Tenda®

User Guide

www.tenda.cn

W300A Wireless-N Access Point

Copyright Statement

All the photos and product specifications mentioned in this manual are for references only. As the upgrade of software and hardware, there will be changes. And if there are changes, Tenda is not responsible for informing in advance. If you want to know more about our product information, please visit our website at www.tenda.cn.

Content

Chapter 1 Product Overview 1

1.1 Features 2
1.2 Package Contents............................. 3
1.3 LED Indicator and Panel Description..... 4

Chapter 2 Hardware Installation 7

Chapter 3 Web Configuration 9

3.1 Web Login.. 9
3.2 Wizard.. 11
3.3 Running Status 12
3.4 LAN Settings 13

Chapter 4 Wireless Settings........................ 15

4.1 Working Mode................................. 15
4.1.1 Access Point (AP) Mode 16
4.1.2 P2P (Point to Point) Bridge Mode.. 32
4.1.3 P2MP Bridge Mode 37
4.1.4 Wireless Repeater Mode 42
4.1.5 Wireless Client Mode 49
4.2 Advanced Settings 53

4.3 WPS Settings.................................55
4.4 Access Control................................57
4.5 Connection Status...........................59
4.6 PING..60

Chapter 5 SNMP Setting............................61

5.1 SNMP Introduction..........................61
5.2 SNMP Setting................................62

Chapter 6 System Tools............................64

6.1 Password Change............................64
6.2 Restore to Factory............................65
6.3 Backup/Restore..............................66
6.4 Time Settings................................67
6.5 Reboot System...............................68
6.6 Firmware Upgrade...........................68
6.7 Syslog..70

Appendix I: Glossary................................71

Appendix II: TCP/IP Address Setting (Take Winxp as example)...74

Chapter 1 Product Overview

W300A, with 2T3R antennas, is an IEEE802.11n (Draft 2.0)-compliant wireless access point with one Gigabit LAN switch port, which utilizes the latest MIMO technology and provides up to 300Mbps stable transmission rate from wireless radio to wired network. With backward compatible with IEEE802.11b/g device, it is suitable for SOHOs and small-sized enterprises to share the wireless network.

W300A supports five working modes: wireless AP mode for other wireless access; Repeater mode for relaying wireless network coverage; P2P, P2MP mode for bridging two or more wireless network and wireless client mode. Besides, it supports multiple encryption methods like 64/128bit WEP, WPA, WPA2 and WPA&WPA2 to protect you network against malicious attack, and WPS can free you from remembering long passwords. Power over Ethernet support can realize data transmission and power supply via one Ethernet cable. Moreover, SNMP and Web-based management interface can help users configure the device more easily.

1.1 Features

- Complies with IEEE802.11n (Draft 2.0), IEEE802.11b and IEEE802.11g standards
- Supports five working modes: wireless AP, Repeater, P2P, P2MP and wireless client
- Provides 300Mbps receiving rate and 300Mbps sending rate
- MIMO technology utilizes reflection signal to increase 8 times transmission distance of original 802.11g standard and reduces the "dead spots" in the wireless coverage area
- Provides one Gigabit Auto-negotiation RJ45 port for LAN connection
- Supports two power supply ways: Power over Ethernet and external power adapter
- Supports SNMP and Web-based management interface
- Supports 64/128bit WEP encryption
- Supports multiple encryption methods as WPA, WPA2 and WPA&WPA2 and security mechanism
- Supports WPS (PBC and PIN) encryption method to free you from remembering long passwords
- Supports five connection modes: AP, WDS P2P

Bridge, WDS P2MP Bridge, WDS AP Bridge and Client

- Supports Auto MDI/MDIX
- Supports Firefox1.0, IE5.5 or above
- Supports authorization access over thirty-two MAC addresses
- Supports auto wireless channel selection
- Provides three detachable antennas

Wireless local network usually is used in a planned environment where each access point is located steadily and with stable radio coverage area. The AP (Access Point) will provide wireless communication service for users around.

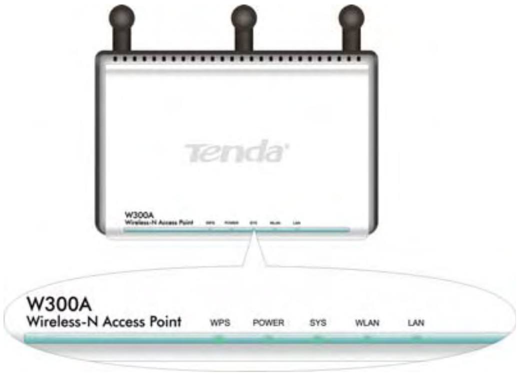
1.2 Package Contents

Please unpack the package and find the following items:

- One W300A Wireless AP
- One Power Adapter
- One Quick Installation Guide
- One CD-ROM

If any of listed items are missing or damaged, please contact the Tenda reseller from whom you purchased for replacement immediately.

1.3 LED Indicator and Panel Description



- **LED indicator description on front panel (from L to R)**

  WPS
  When blinking, it indicates the device is negotiating with client in WPS mode.

  POWER
  When turns green, Always ON indicates the power connects well.

SYS

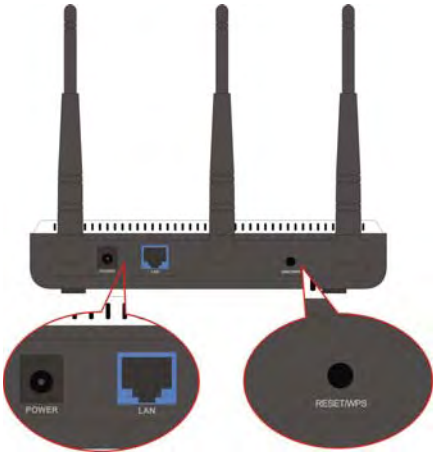
When turns green, blinking indicates the system runs well.

WLAN

Wireless signal LED indicator. When turns green, Always ON indicates the wireless function is enabled; blinking indicates the device is transmitting and/or receiving data.

LAN

Wired local network LED indicator. Always ON indicates it is connected with Ethernet device; green indicates the link speed is 1000Mbps; orange indicates the link speed is 10/100Mbps; blinking indicates the device is transmitting and/or receiving data.



- **Rear Panel：（From L to R）**

POWER

The jack is for power adapter connection. Please use the included 12V DC power adapter.

LAN

The Gigabit Ethernet port is for computer’s NIC or switch connection. It also can be used as PoE interface. When PoE and external power adapter power on the device, the include power adapter is preferred.

RESET / WPS

Compound button is for system reset and WPS. When you press this button for 7 seconds, the device will restore the configured settings to factory default settings. When you press for 1 second, the WPS function will be enabled.

Antenna

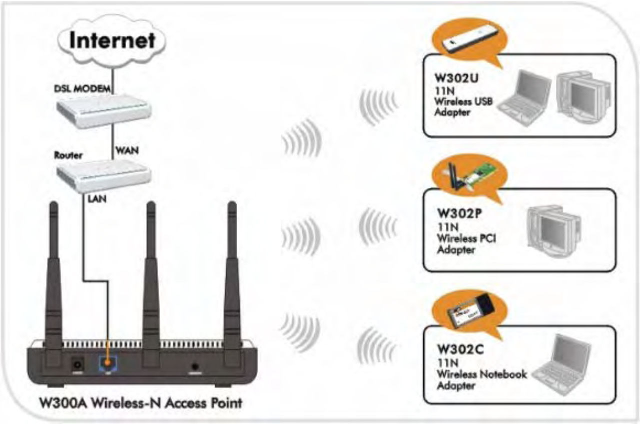
The detachable antenna is for wireless radio transmitting and receiving. Don not detach these antennas for fear of wireless performance.

Chapter 2 Hardware Installation

This chapter explains how to connect the Access Point (take the AP mode installation as example, other installation modes please refer to the Quick Installation Guide). The detailed processes are shown as below:

1. Connect one end of the network cable to your Ethernet broadband router, switch or PC, and the other end to the W300A's LAN port.

2. Connect the power adapter to the AP's Power jack. Then plug the power adapter into an electrical outlet. The power LEDs on the front panel will light up as soon as the AP's powers on. Then, connect wireless adapter to the AP via wireless signals. Please refer to the topology below:



The topology plan of AP mode connection

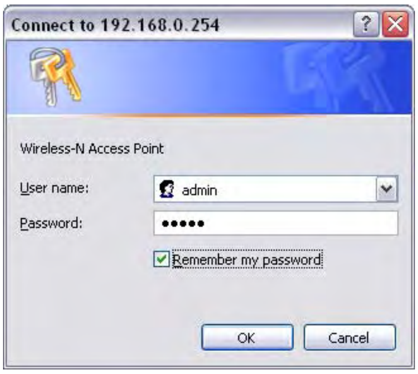
Chapter 3 Web Configuration

3.1 Web Login

Connect to W300A via wired cable and configure 192.168.0.x(x ranges 1-253) as your PC's IP address, and 255.255.255.0 as subnet mask. (Please refer to the Appendix II for details on TCP/IP setting)

Launch Internet Explorer or Netscape Navigator. In the address bar, enter the AP's default IP address, 192.168.0.254 Press Enter key and the login screen will appear.

