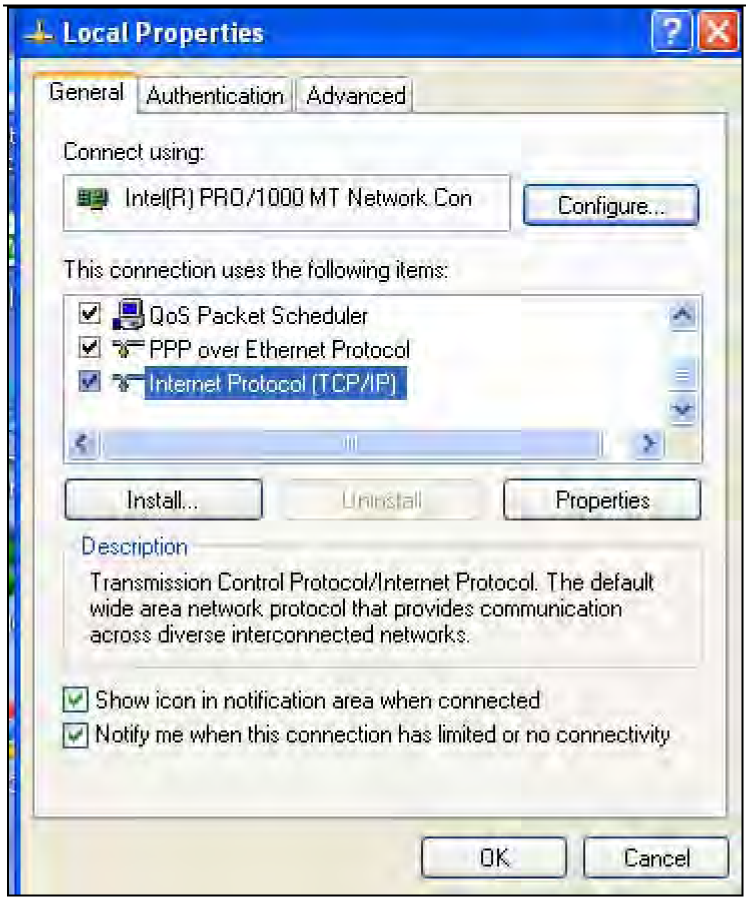
1. Right click **My Network Places** and select **Properties**;



2. Right click **Local** and select **Properties**;



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



Connect using:

Intel(R) PRO/1000 MT Network Con

This connection uses the following items:

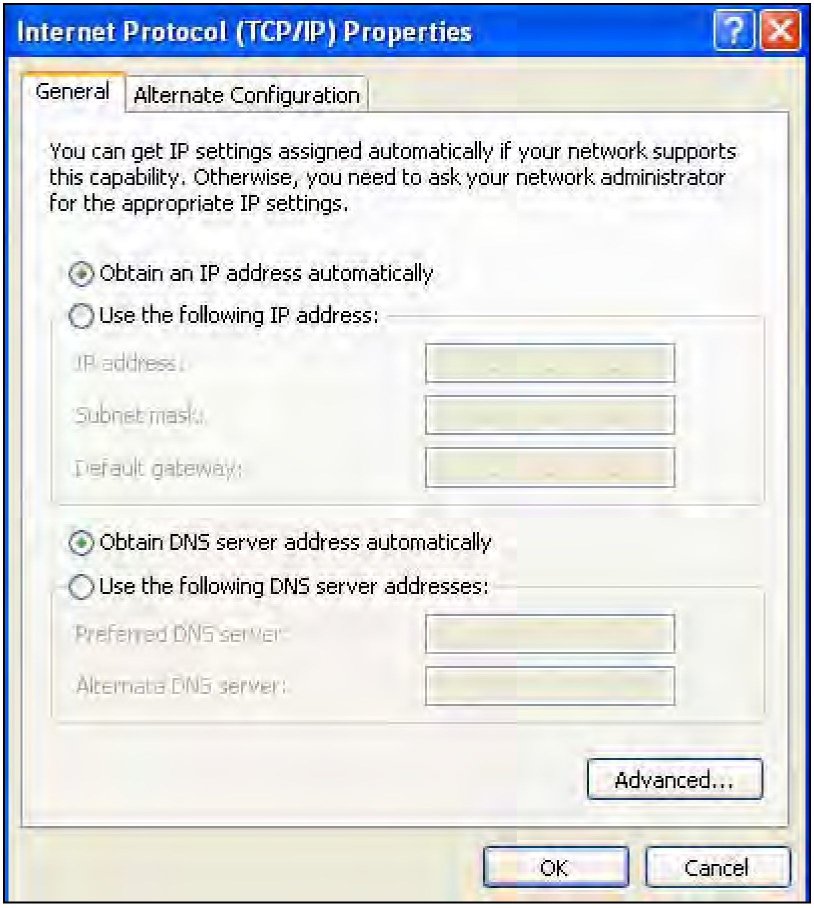
☑ QoS Packet Scheduler
☑ PPP over Ethernet Protocol
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

