Tenda®

User Guide

www.tendacn.com

Wireless N150 Outdoor Long Range AP/Router

Copyright Statement

Tenda® is the registered trademark of Shenzhen Tenda Technology Co., Ltd. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. Without prior expressed written permission from Shenzhen Tenda Technology Co., Ltd, any individual or party is not allowed to copy, plagiarize, reproduce, or translate it into other languages.

All photos and product specifications mentioned in this manual are for references only. Upgrades of software and hardware may occur; Tenda reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes. If you would like to know more about our product information, please visit our website at http://www.tendacn.com.

Table of Contents

Chapter 1 Product Overview

Thanks for purchasing thisW1500A Wireless N150 Outdoor Long Range AP/Router.

The Tenda W1500A is an outdoor long range wireless AP/router with wireless speed up to 150M. Combining the function of a wireless router, wireless AP, WISP, Client+AP and WDS, etc. the device nicely stands out in outdoor long range wireless connections, P2P, P2MP networking, wireless monitoring applications and much more.The W1500A is housed in an IP64 water/dust-proof enclosure. Also, it is lightning proof and power tunable. In addition to internal antenna design, it comes with an optional external antenna connector for DIY or upgrade. Plus, it is PoE capable and can be reset remotely.

1.1 Features

- Compliant with IEEE802.11n and backward compatible with IEEE802.11g/b
- Up to 150Mbps over 2.4G
- 5 operating modes: Wireless Router, Wireless AP, Wireless WAN (WISP), Universal Repeater (Client+AP) and Bridge
- Internal 10dBi directional antenna; plus optional external RP-SMA antenna connector for DIY or upgrade (To use an external antenna, you must first shift antenna type from internal to external on wireless module)
- Power tunable at 3 levels: high, medium and low
- Able to be powered by a passive PoE injector; flexibly deploy your AP at ease
- 6000V lightning proof design (bidirectional);
- Provides encryption methods of 64-/128-bit WEP, WPA-PSK and WPA2-PSK, etc to secure your wireless network
- Provides 1 WAN/LAN/PoE interchangeable port and 1 separate LAN port

- Wireless Roaming technology to ensure high-efficiency wireless connectivity
- Access Control based on MAC address
- Provides logs to record device's usage status;
- Watchdog helps to recover system upon network failure
- Able to reset AP using the Reset button on the PoE injector
- Allow/disallow specified PCs on LAN to access Internet while operating in Router Mode
- Support virtual server and DMZ host when operating in Router Mode
- Support internal firewall to block attacks from hackers when operating in Router Mode

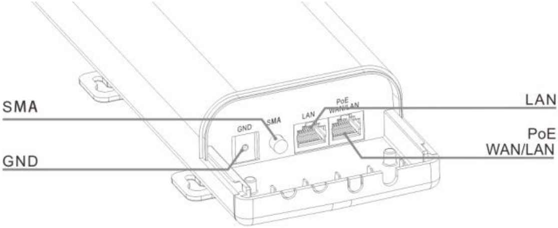
1.2 Package Content

Unpack the box and verify the following items:

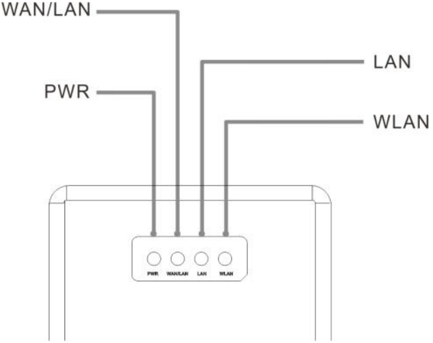
- W1500A x 1
- Screw x 2
- Nylon Ligature x 2
- Plastic Bag x 2
- Ethernet Cable x 1
- Power Adapter x 1
- Injector x 1
- Installation Guide x 1

If any of the above items are incorrect, missing, or damaged, please contact your Tenda reseller for immediate replacement.

1.3 Panel Overview



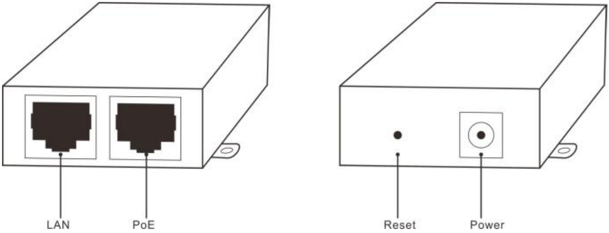
- **LAN/WAN/POE:** Provides 1 WAN/LAN/PoE interchangeable port, which functions as a WAN/PoE interchangeable port in router mode and a LAN/PoE port in AP mode.
- **LAN:** Provides 1 10/100M LAN port.
- **SMA interface**：RP-SMA connector for external antenna.
- **GND**: Connect GND port on device to the ground using a copper wire for better lightning-proof



LEDs are described as below:

LED	Status	Description
PWR	A solid blue light	Device has electrical power
WAN/LAN	A solid blue light	Ethernet cable is connected
	A blinking blue light	Transferring data
LAN	A solid blue light	Ethernet cable is connected
	A blinking blue light	Transferring data
WLAN	Blue	Transmitting wireless signal at a high power level
	Pink	Transmitting wireless signal at a medium power level
	Red	Transmitting wireless signal at a low power level

Injector Overview



- **POE:** Power over Ethernet port.
- **LAN/WAN:** 100M Ethernet port.
- **Reset:** Pressing it for 8-10s restores device to factory default settings.
- **Power:** Power connector**.**

Chapter 2 Hardware Install

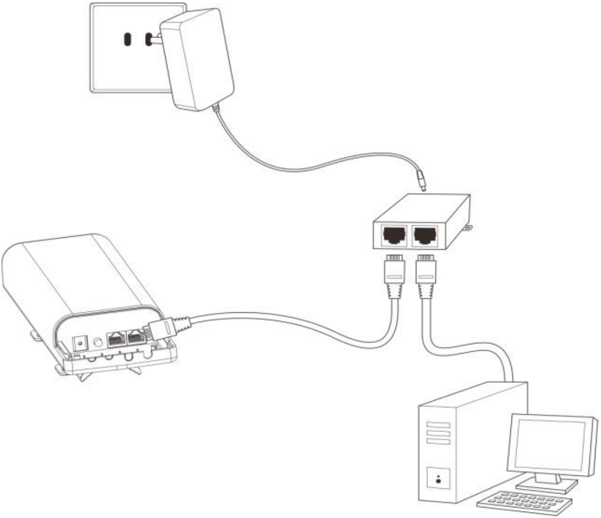
2.1 Hardware Install

Before you start configuring the device, follow below steps to install device. For extended wireless coverage, use an external omni-directional antenna and place device in the center of the area for better performance; to implement long range P2P or P2MP wireless bridge, use the internal directional antenna and position device properly for better performance.

2.1.1 Connect device to a power source

The device comes with a PoE injector. Please use it to power the device.

2.1.2 Network Connection



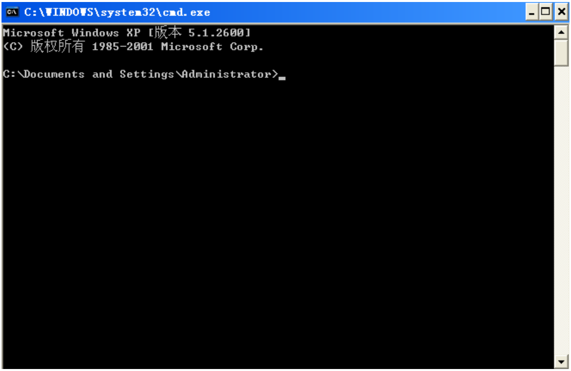
1. Connect the LAN/WAN/POE port on device to the PoE port on the injector using an Ethernet cable.

2. Connect PC to injector's LAN port using an Ethernet cable or wirelessly to the device via the SSID (The default SSID can be found on the label on the back of the device and is not encrypted by default).

Note:

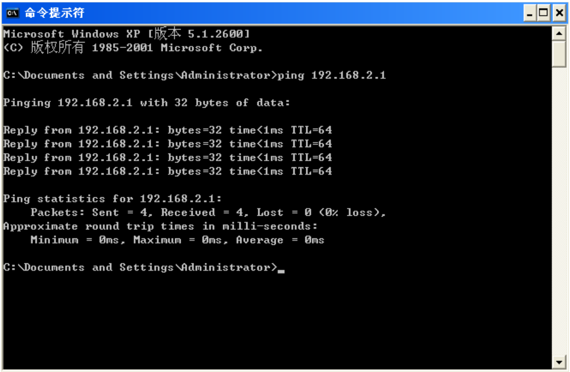
Device operates in AP mode by default. So you need to manually configure a static IP address for your PC. AP's LAN IP address is preset to 192.168.2.1 by default.So your PC's IP address should be 192.168.2.X (where X is any number between 2~254). For IP address configuration, see **Appendix 1**.

3. Use the Ping command to check the connectivity between your device and PC. Click Start -> Run, enter cmd and press Enter or click OK to enter interface below.



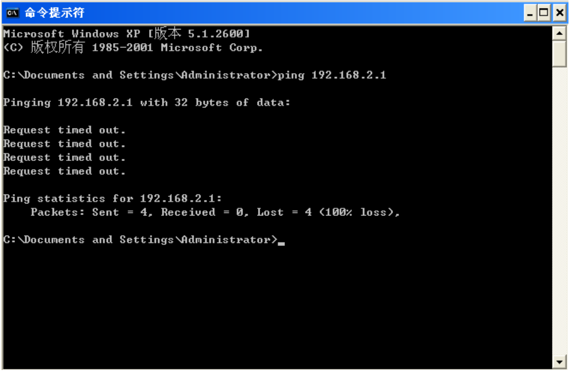
```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>_
```

4. Input **ping 192.168.2.1** and press **Enter**.



```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

If you get a screen as shown in the screenshot above, your PC and device are interconnected.