Enter **admin** both in the user name and password field. When this is your first time to open the Web-based management interface, you can set a new password from the ***System Tool – Change password*** tab.



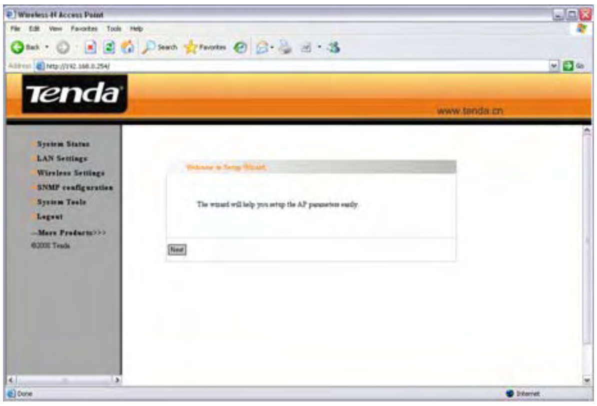
Wireless-N Access Point

User name: admin

Password: ●●●●●

☑ Remember my password

Click OK to enter the first web page of the device.

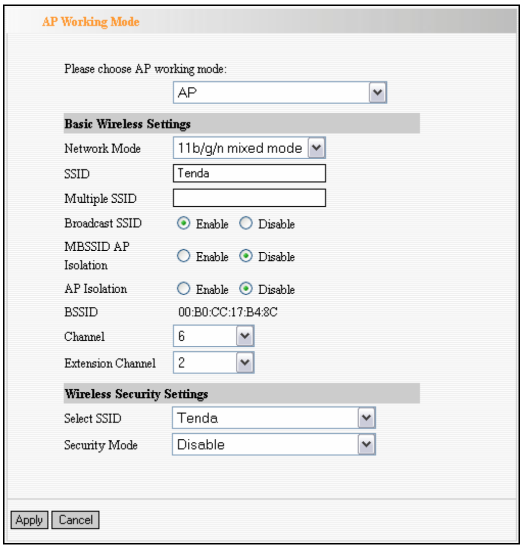


Welcome to Setup Wizard

The wizard will help you setup the AP parameters easily.

3.2 Wizard

Click “Next” in the first page and the next page appears.



AP Working Mode

Please choose AP working mode:

AP

Basic Wireless Settings

Network Mode	11b/g/n mixed mode
SSID	Tenda
Multiple SSID	
Broadcast SSID	● Enable ○ Disable
MBSSID AP Isolation	○ Enable ● Disable
AP Isolation	○ Enable ● Disable
BSSID	00:B0:CC:17:B4:8C
Channel	6
Extension Channel	2

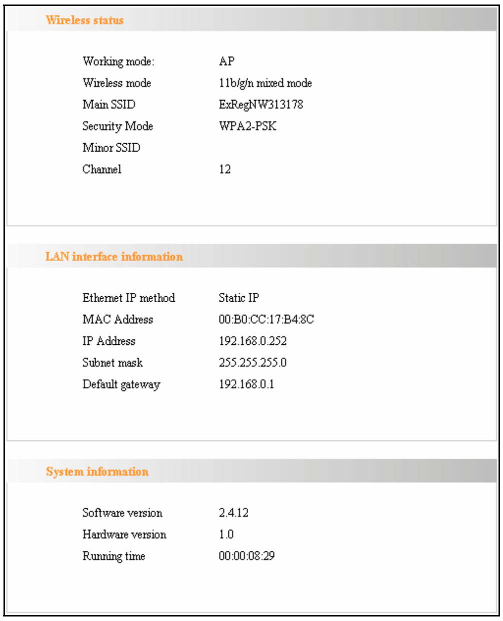
Wireless Security Settings

Select SSID	Tenda
Security Mode	Disable

On this page, you can select one from five wireless network modes: Wireless AP, P2P Bridge Mode, P2MP Bridge Mode, Repeater Mode and Client. And to secure your network, you can configure its corresponding security setting.

3.3 Running Status

This page shows the wireless AP's current status, including wireless status, LAN status and system information.



Wireless status

Working mode:	AP
Wireless mode	11b/g/n mixed mode
Main SSID	ExRegNW313178
Security Mode	WPA2-PSK
Minor SSID	
Channel	12

LAN interface information

Ethernet IP method	Static IP
MAC Address	00:B0:CC:17:B4:8C
IP Address	192.168.0.252
Subnet mask	255.255.255.0
Default gateway	192.168.0.1

System information

Software version	2.4.12
Hardware version	1.0
Running time	00:00:08:29

- ***Wireless Status***

  Here shows the current working status, including working mode, wireless network mode, SSID, Channel, Encryption mode, etc.

- ***LAN Interface information***

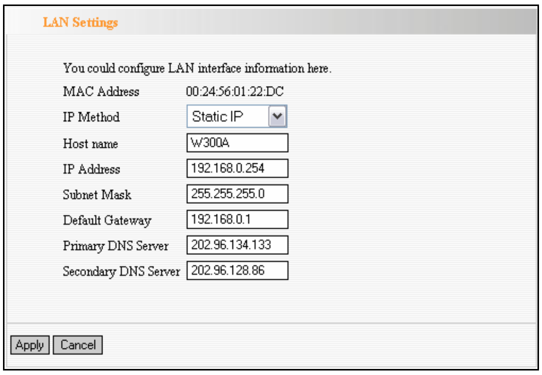
  Here shows LAN IP obtain way, MAC address, IP address, subnet mask, etc.

- ***System information***

  Here shows the device's current software version, hardware version, etc.

3.4 LAN Settings

This section mainly deals with LAN's basic settings.



LAN Settings

You could configure LAN interface information here.

MAC Address	00:24:56:01:22:DC
IP Method	Static IP
Host name	W300A
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
Primary DNS Server	202.96.134.133
Secondary DNS Server	202.96.128.86

Static IP: The default IP address is 192.168.0.254. If necessary, you can configure a new IP address, subnet mask and gateway manually for the device.

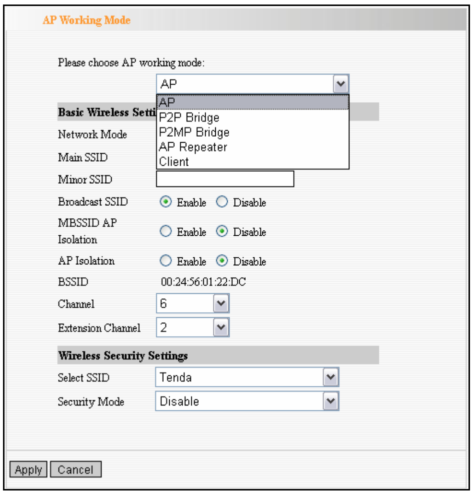
Dynamic IP: Automatically obtain IP address, subnet mask and gateway from DHCP server. (Unless you have got permission to obtain this information from the uplink connected device, otherwise, it is not recommended to select this way).

Note: If the LAN IP address is changed, you need use the new IP address to login the wireless AP's Web interface next time.

Chapter 4 Wireless Settings

4.1 Working Mode

Select "Wireless Setting->Working Mode" to enter the following window. From the drop-down menu of Working Mode, the device supports five working modes: AP, P2P Bridge, P2MP Bridge, AP Repeater and Client.



AP Working Mode

Please choose AP working mode: AP

Basic Wireless Setti

Network Mode

Main SSID

Minor SSID

Broadcast SSID ● Enable ○ Disable

MBSSID AP Isolation ○ Enable ● Disable

AP Isolation ○ Enable ● Disable

BSSID 00:24:56:01:22:DC

Channel 6

Extension Channel 2

Wireless Security Settings

Select SSID Tenda

Security Mode Disable

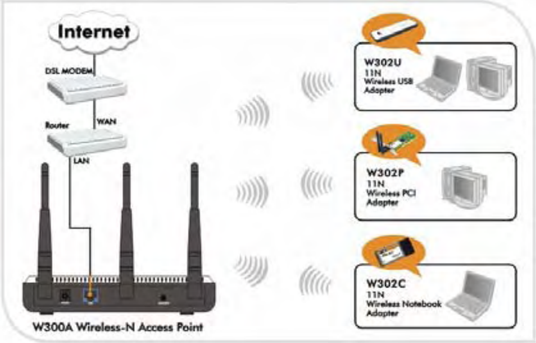
Next, this user guide will explain the five modes one by one:

4.1.1 Access Point (AP) Mode

The AP mode is the basic mode of the device. When the system is reset to the default factory settings, the operating mode reverts to AP mode. In this mode, the AP will act as a central hub for different wireless LAN clients. For example, when traveling to a hotel that has high-speed internet access, you can connect to the internet through the AP which is connected to an Ethernet cable in the room.

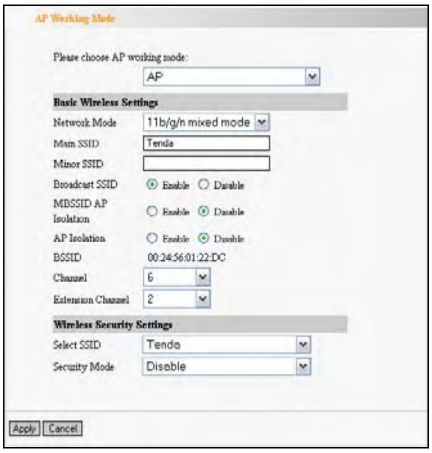
4.1.1.1 Application and Topology Plan

The AP mode can convert the wired transmission into wireless signals. If you have one wired cable connecting to Internet, and want to access the Internet via wireless signals connecting to your notebook computer, this mode fits perfectly.