4. Select **Obtain an IP address automatically** and click **OK** to save the settings.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server:
Alternate DNS server:

Back to Configure Router

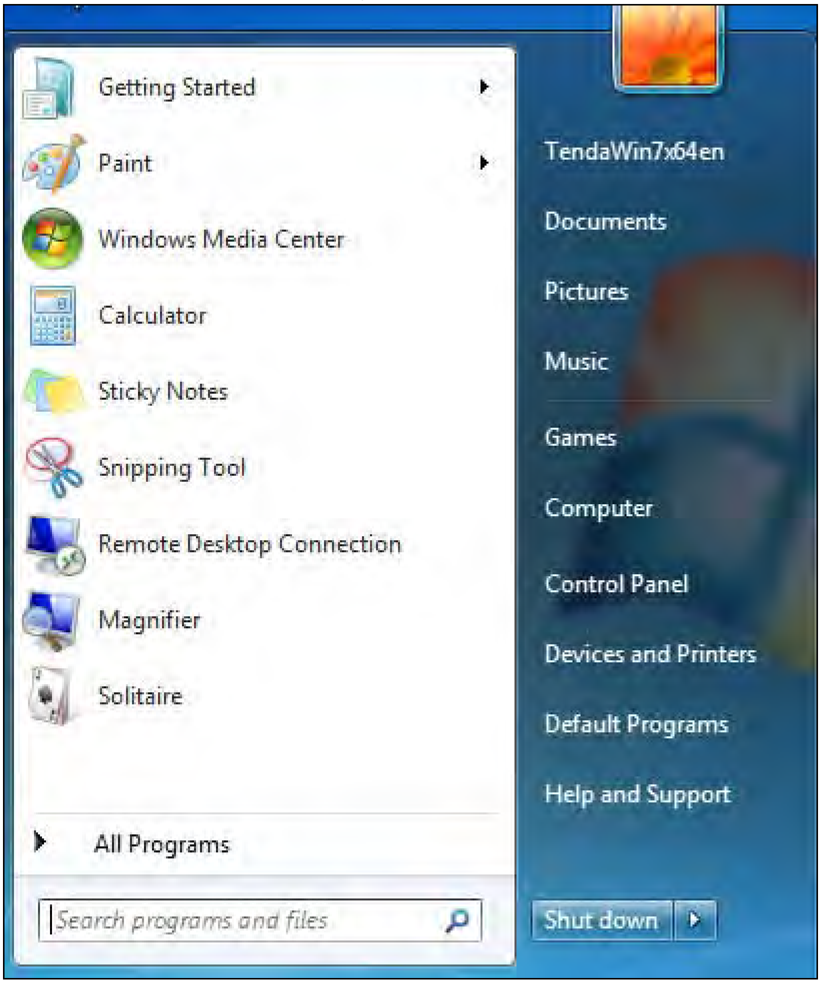