```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>_
```

If you get a screen as shown in the screenshot above, your PC and device are not interconnected. Please follow below steps to troubleshoot the problem.

1) Verify Ethernet cable connection

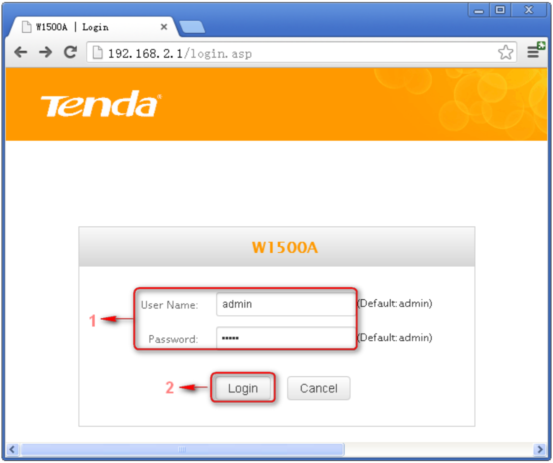
The LAN LED on the device and PC's adapter LED should be on.

2) Verify TCP/IP settings on your PC

To access device web utility while operating in AP mode or universal repeater mode, manually configure a static IP address for the PC. Just note that the IP address you configure must be on the same net segment as device LAN IP address. While in router mode, you can either manually specify an IP address for the PC or set it to **Obtain an IP address automatically**.

2.2 Quick Setup

The device is configurable and manageable through a web browser. Launch a web browser, in the address bar, input **192.168.2.1** and press **Enter**. Enter **admin** in both **User Name** and **Password** fields (Both default user name and password are admin).

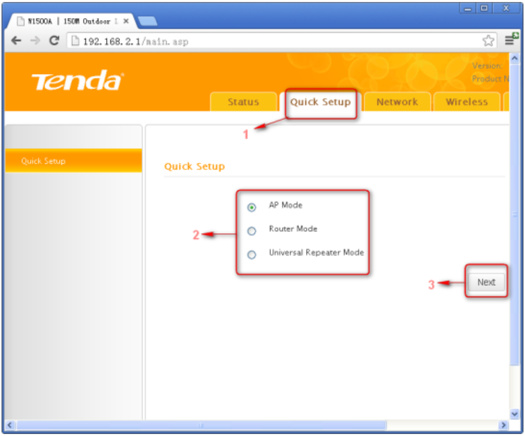


192.168.2.1/login.asp

User Name: admin (Default: admin)

Password: ••••• (Default: admin)

Click **Login** on the login window, and then click **Quick Setup**. Select a proper mode for device to operate on from **AP Mode**, **Router Mode** and **Universal Repeater Mode**.



Quick Setup

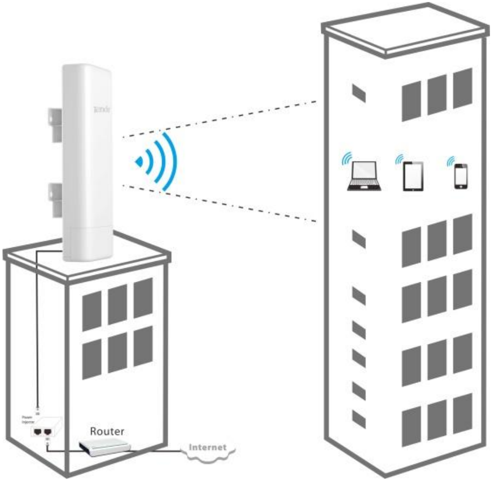
● AP Mode
○ Router Mode
○ Universal Repeater Mode

Operating Mode Overview:

- AP Mode: In this mode, the device converts the wired signal into wireless signals, extending existing network coverage. It works as a central access point for multiple wireless clients (generally, wireless adapters) concurrently.
- **Router Mode:** Operating in this mode, device functions as a regular wireless router. It supports PPPoE, dynamic IP (DHCP) , PPTP, L2TP and static IP Internet connection types and provide DHCP server feature that dynamically assigns IP addresses to DHCP-client-capable PCs for Internet connection sharing. Wireless WAN (WISP) and WDS features are available in this mode.
- **Universal Repeater Mode** （**Client+AP**） **:** Device wirelessly bridges an uplink device to repeat wireless and extend coverage.

2.2.1 AP Mode

See below for the typical network topology. Position device properly according to practical network environment.

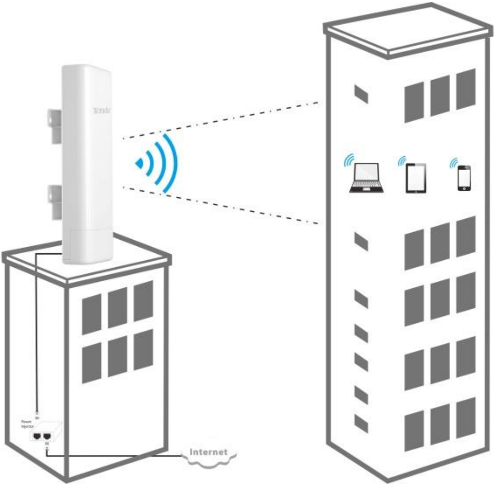


1. Connect the LAN/WAN/POE port on device to the POE port on the injector.
2. Connect the LAN port on the PoE injector to an uplink switch or router.
3. All PCs in the range will then be able to connect to this SSID wirelessly for Internet access.

Device operates in AP mode by default, so simply follow the topology above to establish th network. To configure other features like wireless, simply access the device web management utility. For details, see **Chapter**

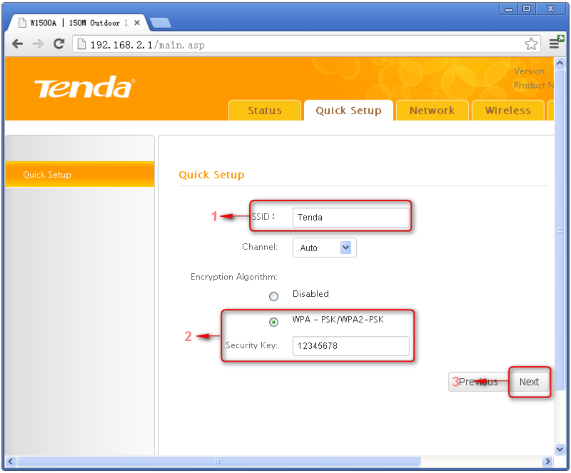
2.2.2 Router Mode

Typical Topology:



1. Connect the LAN/WAN/POE port on device to the POE port on the injector.
2. Connect the LAN port on PoE injector to ISP.
3. All PCs in the range will then be able to connect to this SSID wirelessly for Internet access.

1. Select **Router Mode**, click **Next** and then configure basic wireless settings including SSID, channel and security.



Quick Setup

SSID : Tenda

Channel: Auto

Encryption Algorithm:

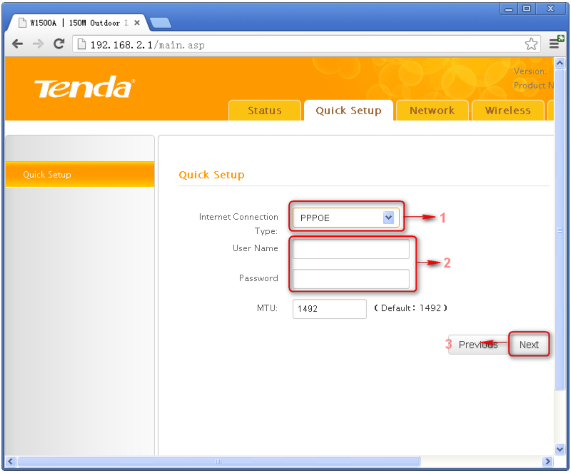
○ Disabled

● WPA – PSK/WPA2-PSK

Security Key: 12345678

- ➢ **SSID:** A SSID (Service Set Identifier) is the public name of a wireless network.
- ➢ **Channel:** For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or **Auto** to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list. The default is **Auto**.
- ➢ **Security Mode (Encryption Algorithm):** Select a proper encryption algorithm: WEP, WPA-PSK or WPA/WPA2-PSK. For more information, see **Chapter 4.**

2. Click **Next** and select a proper Internet connection type, say, **PPPoE**, **Static IP** or **DHCP**.



Quick Setup

Internet Connection Type: PPPOE

User Name

Password

MTU: 1492 (Default: 1492)

PPPoE: Select PPPoE (Point to Point Protocol over Ethernet) if you used to connect to the Internet using a broadband connection that requires a PPPoE user name and a PPPoE password. Simply enter the user name and password provided by your ISP in corresponding fields. If your ISP (Internet Service Providers) requires end-user's MAC address to access their network, you will then need to copy the registered MAC address to the device using the MAC Clone feature. Contact your ISP for help if you have any questions about these parameters.