4.1.1.2 AP Mode Settings

In the working mode, select “AP” to enter the next window.


AP Working Mode

Please choose AP working mode:
AP

Basic Wireless Settings

Network Mode	11b/g/n mixed mode
Main SSID	Tenda
Minor SSID	
Broadcast SSID	● Enable ○ Disable
MBSSID AP Isolation	○ Enable ● Disable
AP Isolation	○ Enable ● Disable
BSSID	00:24:56:01:22:DC
Channel	6
Extension Channel	2

Wireless Security Settings

Select SSID	Tenda
Security Mode	Disable

- **Basic Wireless Settings**
  - ✧ ***Network Mode***: Select one mode from the following. The default is 11b/g/n mode.

    11b mode： Allow the wireless client to connect with the device in 11b mode at the maximum speed of 11Mbps.

    11g mode： Allow the 11g/11n-compliant client device to connect with the AP at the maximum speed of 54Mbps.

    11b/g mode： Allow the 11b/g-compliant client device to connect with the AP with auto-negotiation speed, and 11n wireless client to connect the device with 11g speed.

    11b/g/n mode： Allow 11b/g/n-compliant client device to connect with the AP with auto- negotiation speed.
  - ✧ ***Main SSID：*** SSID (Service Set Identifier) is the unique name of the wireless network. This device has two SSID and the main SSID is necessary.
  - ✧ ***Minor SSID：*** It is optional.
  - ✧ ***MBSSID AP Isolation：*** One access control feature based on wireless MAC address.

When this feature is enabled, wireless clients connected with the same SSID can not communicate with each other. For example, configure main SSID as AP1, minor SSID as AP2. PC1 and PC2 connect to AP1 via wireless adapter, and configure PC1 and PC2 in the same segment. After the feature is enabled, two PCs can not communicate and share network resource each other, but they can communicate with wireless clients connected with AP2. **This feature is to isolate the communication of wireless clients connected with the same SSID.**

✧ ***AP Isolation:*** One access control feature based on wireless MAC address. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. This feature is deployed when you have many guests that frequent your wireless network. For example, configure main SSID as AP1, minor SSID as AP2. PC1 connects to AP1 via wireless adapter; PC2 connecting to AP2. After the feature is enabled, two PCs can not communicate and share network resource each other. **This feature is to isolate the communication of wireless clients connected with different SSID.**

Tip: If you want to isolate all connected wireless client's communication, please enable MBSSID AP Isolation and AP Isolation simultaneously.

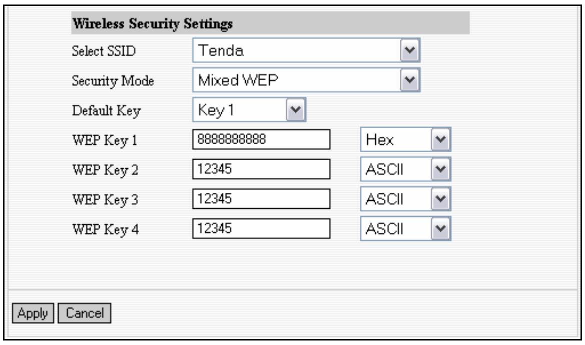
- ✧ ***BSSID*：** Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.
- ✧ ***Channel*：**Specify the effective channel (from 1 to 13\Auto) of the wireless network.
- ✧ ***Extension channel*：** To increase data throughput of wireless network, the extension channel range is used in 11n mode.

- ● **Wireless Security Setting：**

  It is used to configure the AP network’s security setting. Here presents the common ten encryption methods, including Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2- enterprise, etc.

Mixed WEP

WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources. WEP is based on RSA algorithm from RC4. It is the original and weak encryption method, so it is recommended not to use this method. Select Mixed WEP to enter the following window:



Wireless Security Settings

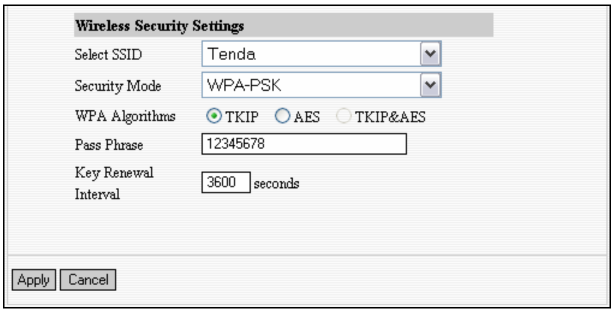
Select SSID	Tenda	
Security Mode	Mixed WEP	
Default Key	Key 1	
WEP Key 1	8888888888	Hex
WEP Key 2	12345	ASCII
WEP Key 3	12345	ASCII
WEP Key 4	12345	ASCII

Setting Explanation

- ***Select SSID：*** Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- ***Security Mode：*** From the drop-down menu select the corresponding security encryption modes.
- ***WEP Key1~4：*** Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13 ASCII characters. Illegal character as "/" is not allowed.) Or 10/26 hex characters.
- ***Default Key：*** Select one key from the four configured keys as the current available one.

WPA- PSK

WPA (Wi-Fi Protected Access), a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. Select "WPA-PSK" from the drop-down menu to enter the following window:



Wireless Security Settings

Select SSID: Tenda

Security Mode: WPA-PSK

WPA Algorithms: ● TKIP ○ AES ○ TKIP&AES

Pass Phrase: 12345678

Key Renewal Interval: 3600 seconds

Setting Explanation

✧ ***Select SSID:*** Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.

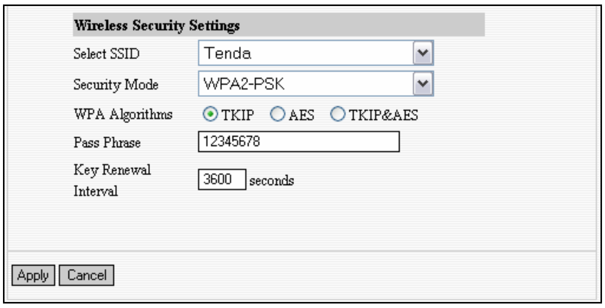
✧ ***WPA Algorithms:*** Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.

✧ ***Pass Phrase:*** Enter the encrypted characters with 8-63 ASCII characters.

✧ ***Key Renewal Interval:*** Set the key's renewal period.

WPA2-PSK

WPA2 provides more secure features than WEP and WPA. Select "WPA2-PSK" from the drop-down menu to enter the following window:



Wireless Security Settings

Select SSID: Tenda

Security Mode: WPA2-PSK

WPA Algorithms: ● TKIP ○ AES ○ TKIP&AES

Pass Phrase: 12345678

Key Renewal Interval: 3600 seconds

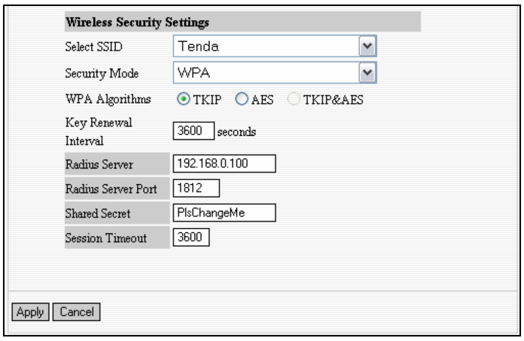
Setting Explanation

- ✧ ***Select SSID:*** Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- ✧ ***WPA Algorithms:*** Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.

- ✧ ***Pass Phrase*：** Enter the encrypted characters with 8-63 ASCII characters.
- ✧ ***Key renewal Interval*：** Set the key's renewal period.

WPA

This security mode is used when a RADIUS server is connected to the device. Select "WPA" from the drop-down menu to enter the following window:



Wireless Security Settings

Select SSID	Tenda
Security Mode	WPA
WPA Algorithms	● TKIP ○ AES ○ TKIP&AES
Key Renewal Interval	3600 seconds
Radius Server	192.168.0.100
Radius Server Port	1812
Shared Secret	PlsChangeMe
Session Timeout	3600

Setting Explanation

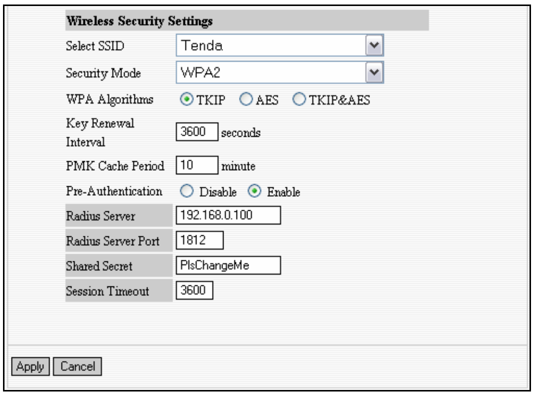
- ✧ ***Select SSID*：** Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- ✧ ***WPA Algorithms*：** Provides TKIP [Temporal Key Integrity Protocol] or AES

[Advanced Encryption Standard]. The default is TKIP mode.