Appendix 2 Join a Wireless Connection

⚠**Note**

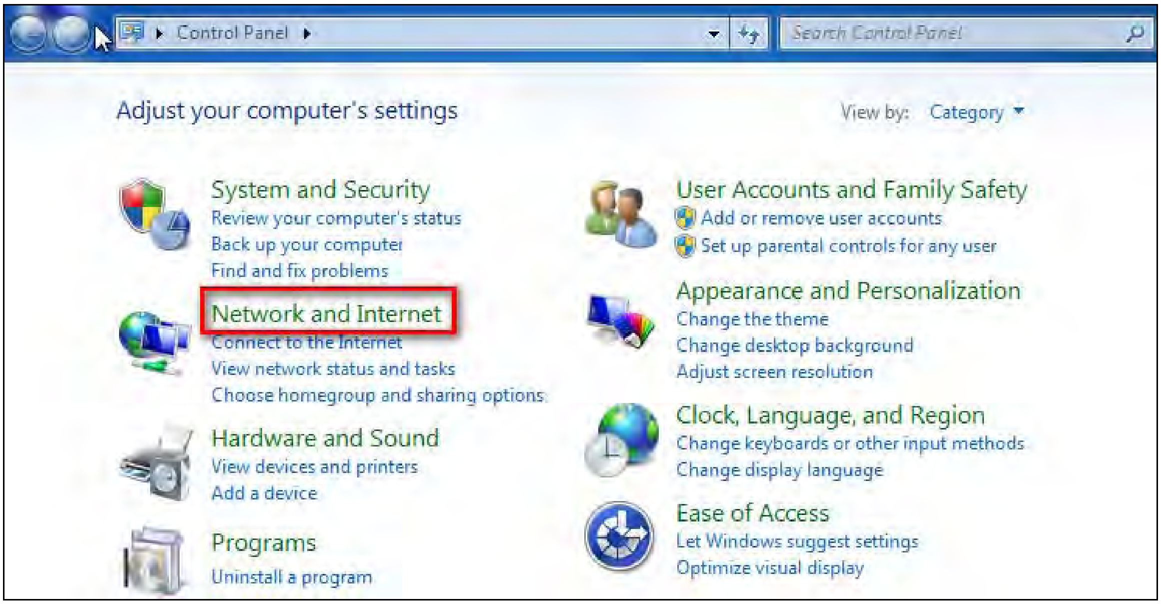
For wireless connection, desktop computers need to be equipped with wireless network cards first.

Win7 OS

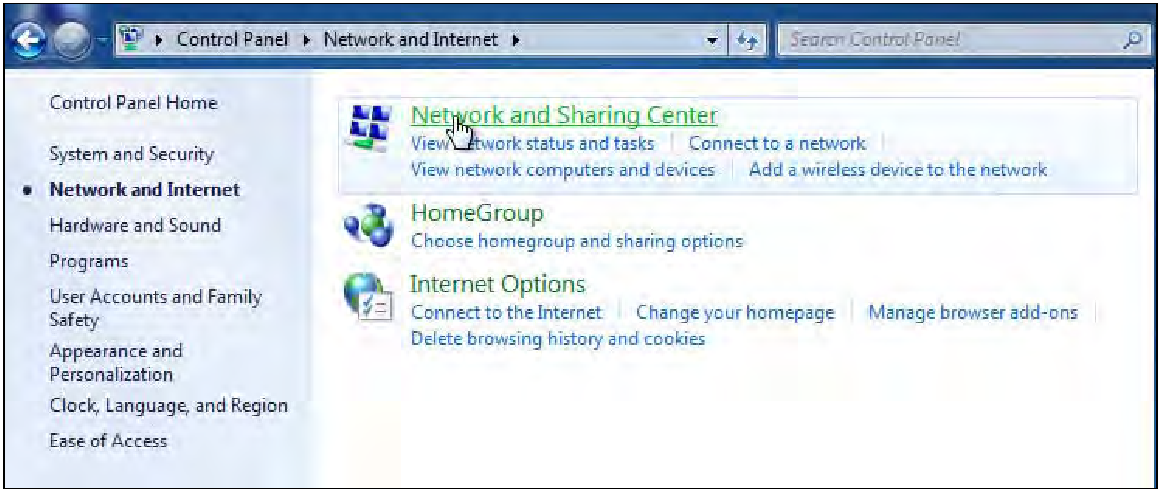
1. Click **Start>Control Panel**;



2. Click **Network and Internet**;

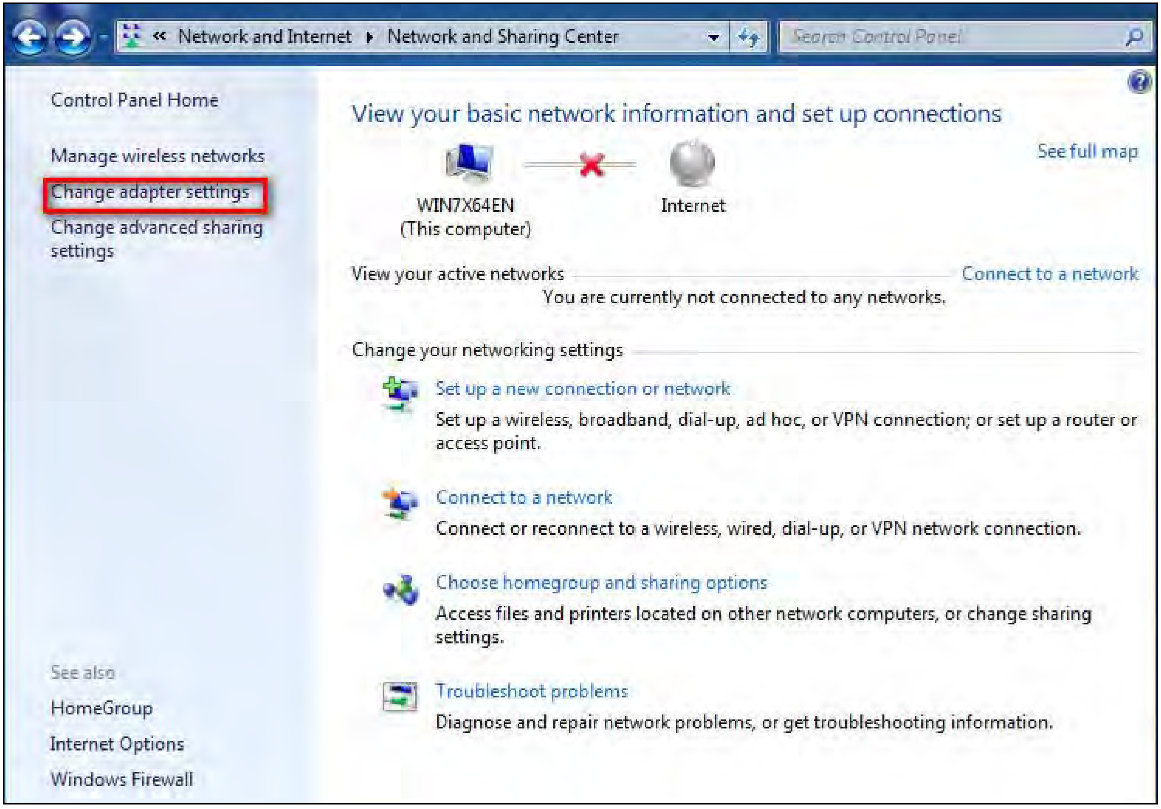

Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
Connect to the Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3. Click **Network and Sharing Center**;



Control Panel ▸ Network and Internet ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Add a wireless device to the network
HomeGroup
Choose homegroup and sharing options
Internet Options
Connect to the Internet
Change your homepage
Manage browser add-ons
Delete browsing history and cookies

4. Click **Change adapter settings**;



« Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Internet Options
Windows Firewall
View your basic network information and set up connections
See full map
WIN7X64EN
(This computer)
Internet
View your active networks
Connect to a network
Change your networking settings
Set up a new connection or network
Connect to a network
Choose homegroup and sharing options
Troubleshoot problems

You are currently not connected to any networks.

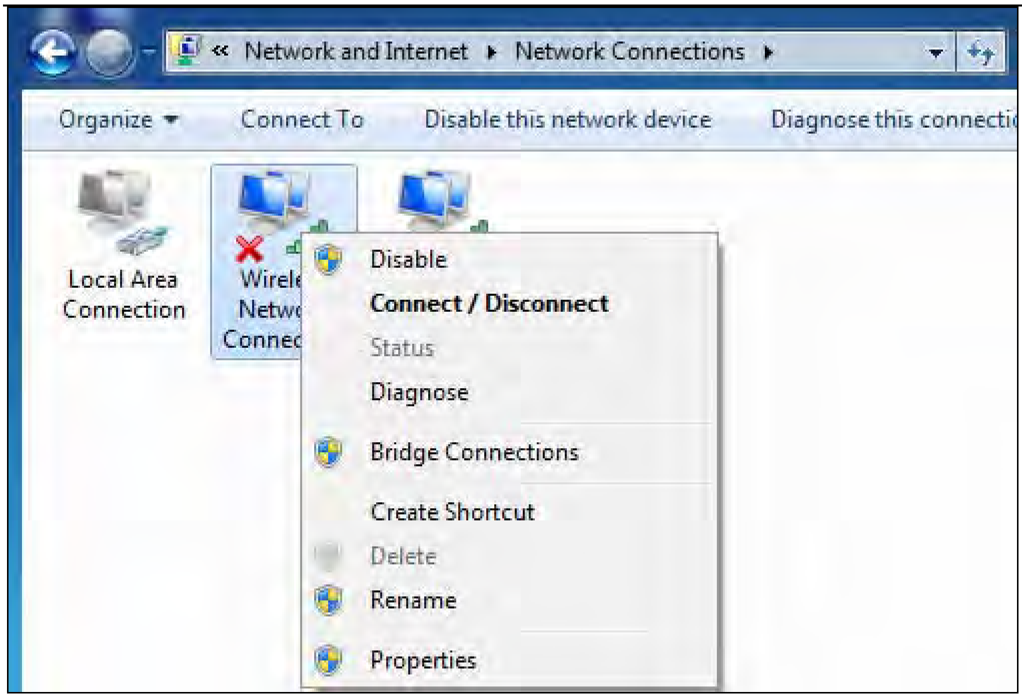
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

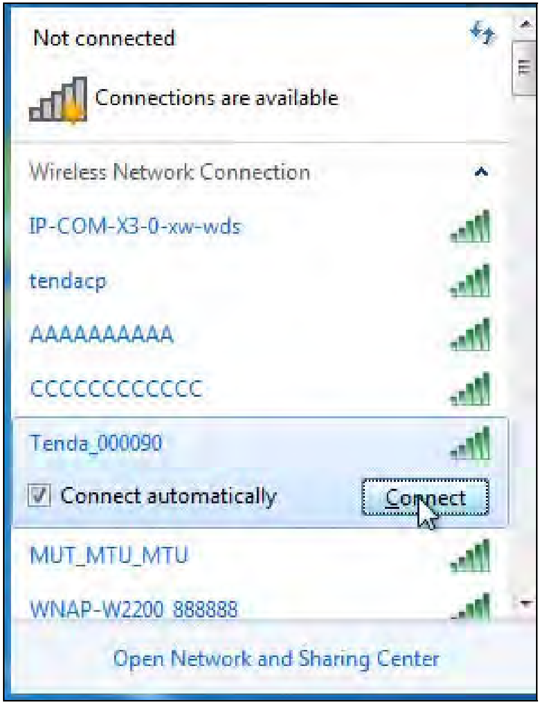
Access files and printers located on other network computers, or change sharing settings.

Diagnose and repair network problems, or get troubleshooting information.

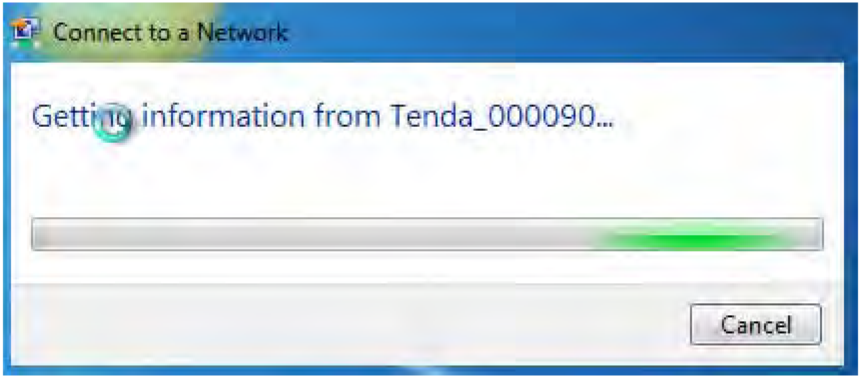
1. Click **Wireless Network Connection** accordingly and select **Connect/Disconnect**;



2. Select the network you wish to connect, such as Tenda-000090; According to different cipher types, here goes two situations:
   A. If you have configured security key, click **Connect**;

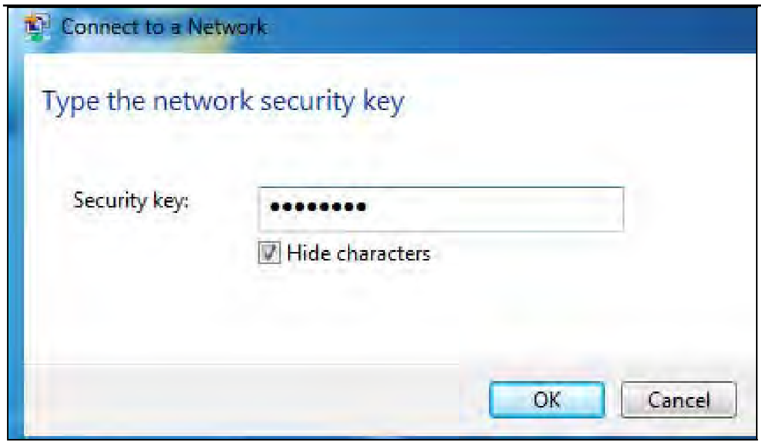


When the following dialog box appears, it indicates connecting to the network;



Getting information from Tenda_000090...

