MANUAL NWA200

Niveo Professional In-Wall 300N PoE Acces Point

Copyright Statement

is the registered trademark of Netstar Products BV. 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 Netstar Products BV. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Netstar Products BV.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Netstar Products BV reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. Netstar Products BV does not assume any liability that may occur due to the use or application of, the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

About This User Guide

Please read this user guide before you start! This user guide instructs you to install and configure the device.

This user guide uses the following formats to highlight special messages:

Icon	Description
Note	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
Tip	This format is used to highlight a procedure that will save time or resources.

How to Use This Book

Chapter	Content
I Product Overview	Describes product appearance and lists features.
II Install	Explains how to install hardware and connect cables.
III Login	Explains how to logs in to the web interface.
IV Features & Configurations	Introduces how to configure the device features.
V Appendix	Explains how to configure PC TCP/IP settings, gives specifications and lists default feature values and Safety and Emission Statement

Table of Contents

ABOUT THIS USER GUIDE ..... **IV**

I PRODUCT OVERVIEW ..... **- 1 -**

1 WHAT IT DOES ..... - 1 -

2 PACKAGE CONTENT ..... - 1 -

3 LED ..... - 2 -

4 BUTTON & INTERFACE ..... - 2 -

5 LABEL ..... - 3 -

Ⅱ INSTALL ..... **- 4 -**

Ⅲ LOGIN ..... **- 6 -**

1 CONFIGURE PC TCP/IP SETTINGS ..... - 6 -

2 LOG IN TO DEVICE ..... - 6 -

Ⅳ FEATURES & CONFIGURATIONS ..... **- 8 -**

1 STATUS ..... - 8 -

1.1 System Status ..... *- 8 -*

1.2 Wireless Status ..... *- 8 -*

1.3 Traffic Statistics ..... *- 9 -*

1.4 Wireless Clients ..... *- 9 -*

2 QUICK SET UP ..... - 10 -

3 LAN SETTINGS ..... - 11 -

4 DHCP SERVER ..... - 12 -

4.1. DHCP Server ..... *- 12 -*

4.2 DHCP Client List ..... *- 13 -*

5 WIRELESS SETTINGS ..... - 13 -

5.1 Basic Settings ..... *- 14 -*

5.2 Radio ..... *- 18 -*

5.3 Channel Scan ..... *- 20 -*

5.4 Advanced Settings ..... *- 20 -*

5.5 Access Control ..... *- 21 -*

5.6 QVLAN ..... *- 22 -*

6 SNMP ..... - 23 -

7 TOOLS ..... - 23 -

7.1 Maintenance ..... *- 24 -*

7.2 Time & Date ..... *- 25 -*

7.3 Logs ..... *- 26 -*

7.4 Configuration ..... *- 27 -*

7.5 User Name & Password ..... *- 29 -*

7.6 Diagnostics ..... *- 30 -*

7.7 Reboot ..... *- 30 -*

7.8 LED ..... *- 32 -*

Ⅴ APPENDIX ..... - 33 -

1 CONFIGURE PC TCP/IP SETTINGS ..... - 33 -

Windows XP ..... *- 33 -*

Windows 7 ..... *- 36 -*

2 FACTORY DEFAULT SETTINGS & SPECIFICATIONS ..... - 39 -

Default Settings ..... *- 39 -*

3 SAFETY AND EMISSION STATEMENT ..... - 41 -

I Product Overview

1 What It Does

The NWA200 is a best-in-class 802.11n indoor access point designed specifically for business-class environments such as hotels, airports, coffee shops, shopping centers, sporting venues, and university campus. With standard install design and stylish appearance, it nicely fits into an 86-type wall jack and seamlessly blends in with most interior decorations in an office or room. No need to rebuild or change existing walls. The unit comes with a built-in USB port that charges mobile devices such as a smart phone via a USB cable as well as a RJ11 port for connecting telephone. Integrated 802.3af Power over Ethernet (PoE) allows installation in areas where power outlets are not readily available. Client connected to the device's LAN port can still communicate with the remote uplink device (PoE switch) even when no power is supplied.

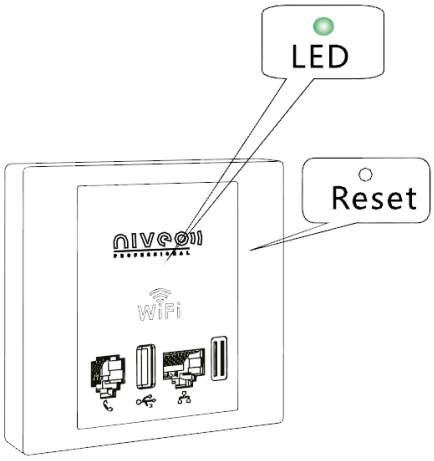
2 Package Content

Unpack the package. Your box should contain the following items:

1. AP
2. 2*Screws
3. Install Guide
4. Resource CD

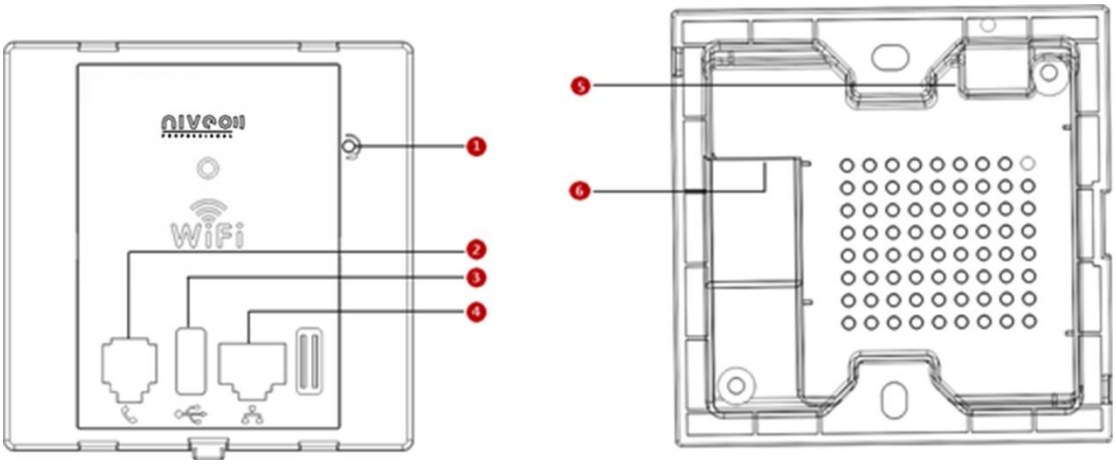
If any of the parts are incorrect, missing, or damaged, contact your dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

3 LED



LED	Color	Status	Description
PWR	Green	Solid	The device is connected to power supply.
		Blinking	The device is functioning correctly.
		Off	Power is not supplied to the device or the device is malfunctioning.

4 Button & Interface



❶ **ReSeT:** Open the housing of the AP and press this reset button for 7 seconds to restore the device to the factory default settings.

❷ **RJ11 Phone Interface:** For connection to a telephone.

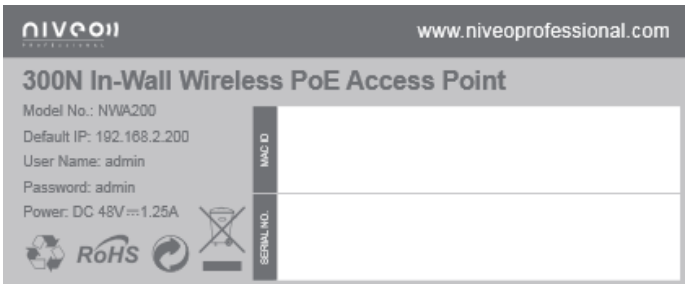
❸ **USB Port:** The USB port that charges terminal devices with a USB cable.

❹ **LAN:** 100M Ethernet Port for connecting to an Ethernet LAN device such as a PC or switch, etc. This port support “Bypass”. Client connected to the device’s LAN port can still communicate with the remote uplink device (PoE switch) even when no power is supplied.

❺ **Green Connector:** For connecting to a 4-core phone cable.

❻ **RJ45:** The RJ45 port for connecting to a PoE switch.