- ***Key Renewal Interval*：** Set the key's renewal period.
- ***Radius Server*：** Enter the IP address of the Radius server.
- ***Radius Server port*：** Enter the authentication port of the Radius server. The default is 1812.
- ***Shared Secret*：** Enter the shared key for authentication server with 8~63 ASCII characters.
- ***Session Timeout*：** The authentication interval period between AP and authentication server. The default is 3600s.

WPA2

This security mode is based on Radius authentication server and WPA2 encryption method. WPA2 is used when a RADIUS server is connected to the device. Select "WPA2" from the drop-down menu to enter the following window:



Wireless Security Settings

Select SSID	Tenda
Security Mode	WPA2
WPA Algorithms	● TKIP ○ AES ○ TKIP&AES
Key Renewal Interval	3600 seconds
PMK Cache Period	10 minute
Pre-Authentication	○ Disable ● Enable
Radius Server	192.168.0.100
Radius Server Port	1812
Shared Secret	PlsChangeMe
Session Timeout	3600

Setting Explanation

✧ ***Select SSID***：Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.

✧ ***WPA Algorithms***：Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.

✧ ***Key Renewal Interval***：Set the key's renewal period.

✧ ***Radius Server***：Enter the IP address of the Radius server.

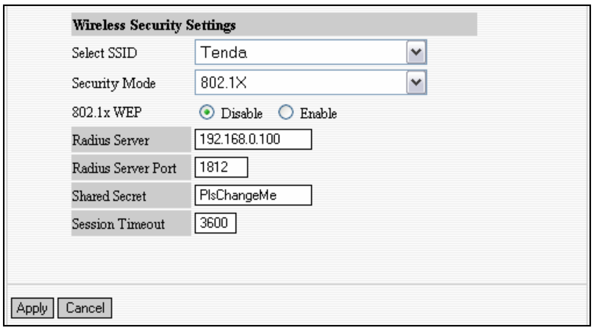
✧ ***Radius Server Port*** ： Enter the

authentication port of the Radius server. The default is 1812.

- ✧ ***Shared Key*：** Enter the shared key for authentication server with 8~63 ASCII characters.
- ✧ ***Session Timeout*：** The authentication interval period between AP and authentication server. The default is 3600s.

802.1x Authentication

This security mode is used when a RADIUS server is connected to the device. 802.1x, a kind of Port-based authentication protocol, is an authentication type and strategy for users. The port can be either a physic port or logic port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.11x authentication is to check if the port can be used. If the port is authenticated successfully, you can open this port which allows all the messages to pass. If the port isn't authenticated successfully, you can keep this port "disable" which just allows 802.1x authentication protocol message to pass. Select "802.1x" from the drop-down menu to enter the following window:



Wireless Security Settings

Select SSID	Tenda
Security Mode	802.1X
802.1x WEP	● Disable ○ Enable
Radius Server	192.168.0.100
Radius Server Port	1812
Shared Secret	PlsChangeMe
Session Timeout	3600

Setting Explanation

✧ ***Select SSID：*** Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.

✧ ***802.1x WEP：*** Click “Enable/Disable” to enable or disable the WEP algorithm.

✧ ***Radius Server：*** Enter the IP address of the Radius server.

✧ ***Radius Server Port：*** Enter the authentication port of the Radius server. The default is 1812.

✧ ***Shared Secret：*** Enter the shared key for authentication server with 8~63 ASCII characters.

✧ ***Session Timeout：*** The authentication interval period between AP and authentication server. The default is 3600s.

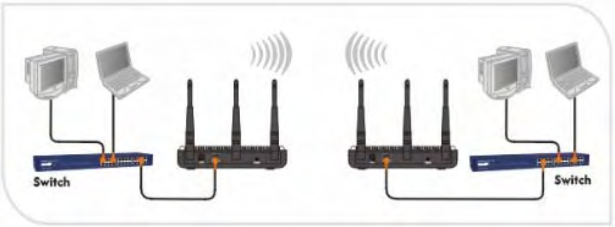
Note: To improve security level, do not use too easy characters.

4.1.2 P2P (Point to Point) Bridge Mode

Two wired local networks communicate and share network resource via two W300A's wireless signals which also can extend the wired network. In this mode, AP can not connect with wireless clients, but serve as wireless bridge.

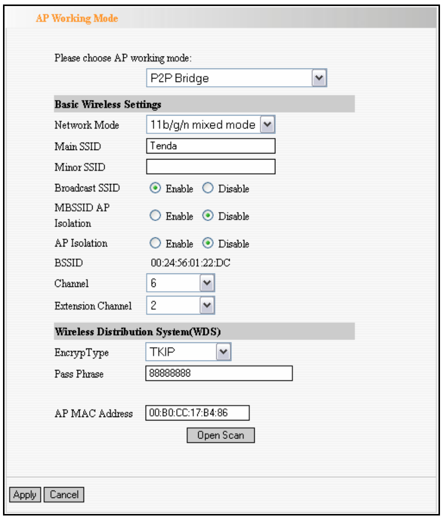
4.1.2.1 Application Plan

P2P bridge mode can connect with two wired network via wireless access points, which communicate by wireless signals and not by cables. This mode can free from the cable trouble. The P2P topology shows below:



4.1.2.2 P2P Bridge Setting

In the working mode, select "WDS P2P" to enter the next screen.



AP Working Mode

Please choose AP working mode: P2P Bridge

Basic Wireless Settings

Network Mode	11b/g/n mixed mode
Main SSID	Tenda
Minor SSID	
Broadcast SSID	● Enable ○ Disable
MBSSID AP Isolation	○ Enable ● Disable
AP Isolation	○ Enable ● Disable
BSSID	00:24:56:01:22:DC
Channel	6
Extension Channel	2

Wireless Distribution System(WDS)

EncrypType	TKIP
Pass Phrase	88888888
AP MAC Address	00:B0:CC:17:B4:86

- **Basic wireless Settings**

✧ ***Network Mode***: Select one mode from the following. The default is 11b/g/n mode.

✧ ***11b mode***: Allow the wireless client to connect with the device in 11b mode at the maximum speed of 11Mbps.

✧ ***11g mode***: Allow the 11g/11n-compliant client device to connect with the AP at the maximum speed of 54Mbps.

✧ ***11b/g mode***: Allow the 11b/g-compliant client device to connect with the AP with auto-negotiation speed, and 11n wireless client to connect the device with 11g speed.

- ✧ ***11b/g/n mode：*** Allow 11b/g/n-compliant client device to connect with the AP with auto- negotiation speed.
- ✧ ***Main SSID：*** SSID (Service Set Identifier) is the unique name of the wireless network. This device has two SSID and the main SSID is necessary.
- ✧ ***Minor SSID：*** It is optional.
- ✧ ***Broadcast SSID***： If disable broadcast SSID is selected, the AP will not broadcast its own SSID. If wireless connection requests approaches, users need to enter the SSID by manual.
- ✧ ***BSSID：*** Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.
- ✧ ***Channel：***Specify the effective channel (from 1 to 13\Auto) of the wireless network.
- ✧ ***Extension channel：*** To increase data throughput of wireless network, the

extension channel range is used in 11n mode.

- **Wireless Distribution System (WDS)Setting**

✧ ***Encryption Type*****：** Select the data encryption method from WEP, TKIP, AES or NONE. The default is NONE.

WEP Encryption Description

✧ ***WEP Key 1~4*****：** Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13 ASCII characters. Illegal character as "/" is not allowed.) Or 10/26 hex characters.

✧ ***Default Key*****：** Select one key from the four configured keys as the current available one.

TKIP Encryption Description

✧ ***Pass Phrase*****：** Enter the encrypted characters with 8-63 ASCII characters.

AES Encryption Description

✧ ***Pass Phrase*****：** Enter the encrypted characters with 8-63 ASCII characters.

✧ ***AP MAC Address*****：** Input the MAC address of remote access point by manual or scan.

Open Scan**：** Enable scan to obtain remote AP MAC address, select one and Click “Save” to complete this part’s setting. The AP will reboot automatically, the setting will go into effect.

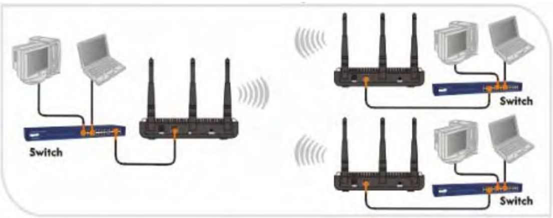
Note: In this mode, the two devices should keep the same channel and encryption method.

4.1.3 P2MP Bridge Mode

The P2MP Bridge Mode which connects scattered wired network together is more complicated than P2P Bridge mode. P2MP usually transmit wireless signals from one access point, and other access points are in charge of receiving signals so as to share network resource. Support up to 4 remote access point connection. In this mode, wireless clients are not allowed to connect.