Static IP: Select Static IP if your ISP provides all the needed IP info. You will need to enter the provided IP address, subnet mask, gateway address, and DNS address(es) in corresponding fields. If your ISP (Internet Service Providers) requires end-user's MAC address to access their network, you will then need to copy the registered MAC address to the device using the MAC

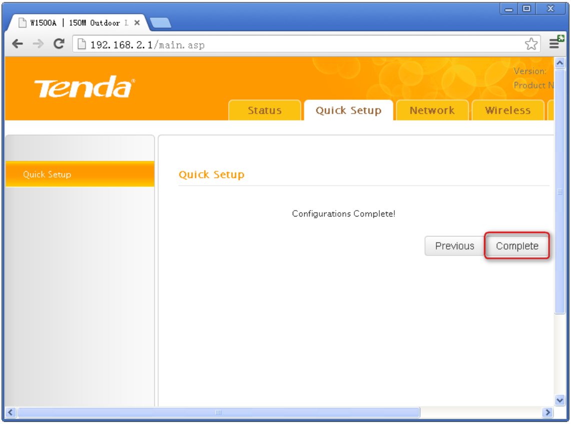
Clone feature. Contact your ISP for help if you have any questions about these parameters.

DHCP: Select DHCP (Dynamic IP) if you can access Internet as soon as your computer directly connects to an Internet-enabled ADSL/Cable modem. For this type, no configurations are required.

PPTP: Select PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. The PPTP connects a router to a VPN server

L2TP: Select L2TP (Layer 2 Tunneling Protocol) if your ISP uses an L2TP connection. The L2TP connects your router to a L2TP server

Click **Next** and then **Finish**. Click **OK** and device will restart and will then operate in **Router Mode**. Now set your local PCs to **Obtain an IP address automatically**.

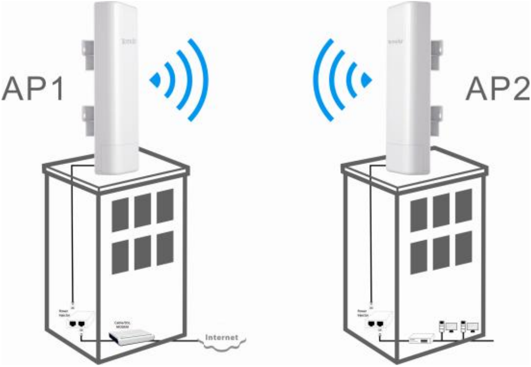


Quick Setup

Configurations Complete!

2.2.3 Universal Repeater Mode

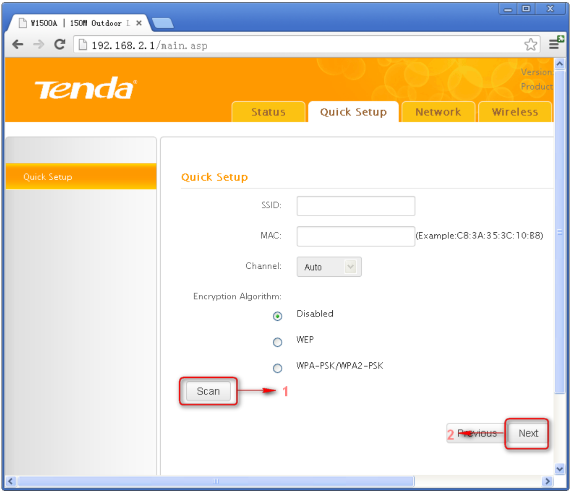
Typical Topology:



AP1 that operates in **Router Mode** has connected to Internet. AP2 connects to AP1 using the **Universal Repeater Mode**. So, clients that connect to AP2 can also access Internet.

1. Select **Universal Repeater Mode** on **Quick Setup** screen and then click **Next**.

2. Click **Scan** and all wireless networks in the area will be displayed. Select the SSID (the name of a wireless network) you wish to connect, say, **Tenda_2**, and then click **Next.**



Quick Setup

SSID:

MAC: (Example:C8:3A:35:3C:10:B8)

Channel: Auto

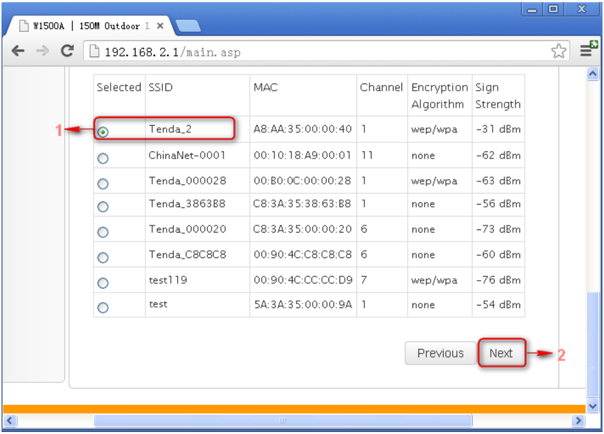
Encryption Algorithm:

● Disabled

○ WEP

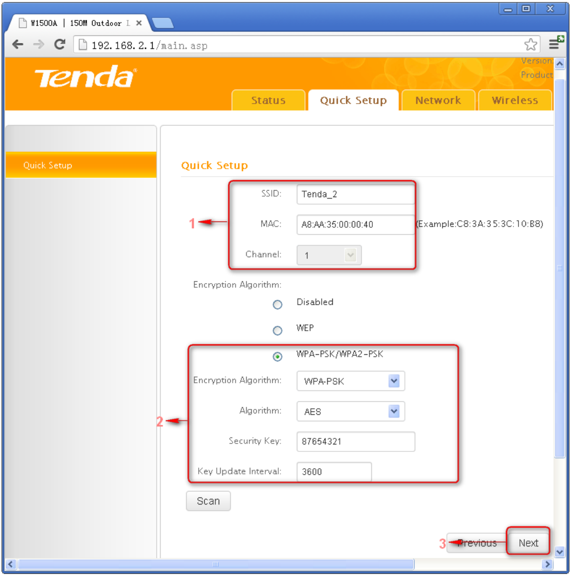
○ WPA-PSK/WPA2-PSK

SSID, MAC address and channel fields will be populated automatically.



Selected	SSID	MAC	Channel	Encryption Algorithm	Sign Strength
●	Tenda_2	A8:AA:35:00:00:40	1	wep/wpa	-31 dBm
○	ChinaNet-0001	00:10:18:A9:00:01	11	none	-62 dBm
○	Tenda_000028	00:B0:0C:00:00:28	1	wep/wpa	-63 dBm
○	Tenda_3863B8	C8:3A:35:38:63:B8	1	none	-56 dBm
○	Tenda_000020	C8:3A:35:00:00:20	6	none	-73 dBm
○	Tenda_C8C8C8	00:90:4C:C8:C8:C8	6	none	-60 dBm
○	test119	00:90:4C:CC:CC:D9	7	wep/wpa	-76 dBm
○	test	5A:3A:35:00:00:9A	1	none	-54 dBm

3. What you need to do is to configure the security settings. For example, the **Security Mode**, **Security Key** and **Key Update Interval** for the SSID **Tenda_2**is **WPA-PSK**, **87654321** and **3600s,** simply enter them.



Quick Setup

SSID: Tenda_2

MAC: A8:AA:35:00:00:40 (Example:C8:3A:35:3C:10:B8)

Channel: 1

Encryption Algorithm:

○ Disabled

○ WEP

● WPA-PSK/WPA2-PSK

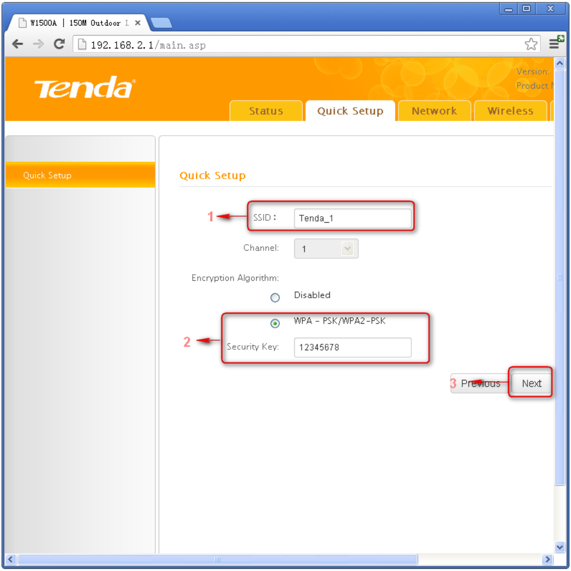
Encryption Algorithm: WPA-PSK

Algorithm: AES

Security Key: 87654321

Key Update Interval: 3600

4. Click **Next** and configure wireless settings for the device. Device MUST operate on the same channel as the uplink AP for successful implementation of the feature. The channel field on device greyed out in this mode. SSID and security settings are configurable (both can be different from the uplink device).



Quick Setup

SSID : Tenda_1

Channel: 1

Encryption Algorithm:

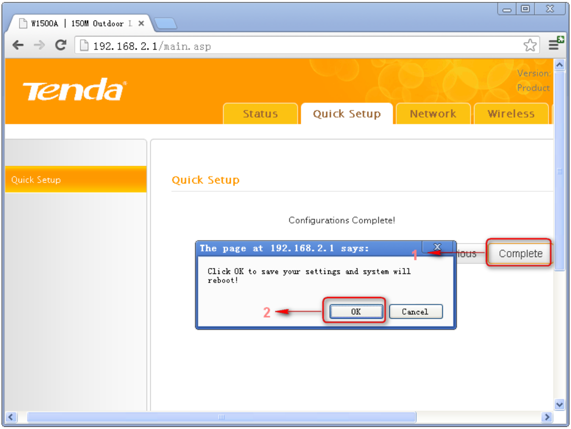
○ Disabled

● WPA - PSK/WPA2-PSK

Security Key: 12345678

5. Click **Next** and then **Finish**. Click **OK** and device will restart and will then operate in **Universal Repeater Mode**.

Now set your local PCs to **Obtain an IP address automatically** and these PCs will then use IP/gateway/DNS addresses assigned by the uplink device to access Internet.



Configurations Complete!

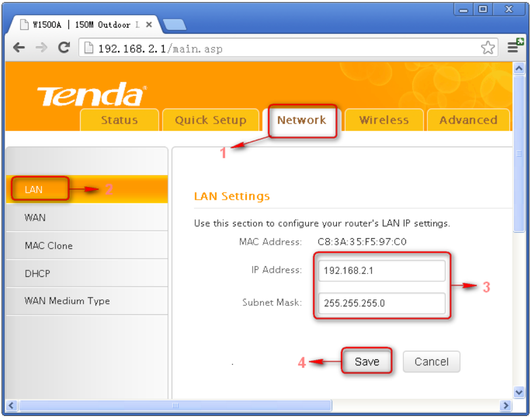
The page at 192.168.2.1 says:

Click OK to save your settings and system will reboot!

Chapter 3 Network Setup

This chapter mainly explains LAN settings in AP Mode, Universal Repeater Mode and Router Mode, as well as WAN settings, MAC Clone, DHCP server and WAN Medium Type (Wired or Wireless WAN).

3.1 LAN Settings



LAN Settings

Use this section to configure your router's LAN IP settings.

MAC Address: C8:3A:35:F5:97:C0

IP Address: 192.168.2.1

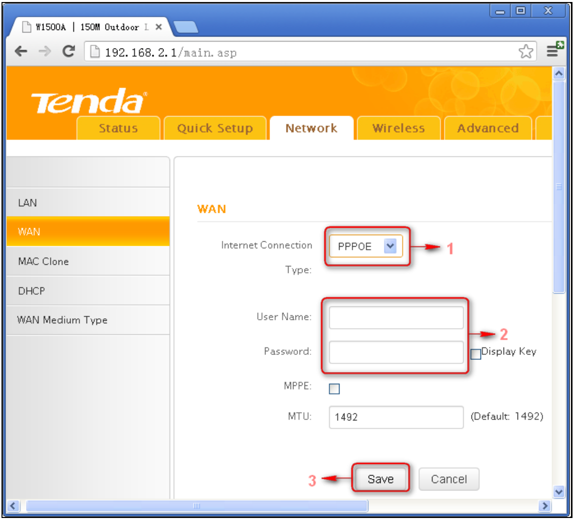
Subnet Mask: 255.255.255.0

- **IP Address:** Device's LAN IP address, 192.168.2.1 by default. You can change it according to your needs; just remember to use the new one to log on to the device's web utility if you changed it.
- **Subnet Mask:** Device's LAN subnet mask, 255.255.255.0 by default.