Enter your security key and click OK;



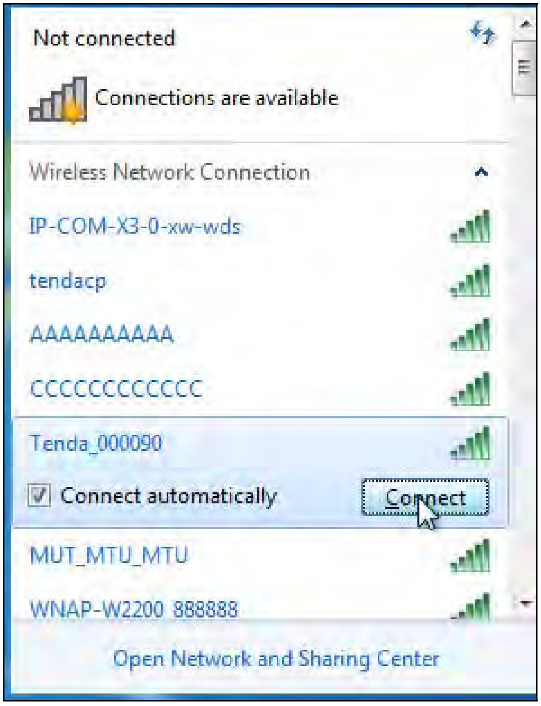
Connect to a Network

Type the network security key

Security key: ●●●●●●●●●

☑ Hide characters

B. If you have configured security key, click **Connect**;



Not connected

Connections are available

Wireless Network Connection

IP-COM-X3-0-xw-wds

tendacp

AAAAAAAAAA

CCCCCCCCCCCC

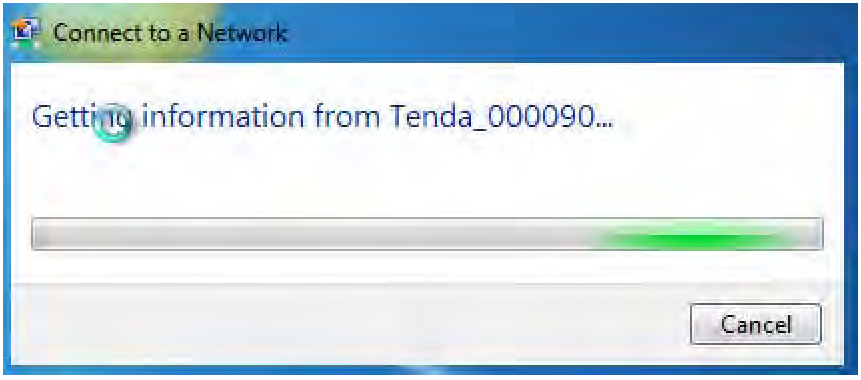
Tenda_000090

☑ Connect automatically

MUT_MTU_MTU

WNAP-W2200_888888

When the following dialog box appears, it indicates connecting to the network;



Connect to a Network

Getting information from Tenda_000090...

7. When displaying Connected, you have connected to network successfully.

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 feel free to go to www.tendacn.com to find a solution or email your problems to: support@tenda.com.cn or support02@tenda.com.cn. We will be more than happy to help you out as soon as possible.

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

a.Check whether device is functioning correctly. The SYS LED should blink a few seconds after device is powered up. If it does not light up, then some internal faults may have occurred.

b.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.

c. Run the "ping 192.168.0.1" command. If you get replies from 192.168.0.1, open your browser and verify that Proxy server is disabled. 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 "ping192.168.0.1" again.

d. 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 for over 7 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.Check if there are other DHCP servers present in your LAN. If there are other DHCP servers except your router, disable them immediately.

b.The default IP address of the device is 192.168.0.1; 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: I cannot access Internet and send/receive emails; what should I do?

This problem mainly happens to users who use the PPPoE or Dynamic IP Internet connection type. You need to change the MTU size (1492 by default). In this case, go to "WAN Settings" to change the MTU value from default 1480 to 1450 or 1400, etc.

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

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 number for Web server is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: Enter Port Forwarding (also called Port Range Forwarding on some products) screen from device web UI.

Step 3: Complete the Start Port (also called External/Ext Port on some products) and End Port (also known as Internal Port on some products) fields, say, 80-80.

Step 4: Input the internal server's IP address. For example, assuming that your Web server's IP address is 192.168. 0.10, then simply input it.

Step 5: Select a proper protocol type: TCP, UDP, or Both depending on which protocol(s) your internal host is using.

Step 6: Click Enable and save your settings.

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
Net Meeting	TCP	1503、1720
MSN Messenger	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

Appendix 4 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.

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.

IEEE 802.1X Authentication

IEEE 802.1X Authentication is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.IEEE 802.1X defines the encapsulation of EAP over LAN or EAPOL. 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. 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. The authenticator acts like a security guard to a protected network. The supplicant (i.e. client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as user name / password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

PPPOE

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. Integrated PPP protocol implements authentication, encryption, and compression functions that traditional Ethernet cannot provide and can also be used in the cable modem and digital subscriber line (DSL) and Ethernet that provide access service to the users. Essentially, it is a protocol that allows to establish a point-to-point tunnel between two Ethernet interfaces within an Ethernet broadcast domain.

DNS

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. A Domain Name Service resolves queries for these names into IP addresses for the purpose of locating computer services and devices worldwide. An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses.

WDS

A wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. All base stations in a wireless distribution system must be configured to use the same radio channel, method of encryption (none, WEP, or WPA) and the same encryption keys. They may be configured to different service set identifiers. WDS also requires every base station to be configured to forward to others in the system. WDS may also be considered a repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging).WDS may be incompatible between different products (even occasionally from the same vendor) since it is not certified by the Wi-Fi Alliance. WDS may provide two modes of wireless AP-to-AP connectivity:

Wireless bridging, in which WDS APs communicate only with each other and don't allow wireless clients or stations (STA) to access them.

Wireless repeating, in which APs communicate with each other and with wireless STAs.

DMZ

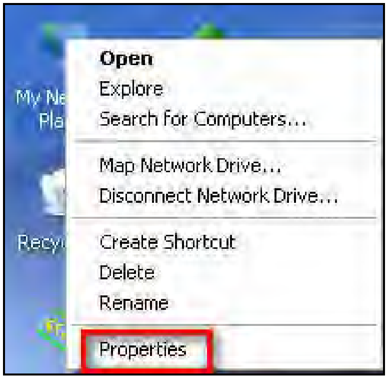
In computer security, a DMZ (sometimes referred to as a perimeter networking) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, although communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external network, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. Any services such as Web servers, Mail servers, FTP servers and VoIP servers, etc. that are being provided to users on the external network can be placed in the DMZ.

Appendix 5 Remove Wireless Network from Your PC

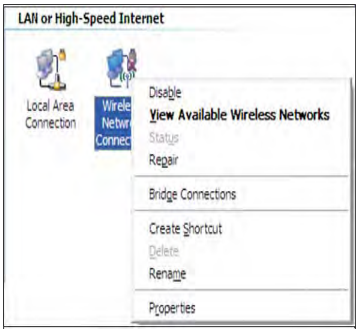
If you change wireless settings on your wireless device, you must remove them accordingly your PC; otherwise, you may not be able to wirelessly connect to the device. Below describes how to do remove a wireless network from your PC.

Windows XP OS

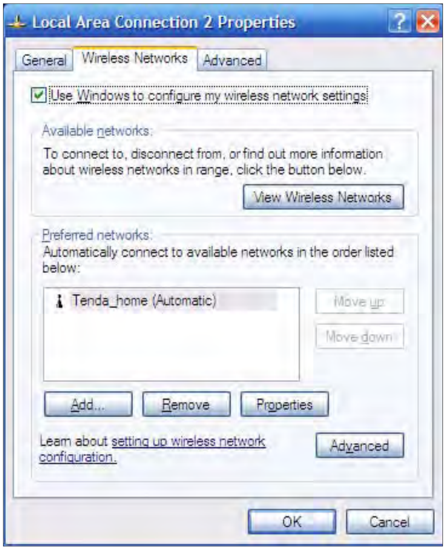
1. Right click **My Network Places** and select **Properties**.



2. Click **Wireless Network Connection** and then select **Properties**.



3. Click **Wireless Networks**, select the item under **Preferred networks** and then click the **Remove** button.



☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

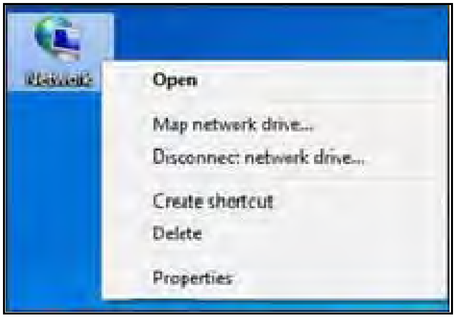
Automatically connect to available networks in the order listed below:

Tenda_home (Automatic)

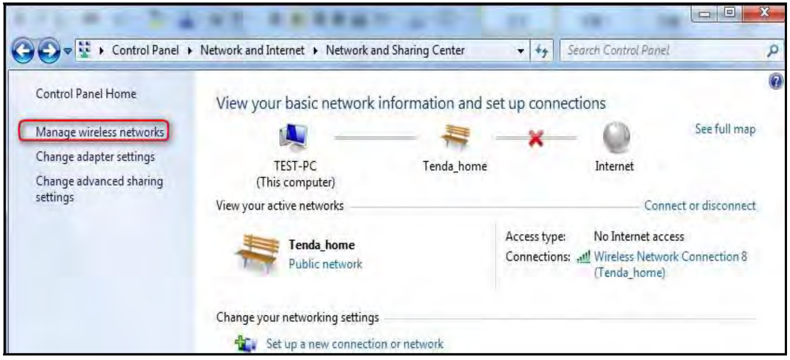
Learn about setting up wireless network configuration.

Windows 7 OS

1. Click **Network** from your desktop and select **Properties**.



2. Select **Manage Wireless Networks**.

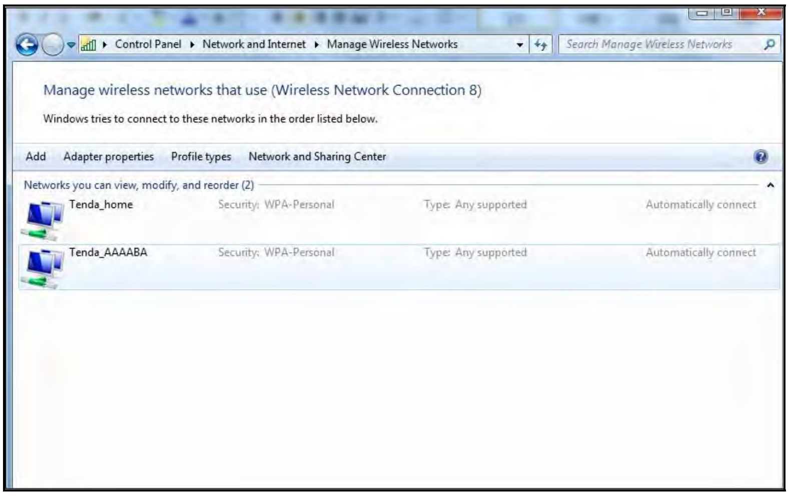

Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
TEST-PC
(This computer)
Tenda_home
Internet
See full map
View your active networks
Connect or disconnect
Tenda_home
Public network
Change your networking settings
Set up a new connection or network

View your basic network information and set up connections

Access type: No Internet access

Connections: Wireless Network Connection 8 (Tenda_home)

3. Click the wireless connection and select **Remove network**.


Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Networks
Add
Adapter properties
Profile types
Network and Sharing Center

Manage wireless networks that use (Wireless Network Connection 8)

Windows tries to connect to these networks in the order listed below.

Networks you can view, modify, and reorder (2)

Tenda_home	Security: WPA-Personal	Type: Any supported	Automatically connect
Tenda_AAAABA	Security: WPA-Personal	Type: Any supported	Automatically connect

Appendix 6 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 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.

This equipment has been tested and found to comply with the limits for a Class B 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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. 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 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.

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 transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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.

NCC Notice

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更設計之特性及功能。

低功率射頻電機之作用不得影響飛航安全及幹擾合法通信；經發現有幹擾現象時，應立即停用，並改善至無幹擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之幹擾。