4.1.3.1 Application and Network Topology

P2MP Bridge mode can connect multiple wireless access point together without cabling. If “Root AP” is configured as P2MP bridge mode, other (less than 4) remote access points should select P2P bridge modes. The topology shows below:

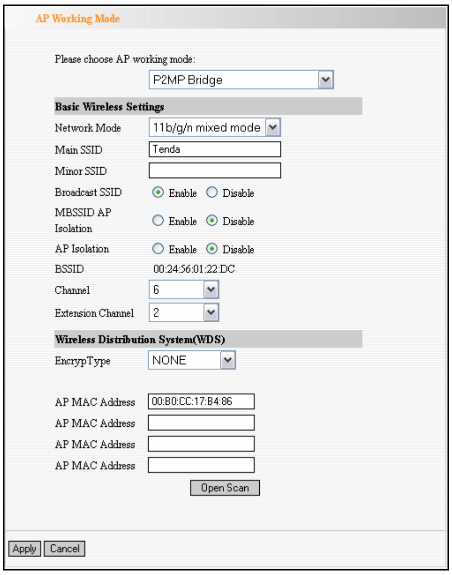


Note: In P2P Bridge and P2MP bridge mode, at

least two wireless APs are needed. For better performance, it is recommended to use the AP with same model.

4.1.3.2 P2MP Setting

In the working mode, select “P2MP Bridge” to enter the next screen.



AP Working Mode

Please choose AP working mode: P2MP Bridge

Basic Wireless Settings

Network Mode: 11b/g/n mixed mode

Main SSID: Tenda

Minor SSID:

Broadcast SSID: ● Enable ○ Disable

MBSSID AP Isolation: ○ Enable ● Disable

AP Isolation: ○ Enable ● Disable

BSSID: 00:24:56:01:22:DC

Channel: 6

Extension Channel: 2

Wireless Distribution System(WDS)

EncrypType: NONE

AP MAC Address: 00:B0:CC:17:B4:86

AP MAC Address:

AP MAC Address:

AP MAC Address:

- **Basic wireless Settings**

- ✧ ***Network Mode***: Select one mode from the following. The default is 11b/g/n mode.
- ✧ ***11b mode***: Allow the wireless client to connect with the device in 11b mode at the maximum speed of 11Mbps.
- ✧ ***11g mode***: Allow the 11g/11n-compliant client device to connect with the AP at the maximum speed of 54Mbps.
- ✧ ***11b/g mode***: Allow the 11b/g-compliant client device to connect with the AP with auto-negotiation speed, and 11n wireless client to connect the device with 11g speed.
- ✧ ***11b/g/n mode***: Allow 11b/g/n-compliant client device to connect with the AP with auto- negotiation speed.
- ✧ ***Main SSID***: SSID (Service Set Identifier) is the unique name of the wireless network. This device has two SSID and the main SSID is necessary.
- ✧ ***Minor SSID***: It is optional.
- ✧ ***Broadcast SSID***: If disable broadcast SSID is selected, the AP will not broadcast its own SSID. If wireless connection requests approaches, users need to enter the SSID by manual.
- ✧ ***BSSID***: Basic Service Set Identifier of

wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.

- ✧ ***Channel*:** Specify the effective channel (from 1 to 13\Auto) of the wireless network.
- ✧ ***Extension channel*:** To increase data throughput of wireless network, the extension channel range is used in 11n mode.

- ● **Wireless Distribution System (WDS)Setting**

- ✧ ***Encryption Type*：** Select the data encryption method from WEP, TKIP, AES or NONE. The default is NONE.

WEP Encryption Description

- ✧ ***WEP Key 1~4*：** Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13 ASCII characters. Illegal character as "/" is not allowed.) Or 10/26 hex characters.
- ✧ ***Default Key*：** Select one key from the four configured keys as the current available one.

TKIP Encryption Description

- ✧ ***Pass Phrase*：** Enter the encrypted characters with 8-63 ASCII characters.

AES Encryption Description

- ***Pass Phrase*：** Enter the encrypted characters with 8-63 ASCII characters.

- ***AP MAC Address*：** Input the MAC addresses (no more than four) of remote access points by manual or scan.

  ***MAC Address 1*：** Input AP1's MAC address;
  ***MAC Address 2*：** Input AP2's MAC address;
  ***MAC Address 3*：** Input AP3's MAC address;
  ***MAC Address 4*：** Input AP4's MAC address;

  ***Open Scan*：** Enable scan to obtain remote AP MAC address, select one and Click "Save" to complete this part's setting. The AP will reboot automatically, the setting will go into effect.

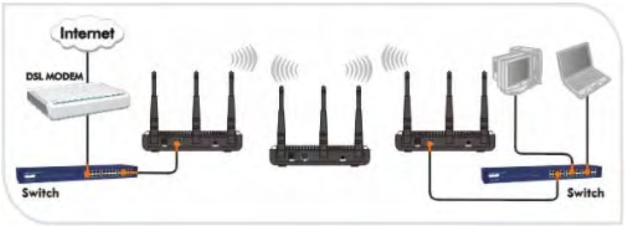
Note: In this mode, the two devices should keep the same channel and encryption method.

4.1.4 Wireless Repeater Mode

Repeater Mode can repeat and amplify wireless signals to extend wireless network coverage. In this mode, wireless clients are allowed to connect.

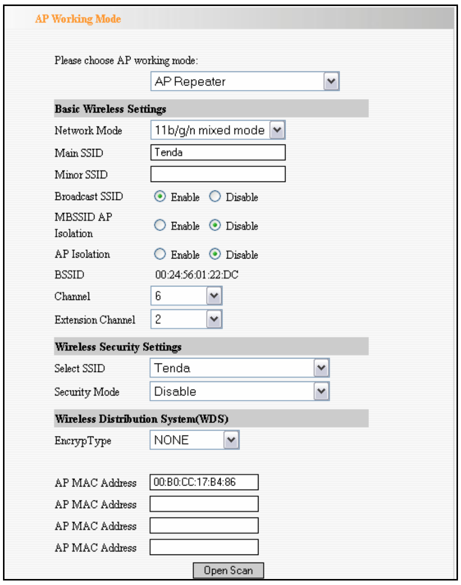
4.1.4.1 Application and Topology Plan

When two LAN's transmission distance is over the wireless device's maximum transmission value, or there is much block among devices, you can use the Repeater mode to deal with these problems by adding MAC addresses. The topology shows below:



4.1.4.2 Repeater Mode Setting

In the working mode, select "AP Repeater" to enter the next window.



AP Working Mode

Please choose AP working mode:

AP Repeater

Basic Wireless Settings	
Network Mode	11b/g/n mixed mode
Main SSID	Tenda
Minor SSID	
Broadcast SSID	● Enable ○ Disable
MBSSID AP Isolation	○ Enable ● Disable
AP Isolation	○ Enable ● Disable
BSSID	00:24:56:01:22:DC
Channel	6
Extension Channel	2
Wireless Security Settings	
Select SSID	Tenda
Security Mode	Disable
Wireless Distribution System(WDS)	
EncrypType	NONE
AP MAC Address	00:B0:CC:17:B4:86
AP MAC Address	
AP MAC Address	
AP MAC Address	

- **Basic wireless Settings**
  - ✧ ***Network Mode***: Select one mode from the following. The default is 11b/g/n mode.
  - ✧ ***11b mode:*** Allow the wireless client to connect with the device in 11b mode at the maximum speed of 11Mbps.
  - ✧ ***11g mode:*** Allow the 11g/11n-compliant client device to connect with the AP at the maximum speed of 54Mbps.

- ✧ ***11b/g mode：*** Allow the 11b/g-compliant client device to connect with the AP with auto-negotiation speed, and 11n wireless client to connect the device with 11g speed.
- ✧ ***11b/g/n mode：*** Allow 11b/g/n-compliant client device to connect with the AP with auto- negotiation speed.
- ✧ ***Main SSID：*** SSID (Service Set Identifier) is the unique name of the wireless network. This device has two SSID and the main SSID is necessary.
- ✧ ***Minor SSID：*** It is optional.
- ✧ ***Broadcast SSID***： If disable broadcast SSID is selected, the AP will not broadcast its own SSID. If wireless connection requests approaches, users need to enter the SSID by manual.
- ✧ ***MBSSID AP Isolation：*** One access control feature based on wireless MAC address. When this feature is enabled, wireless clients connected with the same SSID can not communicate with each other. For example, configure main SSID as AP1, minor SSID as AP2. PC1 and PC2 connect to AP1 via wireless

adapter, and configure PC1 and PC2 in the same segment. After the feature is enabled, two PCs can not communicate and share network resource each other, but they can communicate with wireless clients connected with AP2. **This feature is to isolate the communication of wireless clients connected with the same SSID.**

✧ ***AP Isolation:*** One access control feature based on wireless MAC address. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. This feature is deployed when you have many guests that frequent your wireless network. For example, configure main SSID as AP1, minor SSID as AP2. PC1 connects to AP1 via wireless adapter; PC2 connecting to AP2. After the feature is enabled, two PCs can not communicate and share network resource each other. **This feature is to isolate the communication of wireless clients connected with different SSID.**

Tip: If you want to isolate all connected wireless client's communication, please enable MBSSID AP and AP Isolation simultaneously.

- ✧ ***BSSID*：** Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.
- ✧ ***Channel*：** Specify the effective channel (from 1 to 13\Auto) of the wireless network.
- ✧ ***Extension channel*：** To increase data throughput of wireless network, the extension channel range is used in 11n mode.