- **Note:** If you change the device's LAN IP address, you must use the new one to log on to the web-based configuration utility. To synchronize system time in AP Mode and Universal Repeater Mode, make sure your device's LAN IP address is on the same net segment as the uplink device, and set gateway and DNS addresses the same as uplink device's IP address.

3.2. WAN Settings

WAN settings are only available in Router Mode.

PPPoE



WAN

Internet Connection Type: PPPOE

User Name:

Password: □Display Key

MPPE: □

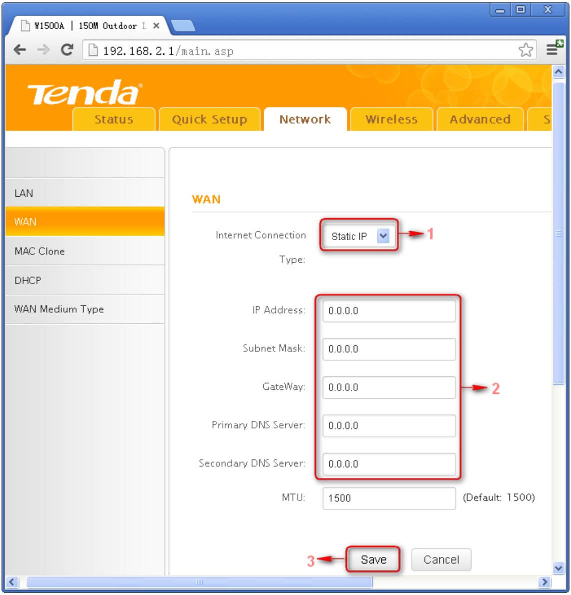
MTU: 1492 (Default: 1492)

- ➢ **Internet connection Type:** Displays the current Internet connection type.
- ➢ **User Name:** Enter the User Name provided by your ISP.
- ➢ **Password:** Enter the password provided by your ISP.
- ➢ **MPPE:** Microsoft Point-to-Point Encryption (MPPE) is a protocol for encrypting data across Point-to-Point Protocol (PPP) and virtual private network (VPN) links.By default it is disabled. However if ISP enables MPPE on his PPPoE server, you must also enable it on

the device. Consult your ISP, if you don't know whether he has enabled the MPPE or not.

- **MTU:** Maximum Transmission Unit. DO NOT change it from the factory default of 1492 unless necessary. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled; in this case, try 1450, 1400, etc.

Static IP



WAN

Internet Connection Type: Static IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

GateWay: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

MTU: 1500 (Default: 1500)

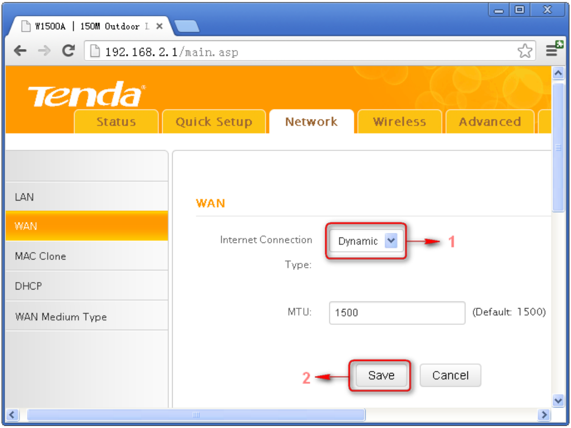
If your ISP assigns a fixed IP address to you, then select Static IP, and enter the IP address, subnet mask, primary DNS and secondary DNS (optional) info provided by your ISP in corresponding fields.

- **IP Address:** Enter the WAN IP address provided by your ISP. Consult your ISP if you are not clear.
- **Subnet Mask:** Enter WAN Subnet Mask provided by your ISP. The default is 255.255.255.0.
- **Gateway:** Enter the WAN Gateway provided by your ISP. Consult your ISP if you are not clear.

- **Primary DNS Server:** Enter the DNS address provided by your ISP.
- **Secondary DNS Server:** Enter the other DNS address if your ISP provides 2 such addresses (optional).
- **MTU**: Maximum Transmission Unit. DO NOT change it from the factory default of 1500 unless necessary. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled; in this case, try 1450, 1400, etc.

DHCP (Dynamic IP)

Select DHCP (Dynamic IP) if you can access Internet as soon as your computer directly connects to an Internet-enabled ADSL/Cable modem. Device will automatically obtain an IP address from ISP.



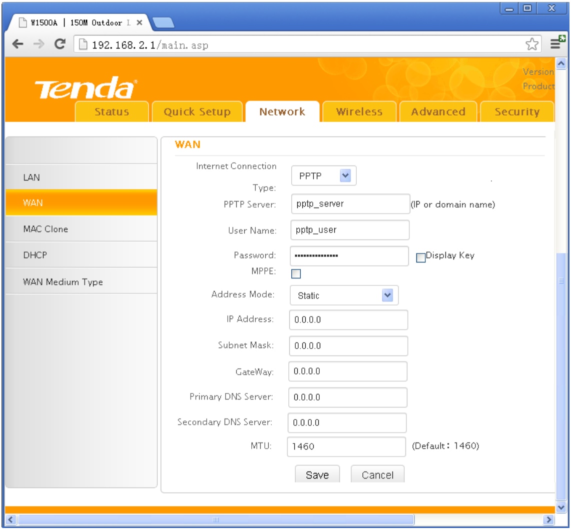
WAN

Internet Connection Type: Dynamic

MTU: 1500 (Default: 1500)

PPTP

Select PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. The PPTP connects a router to a VPN server. For example：A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other’s resources.



WAN

Internet Connection Type: PPTP

PPTP Server: pptp_server (IP or domain name)

User Name: pptp_user

Password: •••••••••••••••• □Display Key

MPPE: □

Address Mode: Static

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

GateWay: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

MTU: 1460 (Default：1460)

Save Cancel

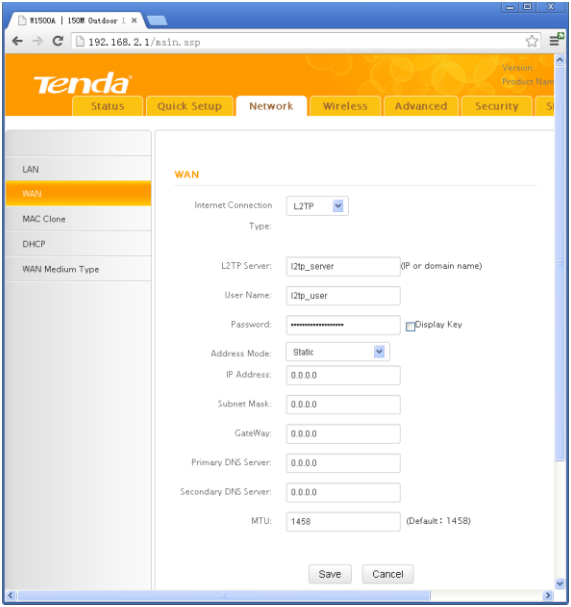
- **Internet connection Type**: Displays a list of available Internet connection types.
- **PPTP Server**: Enter the IP address of a PPTP server.
- **User Name**: Enter your PPTP User Name.
- **Password**: Enter your Password.
- **MPPE:** Microsoft Point-to-Point Encryption (MPPE) is a protocol for encrypting data across Point-to-Point Protocol (PPP) and virtual private network (VPN) links. By default it is disabled. However if ISP enables

MPPE on his PPPoE server, you must also enable it on the device. Consult your ISP, if you don't know whether he has enabled the MPPE or not.

- **Address mode**: Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
- **IP Address**: Enter the IP address provided by your ISP. Consult your local ISP if you are not clear.
- **Subnet Mask**: Enter the subnet mask provided by your ISP. Consult your ISP if you are not clear.
- **Gateway**: Enter the gateway provided by your ISP. Consult your local ISP if you are not clear.
- **Primary/Secondary DNS Server**: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.
- **MTU**: Maximum Transmission Unit. The factory default is 1460.

L2TP

Select L2TP (Layer 2 Tunneling Protocol) if your ISP uses an L2TP connection. The L2TP connects your router to a L2TP server. For example: A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.



WAN

Internet Connection Type: L2TP

L2TP Server: l2tp_server (IP or domain name)

User Name: l2tp_user

Password: •••••••••••••••••• □Display Key

Address Mode: Static

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

GateWay: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

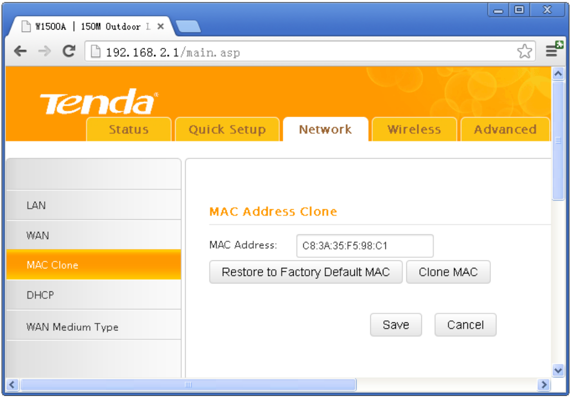
MTU: 1458 (Default：1458)

- **Internet connection Type**: Displays a list of available Internet connection types.
- **L2TP Server**: Enter the L2TP IP address provided by your ISP.
- **User Name**: Enter your L2TP User Name.

- **Password**: Enter your Password.
- **Address Mode**: Select **Dynamic** if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
- **IP Address**: Enter the IP address provided by your ISP. Consult your local ISP if you are not clear.
- **Gateway**: Enter the gateway provided by your ISP. Consult your local ISP if you are not clear.
- **Primary/Secondary DNS Server**: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.
- **MTU**: Maximum Transmission Unit. The factory default is 1458.

3.3 MAC Clone

This section allows you to configure Device’s WAN MAC address. This feature is only available in Router Mode.



MAC Address Clone

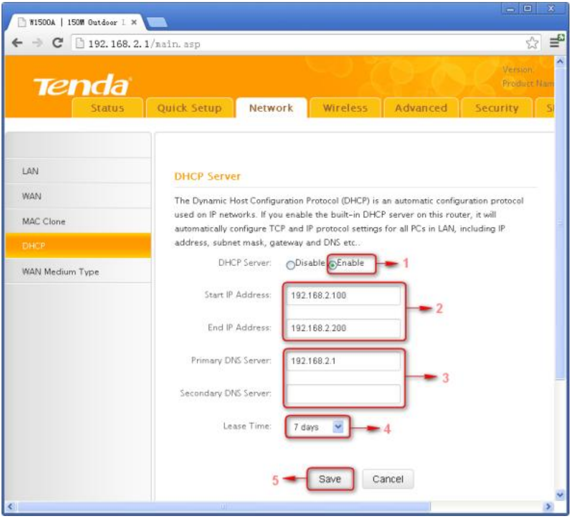
MAC Address: C8:3A:35:F5:98:C1

Normally you don't need to change device's default WAN MAC address. However, some ISPs may bind client PC's MAC address for Internet connection authentication. In this case, simply enter the bound MAC in the WAN MAC Address field or click "Copy My PC's MAC" (or Clone MAC) to copy your PC's MAC to the device.

- **MAC Address:** Config device’s WAN MAC address and click **Save** to save your settings.
- **Clone MAC**: Click to automatically copy your local PC's MAC address to the device as device's new WAN MAC address.
- **Restore to Factory Default MAC:** Reset Device’s WAN MAC to factory default.

3.4. DHCP

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on this device, it will automatically configure TCP/IP protocol settings for all DHCP-Client-enabled PCs in your LAN (Namely, PCs are set to "Obtain an IP address automatically" and "Obtain DNS server address automatically"), including IP address, subnet mask, gateway and DNS etc, eliminating the need for manual intervention.



DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on this router, it will automatically configure TCP and IP protocol settings for all PCs in LAN, including IP address, subnet mask, gateway and DNS etc..

DHCP Server: ○ Disable ● Enable

Start IP Address: 192.168.2.100

End IP Address: 192.168.2.200

Primary DNS Server: 192.168.2.1

Secondary DNS Server:

Lease Time: 7 days

Save Cancel

- **DHCP Server:** enable or disable the device's DHCP server feature. If enabled, the DHCP server will assign IP addresses to requesting clients.
- **Start IP Address:** Specify the starting IP address for the DHCP server IP assignment.

- **End IP Address:** Specify the ending IP address for the DHCP server IP assignment.
- **Primary DNS Server:** Specify a primary DNS address for requesting clients.
- **Secondary DNS Server:** Specify a secondary DNS address for requesting clients. This field is optional.
- **Lease Time:** The length of time for the IP address lease. Configuring a proper lease time improves the efficiency for the DHCP server to reclaim disused IP addresses.
- **For example:** If the lease time is set to one hour, then the DHCP server will reclaim disused IP addresses every hour.

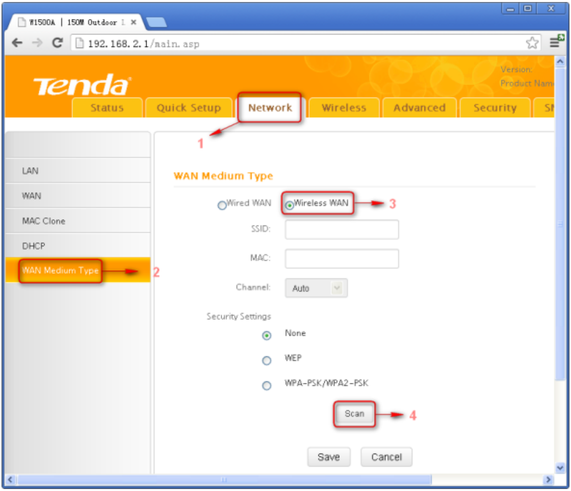
3.5 WAN Medium Type

Here you can select a proper WAN medium type to use: Wireless WAN (WISP) or Wired WAN to connect to the uplink device. Internet connection types are the same for the two medium types.

- **Wired WAN:** Connect to uplink device via an Ethernet cable.
- **Wireless WAN:** Connect to uplink device (WISP AP) wirelessly.

Please do following the steps as below if you connect to the Internet wirelessly.

1. Select **Wireless WAN** (**WISP**) **and click Scan**. Currently available wireless networks will then be displayed.



WAN Medium Type

○ Wired WAN ● Wireless WAN

SSID:

MAC:

Channel: Auto

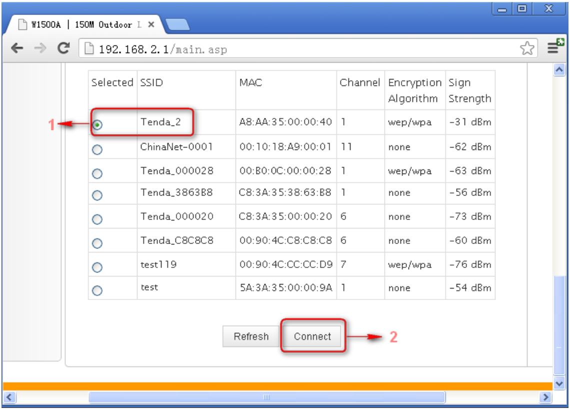
Security Settings

● None

○ WEP

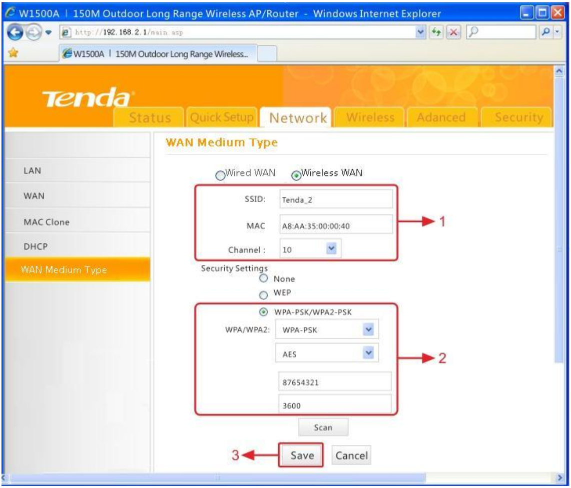
○ WPA-PSK/WPA2-PSK

2. Select the SSID you wish to connect and SSID, MAC address and channel fields will then be automatically populated. For example, the security mode (encryption algorithm) and security key for the SSID Tenda_2 is WPA-PSK, and 87654321 3600s, simply enter them and click **Save**.



Selected	SSID	MAC	Channel	Encryption Algorithm	Sign Strength
●	Tenda_2	A8:AA:35:00:00:40	1	wep/wpa	-31 dBm
○	ChinaNet-0001	00:10:18:A9:00:01	11	none	-62 dBm
○	Tenda_000028	00:B0:0C:00:00:28	1	wep/wpa	-63 dBm
○	Tenda_3863B8	C8:3A:35:38:63:B8	1	none	-56 dBm
○	Tenda_000020	C8:3A:35:00:00:20	6	none	-73 dBm
○	Tenda_C8C8C8	00:90:4C:C8:C8:C8	6	none	-60 dBm
○	test119	00:90:4C:CC:CC:D9	7	wep/wpa	-76 dBm
○	test	5A:3A:35:00:00:9A	1	none	-54 dBm

Figure 1


W1500A | 150M Outdoor Long Range Wireless AP/Router - Windows Internet Explorer
http://192.168.2.1/main.asp
W1500A | 150M Outdoor Long Range Wireless...
Tenda
Status
Quick Setup
Network
Wireless
Adanced
Security
LAN
WAN
MAC Clone
DHCP
WAN Medium Type
1
2
3
Scan
Save
Cancel

WAN Medium Type

○ Wired WAN ● Wireless WAN

SSID: Tenda_2

MAC A8:AA:35:00:00:40

Channel : 10

Security Settings

○ None

○ WEP

● WPA-PSK/WPA2-PSK

WPA/WPA2: WPA-PSK

AES

87654321

3600

Figure 2

3. Click **OK** and device will restart and will then operate in Wireless WAN (also known as WISP Mode).

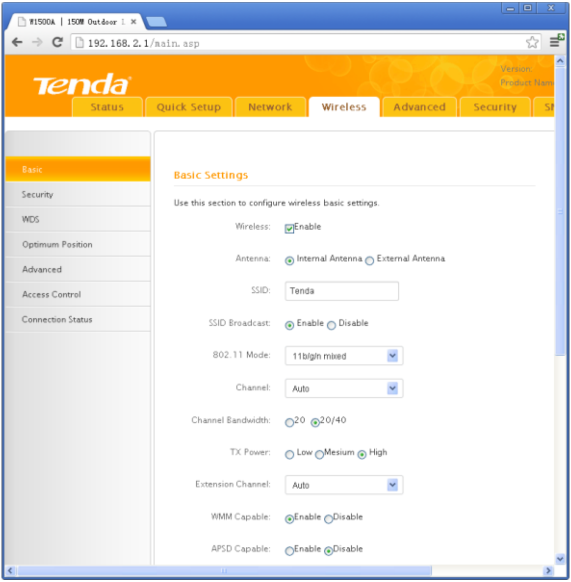
Note:

When operating in **Wireless WAN (WISP Mode)**, make sure device is operating on the same channel as the uplink device (WISP AP). While SSID and security settings on device are not required so.

Chapter 4 Wireless Settings

This chapter mainly presents wireless settings, including basic wireless settings, security, WDS, access control settings and connection status.

4.1 Basic



Basic Settings

Use this section to configure wireless basic settings.

Wireless:	☑Enable
Antenna:	● Internal Antenna ○ External Antenna
SSID:	Tenda
SSID Broadcast:	● Enable ○ Disable
802.11 Mode:	11b/g/n mixed
Channel:	Auto
Channel Bandwidth:	○20 ●20/40
TX Power:	○ Low ○Mesium ● High
Extension Channel:	Auto
WMM Capable:	●Enable ○Disable
APSD Capable:	○Enable ●Disable

- **Wireless:** Check to enable the wireless feature.
- **Antenna:** Select to use internal antenna or external antenna.
- **SSID:** This is the public name of your wireless network. This field does not allow Chinese characters and special characters:; \ ~ ,;" & %, etc.
- **SSID Broadcast:** Select "Enable"/"Disable" to make your wireless network visible/ invisible to any wireless clients within coverage when

they perform a scan to see what's available. When disabled, this SSID becomes invisible to any wireless clients within the coverage. Manually enter the SSID if you want to connect to it.

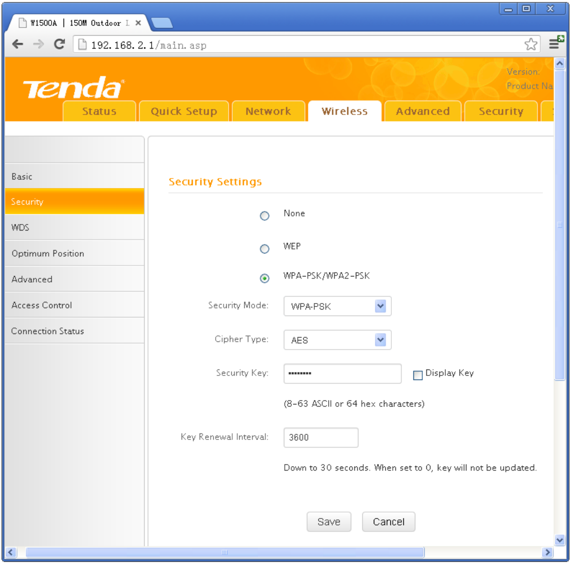
- **802.11 Mode:** Select a wireless network mode.
  11b mode: Select it if you have only Wireless-B clients in your wireless network.
  11g mode: Select it if you have only Wireless-G clients in your wireless network.
- **11b/g mixed mode:** Select it if you have only Wireless-B and Wireless-G clients in your wireless network.
- **11b/g/n mixed mode:** Select it if you have Wireless-b/g/n clients in your wireless network.
- **Channel:** For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or **Auto** to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.
- **Channel Bandwidth:** Select a proper channel bandwidth to enhance wireless performance. When there are 11b/g and 11n wireless clients, please select the 802.11n mode of 40M frequency band; when there are only non-11n wireless clients, select 20M frequency band mode; when the wireless network mode is 11n mode, please select 20/40 frequency band to boost its throughput.
- **TX Power:** Select a proper transmission power level for device (Low power: 100mW, medium power: 200mW, high power: 300mW). The default TX power level is **High**.
- Extension Channel: It is used to ensure N speed for 802.11n devices on the network.
- **WMM-Capable:** WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data (such as video or audio).
- **ASPD Capable**: Select to enable/disable the auto power saving mode.

4.2 Security

This section allows you to secure your wireless network to block unauthorized accesses and malicious packet sniffing. For better security, it is advisable to use the WPA-AES encryption.

4.2.1 WPA-PSK

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. WPA adopts enhanced encryption algorithm over WEP.



Security Settings

○ None

○ WEP

● WPA-PSK/WPA2-PSK

Security Mode: WPA-PSK

Cipher Type: AES

Security Key: •••••••• □ Display Key

(8-63 ASCII or 64 hex characters)

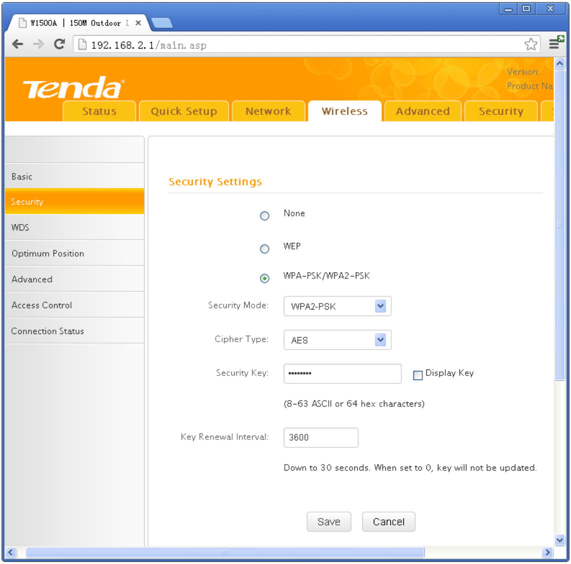
Key Renewal Interval: 3600

Down to 30 seconds. When set to 0, key will not be updated.

- **Cipher Type**: Select AES (advanced encryption standard), or TKIP (temporary key integrity protocol).
- **Security Key:** Enter a security key, which must be between 8-63 ASCII characters long or 64 HEX characters long.
- **Key Renewal Interval**: Specify a valid time interval for the key to be updated.

4.2.2 WPA2-PSK

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.



Security Settings

○ None

○ WEP

● WPA-PSK/WPA2-PSK

Security Mode: WPA2-PSK

Cipher Type: AES

Security Key: •••••••• □ Display Key

(8-63 ASCII or 64 hex characters)

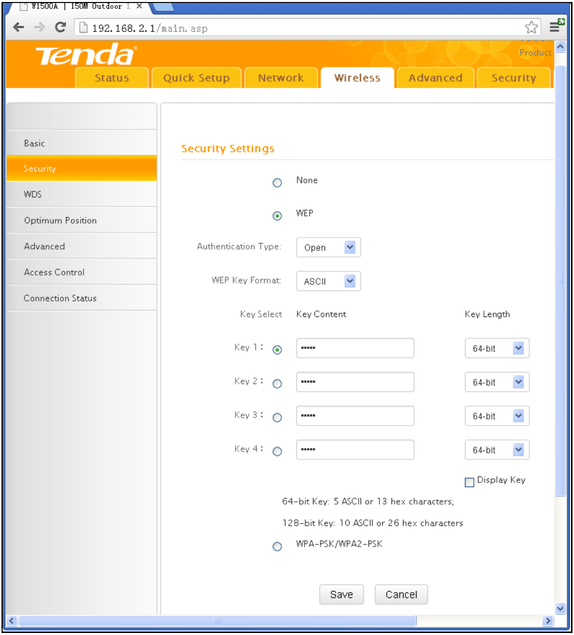
Key Renewal Interval: 3600

Down to 30 seconds. When set to 0, key will not be updated.

- **Cipher Type:** Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol) &AES.
- **Security Key:** Enter a security key, which must be between 8-63 ASCII characters long or 64 HEX characters long.
- **Key Renewal (Update) Interval**: Specify a valid time interval for the key to be updated.

4.2.3 WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network.



Security Settings

○ None

● WEP

Authentication Type: Open

WEP Key Format: ASCII

Key Select		Key Content	Key Length
Key 1：	●	•••••	64-bit
Key 2：	○	•••••	64-bit
Key 3：	○	•••••	64-bit
Key 4：	○	•••••	64-bit

□ Display Key

64-bit Key: 5 ASCII or 13 hex characters;

128-bit Key: 10 ASCII or 26 hex characters

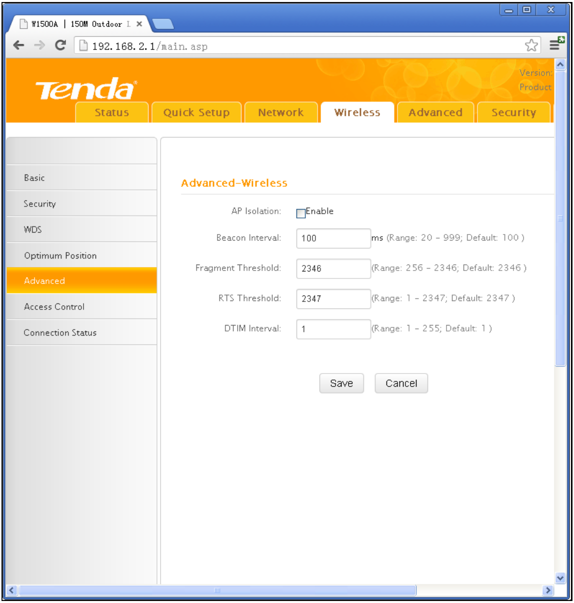
○ WPA-PSK/WPA2-PSK

Save Cancel

- **Authentication Type:** Select a proper authentication type.
- **WEP Key Format:** Select a proper key format: HEX or ASCII.
- **Key Select:** Select a key from the preset keys 1-4 for current use.

4.3 Advanced Settings

This section allows you to config advanced settings, including AP Isolation, Beacon interval, Fragment threshold, RTS threshold and DTIM interval, etc, for your wireless networks.



Advanced-Wireless

AP Isolation: □Enable

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)

DTIM Interval: 1 (Range: 1 - 255; Default: 1)

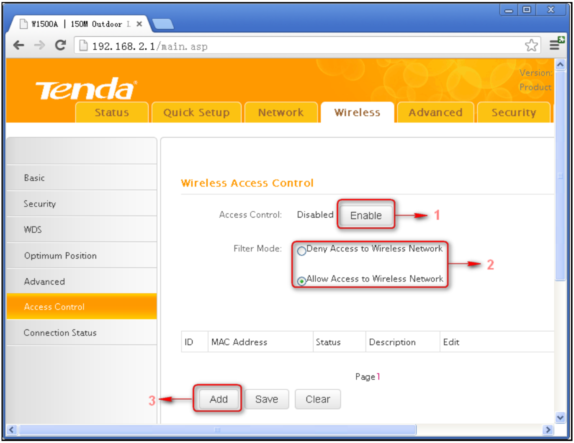
- **AP Isolation:** Isolates clients connecting to master SSID.
- **Beacon Interval:** A time interval between any 2 consecutive Beacon packets sent by an Access Point to synchronize a wireless network. Do NOT change the default value of 100 unless necessary.
- **Fragment Threshold:** Specify a Fragment Threshold value. Any

wireless packet exceeding the preset value will be divided into several fragments before transmission. DO NOT change the default value of 2346 unless necessary.

- **RTS Threshold:** If a packet exceeds such set value, RTS/CTS scheme will be used to reduce collisions. Set it to a smaller value provided that there are distant clients and interference. For normal SOHO, it is recommended to keep the default value unchanged; otherwise, device performance may be degraded.
- **DTIM Interval:** A DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next window for listening to broadcast and multicast messages. When such packets arrive at device's buffer, the device will send DTIM (delivery traffic indication message) and DTIM interval to wake clients up for receiving these packets.

4.4 Access Control

The MAC-based Wireless Access Control feature can be used to allow or disallow clients to connect to your wireless network.



Wireless Access Control

Access Control: Disabled Enable

Filter Mode: ○ Deny Access to Wireless Network
● Allow Access to Wireless Network

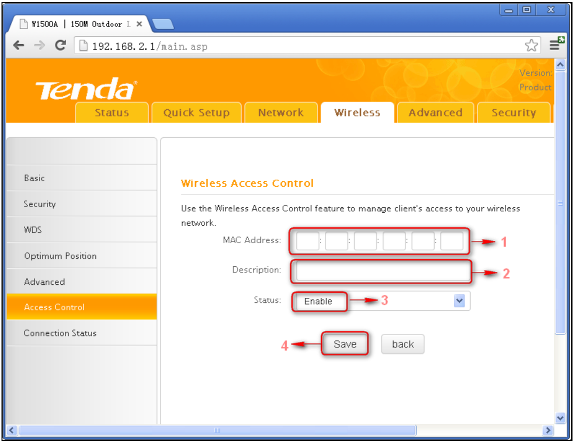
ID	MAC Address	Status	Description	Edit

Page 1

Add Save Clear

- **Access Control:** Disabled by default. Click Enable to enable the feature.
- **Deny Access to Wireless Network:** Block only PCs at specified MAC addresses from connecting to your wireless network.
- **Allow Access to Wireless Network:** Allow only PCs at specified MAC addresses to connect to your wireless network.

Click **Add** and below screen appears:



Wireless Access Control

Use the Wireless Access Control feature to manage client's access to your wireless network.

MAC Address: : : : : : 1

Description: 2

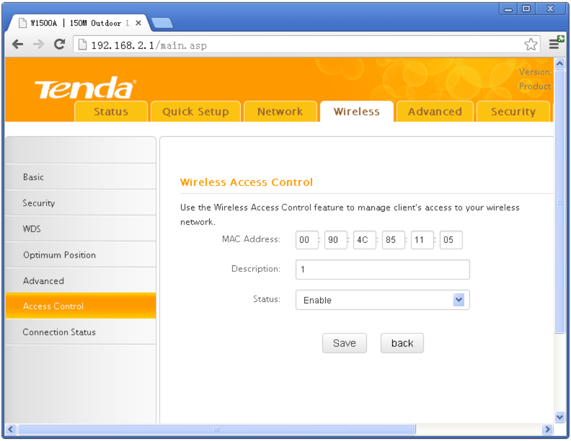
Status: Enable 3

4 Save back

- **MAC Address:** Enter the MAC address of a wireless client.
- **Description:** Briefly describe the current entry/rule.
- **Status:** Select **Enable** or **Disable**.
- Up to 6 rules can be added.

Example: To allow only the PC at the MAC address of 00:90:4C:85:11:05 to connect to your wireless network, do as follows:

1. Click **Add**, enter **00:90:4C:85:11:05** in the **MAC Address** field, select **Enable** and then click **Save** as seen in the screenshot below.



Wireless Access Control

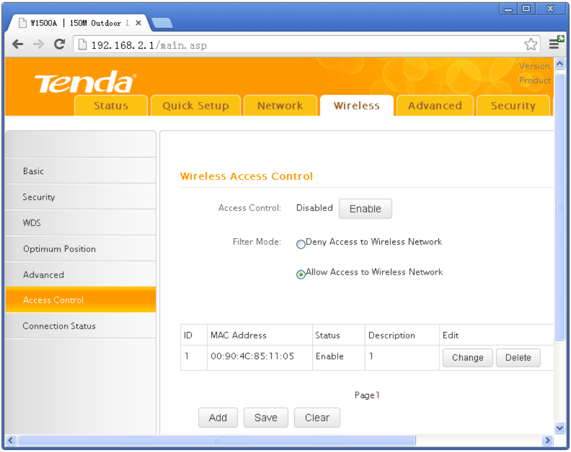
Use the Wireless Access Control feature to manage client's access to your wireless network.

MAC Address: 00 : 90 : 4C : 85 : 11 : 05

Description: 1

Status: Enable

2. You will be redirected to the initial page of this feature. The rule you just added will be displayed there. Select **Allow Access to Wireless Network** and **Enable** as seen in the screenshot below:



Wireless Access Control

Access Control: Disabled [Enable]

Filter Mode: ○ Deny Access to Wireless Network

● Allow Access to Wireless Network

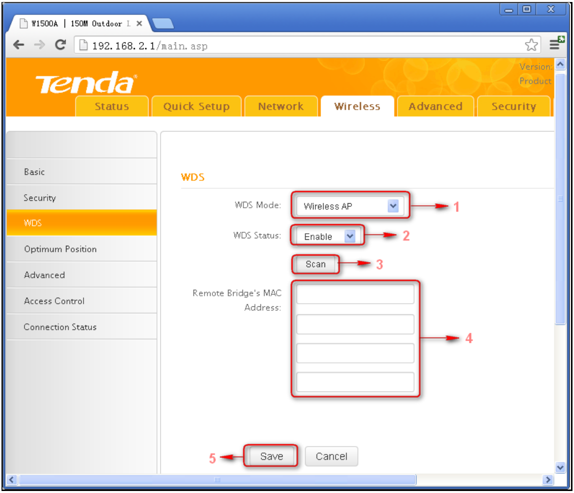
ID	MAC Address	Status	Description	Edit
1	00:90:4C:85:11:05	Enable	1	Change Delete

Page 1

[Add] [Save] [Clear]

4.5 WDS Settings

WDS Bridge Mode: 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.Note: The Access Points you select MUST support WDS. Select **Wireless AP** from **WDS Mode** and **Enable** from **WDS Status** to enter screen below:



WDS

WDS Mode: Wireless AP

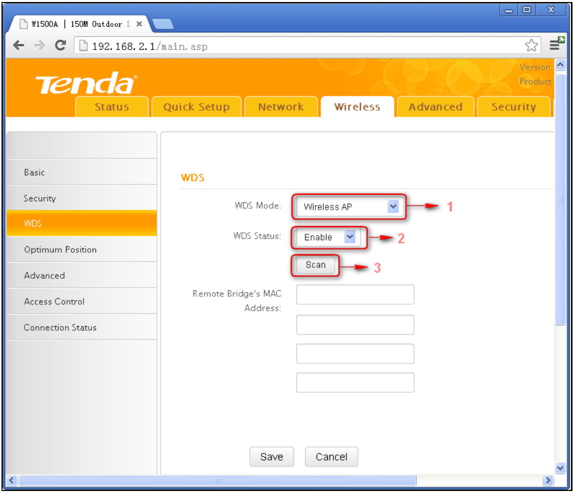
WDS Status: Enable

Remote Bridge's MAC Address:

- ➢ **WDS Mode**: Select Wireless AP or Bridge. When operating in Bridge mode, other wireless clients (excluding bridge participants) will not be able to connect to the device; when operating in Wireless AP mode, other wireless clients will still be able to connect to the device via SSID.
- ➢ **WDS Status:** Select Enable or Disable.
- ➢ **Scan:** Click to scan wireless networks (SSIDs and BSSID) in the area after you enable the WDS feature.

- **Remote Bridge's MAC Address:** Enter the MAC address of the wireless device you want to connect (link partner).

Take two W1500As as an example to illustrate WDS implementation. Select **Wireless AP** from **WDS Mode** and **Enable** from **WDS Status**.



WDS

WDS Mode: Wireless AP

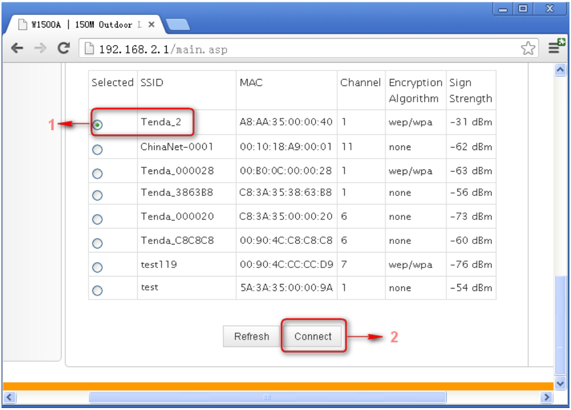
WDS Status: Enable

Remote Bridge's MAC Address:

1 Directly enter the MAC address of the link partner if you already know it and then click **OK**.

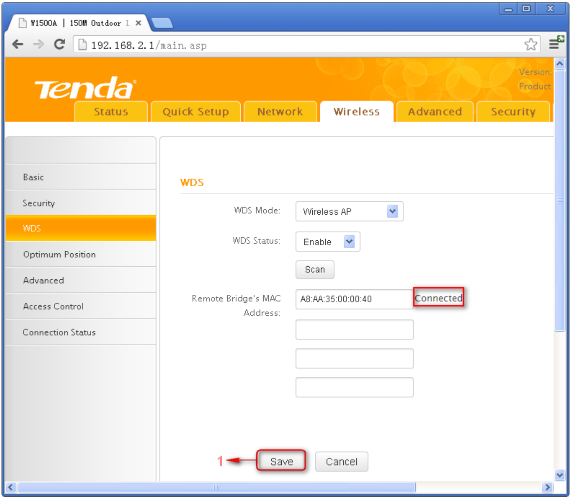
2 Enable scan on one associated device to search for the link partner.

1) Click **Scan**.



Selected	SSID	MAC	Channel	Encryption Algorithm	Sign Strength
●	Tenda_2	A8:AA:35:00:00:40	1	wep/wpa	-31 dBm
○	ChinaNet-0001	00:10:18:A9:00:01	11	none	-62 dBm
○	Tenda_000028	00:B0:0C:00:00:28	1	wep/wpa	-63 dBm
○	Tenda_3863B8	C8:3A:35:38:63:B8	1	none	-56 dBm
○	Tenda_000020	C8:3A:35:00:00:20	6	none	-73 dBm
○	Tenda_C8C8C8	00:90:4C:C8:C8:C8	6	none	-60 dBm
○	test119	00:90:4C:CC:CC:D9	7	wep/wpa	-76 dBm
○	test	5A:3A:35:00:00:9A	1	none	-54 dBm

2) Select the SSID you wish to connect, click **Connect** and its MAC address will then be added automatically to device.



WDS

WDS Mode: Wireless AP

WDS Status: Enable

Remote Bridge's MAC Address: A8:AA:35:00:00:40 Connected

Click **Save** to save your settings. And then configure same settings on the bridge partner device. When **Connected** appears, you have successfully connected to it.

⚠ **Note:**

WDS feature can only be implemented between 2 WDS-capable wireless devices. Plus, SSID, channel, security settings and security key must be exactly the same on both such devices.

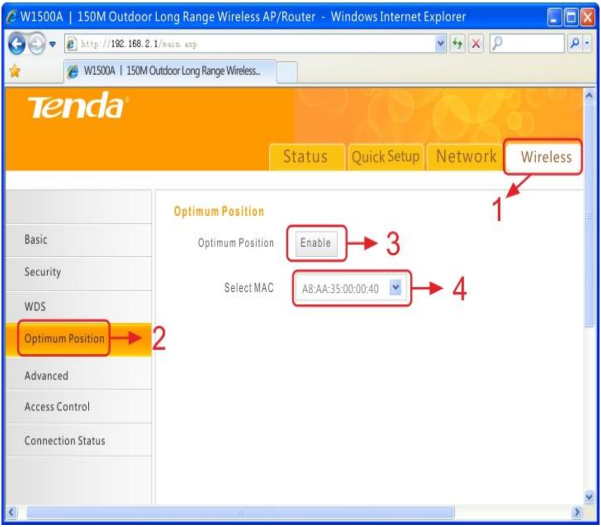
To authenticate on wireless client access, go to Wireless -> Security. After you finish the configurations, remember to reboot the device for proper WDS communication.

3. Each device can bridge up to 4 wireless devices.

4.6 Optimum Position Setup

Optimum Position: Enable this option for a best reference position of device for optimum performance.

1. Click **Wireless** -> **Optimum Position** to enter the configuration interface.



W1500A | 150M Outdoor Long Range Wireless AP/Router - Windows Internet Explorer

http://192.168.2.1/main.asp

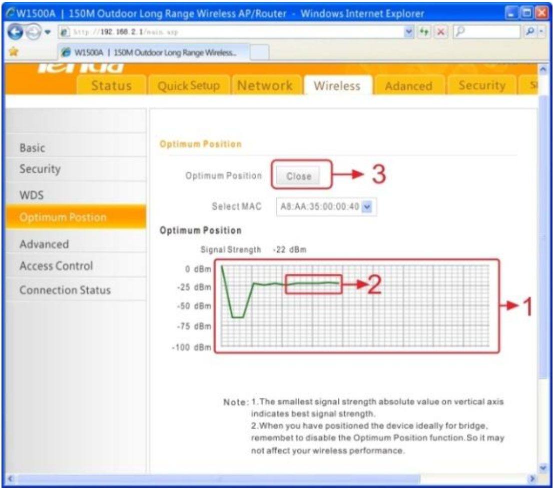
Optimum Position

Optimum Position: Enable

Select MAC: A8:AA:35:00:00:40

2. Select **Enable** to enable the **Optimum Position** function.

Select MAC: Select the MAC address of the remote device to bridge . (Before performing this action, make sure you have added it on **WDS** or **Universal Repeater** section)



Optimum Position

Optimum Position: Close

Select MAC: A8:AA:35:00:00:40

Optimum Position

Signal Strength -22 dBm

Note: 1.The smallest signal strength absolute value on vertical axis indicates best signal strength.
2.When you have positioned the device ideally for bridge, remembet to disable the Optimum Position function.So it may not affect your wireless performance.

Place and hold the device in different places for a certain period of time (5 seconds is recommended), observe signal strength change from the graph. Position device exactly where as it is when strongest signal appears on the graph.

Note:

1. The smallest signal strength absolute value on vertical axis indicates best signal strength.

2. When you have positioned the device ideally for bridge, remember to disable the **Optimum WDS Position** function. So it may not affect your wireless performance.