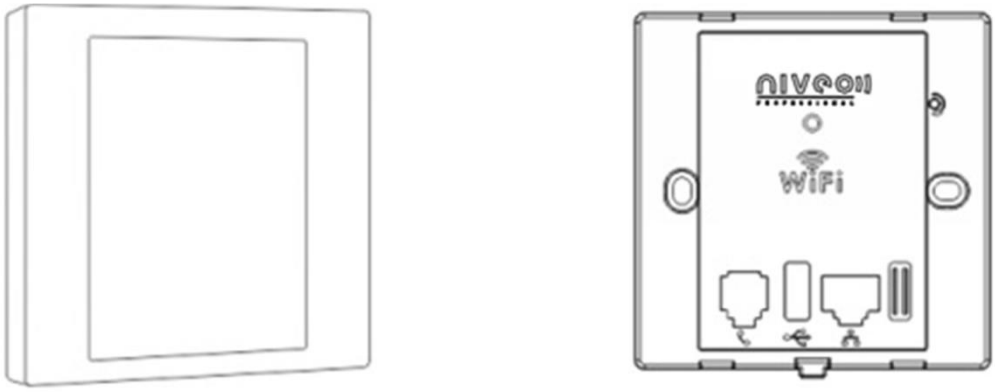
5 Label



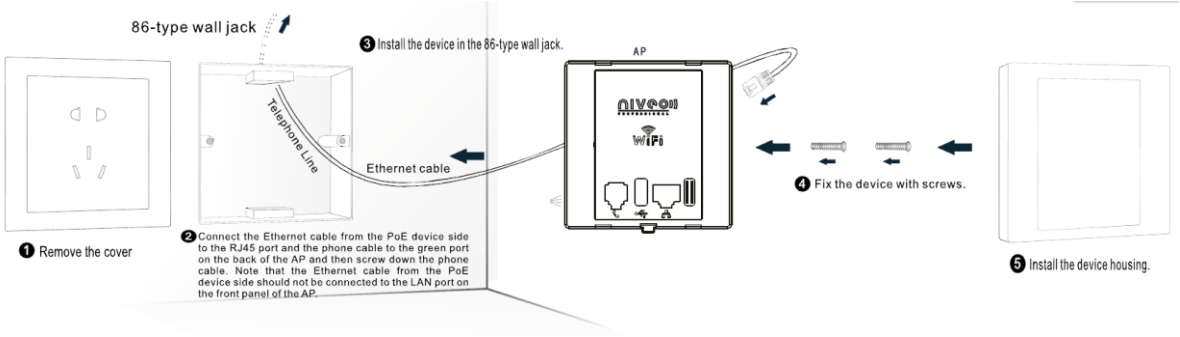
1. Default Login IP address: **192.168.2.200.**This IP address is to be used to access the router’s settings through a web browser. If you change it, you have to open a new connection to the new IP address and log in again.
2. Administrator user name: **admin**
3. Password; **admin**

Ⅱ Install

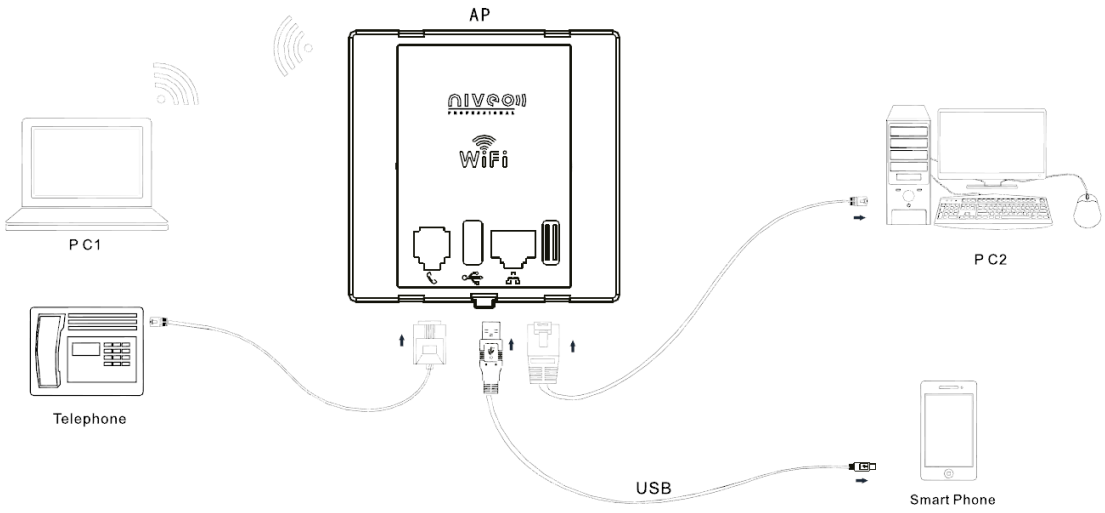
1. Remove the cover of the device.



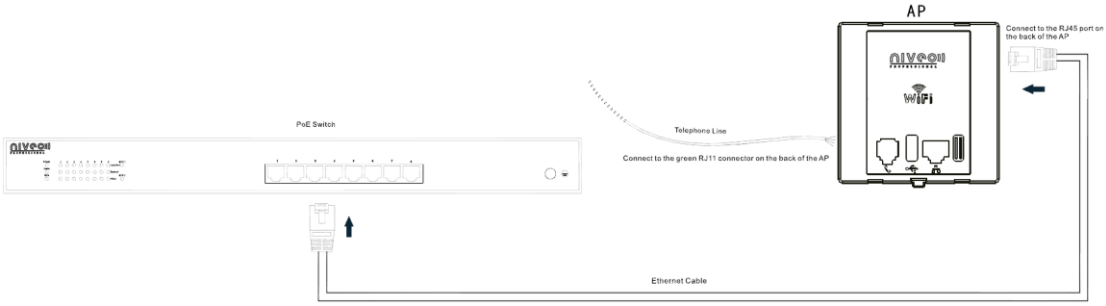
2. Install and power the device (Connect one end of an Ethernet cable to the PoE switch and the other end to the Ethernet port on the back panel of the device; connect the phone cable to the green connector).



3. Connect terminal devices.



4. Make sure all connections are established correctly as seen in the diagram.



Ⅲ Login

1 Configure PC TCP/IP Settings

Connect your PC to this device wirelessly or using an Ethernet cable. The default IP address of your wireless access point is 192.168.2.200. If you are using the default IP subnet, the computer you are using to connect to the device should be configured with an IP address that starts with 192.168.2.x (where x can be any number between 2~253) and a Subnet Mask of 255.255.255.0; if you have changed the subnet of the wireless access point, the computer you are using to connect must be within the same subnet.

Tip

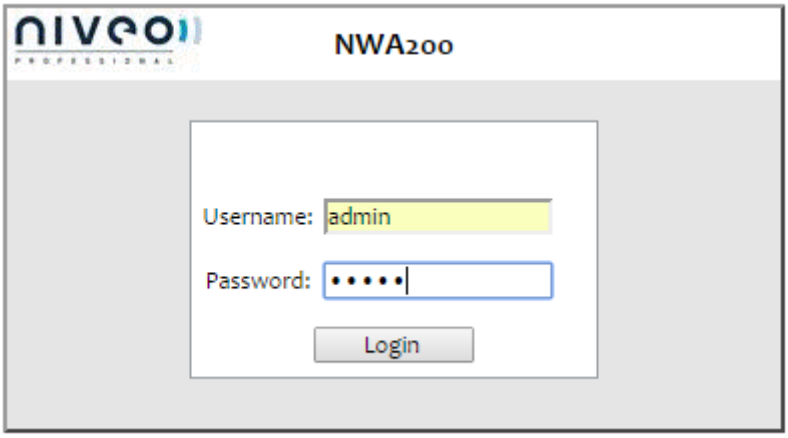
If you are not clear about how to set up your PC's IP address, see*1 Configure PC TCP/IP Settings*.

2 Log in to Device

1. Launch a web browser, say, IE, input 192.168.2.200 and press **Enter**.
2. The login window appears. Enter the login user name and password (Both are "admin" by default) and click **Login**.

Tip

You can click **Tools -> User Name & Password** to manage this user name and password. For more information, see 6.5 User Name & Password.



3. You will now enter the web configuration interface as seen below.

Ⅳ Features & Configurations

1 Status

This section includes the following:

1.1 System Status: View the device's system information and LAN settings.

***1.2 Wireless Status*:** View the device's wireless information and current SSID settings.

***1.3 Traffic Statistics*:** View current traffic statistics of each SSID.

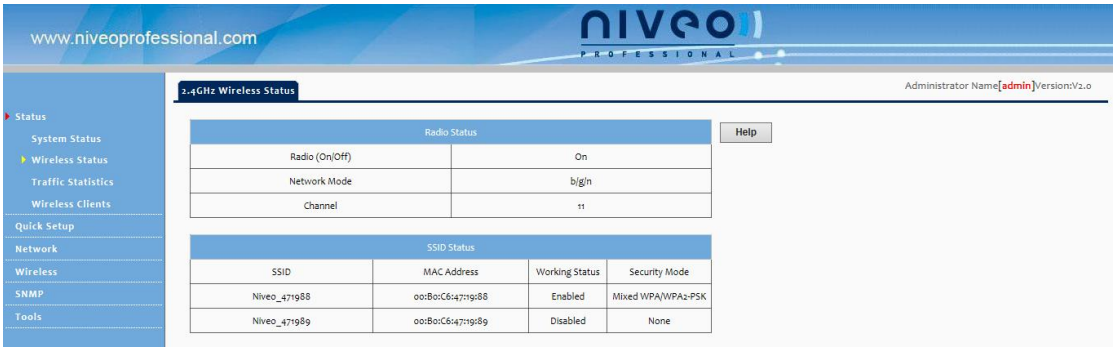
***1.4 Wireless Clients*:** View the MAC addresses and connection speed of the wireless clients that currently connect to each SSID.

1.1 System Status

Here you can view the device's system status and LAN status.

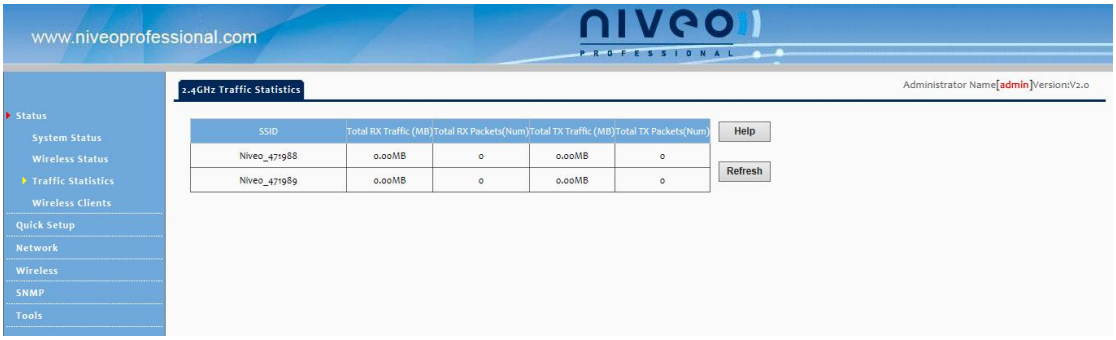
1.2 Wireless Status

Click **Status -> Wireless Status** and you can view the device's wireless information and current SSID settings.



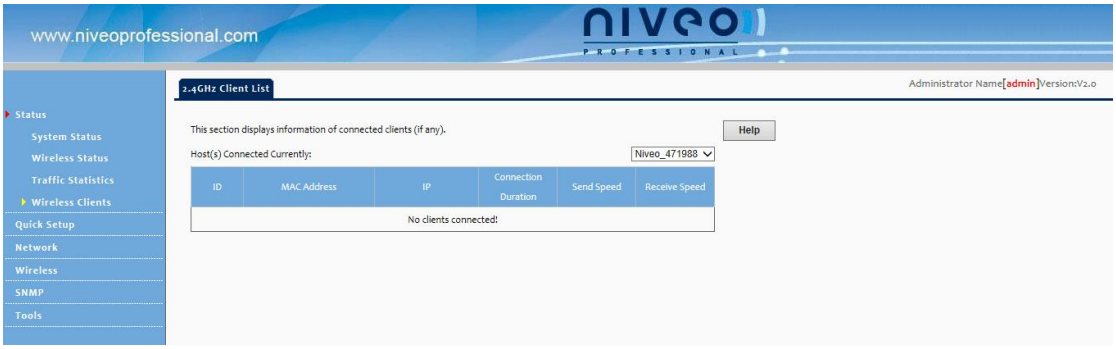
1.3 Traffic Statistics

Click **Status -> Traffic Statistics** and you can view current traffic statistics of the device's SSID.



1.4 Wireless Clients

Click **Status -> Wireless Clients** and you can view the MAC addresses and connection speed of the wireless clients that currently connect to each SSID.

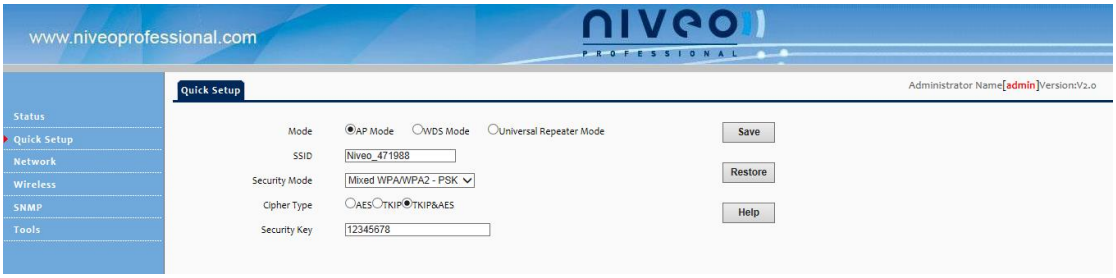


To view wireless clients connected to a specific SSID, simply select it from the drop-down list on the screen.

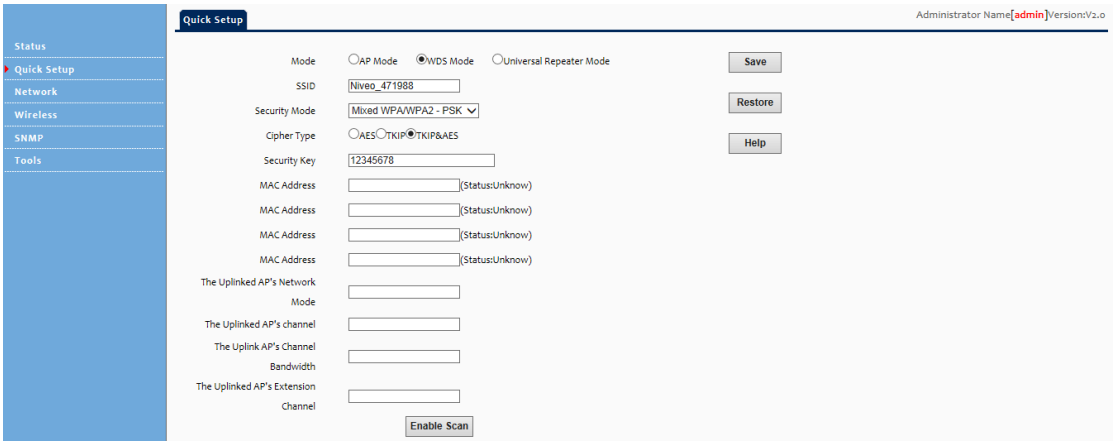
2 Quick Set up

Here you can quickly change the standard settings from default to customized values.

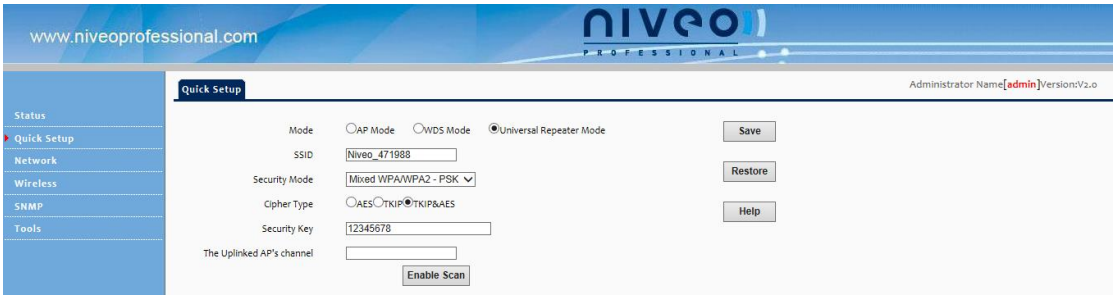
AP Mode: In this mode, this device can be connected to wireless clients, but cannot connect other APs actively.



WDS Mode: In this mode, this device can provide access to at most 4 APs.



Universal Repeater Mode (AP Client Mode): In this mode, NWA200 negotiates with the uplinked AP successfully and also provides access to lower clients.



3 LAN Settings

Here you can configure the device's LAN IP address for Internet access. This IP address is also to be used to access the device's settings through a web browser. Most of the default settings work in most cases. However, if your access point is part of a more complex LAN network, then modify the settings to meet the requirements of your network based on the explanation of the various fields.

Address Mode-Static IP: Manually specify the Static IP information (LAN IP address, subnet mask, gateway, DNS server address) that corresponds with your existing networking equipment.

Address Mode-Dynamic IP: Select it if you already have an active DHCP server on your existing network. The wireless access point gets its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the access point to your existing network.

Tip

1. Default IP address and subnet mask are respectively 192.168.2.200 and 255.255.255.0.

2. Be sure to make a note of any changes you apply to this page. If you change the LAN IP address of this device, you have to update your PC's TCP/IP settings and open a new connection to the new IP address and then log in again.

4 DHCP Server

This section includes the following:

4.1. DHCP Server: Configure DHCP server settings.

4.2 DHCP Client List: View the information of the DHCP clients that currently obtain IP addresses from the DHCP server.

4.1. DHCP Server

DHCP (Dynamic Host Configuration Protocol) assigns an IP address to each device on the LAN/private network. When you enable the DHCP Server, the DHCP Server will automatically allocate an unused IP address from the IP address pool specified in this screen to the requesting device as long as the device is set to "Obtain an IP Address Automatically". If you disable this feature, you have to manually configure the TCP/IP settings for all PCs on your LAN to access Internet.

Click **DHCP Server** to enter the configuration screen.

To set up the DHCP Server:

1. Enable the DHCP Server.
2. Specify the starting and ending address of the IP address pool. These addresses should be part of the same IP segment as the remote Internet enabled device's LAN IP Address.
3. Specify the lease time. It is a time length that the IP address is assigned to each device before it is refreshed.
4. Specify the subnet mask. It should match the remote Internet enabled device's LAN

subnet.

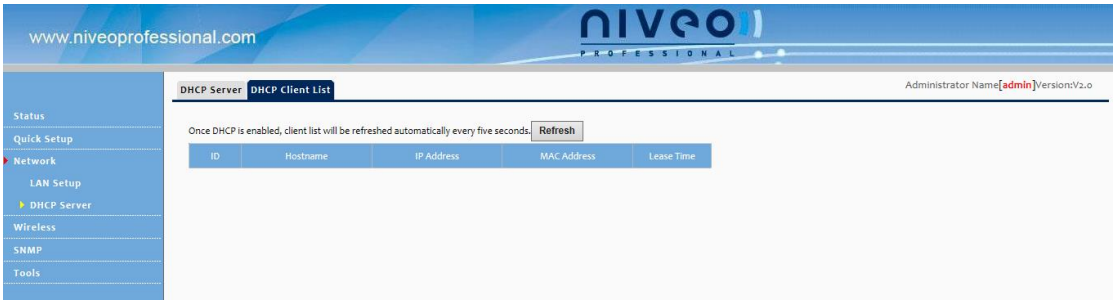
5. Set the gateway address to the LAN IP address of the remote device.
6. Configure correct DNS settings. If a wrong DNS server address is entered, Web pages may not be open.

Note

If there is already an active DHCP server on your network, make sure the IP address pool you specified here is not a part of that existing DHCP server. Otherwise, IP collisions may occur.

4.2 DHCP Client List

Click **DHCP Server -> DHCP Client List** to enter the DHCP clients screen. Here you can view the host name, IP address, MAC address, and lease time information.



5 Wireless Settings

This section describes the following.

***5.1 Basic Settings*:** Here you can configure the basic wireless settings of the device such as the SSID (name of the network) and broadcast SSID, etc.

***5.2 Radio*:** Here you can configure basic wireless settings including network mode and channel, etc.

***5.3 Channel Scan*:** Here you can scan current wireless signals.

***5.4 Advanced Settings*:** Here you can configure advanced wireless settings. This is only recommended to advanced users.

***5.5 Access Control*:** Specify a list of devices to allow or disallow a connection to your wireless network via the device's MAC addresses.

***5.6 QVLAN*:** Here you can configure the QVLAN feature to better manage wireless traffic and enhance wireless security.

5.1 Basic Settings

Here you can configure the basic wireless settings of the device such as the SSID (name of the network) and security.

SSID: Select the SSID you wish to use. This is the public name of your wireless network. Two SSIDs are supported.

Enable: Select whether to enable the selected SSID.

Broadcast SSID: This option allows you to have your network names (SSIDs) publicly broadcast or if you choose to disable it, the SSIDs will be hidden. To join your hidden wireless network, you must enter the SSID manually.

AP Isolation: Isolates clients connecting to this SSID.

Maximum Clients: Set the number of wireless clients that can join your wireless network. When the number of wireless clients reaches the set value, new connections to this SSID will be denied.

SSID: This field is configurable. You can change the current SSID.

Security Mode: Configure security settings for the current SSID. This device supports WEP, WPA-PSK, WPA2-PSK, WPA/WPA2-PSK Mixed, WPA and WPA2 (To learn more, read the following).

WEP

WEP (Wired Equivalent Privacy): WEP is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard, its intention was to provide data confidentiality comparable to that of a traditional wired network. Wireless speed can reach up to 54Mbps if WEP is used.

Open, Shared and 802.1x are the same in encryption progression yet different in authentication mode.

Open: Uses "no authentication" + WEP Encryption. Wireless clients can be associated with the device without going through authentication. Only data in transmission is encrypted with WEP encryption.

Shared: Uses shared key authentication + WEP Encryption. A WEP key that is mutually agreed in advance is required from both sides while wireless clients try to associate with the device. Association is established only if the two sides provide the same WEP key.

802.1x: Adopts802.1x identity authentication + WEP encryption mode. The supplicant (i.e., client device) is not allowed to access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. If authentication is successful, the authenticator sets the port to the "authorized" state and normal traffic is allowed, if it is unsuccessful the port remains in the "unauthorized" state and blocks traffic.

Default Key: Specify a WEP key from the preset keys for current use. For example, if you select Key 2, wireless clients must join your wireless network using this Key 2.

WEP-802.1x Configuration Procedures:

SSID: This is the public name of your wireless network. Select the SSID you wish to configure from the drop-down list.

1. **Security Mode:** Select WEP.

   Encryption Mode: Select 802.1X.

2. **Radius Server:** Enter the IP address of Radius server on your LAN.

3. **Radius Port:** Enter the Authentication port for the Radius server on your LAN.

4. **Radius Key:** Enter the Authentication key for the Radius server.

WPA-PSK, WPA2-PSK

WPA: 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 tampered with. Only authorized network users can access the wireless network. WPA adopts enhanced encryption algorithm over WEP.

WPA2: WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP. It is more secure than WPA and WEP.

Security Mode: Supports WPA-PSK, WPA2-PSK and WPA/WPA2-PSK Mixed.

WPA-PSK: Supports AES and TKIP cipher types.

WPA2-PSK: Supports AES, TKIP and TKIP+AES cipher types.

WPA/WPA2-PSK mixed: If selected, both WPA-PSK and WPA2-PSK secured wireless clients can join your wireless network.

Cipher Type: Includes AES, TKIP and TKIP&AES.

AES: If selected, wireless speed can reach up to 300Mbps.

TKIP: If selected, wireless speed can reach up to 54Mbps.

TKIP+AES: If selected, both AES and TKIP secured wireless clients can join your wireless network.

Key Update Interval: Enter a valid time period for the key to be changed.

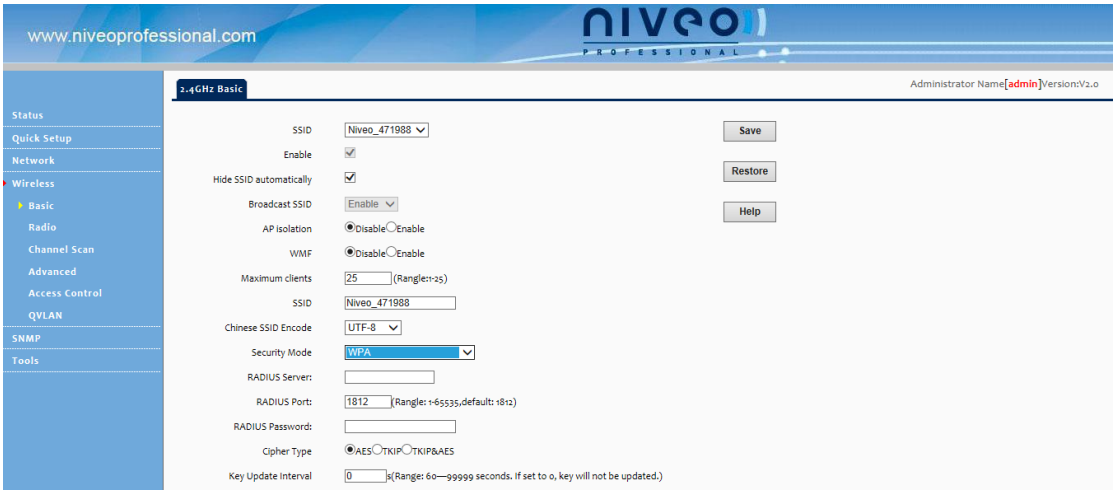
Configuration Procedures:

1. **SSID:** This is the public name of your wireless network. Select the SSID you wish to configure from the drop-down list.
2. **Security Mode:** Select WPA-PSK, WPA2-PSK or WPA/WPA2-PSK Mixed.
3. **Cipher Type:** Select the cipher type you wish to use.
4. **Key:** Enter a security key.

WPA, WPA2

The Wi-Fi Alliance defined the WPA/WPA2 in response to weaknesses found in WPA-PSK or WPA2-PSK in key management. It uses 802.1x to authenticate users and generate a root key for encrypting data instead of using a manually set pre-shared key.

With 802.1X authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network. Data transmission over the wireless network is encrypted with dynamic keys assigned by the Radius server, which greatly enhances security. WPA/WPA2 becomes the most preferred security mode.



Configuration Procedures:

1. **SSID:** This is the public name of your wireless network. Select the SSID you wish to configure from the drop-down list.
2. **Security Mode:** Select WPA or WPA2.
3. **RADIUS Server:** Enter the IP address of Radius server on your LAN.
4. **RADIUS Port:** Enter the Authentication port for the Radius server on your LAN.
5. **RADIUS Key:** Enter the Authentication key for the Radius server.
6. **Cipher Type:** Select the cipher type you wish to use.

5.2 Radio

Click **Wireless -> Radio** to enter the configuration screen. Here you can configure basic wireless settings including network mode, channel and etc.

Enable Wireless: Enable or disable the wireless feature.

Network Mode: Select a correct mode according to your wireless clients. The default is 11b/g/n mixed.

11b: This network mode delivers wireless speed up to 11Mbps and is only compatible with 11b wireless clients.

11g: This network mode delivers wireless speed up to 54Mbps and is only compatible with 11g wireless clients.

11b/g: This network mode delivers wireless speed up to 54Mbps and is compatible with 11b and 11g wireless clients.

11b/g/n mixed: This network mode delivers wireless speed up to 300Mbps and is compatible with 11b/g/n wireless clients.

Channel: Select a channel or select Auto to let system automatically select one for your wireless network to operate on if you are unsure. The best selection is a channel that is the least used by neighboring networks.

Channel Bandwidth: Select a proper channel bandwidth to enhance wireless performance. This option is available only in 802.11b/g/n. Wireless speed in the channel bandwidth of 20/40 is 2 times in 20.

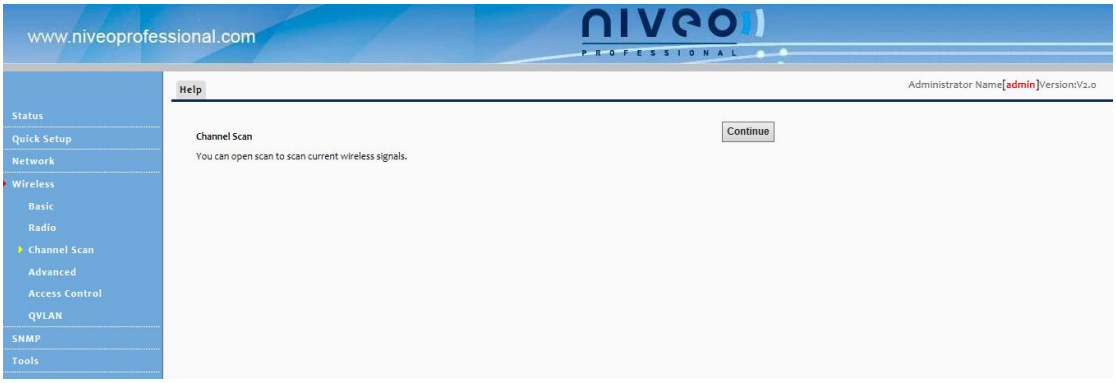
Extension Channel: This is used to ensure N speeds for 802.11n devices on the network. This option is available in 11b/g/n mixed mode with channel bandwidth of 20/40.

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: Auto power saving mode. This option is effective only if WMM is enabled. It is advisable to keep it disabled.

5.3 Channel Scan

Here you can scan current wireless signals.

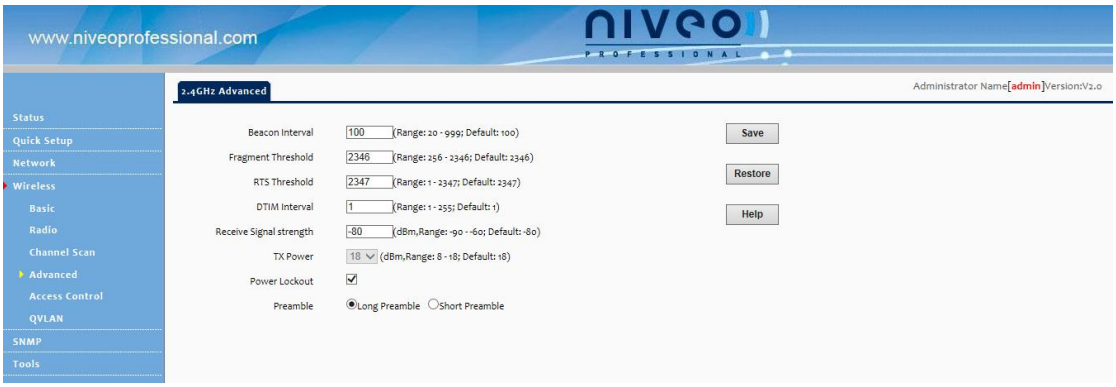


5.4 Advanced Settings

Here you can configure the advanced wireless settings including AP Isolation, Beacon interval, Fragment threshold, RTS threshold and DTIM interval, etc, for your wireless networks. Normally, the default settings will work. If not, change them according to the suggestions given by your ISP or our technical staff. Click **Wireless -> Advanced** to enter the configuration interface.

Note

Only change the default settings if instructed by your ISP or our technical staff. Wrong configurations may degrade your wireless performance.



Beacon Interval: A time interval between any two consecutive Beacon packets sent by an Access Point to synchronize a wireless network. The valid value range is between 20~999.

Fragment Threshold: Specify a Fragment Threshold value. Any wireless packet exceeding the preset value will be divided into several fragments before transmission. The valid value range is between 256~2346.

RTS Threshold: If a packet exceeds the 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. The valid value range is between 1~2347.

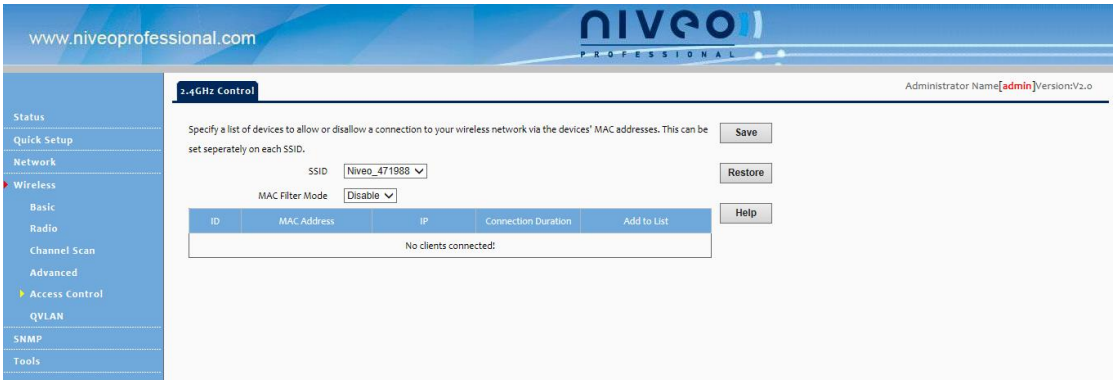
DTIM Interval: A DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next window for listening to broadcast and multicast messages. When such packets arrive in the router's buffer, the router will send DTIM (delivery traffic indication message) and DTIM interval to alert clients of the receiving packets.

TX Power: Here you can adjust the power of the wireless signal

Preamble: There are two types of preambles: long preamble and short preamble. The preamble signals to the receiving node that data is incoming and indicates when the data flow is about to begin. For wireless transmission, the longer the preamble is, the less the data is. So support of a short preamble can boost the transmission efficiency of a wireless interface. Support of short preamble is optional for 802.11b yet a must for 802.11g.

5.5 Access Control

Specify a list of devices to "Permit" or "Forbid" a connection to your wireless network via the devices' MAC Addresses. Click **Wireless -> Access Control** to enter the configuration screen.



MAC Filter: There are three options available: **Disable**, **Deny** and **Allow**.

Disable: Disable the access control feature.

Allow: Allow only devices at specified MAC addresses to join your wireless network.

Deny: Blocks only devices at specified MAC addresses from joining your wireless network.

Configuration Procedures:

1. **SSID:** This is the public name of your wireless network. Select the SSID you wish to configure from the drop-down list.
2. **MAC Filter Mode:** Select a MAC filter mode from the drop-down list.
3. Enter the wireless MAC address you wish to restrict and click **Add**. (Also, you can simply select a wireless MAC address from the MAC addresses displayed on this page to quickly add it)

5.6 QVLAN

This device supports IEEE 802.1Q VLAN. With QVLAN enabled, this device can work together with a VLAN capable switch to create multiple wireless subnets. Wireless stations with different VLAN IDs will not be able to intercommunicate.

Note

When you enable QVLAN, only one SSID can be encrypted.

Click **Wireless -> QVLAN** to enter the configuration interface.

Configuration Procedures:

Step1: Check **Enable**.

Step2: Configure a VLAN ID for a corresponding SSID.

6 SNMP

The NWA200 can be managed from SNMP management utility. Click **SNMP** to enter the configuration screen. Here you can configure the SNMP settings.

Configuration Procedures:

1. **SNMP:** Select **Enable** to enable the SNMP proxy feature.
2. Specify the Administrator Name, Device Name and Location.
3. **Read Community:** Specify a community string for SNMP management utility to read the device's MIB information.
4. **Write/Read Community:** Specify a community string for SNMP management utility to write/read the device's MIB information.

7 Tools

This section explains the following:

7.1 Maintenance: Explains firmware upgrade and device reboot.

7.2 Time & Date: Explains how to set up system time and web login timeout.

7.3 Logs: View the history of the device's actions, log events and simultaneously send them to the specified log server.

7.4 Configuration: Explains how to save, restore configurations as well as restore factory defaults.

7.5 User Name & Password: Explains how to change login user name and password.

7.6 Diagnostics: Explains how to locate a network failure.

7.7 Reboot: For some settings to be effective, a reboot is required. All connections will be lost while rebooting.

7.8 LED: Here you can disable all LED lights

7.1 Maintenance

Firmware Upgrade

Firmware upgrade is released periodically to improve the functionality of your device and also to add new features. Click **Tools -> Maintenance** to enter the configuration screen.

To update firmware, do as follows:

Step 1: Click **Browse** to locate the firmware.

Step 2: Click **Upgrade** and wait until the Progress Indicator bar shows 100% completed.

Note

Do NOT disconnect the device from power supply when uploading software to the device. If the power supply is interrupted, the upload may fail, corrupt the software, and render the device inoperable. When the upload completes, your wireless access point will automatically restart. The upgrade process typically takes about several minutes.

To better experience stability or added features, restore the device to factory default settings after upgrading firmware and then reconfigure it.

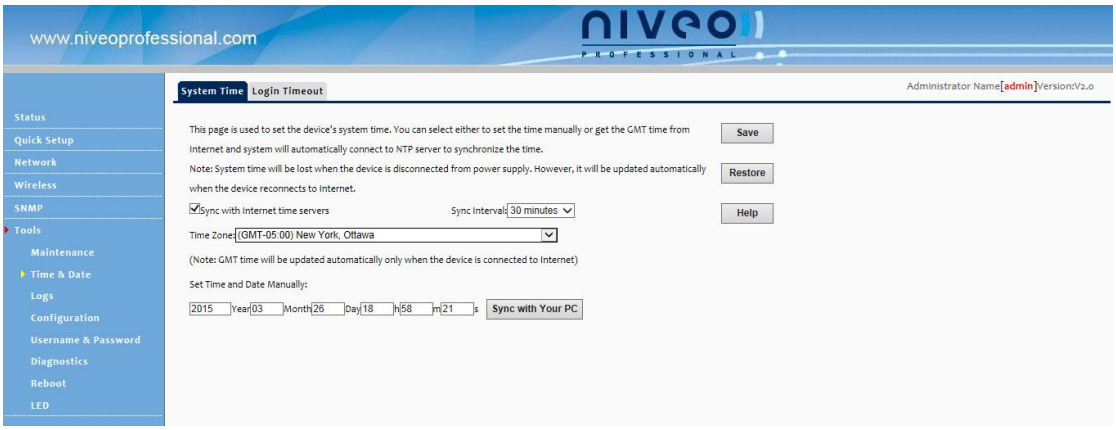
7.2 Time & Date

System Time

Click **Tools -> Time** to enter the time screen. System can be configured using the following 2 methods:

Sync with Internet time servers: If enabled, system automatically connects to NTP server on the Internet to synchronize the time.

Set Time and Date Manually/Sync with Your PC: Specify the time and date manually or click **Sync with Your PC** to automatically copy your current PC's time to the device.



To Sync with Internet time servers:

1. Enable **Sync with Internet time servers.**
2. Select a Sync Interval from the drop-down list.
3. Select your time zone.

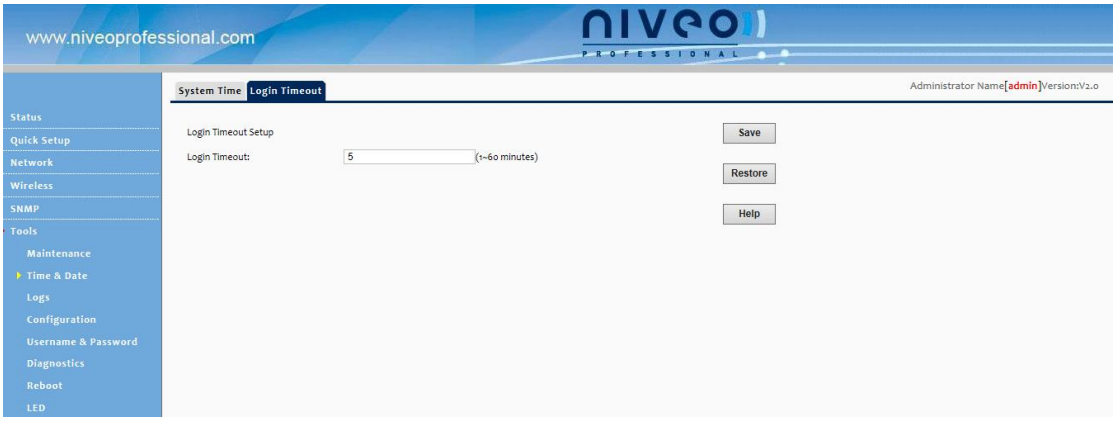
To set time and date manually:

1. Disable **Sync with Internet time servers.**
2. Specify the time and date manually or click **Sync with Your PC** to automatically copy your PC's time to the device.

And then go to **Status** to make sure the system time is correctly updated.

Web Login Timeout

Click **Tools -> Time -> Login Timeout** to enter the configuration screen. Here you can set up the web Login Timeout. The device returns to login window automatically depending on the specified login timeout and user name/password will be required.



7.3 Logs

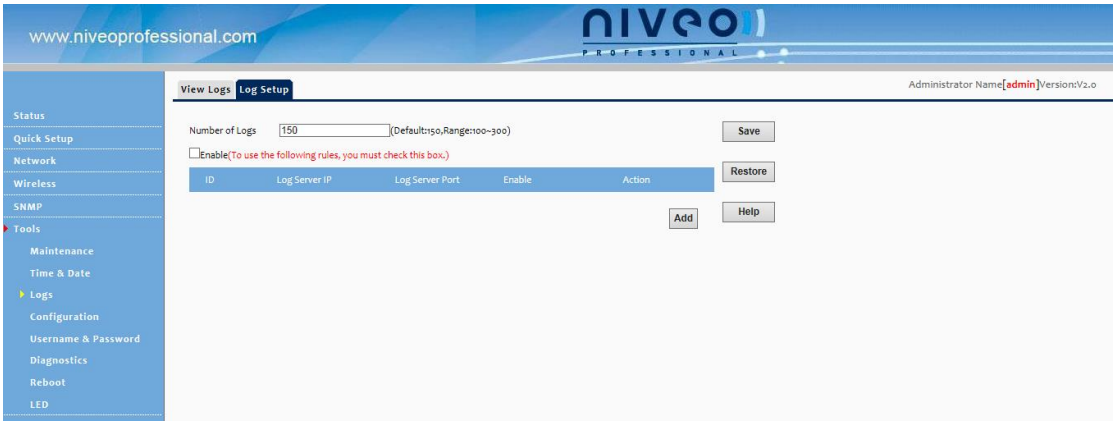
View Logs

Click **Tools -> View Logs** to enter the logs screen. Here you can view the history of the device's actions.

There are three types of logs are available: All, system and LAN. To view a specific type of log, simply select it from the **View Log Levels** drop-down list.

Log Setup

Click **Tools -> Log Setup** to configure the system Log options. You can set the maximum number of logs that can be displayed and configure the log server settings.



To configure the log server:

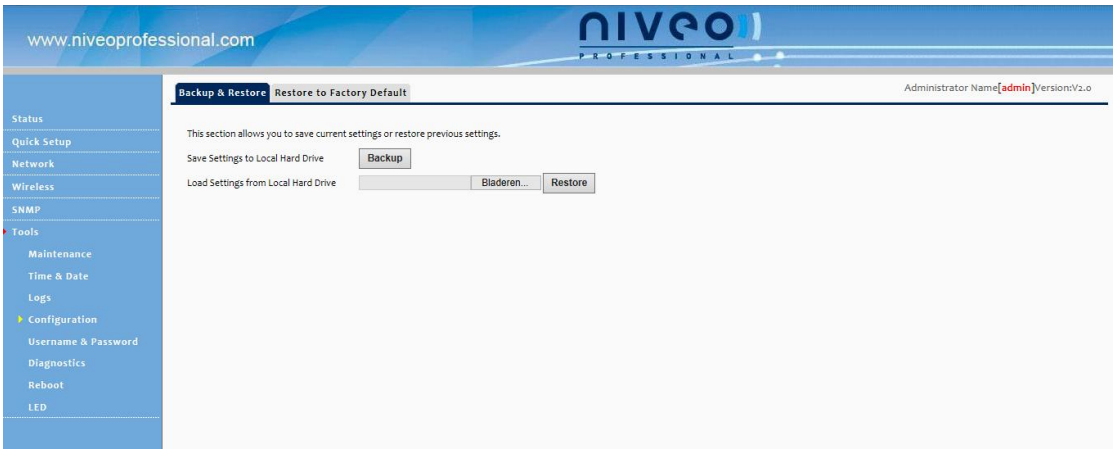
1. Click **Add** to add a log server.
2. Specify the IP address and port of the syslog server on your LAN and enable the log server.
3. Check the "To use the following rules, you must check this checkbox." option.

If configured successfully, the system will begin to log events and simultaneously send them to the specified log server on your LAN. You can view all logs there.

7.4 Configuration

Backup & Restore

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



Configuration Procedures:

1. Click **Backup**.
2. Click **Save** on the **File Download** window and select a hard drive to save the file.

Tip

Do include the file name suffix of ".cfg" when renaming the file name to avoid problems.

Configuration Procedures:

1. Click **Browse**.
2. Select and load the configuration file that is saved previously to your local hard drive and click the **Restore** button.

Restore to Factory Default

If the device or clients connected to the device fail to access the Internet due to incorrect configurations and you cannot solve the problem, click **Tools -> Configuration -> Restore to Factory Default** to reset the device and then reconfigure it.

Method 1: To restore factory default using UI: Click the **Restore to Factory Default** button and wait until the progress indicator displays 100% completed.

Method 2: To restore factory default by pressing the hardware reset button:

1. Remove the cover of the device.
2. Press the RST button with a needle for about 7 seconds.

Factory Default Settings are listed below:

Default User Name: admin

Default Password: admin

Default LAN IP Address: 192.168.2. 200**.** This IP address is to be used to access the device's settings through a web browser.

Default LAN Subnet Mask: 255.255.255.0

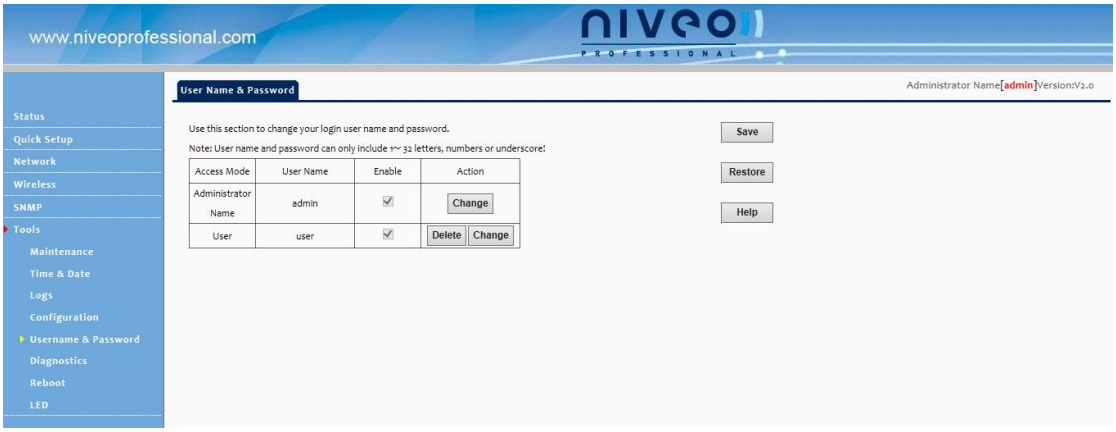
Tip

1. The action of "restore factory default" removes all your configurations from the device. So if you want to keep your configurations, do not perform this action.
2. Do not restore factory default settings unless the following happens:

You need to join a different network or unfortunately forget the login password.

7.5 User Name & Password

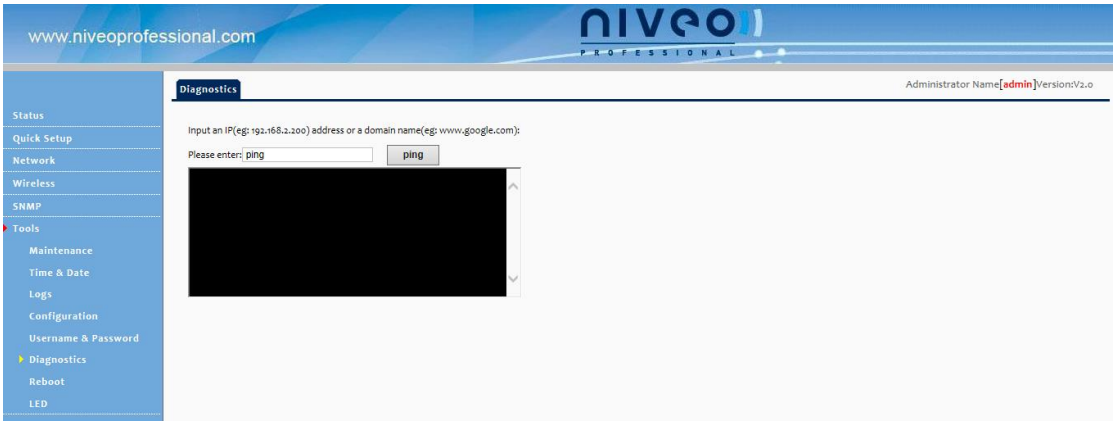
Click **Tools -> User Name & Password**. Here you can change the user name and password for web login. We suggest that you change the default password to a more secure password.



- **Administrator:** If you log in to the device as an administrator, you have all available rights to access the device.
- **User:** If you log in to the device as a user, you can only view configurations instead of configuring or changing any existing configurations.

7.6 Diagnostics

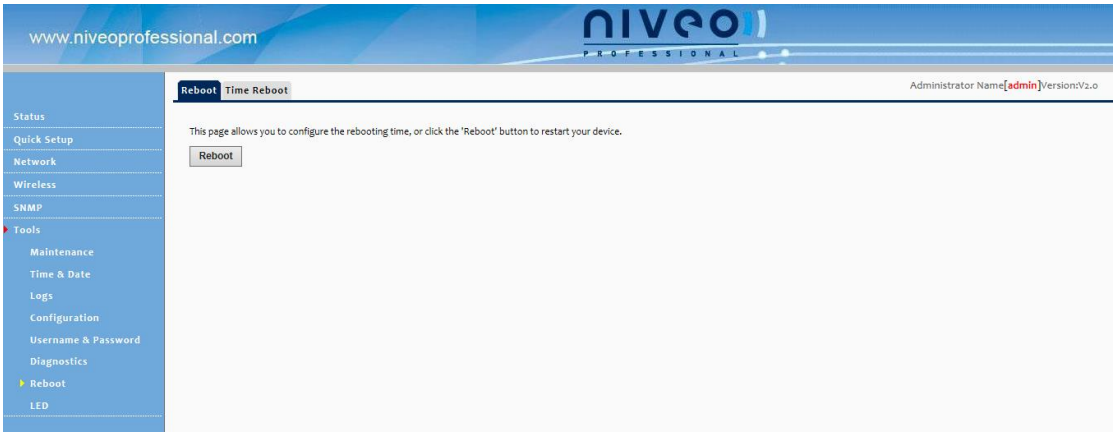
The device is capable of testing your connection. If your network is malfunctioning, click **Tools -> Diagnostics** to use the ping utility to test your network and find out where the problem is.



7.7 Reboot

Reboot

For some settings to be effective, a reboot is required. All connections will be lost while rebooting. Click **Tools -> Reboot** to enter the configuration screen.



Time Reboot: here you schedule a time to do a reboot

7.8 LED

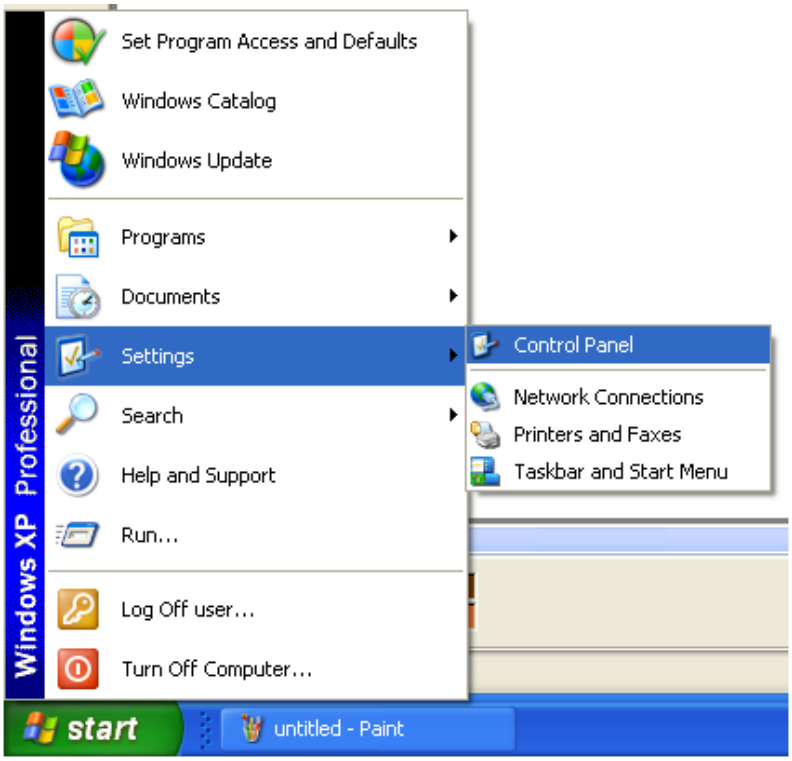
Here you can turn on / off all LED lights

Ⅴ Appendix

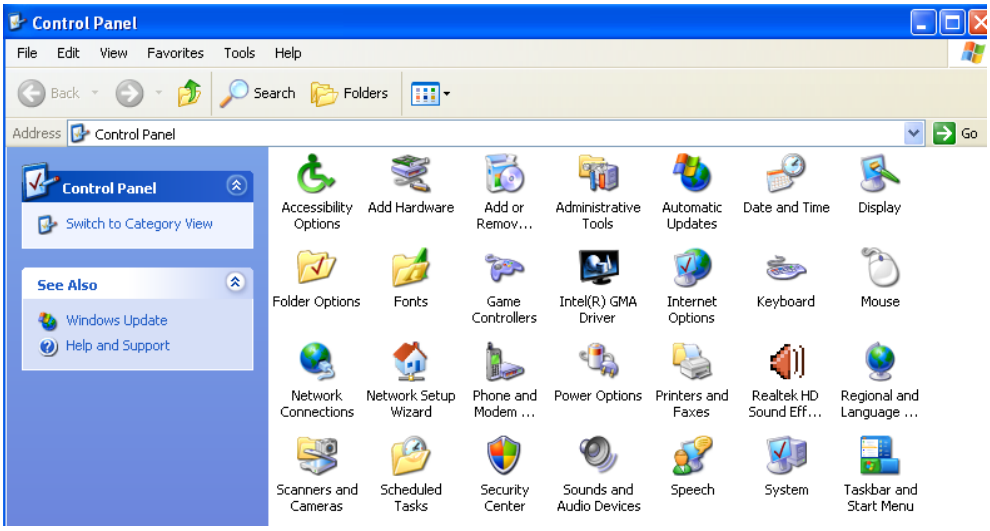
1 Configure PC TCP/IP Settings

Windows XP

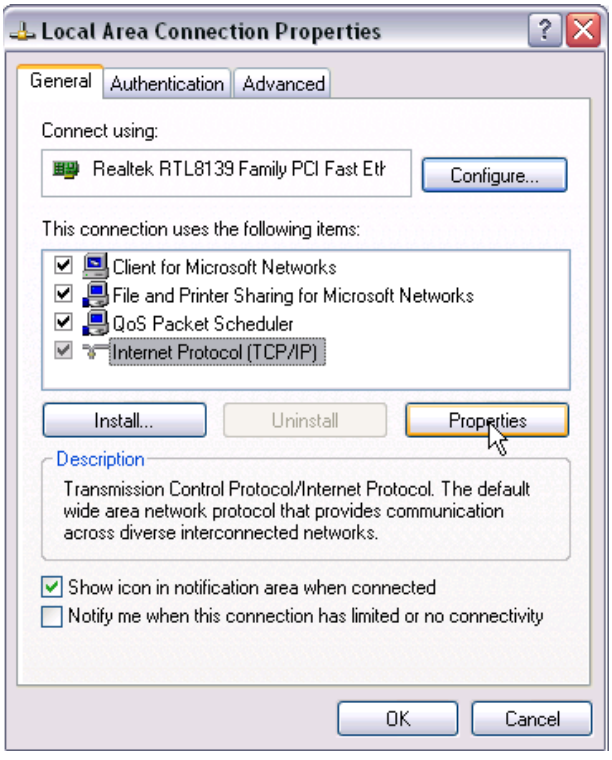
1. Click **Start -> Settings -> Control Panel**.



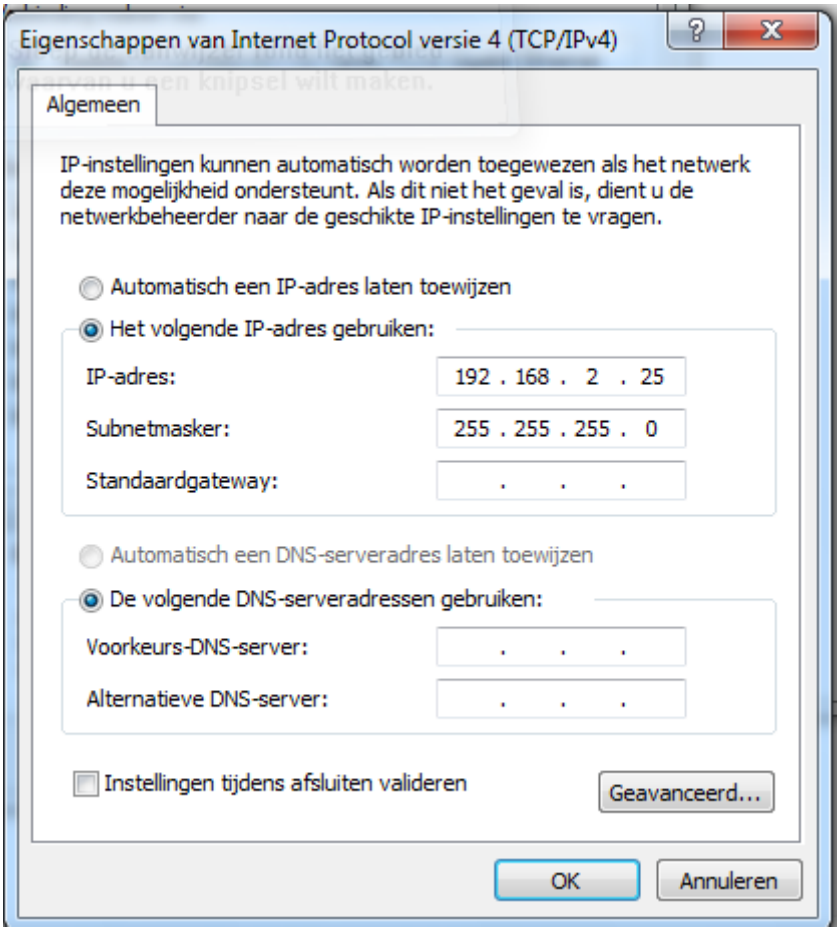
2.Click **Network Connections**.



3.Right click **Local Area Connection**，click **Properties,** select **Internet Protocol (TCP/IP)** on the appearing window and then click **Properties**.



4. Select **Use the following IP address** and configure as below:
IP address: 192.168.2.x (where x can be any number between 2~253)
Subnet Mask: 255.255.255.0.



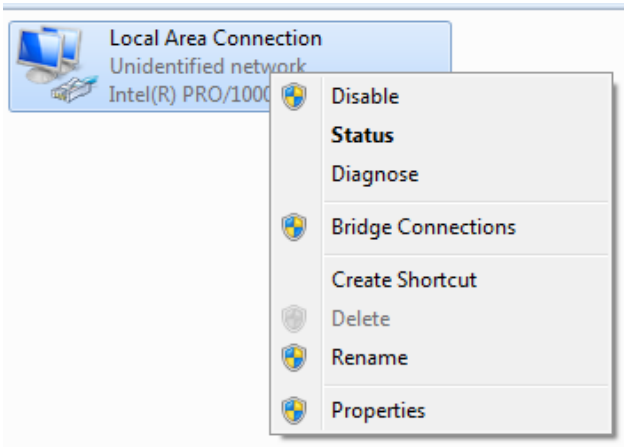
5. Click **OK** twice to exit.

Windows 7

1. Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

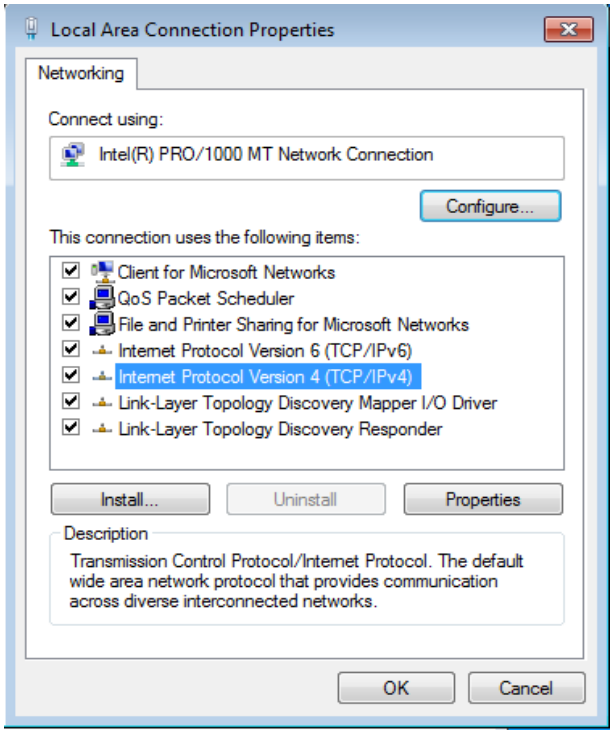
2. Click **Change adapter settings**.

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

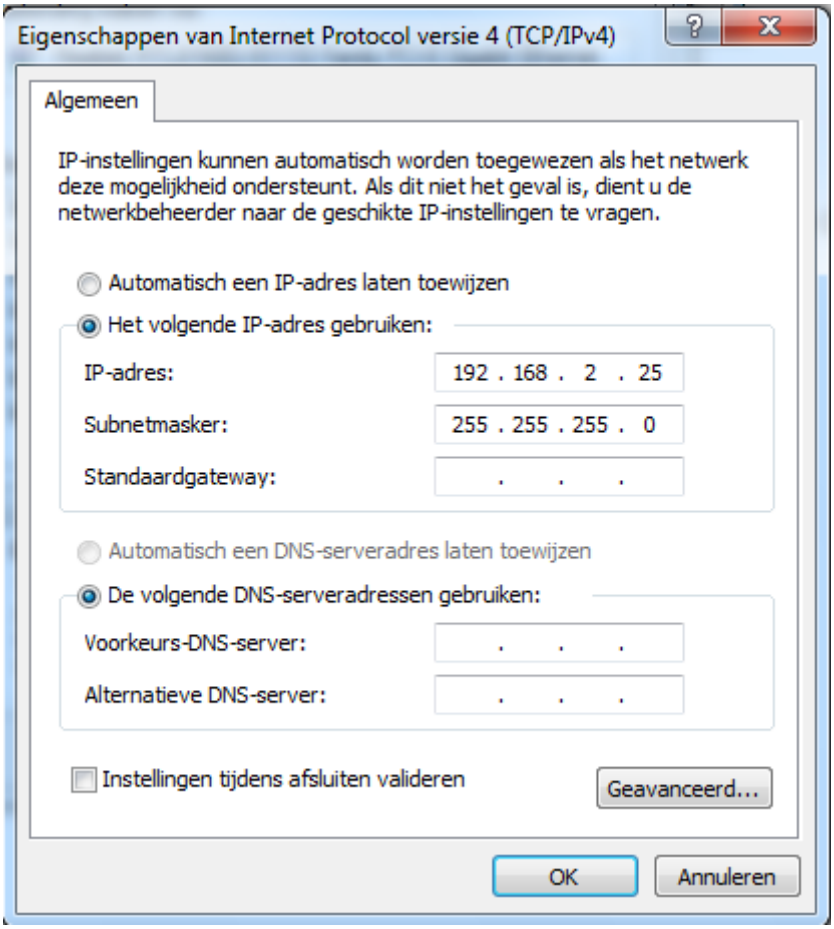


4. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties** or directly

double-click on **Internet Protocol Version 4 (TCP/IPv4)**.



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



IP address: Enter 192.168.2.xxx where xxx can be any number between 2~253.

Subnet mask: Enter 255.255.255.0

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

2 Factory Default Settings & Specifications

Default Settings

Item		Default Settings
Login	Login IP Address	192.168.2.200
	Login User Name	admin
	Login Password	admin
LAN Settings （LAN）	IP Address	192.168.2.200
	Subnet Mask	255.255.255.0
	DHCP Server	Disabled
	IP Pool	192.168.2.100~192.168.2.199
Wireless	Wireless	Enabled
	Network Mode	11b/g/n mixed
	Channel| Channel Bandwidth Extension Channel	Auto|20/40|Auto
	WMM	Enabled
	APSD	Disabled
	SSID	Primary SSID: Niveo_1 Secondary SSID: Niveo_2
	SSID Status	Primary SSID: Enabled Secondary SSID: Disabled
	Broadcast SSID	Enabled
	AP isolation	Disabled
	Number of Clients	25
	Beacon Interval	100ms
	Fragment Threshold	2346

	RTS Threshold	2347
	DTIM Interval	1
	Wireless LED On/Off	Enable
	Preamble	Long Preamble
	Wireless Security	Disabled
	Wireless Access Control	Disabled
Tools	SNMP	Disabled
	SNMP	Administrator Name: Administrator Device Name: NWA200 Location: Shenzhen Read Community String: public Write/Read Community String: private
	System Time	Sync with Internet Time Servers Time Zone: (GMT-5:00)New York
	Web Login Timeout	5 minutes
	Number of Logs	200
	User Name & Password	Administrator: User Name | Password (admin | admin) User: User Name | Password (user | user)

3 Safety and Emission Statement

CE Mark Warning

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

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

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

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

Radiation Exposure Statement

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

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