- **Wireless Security Settings**
  - ✧ ***Select SSID*：** Select the SSID for security setting, main SSID or minor SSID.
  - ✧ ***Security Mode*:** select wireless encryption method, WEP, WPA-PSK, WPA2-PSK. (Note: when you select “Disable”, security mode can’t be used.) Here security setting is for wireless client’s encryption authentication. ***More details please refer to 4.1.1.2.***

- **Wireless Distribution System (WDS)Setting**
  - ✧ ***Encryption Type*：** Select the data

encryption method from WEP, TKIP, AES or NONE. The default is NONE.

WEP Encryption Description

✧ ***WEP Key 1~4*:** Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13 ASCII characters. Illegal character as "/" is not allowed.) Or 10/26 hex characters.

✧ ***Default Key*:** Select one key from the four configured keys as the current available one.

TKIP Encryption Description

✧ ***Pass Phrase* :** Enter the encrypted characters with 8-63 ASCII characters.

AES Encryption Description

✧ ***Pass Phrase* :** Enter the encrypted characters with 8-63 ASCII characters.

✧ ***AP MAC Address*:** Input the MAC addresses (no more than four) of remote access points by manual or scan.

***MAC Address 1*:** Input AP1's MAC address;

MAC Address 2： Input AP2's MAC address;
MAC Address 3： Input AP3's MAC address;
MAC Address 4： Input AP4's MAC address;

Open Scan： Enable scan to obtain remote AP MAC address, select one and Click "Save" to complete this part's setting. The AP will reboot automatically, the setting will go into effect.

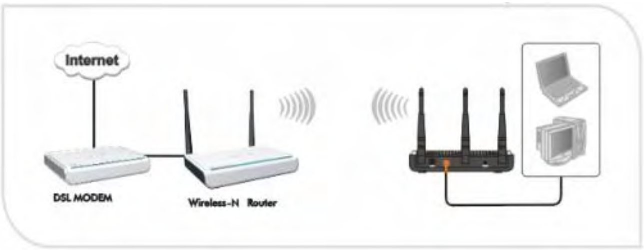
Note: 1. in this mode, the two devices should keep the same channel and encryption method.
2. AP-Security Setting can differentiate with WDS-Security setting in encryption method and secrete key.

4.1.5 Wireless Client Mode

In this mode, connect the device's LAN port to wired network adapter port. In this case, AP is used as a wireless Adapter. When you select this mode, please keep the device and the connecting network in the same segment.

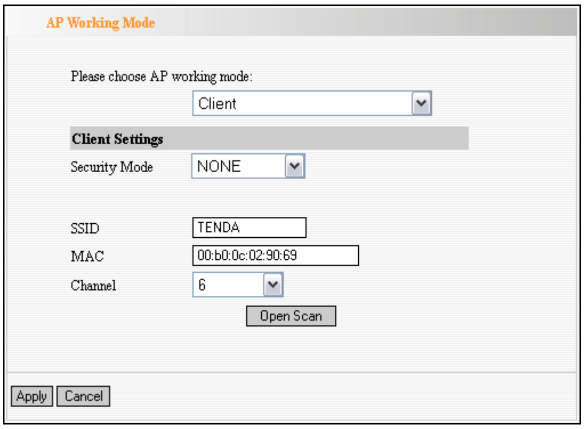
4.1.5.1 Application and Topology Plan

If you select this mode to establish your network, please follow the next topology plan:



4.1.5.2 Client Mode Settings

In the working mode, select “Client” to enter the next window.



AP Working Mode

Please choose AP working mode: Client

Client Settings

Security Mode: NONE

SSID: TENDA

MAC: 00:b0:0c:02:90:69

Channel: 6

✧ ***Security Mode***：Select wireless encryption method from WEP, WPA-PSK and WPA2- PSK (Note: when you select “NONE”, the security mode is disabled.).

WEP Encryption Description

✧ ***WEP Type***：Select the connected device’s WEP authentication method. OPEN and SHARED is supporte*d.*

✧ ***WEP Key1~4***：Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13 ASCII characters. Illegal character as “/” is not allowed.) Or 10/26 hex characters.

- ✧ ***Default Key：*** Select one key from the four configured keys as the current available one.

WPA-PSK Encryption Description

- ✧ ***WPA-WPA2 Algorithms：*** Select one from TKIP and AES.
- ✧ ***Pass Phrase ：*** Enter the encrypted characters with 8-63 ASCII characters.

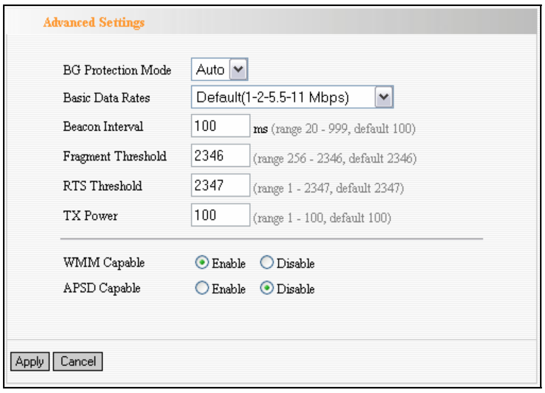
WPA2-PSK Encryption Description

- ✧ ***WPA-WPA2 Algorithms：*** Select one from TKIP and AES. Usually WPA2-personal supports AES.
- ✧ ***Pass Phrase ：*** Enter the encrypted characters with 8-63 ASCII characters.
- ✧ ***SSID：*** SSID for connected device, obtained by scan or manual.
- ✧ ***MAC:*** The MAC address for connected device, obtained by scan or manual.
- ✧ ***Channel：***Specify the effective channel (from 1 to 13\Auto) of the wireless network, obtained by scan or manual.

- ✧ ***Open Scan*：** Enable scan to obtain remote AP MAC address. Select one and Click “Save” to complete this part’s setting. The AP will reboot automatically, and then the setting will go into effect.

4.2 Advanced Settings

This section mainly deals with wireless advanced settings, including Speed, Beacon Interval, Fragment Threshold, etc. Select “Wireless Setting->Advanced Setting” to enter the following screen:



Advanced Settings

BG Protection Mode: Auto
Basic Data Rates: Default(1-2-5.5-11 Mbps)
Beacon Interval: 100 ms (range 20 - 999, default 100)
Fragment Threshold: 2346 (range 256 - 2346, default 2346)
RTS Threshold: 2347 (range 1 - 2347, default 2347)
TX Power: 100 (range 1 - 100, default 100)

WMM Capable: ● Enable ○ Disable
APSD Capable: ○ Enable ● Disable

Setting Explanation:

✧ ***BG Protection Mode:*** For 11b/g wireless client, it is easier to connect with 11n wireless device. The default is “Auto”.

✧ ***Basic Data Rates:*** In term of different requirements, you can select one of the suitable Basic Data Rates from the drop-down menu. Here, default value is (1-2-5.5-11Mbps…). It is recommended not to modify the default value.

✧ ***Beacon Interval*：** The frequency interval of the beacon, which is a packet broadcast by an AP to synchronize a wireless network. The default value is 100 ms.

✧ ***Fragment Threshold*：** The fragmentation threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if the arrival is bigger than the threshold setting. The default size is 2346 bytes.

✧ ***RTS Threshold*：** RTS stands for "Request to send". This parameter controls what size data packet the frequency protocol issues to RTS packet. If the device works in SOHO, do not modify the default value.

✧ ***TX Power*：** Set the wireless output power level. The default value is 100.

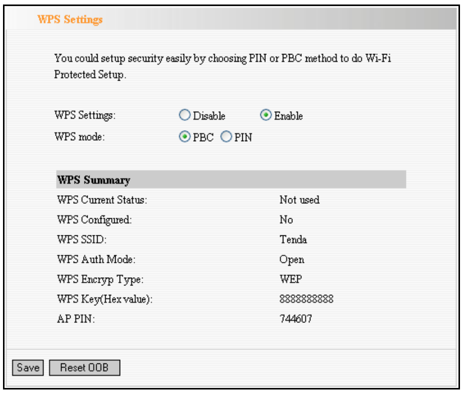
✧ ***WMM Capable*：** To enhance wireless multimedia transfer performance (0n-line video and voice). If you are not clear about this, enable it.

✧ ***APSD Capable*：** It is used for auto power-saved service. The default is disabled.

4.3 WPS Settings

WPS (Wi-Fi Protected Setting) can be easy and quick to establish the connection between the wireless network clients and the device through encrypted contents. The users only enter the PIN code or the WPA button on the front panel to configure it without selecting encryption method and secret keys by manual.

In the “Wireless settings” menu, click “WPS settings” to enter the next screen.



WPS Settings

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Settings: ○ Disable ● Enable

WPS mode: ● PBC ○ PIN

WPS Summary	
WPS Current Status:	Not used
WPS Configured:	No
WPS SSID:	Tenda
WPS Auth Mode:	Open
WPS Encryp Type:	WEP
WPS Key(Hex value):	8888888888
AP PIN:	744607

Setting Explanation:

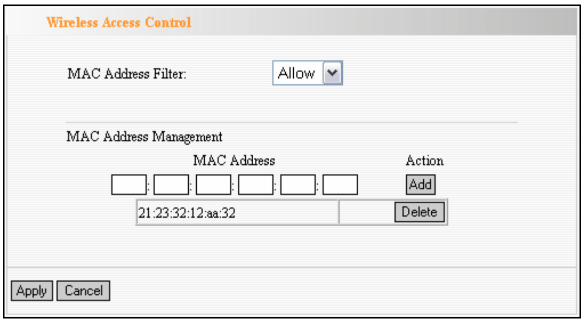
✧ ***WPS settings:*** To enable or disable WPS function. The default is “disable”.

- ✧ ***WPS mode*** **：** Provide two ways: PBC (Push-Button Configuration) and PIN code.
- ✧ ***PBC:*** Select the PBC or press the WPS button on the front panel of the device for about one second (Press the button for about one second and WPS indicator will be blinking for 2 minutes, which means the WPS is enabled. During the blinking time, you can enable another device to implement the WPS/PBC negotiation between them. At present, the WPS only supports up to 32 clients access. Two minutes later, the WPS indicator will be off. If more clients are added, repeat the above steps).
- ✧ ***PIN:*** If this option is enabled, you need to enter a wireless client's PIN code in the field and keep the same code in the WPS client. The user is required to enter an 8-digit PIN Code.
- ✧ ***WPS summary:*** Show Wi-Fi current protection state, authentication mode, encryption method, etc.

Note：Press the WPS/Reset button for 1 second on the front panel to run PBC. Press for 7 seconds, the device's setting will restore to default setting. The access client has to support WPS function when you implement WPS settings.

4.4 Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management. Select “Wireless Setting->Access Control” to display the following screen:



Wireless Access Control

MAC Address Filter: Allow

MAC Address Management

MAC Address	Action
□:□:□:□:□:□	Add
21:23:32:12:aa:32	Delete

Setting Explanation

✧ ***MAC Address Filter*：** Enable/disable MAC address filter. Select “Close” to malfunction MAC address; “disable” to prevent the MAC addresses in the list from accessing the wireless network; “Allow” to allow the MAC address in the list to access the wireless network.

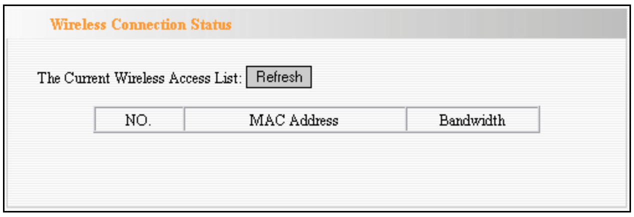
✧ ***MAC Address Management*：** Input the MAC address to implement the filter policy. Click “Add” to finish the MAC add operation.

✧ ***MAC list***： Show the added MAC address. You can add or delete them.

Note: This AP can support no more than 32 MAC addresses.

4.5 Connection Status

This page shows wireless client's connection status, including MAC address, Channel bandwidth, etc. Select "Wireless Setting->connection status" to enter the following screen:



Wireless Connection Status

The Current Wireless Access List:

NO.	MAC Address	Bandwidth

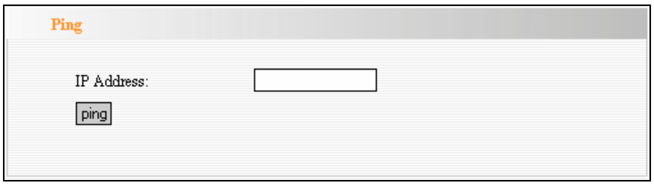
Explanation:

✧ ***MAC Address:*** Shows current connecting host's MAC address.

✧ ***Bandwidth:*** Shows current connecting host's (wireless client) bandwidth (20MHz or 40MHz).

4.6 PING

Ping is used to check device’s connectivity. If the connecting device has established connection with AP, the result will show “connected”, otherwise, shows “destination host unreachable”. Select “Wireless Setting->Ping” to show the following window:



Explanation:

✧ ***IP Address:*** Enter the device’s IP address.

✧ ***ping :*** Click “Diagnose” button to show connectivity result after a few seconds. This is to check the connectivity between devices for trouble shooting.

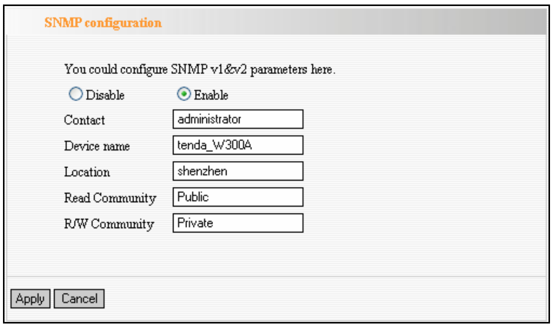
Chapter 5 SNMP Setting

5.1 SNMP Introduction

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, such as servers, printers, hubs, switches, and routers from a management host. Managed devices that support SNMP including software are referred to as an SNMP agent, which usually interacts with third-party SNMP management software to enable the sharing of network status information between monitored devices and applications and the SNMP management system. A defined collection of variables (managed objects) are maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

5.2 SNMP Setting

This device supports SNMP v1 and SNMP v2c. Please click "SNMP Setting" in the left page to enter the following window:



SNMP configuration

You could configure SNMP v1&v2 parameters here.

○ Disable ● Enable

Contact	administrator
Device name	tenda_W300A
Location	shenzhen
Read Community	Public
R/W Community	Private

Click "enable" or "disable" to enable and disable SNMP management.

Setting Explanation:

✧ ***Contact:*** Set the name to access the AP. Usually set the administrator's name.

✧ ***Device Name:*** Set the AP's name, such as Tenda_300A.

✧ ***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.

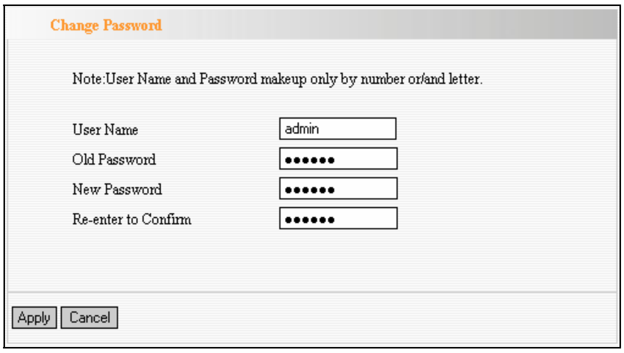
✧ ***Read/Write Community:*** Indicates the community read/write access string to permit reading and re-writing this AP's SNMP information. The default is Private.

Chapter 6 System Tools

This section focuses on how to maintain AP, including Restore to Factory Default Setting, Backup/Restore, Firmware Upgrade, Reboot, Password Change, Syslog.

6.1 Password Change

This section is to set a new user name and password to better secure your device and network. Click "Apply" to finish changing password.



Change Password

Note:User Name and Password makeup only by number or/and letter.

User Name	admin
Old Password	••••••
New Password	••••••
Re-enter to Confirm	••••••

User Name: Enter a new user name for the device.

Old Password: Enter the old password.

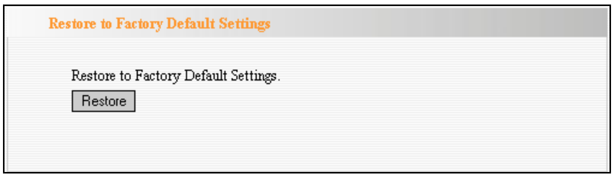
New Password: Enter a new password.
Re-enter to Confirm: Re-enter to confirm the new password.

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

6.2 Restore to Factory

This button is to reset all configurations to the default values. It means the device will lose all the settings you have set.

Restore: Click this button to restore to default settings.
Factory Default Settings:
User Name: admin
Password: admin
IP Address: 192.168.0.254
Subnet Mask: 255.255.255.0



Restore to Factory Default Settings

Restore to Factory Default Settings.

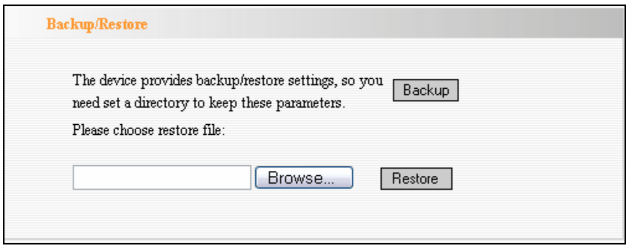
6.3 Backup/Restore

The device provides backup/restore settings, so you need set a directory to keep these settings.

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

Browse: 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.



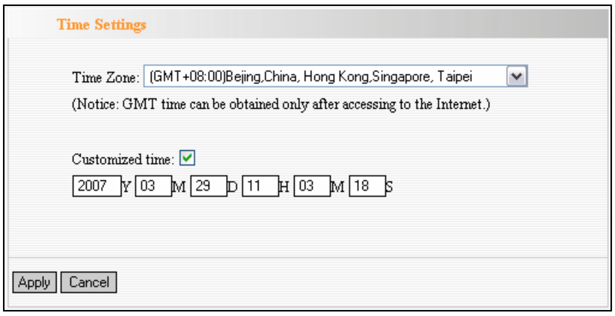
Backup/Restore

The device provides backup/restore settings, so you need set a directory to keep these parameters.

Please choose restore file:

6.4 Time Settings

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.



Time Settings

Time Zone: (GMT+08:00)Bejing,China, Hong Kong,Singapore, Taipei

(Notice: GMT time can be obtained only after accessing to the Internet.)

Customized time: ☑

2007 Y 03 M 29 D 11 H 03 M 18 S

Setting Explanation:

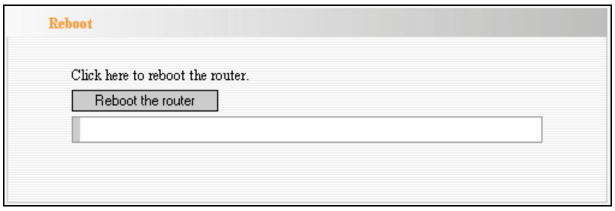
✧ **Time Zone:** Select your time zone from the drop-down menu.

✧ **Customized time:** Enter the time you customize.

6.5 Reboot System

This page is used to reboot wireless access point. Rebooting the device makes the settings configured go into effect.

Reboot: Click this button to reboot the device.

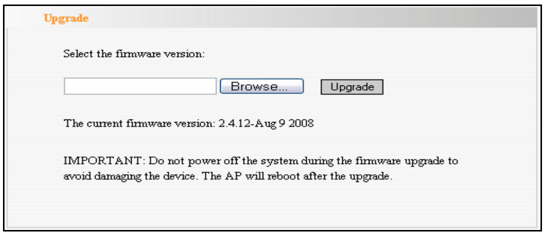


Reboot

Click here to reboot the router.

6.6 Firmware Upgrade

The device provides the firmware upgrade by clicking the "Upgrade" after browsing for the firmware upgrade packet which you can download from www.tenda.cn. After the upgrade is completed, the device will reboot automatically.



Upgrade

Select the firmware version:

The current firmware version: 2.4.12-Aug 9 2008

IMPORTANT: Do not power off the system during the firmware upgrade to avoid damaging the device. The AP will reboot after the upgrade.

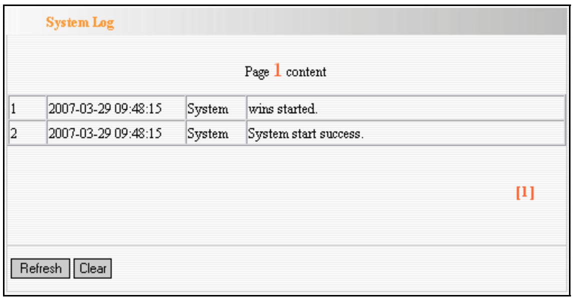
Upgrade Steps:

1. Download the higher firmware version from our website: www.tenda.cn.
2. Extract the firmware file on your computer.
3. On the Firmware Upgrade screen, enter the location directory of the firmware file in the field provided, or click the **Browse** button and find the file.
4. Click **Upgrade** button, and follow the on-screen instructions.
5. After the upgrade is completed, the device will reboot automatically.

IMPORTANT: Do not power off the system during the firmware upgrade to avoid damaging the device.

6.7 Syslog

The section is to view the system log. Click the "Refresh" to update the log. Click "Clear" to clear all shown information. If the log is over 150 records, it will clear them automatically.



1	2007-03-29 09:48:15	System	wins started.
2	2007-03-29 09:48:15	System	System start success.

Refresh: Click this button to update the log.

Clear: Click this button to clear the current log.

Appendix I: Glossary

Access Point(AP): Any entity that has station functionality and provides access to the distribution services, via the wireless medium(WM) for associated stations.

Channel: An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume of space, with other instances of medium use(on other channels) by other instances of the same physical layer (PHY),with an acceptably low frame error ratio(FER) due to mutual interference.

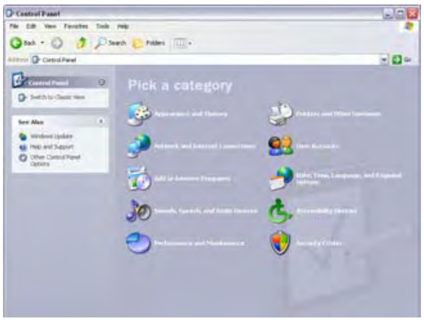
SSID: Service Set identifier. An SSID is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and identical for all devices within the network. It is case-sensitive and must not exceed 20 characters (use any of the characters on the keyboard).Make sure this setting is the same for all devices in your wireless network.

WEP: Wired Equivalent Privacy (WEP) is the method for secure wireless data transmission. WEP adds data encryption to every single packet transmitted in the wireless network. The 40bit and 64bit encryption are the same because of out 64 bits, 40 bits are private. Conversely, 104 and 128 bit are the same. WEP uses a common KEY to encode the data. Therefore, all devices on a wireless network must use the same key and same type of encryption. There are 2 methods for entering the KEY; one is to enter a 16-bit HEX digit. Using this method, users must enter a 10-digit number (for 64-bit) or 26-digit number (for 128-bit) in the KEY field. Users must select the same key number for all devices. The other method is to enter a text and let the computer generate the WEP key for you. However, since each product use different method for key generation, it might not work for different products. Therefore, it is NOT recommend using.

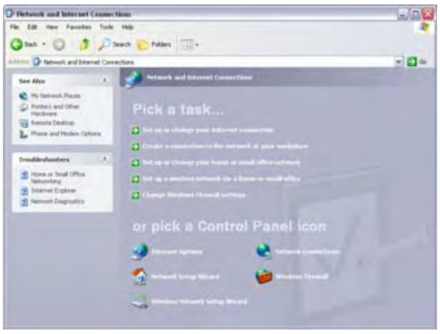
WPA/WPA2: A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.

Appendix II: TCP/IP Address Setting (Take Winxp as example)

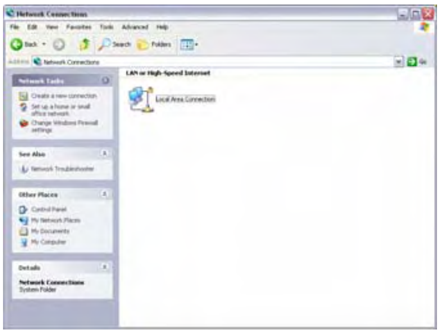
Click the “Start—>Settings—>Control Panel” (Fig- 1):



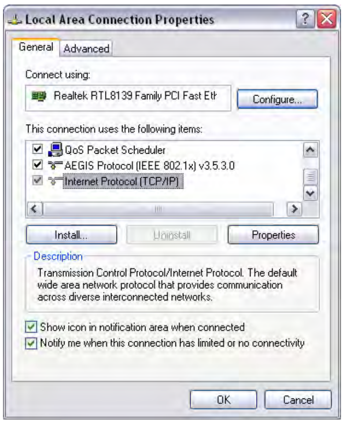
Click “Network and Internet Connections”, the windows as below will appear (Fig- 2):


Network and Internet Connections
Pick a task...
or pick a Control Panel icon

Click the “Network Connections”, as Fig-3:



Choose “Local Area Connection”, right-click on the icon, choose the “Properties”, then the “Local Area Connection Properties”windows appear, choose the “Internet Protocol (TCP/IP)” in the “This connection uses the following items”, click the “Properties”.



Local Area Connection Properties

General | Advanced

Connect using:

Realtek RTL8139 Family PCI Fast Eth

Configure...

This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.5.3.0
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

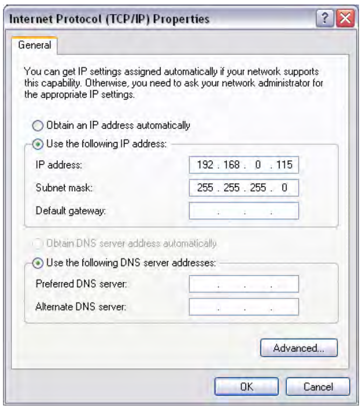
Description

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

OK | Cancel

Choose the “Use the following IP address”, enter the IP address as: 192.168.0.xxx. (xxx ranges 1~253), Subnet mask is: 255.255.255.0(As Showed in Fig- 5)



Internet Protocol (TCP/IP) Properties

General

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: 192 . 168 . 0 . 115

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Click “OK” to apply and return to the “Local Area Connection Properties” windows.

Continue click “OK” to exit the setting windows.

FCC Statement

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 or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

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

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

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example- use only shielded interface cables when connecting to computer or peripheral devices).

"The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter."

FCC 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 the minimum distance of 20 cm from user and bystanders. Operation is subject to the following two conditions:

1) This device may not cause interference, and

2) This device must accept any interference, including interference that may cause undesired operation of the device.

Caution!

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user authority to operate the equipment.

Canada Statement

This Device complies with RSS-210 of the IC Rules; Operation is subject to the following two conditions:
(1). This device may not cause interference and
(2). This device must accept any interference received,, including interference that may cause undesired operation.

This device has been designed to operate with an antenna having a maximum gain of 3.0 dBi.
Antenna having a higher gain is strictly prohibited per regulations of Industry Canada.
The required antenna impedance is 50 ohms
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication
To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding