

# DrayTek

## VigorAP 710

802.11n Access Point



*Your reliable networking solutions partner*

## *User's Guide*

**V1.0**



# **VigorAP 710**

## **802.11n Access Point**

### **User's Guide**

**Version: 1.0**

**Firmware Version: V1.1.0**

**(For future update, please visit DrayTek web site)**

**Date: February 24, 2014**

## Copyright Information

### Copyright Declarations

Copyright 2014 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

### Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

## Safety Instructions and Approval

### Safety Instructions

- Read the installation guide thoroughly before you set up the modem.
- The modem is a complicated electronic unit that may be repaired only by authorized and qualified personnel. Do not try to open or repair the modem yourself.
- Do not place the modem in a damp or humid place, e.g. a bathroom.
- The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the modem to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the modem, please follow local regulations on conservation of the environment.

### Warranty

We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of one (1) year from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

### Be a Registered Owner

Web registration is preferred. You can register your Vigor modem via <http://www.draytek.com>.

### Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all modems will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

<http://www.draytek.com>

## European Community Declarations

Manufacturer: DrayTek Corp.  
Address: No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303  
Product: VigorAP 710

DrayTek Corp. declares that VigorAP 710 is in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC, ErP 2009/125/EC and RoHS 2011/65/EU.

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 2004/108/EC by complying with the requirements set forth in EN55022/Class B and EN55024/Class B.

The product conforms to the requirements of Low Voltage (LVD) Directive 2006/95/EC by complying with the requirements set forth in EN60950-1.

## Federal Communication Commission Interference Statement

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

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 may accept any interference received, including interference that may cause undesired operation.

The antenna/transmitter should be kept at least 20 cm away from human body.

This product is designed for 2.4GHz WLAN network throughout the EC region and Switzerland with restrictions in France.



Please visit <http://www.draytek.com/user/SupportDLRTTECE.php>

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

## FCC RF Radiation Exposure Statement

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.



## Table of Contents

# 1

<b>Preface .....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 LED Indicators and Connectors .....	2
1.3 Hardware Installation .....	4

# 2

<b>Network Configuration.....</b>	<b>5</b>
2.1 Windows 7 IP Address Setup.....	5
2.2 Windows 2000 IP Address Setup.....	7
2.3 Windows XP IP Address Setup.....	8
2.4 Windows Vista IP Address Setup.....	9
2.5 Accessing to Web User Interface.....	10
2.6 Changing Password.....	11
2.7 Quick Start Wizard .....	12
2.7.1 Configuring 2.4GHz Wireless Settings – General .....	12
2.7.2 Configuring 2.4GHz Wireless Settings based on the Operation Mode .....	14
2.7.3 Configuring 2.4GHz Security Settings .....	19
2.7.4 Finishing the Wireless Settings Wizard .....	21
2.8 Online Status.....	21

# 3

<b>Advanced Configuration .....</b>	<b>23</b>
3.1 Operation Mode .....	24
3.2 LAN .....	25
3.3 General Concepts for Wireless LAN .....	27
3.4 Wireless LAN Settings for AP Mode .....	29
3.4.1 General Setup.....	29
3.4.2 Security .....	33
3.4.3 Access Control.....	36
3.4.4 WPS.....	37
3.4.5 AP Discovery .....	38
3.4.6 WMM Configuration .....	39
3.4.7 Station List .....	41
3.5 Wireless LAN Settings for AP Bridge-Point to Point/AP Bridge-Point to Multi-Point Mode ..	42
3.5.1 General Setup.....	42
3.5.2 AP Discovery .....	45
3.5.3 WDS AP Status .....	46

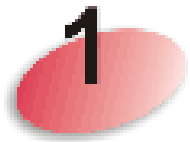
3.6 Wireless LAN Settings for AP Bridge-WDS Mode .....	46
3.6.1 General Setup.....	46
3.6.2 Security .....	51
3.6.3 Access Control.....	54
3.6.4 WPS.....	55
3.6.5 AP Discovery .....	56
3.6.6 WDS AP Status .....	57
3.6.7 WMM Configuration .....	57
3.6.8 Station List .....	59
3.7 Wireless LAN Settings for Universal Repeater Mode .....	60
3.7.1 General Setup.....	60
3.7.2 Security .....	64
3.7.3 Access Control.....	67
3.7.4 WPS.....	68
3.7.5 AP Discovery .....	69
3.7.6 Universal Repeater .....	70
3.7.7 WMM Configuration .....	72
3.7.8 Station List .....	74
3.8 RADIUS Server .....	75
3.9 Applications .....	76
3.9.1 Schedule.....	76
3.9.2 Apple iOS Keep Alive .....	78
3.10 System Maintenance.....	79
3.10.1 System Status.....	79
3.10.2 TR-069 .....	80
3.10.3 Administrator Password.....	82
3.10.4 Configuration Backup .....	83
3.10.5 Time and Date .....	84
3.10.6 Management.....	85
3.10.7 Reboot System .....	85
3.10.8 Firmware Upgrade .....	86
3.11 Diagnostics .....	86
3.11.1 System Log .....	86
3.11.2 Speed Test .....	87
3.12 Support Area .....	87

# 4

## **Trouble Shooting.....89**

4.1 Checking If the Hardware Status Is OK or Not.....	89
4.2 Checking If the Network Connection Settings on Your Computer Is OK or Not .....	90
4.3 Pinging the Modem from Your Computer.....	92
4.4 Backing to Factory Default Setting If Necessary .....	93
4.5 Contacting Your Dealer .....	94





# Preface

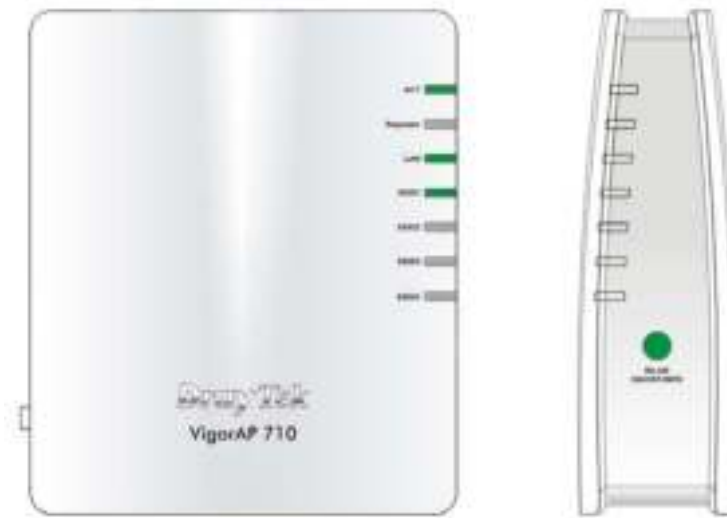
## 1.1 Introduction

Thank you for purchasing this VigorAP 710, the concurrent dual band wireless access point offering high-speed data transmission. With this high cost-efficiency VigorAP 710, computers and wireless devices which are compatible with 802.11n/802.11a can connect to existing wired Ethernet network via this VigorAP 710, at the speed of 300Mbps.

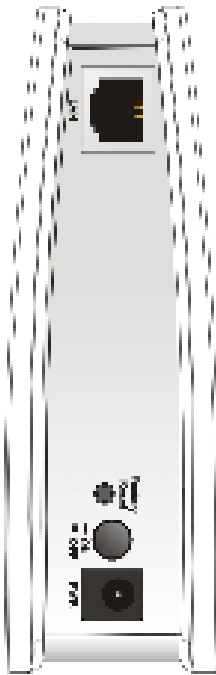

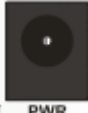

Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced users. Just follow the instructions given in this user manual, you can complete the setup procedure and release the power of this access point all by yourself!

## 1.2 LED Indicators and Connectors

Before you use the Vigor modem, please get acquainted with the LED indicators and connectors first.



LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
Repeater	On	The Repeater mode is on.
	Blinking	The Repeater mode is off.
LAN	On	LAN is connected.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
SSID1 – SSID4	On	The function of SSID is on.
	Off	The function of SSID is off.
WLAN ON/OFF/WPS (Green LED)	On (Green)	Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on.
	Off	Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off.
	Blinking (Green)	Data is transmitting (sending/receiving).
WLAN ON/OFF/WPS (Orange LED)	Blinking (Orange)	When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS. When the orange LED blinks with 1 second cycle for 2 minutes, it means that the AP is waiting for wireless client to connect with it.

	Interface	Description
	LAN	Connector for xDSL / Cable modem or router.
		Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 6 seconds. Then the router will restart with the factory default configuration.
		PWR: Connector for a power adapter.
		ON/OFF: Power switch.

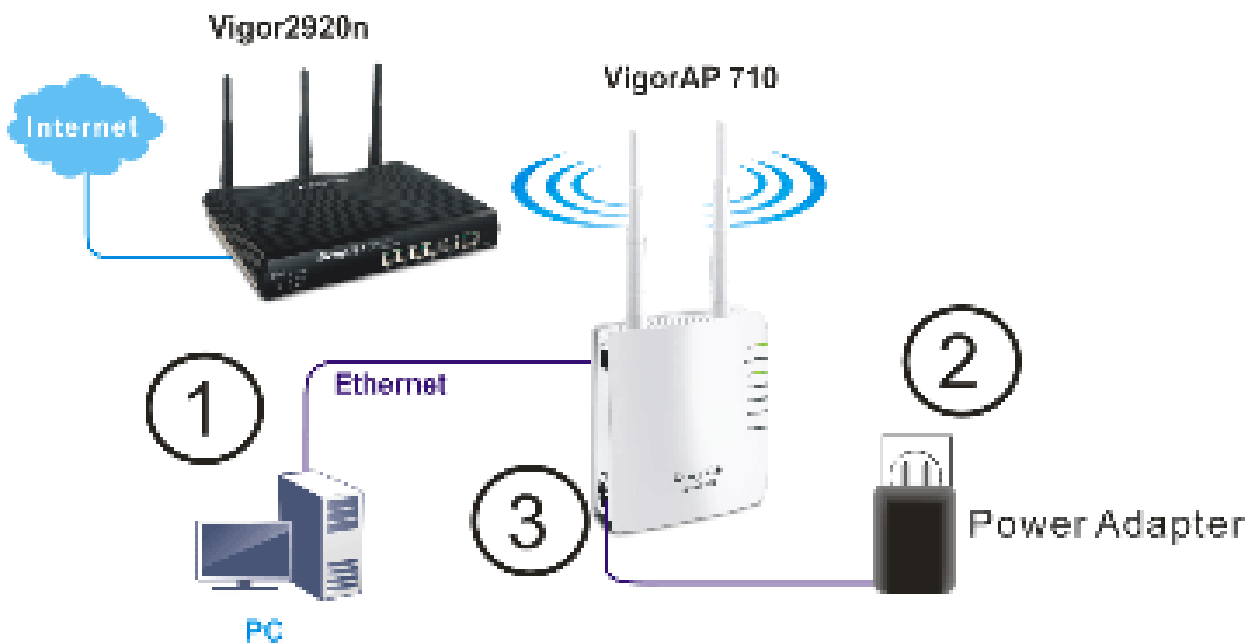
## 1.3 Hardware Installation

This section will guide you to install the VigorAP 710 through hardware connection and configure the device's settings through web browser.

Before starting to configure VigorAP 710, you have to connect your devices correctly.

1. Connect a computer to VigorAP710.
2. Connect the A/C power adapter to the wall socket, and then connect it to the PWR connector of the access point.
3. Power on VigorAP 710.
4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **SSID** LEDs should be on if the access point is correctly connected to the computer.

(For the detailed information of LED status, please refer to section 1.2.)



# 2

## Network Configuration

After the network connection is built, the next step you should do is setup VigorAP 710 with proper network parameters, so it can work properly in your network environment.

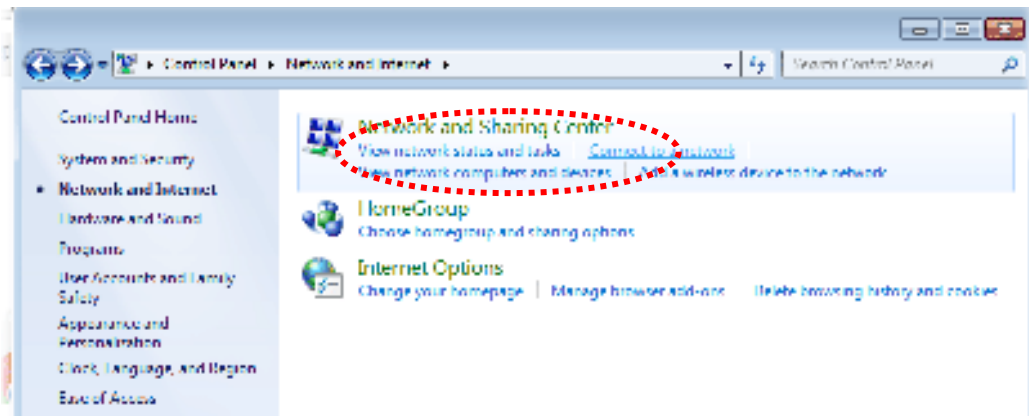
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic IP address:

For the default IP address of this AP is set "192.168.1.2", we recommend you to use "192.168.1.X (except 2)" in the field of IP address on this section for your computer.  
*If the operating system of your computer is...*

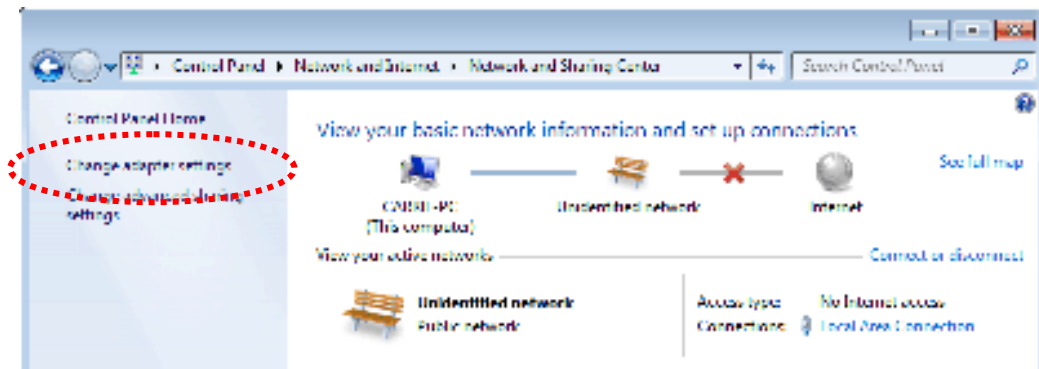
- Windows 7 - please go to section 2.1
- Windows 2000 - please go to section 2.2
- Windows XP - please go to section 2.3
- Windows Vista - please go to section 2.4

### 2.1 Windows 7 IP Address Setup

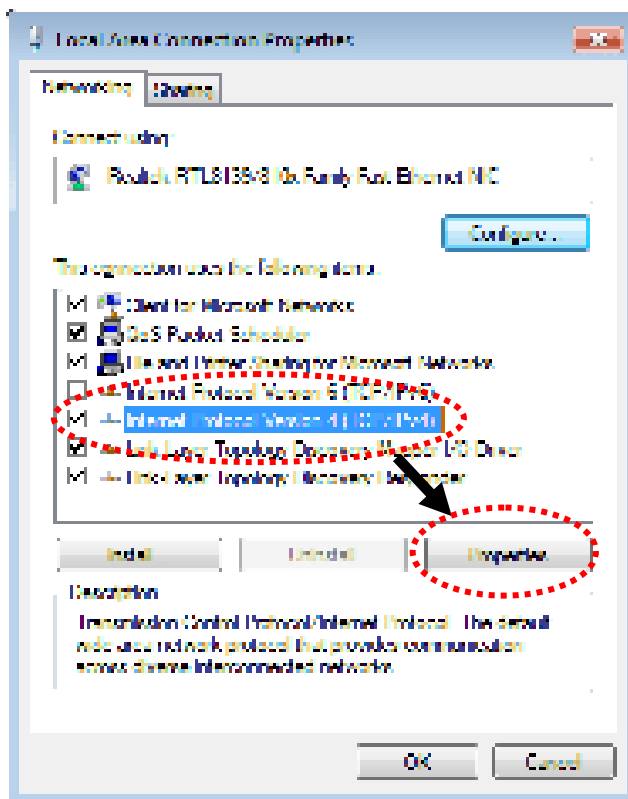
Click **Start** button (it should be located at lower-left corner of your computer), then click Control Panel. Double-click **Network and Internet**, and the following window will appear. Click **Network and Sharing Center**.



Next, click **Change adapter settings** and click **Local Area Connection**.



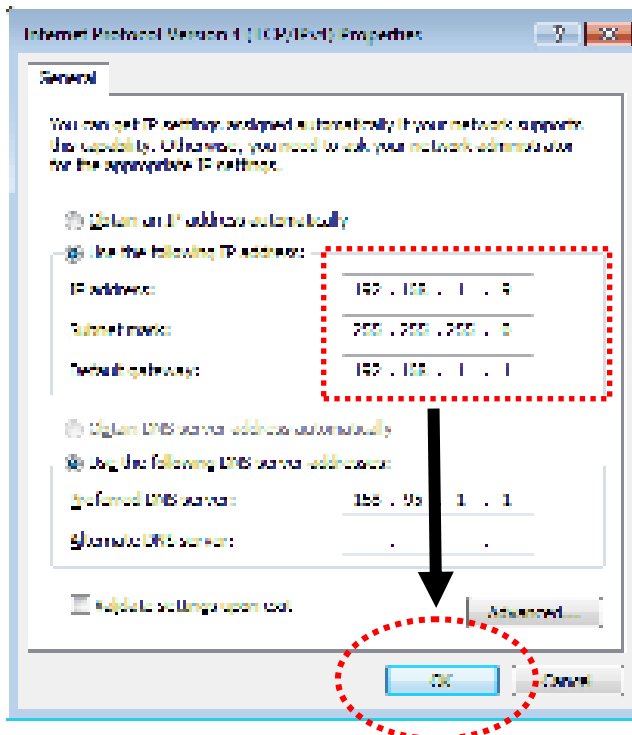
Then, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



Under the General tab, click **Use the following IP address**. Then input the following settings in respective field and click **OK** when finish.

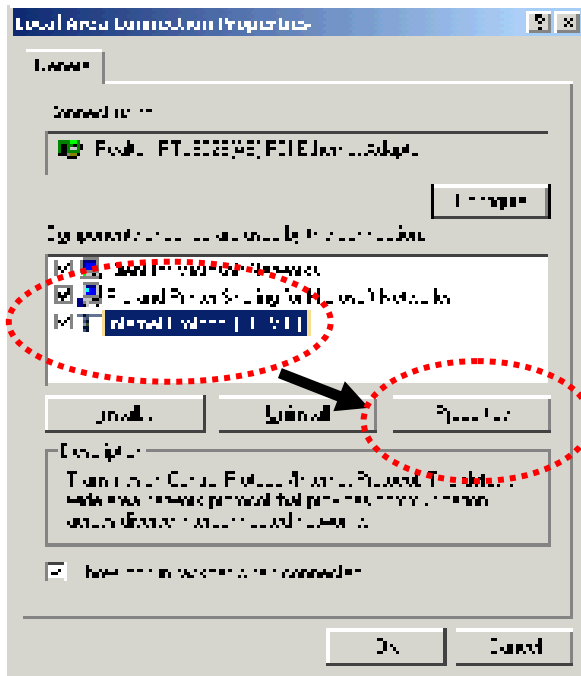
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



## 2.2 Windows 2000 IP Address Setup

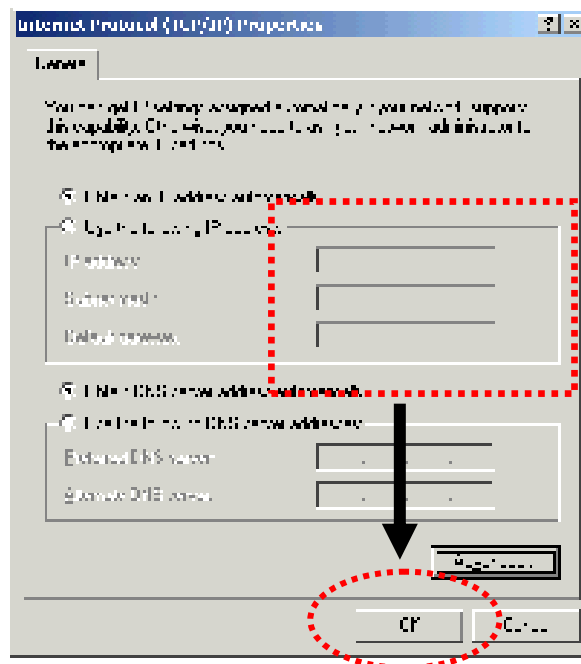
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Dial-up Connections** icon, double click **Local Area Connection**, and **Local Area Connection Properties** window will appear. Select **Internet Protocol (TCP/IP)**, then click **Properties**.



Select **Use the following IP address**, then input the following settings in respective field and click **OK** when finish.

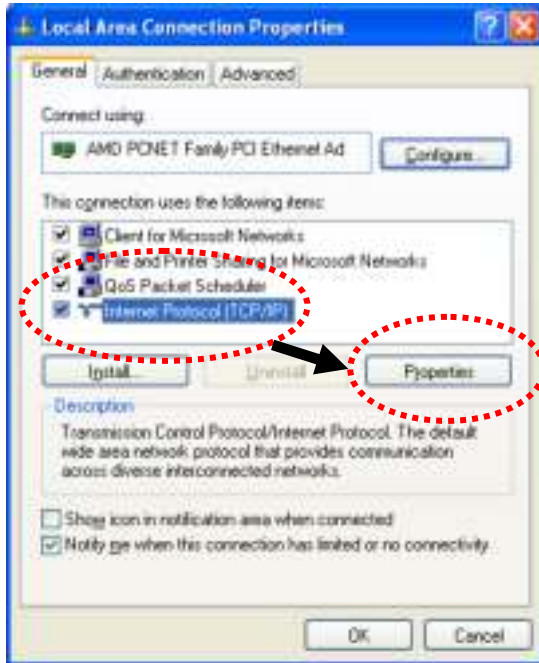
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



## 2.3 Windows XP IP Address Setup

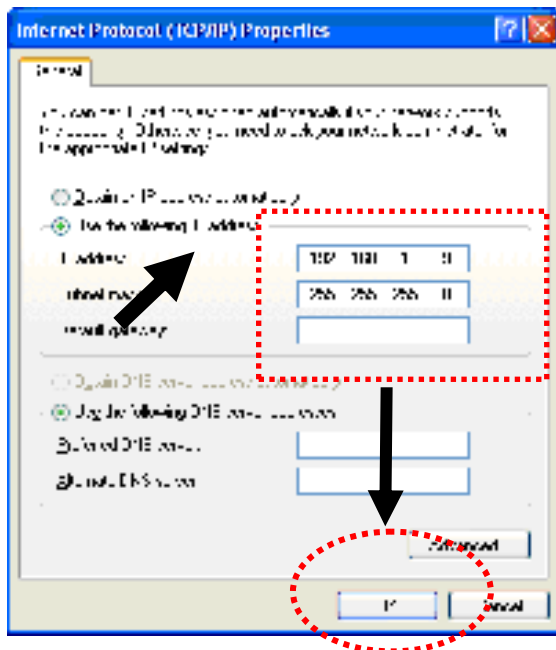
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Internet Connections** icon, click **Network Connections**, and then double-click **Local Area Connection, Local Area Connection Status** window will appear, and then click **Properties**.



Select **Use the following IP address**, then input the following settings in respective field and click **OK** when finish:

IP address: **192.168.1.9**

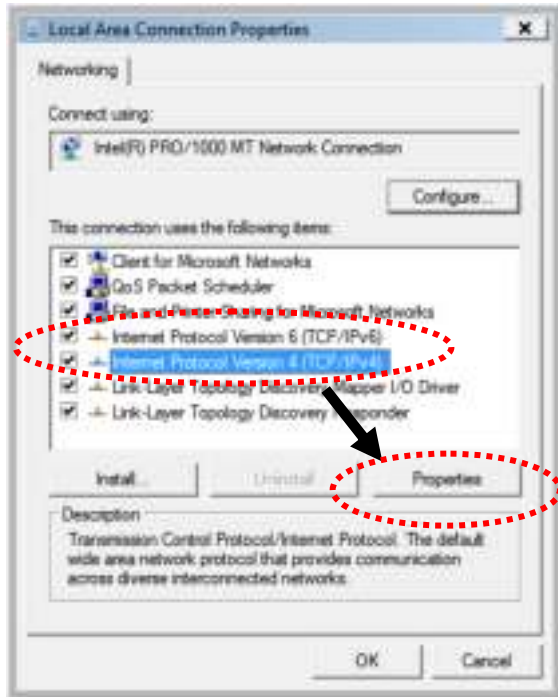
Subnet Mask: **255.255.255.0**.





## 2.4 Windows Vista IP Address Setup

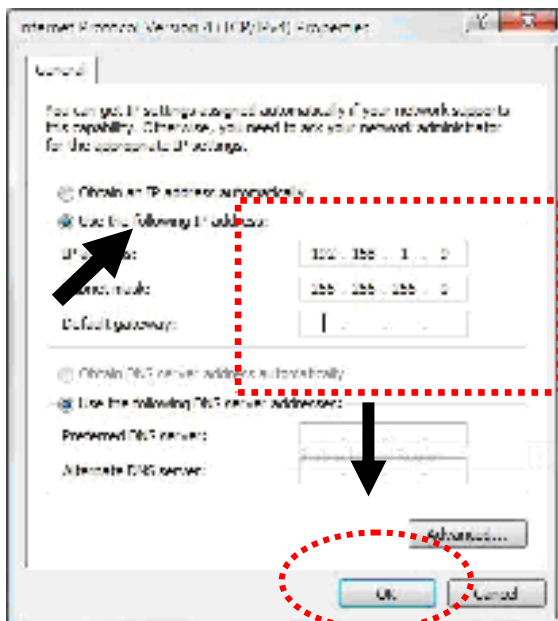
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Click **View Network Status and Tasks**, then click **Manage Network Connections**. Right-click **Local Area Network**, then select **'Properties'**. **Local Area Connection Properties** window will appear, select **Internet Protocol Version 4 (TCP / IPv4)**, and then click **Properties**.



Select **Use the following IP address**, then input the following settings in respective field and click **OK** when finish:

IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



## 2.5 Accessing to Web User Interface

All functions and settings of this access point must be configured via web user interface. Please start your web browser (e.g., IE, Firefox, Google Chrome).

1. Make sure your PC connects to the VigorAP 710 correctly.



**Notice:** You may either simply set up your computer to get IP dynamically from the modem or set up the IP address of the computer to be the same subnet as **the default IP address of VigorAP 710 192.168.1.2**. For the detailed information, please refer to the later section - Trouble Shooting of the guide.

2. Open a web browser on your PC and type **http://192.168.1.2**. A pop-up window will open to ask for username and password. Please type “admin/admin” on Username/Password and click **Log In**.

Authentication Required

The server http://192.168.1.2:80 requires a username and password.  
The server says: VigorAP710.

User Name:

Password:

3. The **Main Screen** will pop up.

**DrayTek VigorAP 710**

System Status

Model : VigorAP710  
Firmware Version : 1.1.0RC2a  
Build Date/Time : 11:37:18 Thu Jun 18 17:58:53 CST 2014  
System Uptime : 0d 00:04:07  
Operation Mode : Universal Repeater

System		LAN	
MAC Address	52:54:00:12:34:56	MAC Address	18:1C:4E:7851:71
Memory Left	3792 K	IP Address	192.168.1.2
Uplink	10/100/1000 Mbps	IP Mask	255.255.255.0
Wireless			
MAC Address	18:1C:4E:7851:71		
SSID	DrayTek		
Channel	11		

Admin mode  
Universal Repeater Mode

**Note:** If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem. For using the device properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

## 2.6 Changing Password

1. Please change the password for the original security of the modem.
2. Go to **System Maintenance** page and choose **Administrator Password**.

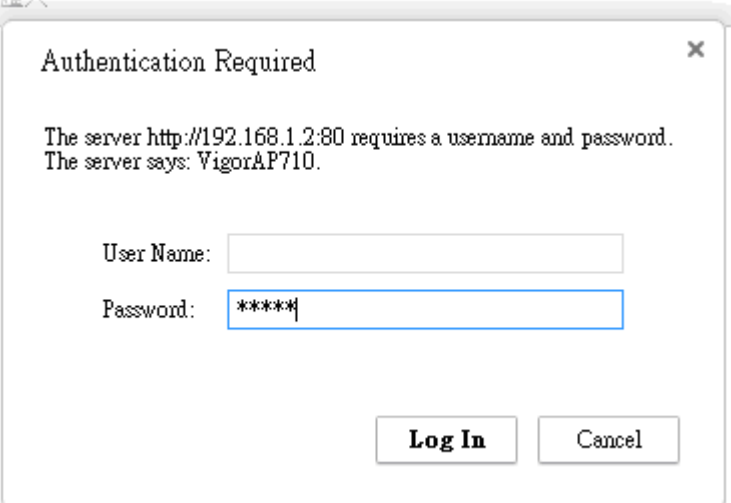
System Maintenance >> Administrator Password

### Administrator Settings

Account	admin
Username	admin
Confirm Password	

Note: Administrator account already exists. (192.168.1.2:80) - IP Address: 192.168.1.2

3. Enter the new login password on the field of **Password**. Then click **OK** to continue.
4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.



The image shows a dialog box titled "Authentication Required" with a close button (X) in the top right corner. The text inside the dialog box reads: "The server http://192.168.1.2:80 requires a username and password. The server says: VigorAP710." Below the text, there are two input fields: "User Name:" followed by an empty text box, and "Password:" followed by a text box containing "\*\*\*\*\*". At the bottom of the dialog box, there are two buttons: "Log In" and "Cancel".


## 2.7 Quick Start Wizard


Quick Start Wizard will guide you to configure 2.4G wireless setting, 5G wireless setting and other corresponding settings for Vigor Access Point step by step.


### 2.7.1 Configuring 2.4GHz Wireless Settings – General


This page displays general settings for the operation mode selected.


Quick Start Wizard >> 2.4G Wireless

Operation Mode:    
Vigor AP can act as a wireless repeater; it can be Station and AP at the same time.

Wireless Mode:  

Main SSID:  

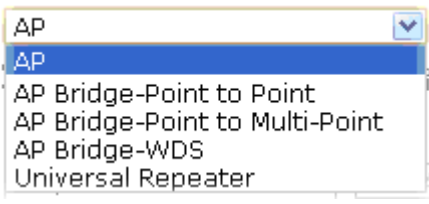
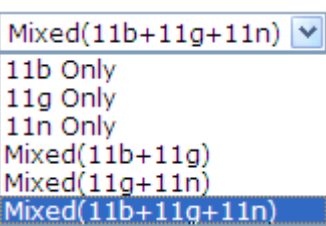
Channel:  

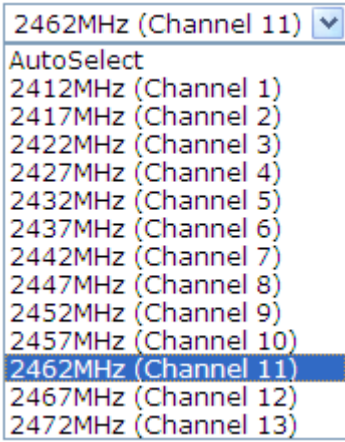
Extension Channel:  

Station List:

AP Discovery:

Available settings are explained as follows:

Item	Description
<b>Operation Mode</b>	<p>There are six operation modes for wireless connection. Settings for each mode are different.</p> 
<b>Wireless Mode</b>	<p>At present, VigorAP 710 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.</p> 
<b>Main SSID</b>	<p>Set a name for VigorAP 710 to be identified.</p> <p><b>Multiple SSID</b> - You can specify subnet interface for SSID2 ~ SSID4.</p>
<b>Channel</b>	<p>Means the channel frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the</p>

	<p>frequency, please select <b>AutoSelect</b> to let system determine for you.</p> 
<b>Extension Channel</b>	<p>With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above.</p>
<b>Station List</b>	<p>Click the <b>Display</b> button to open the Station List dialog. It provides the knowledge of connecting wireless clients now along with its status code.</p>
<b>AP Discovery</b>	<p>Click this button to open the AP Discovery dialog. VigorAP 710 can scan all regulatory channels and find working APs in the neighborhood.</p> <p>This option is available when <b>AP-Bridge/Universal Repeater</b> is selected as the <b>Operation Mode</b>.</p>

After finishing this web page configuration, please click **Next** to continue.

## 2.7.2 Configuring 2.4GHz Wireless Settings based on the Operation Mode

In this page, the advanced settings will vary according to the operation mode chosen on 2.7.1.

### Advanced Settings for AP Bridge-Point to Point

When you choose AP Bridge-Point to Point, you will need to configure the following page.

Quick Start Wizard >> Wireless LAN (2.4GHz)

---

Note: After the configuration of Advanced AP 2.4GHz is completed.

Phy Mode: HTMIX

Security:

Disabled  WEP  TKIP  AES

Key: \_\_\_\_\_

Peer MAC Address:

\_\_\_\_\_|\_\_\_\_\_|\_\_\_\_\_|\_\_\_\_\_|\_\_\_\_\_|\_\_\_\_\_

Available settings are explained as follows:

Item	Description
<b>Phy Mode</b>	Data will be transmitted via HTMIX communication channel. Each access point should be setup to the same <b>Phy</b> mode for connecting with each other.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required.
<b>Peer MAC Address</b>	Type the peer MAC address for the access point that VigorAP 710 connects to.

## Advanced Settings for AP Bridge-Point to Multi-Point

When you choose AP Bridge-Point to Multi-Point, you will need to configure the following page.

Quick Start Wizard >> Wireless LAN (2.4GHz)

Note: Enter the configuration of APs which AP 410 wants to connect.

Phy Mode: HTMIX

1. Security:

Disabled  WEP  TKIP  AES

Key: \_\_\_\_\_

Peer MAC Address:

\_\_\_\_

3. Security:

Disabled  WEP  TKIP  AES

Key: \_\_\_\_\_

Peer MAC Address:

\_\_\_\_

---

2. Security:

Disabled  WEP  TKIP  AES

Key: \_\_\_\_\_

Peer MAC Address:

\_\_:\_\_:\_\_:\_\_:\_\_:\_\_

4. Security:

Disabled  WEP  TKIP  AES

Key: \_\_\_\_\_

Peer MAC Address:

\_\_\_\_

Available settings are explained as follows:

Item	Description
<b>Phy Mode</b>	Data will be transmitted via HTMIX communication channel. Each access point should be setup to the same <b>Phy</b> mode for connecting with each other.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required.
<b>Peer MAC Address</b>	Type the peer MAC address for the access point that VigorAP 710 connects to.

## Advanced Settings for AP Bridge-WDS

When you choose AP Bridge-WDS, you will need to configure the following page.

Quick Start Wizard >> Wireless LAN (2.4GHz)

Note: When the configuration of APs with AP-4111 is completed, the Peer MAC Address always set LAN-A MAC address of the connected AP-4111.

Phy Mode: HTMIX

<p>1. Subnet LAN-A Security:</p> <p><input type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key: _____</p> <p>Peer MAC Address: _____</p>	<p>3. Subnet LAN-A Security:</p> <p><input type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key: _____</p> <p>Peer MAC Address: _____</p>
<p>2. Subnet LAN-A Security:</p> <p><input type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key: _____</p> <p>Peer MAC Address: _____</p>	<p>4. Subnet LAN-A Security:</p> <p><input type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key: _____</p> <p>Peer MAC Address: _____</p>

Available settings are explained as follows:

Item	Description
<b>Phy Mode</b>	Data will be transmitted via HTMIX communication channel. Each access point should be setup to the same <b>Phy</b> mode for connecting with each other.
<b>Subnet</b>	LAN-A is specified for connection.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required.
<b>Peer MAC Address</b>	Type the peer MAC address for the access point that VigorAP 710 connects to.



## Advanced Settings for AP Bridge-Universal Repeater

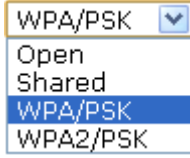
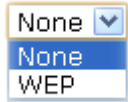
When you choose AP Bridge-Universal Repeater you will need to configure the following page.

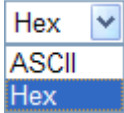

Quick Start Wizard >> Wireless LAN (2.4GHz)

Please input the SSID you want to connect to :  
Universal Repeater Parameters

SSID	04-14-31-11-11-11
MAC Address (Optional)	00:0c:8a:00:00:00
Security Mode	WPA2/PSK
Encryption Type	None
WEP Keys	00000000

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
<b>MAC Address (Optional)</b>	Type the MAC address for the access point.
<b>Security Mode</b>	<p>There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.</p> 
<b>Encryption Type for Open/Shared</b>	<p>This option is available when Open/Shared is selected as Security Mode.</p> <p>Choose <b>None</b> to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose <b>WEP</b>.</p>  <p><b>WEP Keys</b> - Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and '':</p>

	
<b>Encryption Type for WPA/PSK and WPA2/PSK</b>	<p>This option is available when <b>WPA/PSK</b> or <b>WPA2/PSK</b> is selected as <b>Security Mode</b>.</p> <p>Select <b>TKIP</b> or <b>AES</b> as the algorithm for WPA.</p> 
<b>Pass Phrase</b>	<p>It is available when WPA/PSK or WPA2/PSK is selected.</p>

After finishing this web page configuration, please click **Next** to continue.

### 2.7.3 Configuring 2.4GHz Security Settings

VigorAP 710 offers 2.4GHz wireless connection capability. You can setup 2.4GHz features in Quick Start Wizard first.

Quick Start Wizard >> 2.4G Security

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p> <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p><b>WEP/802.1x</b> - The built-in RADIUS client feature enables VigorAP 710 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p><b>WPA/802.1x</b> - The WPA encrypts each frame transmitted from</p>

	<p>the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p><b>WPA2/802.1x</b> - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>
<b>WPA Algorithm</b>	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Pass Phrase</b>	Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Key Renewal Internal</b>	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>PMK Cache Period</b>	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for <b>WPA2/802.1</b> mode.
<b>Pre-Authentication</b>	<p>Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2)</p> <p><b>Enable</b> - Enable IEEE 802.1X Pre-Authentication.</p> <p><b>Disable</b> - Disable IEEE 802.1X Pre-Authentication.</p>
<b>Key 1 – Key 4</b>	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.
<b>802.1x WEP</b>	<p><b>Disable</b> - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p><b>Enable</b> - Enable the WEP Encryption.</p> <p>Such feature is available for <b>WEP/802.1x</b> mode.</p>

After finishing this web page configuration, please click **Next** to continue.

## 2.7.4 Finishing the Wireless Settings Wizard

When you see this page, it means the wireless setting wizard is almost finished. Just click **Finish** to save the settings and complete the setting procedure.

Quick Start Wizard

Vigor Wizard Setup is now finished!

Basic Settings for VigorAP is completed.

Press Finish button to save and finish the wizard setup.

Note that the configuration process takes a few seconds to complete.

Back Finish Cancel

## 2.8 Online Status

The online status shows the LAN status, Station Link Status for such device.

Online Status

System Status		System Uptime: 0d 00:02:40		
<b>LAN Status</b>				
IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
10.28.108.1.3	370	2	3778	1228
<b>Universal Repeater Status</b>				
IP	Gateway	SSID	Channel	
10.28.10.1.3	10.28.10.254	DrayTek 8800rrr	--	
Mac	Security Mode	TX Packets	RX Packets	
00:1d:0a:0a:8c:08	WPA2PSK	133804	17180	

Detailed explanation is shown below:

Item	Description
<b>IP Address</b>	Displays the IP address of the LAN interface.
<b>TX Packets</b>	Displays the total transmitted packets at the LAN interface.
<b>RX Packets</b>	Displays the total number of received packets at the LAN interface.
<b>TX Bytes</b>	Displays the total transmitted size at the LAN interface.
<b>RX Bytes</b>	Displays the total number of received size at the LAN interface.



# 3

## Advanced Configuration

This chapter will guide users to execute advanced (full) configuration. As for other examples of application, please refer to chapter 5.

1. Open a web browser on your PC and type **http://192.168.1.2**. The window will ask for typing username and password.
2. Please type “admin/admin” on Username/Password for administration operation.

Now, the **Main Screen** will appear. Be aware that “Admin mode” will be displayed on the bottom left side.

The screenshot displays the DrayTek VigorAP 710 web interface. The top header shows the DrayTek logo and the device model 'VigorAP 710'. On the left side, there is a navigation menu with the following items: Quick Start Wizard, Online Status, Operation Mode, LAN, Wireless LAN, RADIUS Server, Applications, System Maintenance, and Diagnostics. Below the menu, there is a 'Support Area' section with links for FAQ/Application Note, Product Registration, and RJ-45 Port. At the bottom left of the page, it indicates 'Admin mode' and 'Universal Repeater Mode'. The main content area is titled 'System Status' and contains the following information:

System Status	
Model	: VigorAP710
Firmware Version	: 1.1.0
Build Date/Time	: r3805 Wed Feb 5 09:56:25 CST 2014
System Uptime	: 00:00:12.5
Operation Mode	: Universal Repeater

System	
Memory Total	323 B
Memory Used	11212 KB
Code Memory	15476 KB / 57164 KB

Wireless	
MAC Address	00:0C:4B:70:5C:78
BSSID	00-14-00-00-00-00
Channel	11

LAN	
MAC Address	00:0C:4B:70:5C:78
IP Address	192.168.1.2
IP Net	255.255.255.0

## 3.1 Operation Mode

This page provides several available modes for you to choose for different conditions. Click any one of them and click **OK**. The system will configure the required settings automatically.

### Operation Mode Configuration

#### 2.4G Wireless

- AP :**  
VigorAP will act as a bridge between wireless devices and wired network and exchanges data between them.
- AP Bridge-Point to Point :**  
VigorAP will connect to another VigorAP which uses the same mode, and all wired Ethernet ports of both VigorAPs will be connected together.
- AP Bridge-Point to Multi-Point :**  
VigorAP will connect to up to four VigorAPs which uses the same mode, and all wired Ethernet ports of every VigorAP will be connected together.
- AP Bridge-WDS :**  
VigorAP will connect to up to four VigorAPs which uses the same mode, and all wired Ethernet ports of every VigorAP will be connected together.  
This mode is still able to accept wireless clients.
- Universal Repeater :**  
VigorAP will act as a wireless repeater and be able to function as AP at the same time.

OK

Available settings are explained as follows:

Item	Description
<b>AP</b>	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
<b>AP Bridge-Point to Point</b>	This mode can establish wireless connection with another VigorAP 710 using the same mode, and link the wired network which these two VigorAP 710s connected together. Only one access point can be connected in this mode.
<b>AP Bridge-Point to Multi-Point</b>	This mode can establish wireless connection with other VigorAP 710s using the same mode, and link the wired network which these VigorAP 710s connected together. Up to 4 access points can be connected in this mode.
<b>AP Bridge-WDS</b>	This mode is similar to AP Bridge to Multi-Point, but access point is not work in bridge-dedicated mode, and will be able to accept wireless clients while the access point is working as a wireless bridge.
<b>Universal Repeater</b>	This product can act as a wireless range extender that will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless clients within its coverage.



**Note:** The **Wireless LAN** settings will be changed according to the **Operation Mode** selected here. For the detailed information, please refer to the section of **Wireless LAN**.

### 3.2 LAN

Local Area Network (LAN) is a group of subnets regulated and ruled by modem.



Click **LAN** to open the LAN settings page and choose **General Setup**.

**Note:** Such page will be changed according to the **Operation Mode** selected. The following screen is obtained by choosing **AP** as the operation mode.

LAN >> General Setup

Ethernet TCP/IP and DHCP Setup

<b>Ethernet TCP/IP and DHCP Setup</b> Specify an IP address: IP Address: <input type="text" value="192.168.1.2"/> Subnet Mask: <input type="text" value="255.255.255.0"/> Default Gateway: <input type="text"/>		<b>DHCP Server Configuration</b> <input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server <input type="radio"/> Relay Agent Server IP Address: <input type="text"/> Client IP Address: <input type="text"/> Subnet Mask: <input type="text"/> Default Gateway: <input type="text"/> Lease Time: <input type="text" value="1:00:00"/> DHCP Server Address for Relay Agent: <input type="text"/> Primary DNS Server: <input type="text"/> Secondary DNS Server: <input type="text"/>	
<input type="checkbox"/> Enable Management VLAN VLAN ID: <input type="text" value="0"/>			

Available settings are explained as follows:

Item	Description
<b>IP Address</b>	Type in private IP address for connecting to a local private network (Default: 192.168.1.2).
<b>Subnet Mask</b>	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
<b>Default Gateway</b>	In general, it is not really necessary to specify a gateway for VigorAP 710. However, if it is required, simply type an IP address as the gateway for VigorAP 710. It will be convenient for the access point acquiring more service (e.g., accessing NTP server) from Vigor router.
<b>Enable Management VLAN</b>	VigorAP 710 supports tag-based VLAN for wireless clients accessing Vigor router. Only the clients with the specified VLAN ID can access into VigorAP 710.  <b>VLAN ID</b> - Type the number as VLAN ID tagged on the

	transmitted packet. "0" means no VLAN tag.
<b>DHCP Server Configuration</b>	DHCP stands for Dynamic Host Configuration Protocol. DHCP server can automatically dispatch related IP settings to any local user configured as a DHCP client.
<b>Enable Server / Disable Server</b>	Enable Server lets the modem assign IP address to every host in the LAN.  Disable Server lets you manually or use other DHCP server to assign IP address to every host in the LAN.
<b>Relay Agent</b>	Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
<b>Start IP Address</b>	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your modem is 192.168.1.2, the starting IP address must be 192.168.1.3 or greater, but smaller than 192.168.1.254.
<b>End IP Address</b>	Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
<b>Subnet Mask</b>	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
<b>Default Gateway</b>	Enter a value of the gateway IP address for the DHCP server.
<b>Lease Time</b>	It allows you to set the leased time for the specified PC.
<b>DHCP Server IP Address for Relay Agent</b>	It is available when Enable Relay Agent is selected. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
<b>Primary DNS Server</b>	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
<b>Secondary DNS Server</b>	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

After finishing this web page configuration, please click **OK** to save the settings.

### 3.3 General Concepts for Wireless LAN

The VigorAP 710 is equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the VigorAP 710 is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps\*. Hence, you can finally smoothly enjoy stream music and video.

**Note:** \* The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, VigorAP 710 plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via VigorAP 710. The **General Setup** will set up the information of this wireless network, including its SSID as identification, located channel etc.

#### Security Overview

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

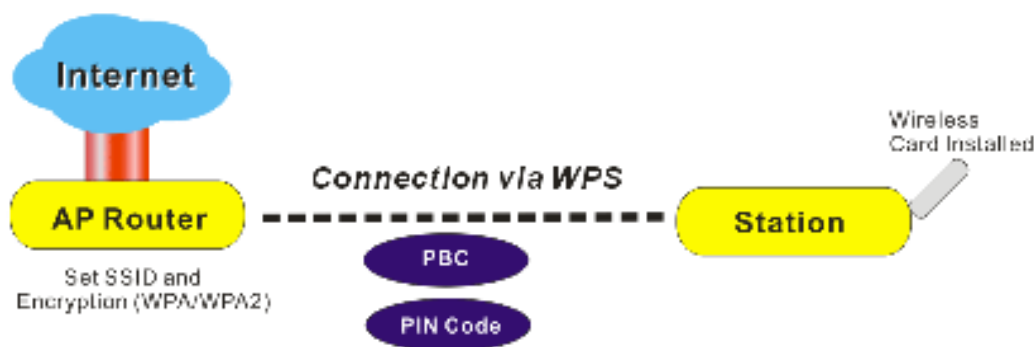
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The VigorAP 710 is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

#### WPS Introduction

**WPS (Wi-Fi Protected Setup)** provides easy procedure to make network connection between wireless station and wireless access point (VigorAP 710) with the encryption of WPA and WPA2.

It is the simplest way to build connection between wireless network clients and VigorAP 710. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 710 automatically.



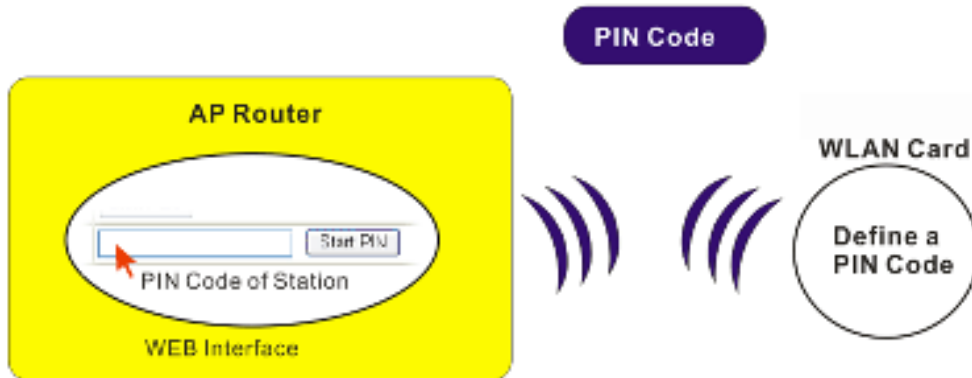
**Note:** Such function is available for the wireless station with WPS supported.

There are two methods to do network connection through WPS between AP and Stations: pressing the **Start PBC** button or using **PIN Code**.

On the side of VigorAP 710 series which served as an AP, press **WPS** button once on the front panel of VigorAP 710 or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 710.



### 3.4 Wireless LAN Settings for AP Mode

When you choose **AP** as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, AP Discovery and Station List.



**Note:** The **Wireless LAN** settings will be changed according to the **Operation Mode** selected in section 3.1.

#### 3.4.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

Wireless LAN >> General Setup

---

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Limit Client (3-04):  (default: 0)

Mode:

Sec	SSID	Isolate Member	WLAN ID	MAC Clone
1	DrayTek	<input type="checkbox"/>	0	<input type="checkbox"/>
2		<input type="checkbox"/>	1	
3		<input type="checkbox"/>	0	
4		<input type="checkbox"/>	1	

Hide SSID:  Prevent SSID from being scanned.

Isolate Member:  Wireless clients (stations) with the same SSID cannot access to each other.

MAC Clone:  Set the MAC address of SSID 1. The MAC addresses of other SSIDs are the Wireless client will also change based on the MAC address. Please notice that the last byte of the MAC address must be a multiple of 8.

Channel:

Extended Channel:

---

Radio-Over-SD-WiFi

Fix Power

Note:

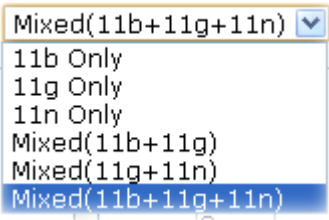
1. The test only supports 5GHz mode.
2. The same technology must also be supported in clients to boost WLAN performance.

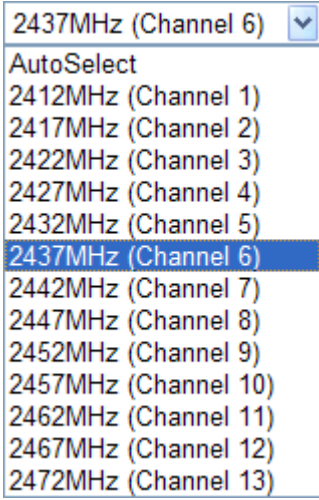
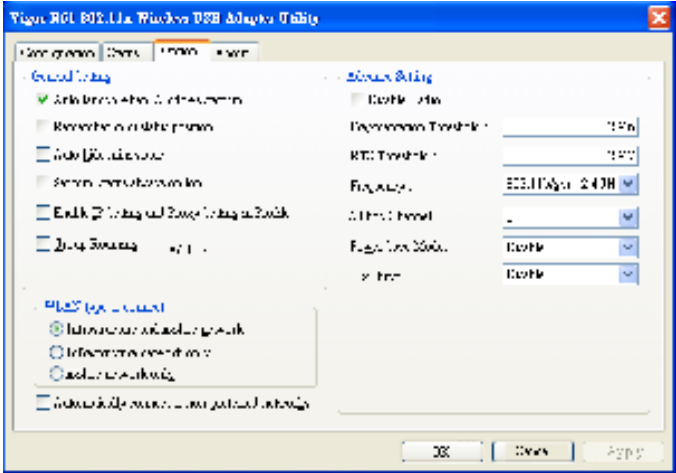
Antenna:

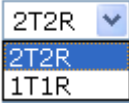
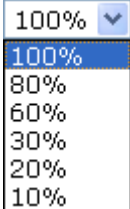
Power:

Channel Width:  Auto 20/40MHz  20MHz

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Enable Limit Client</b>	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor router. The number you can set is from 3 to 64.
<b>Mode</b>	<p>At present, VigorAP 710 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.</p> 
<b>Hide SSID</b>	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 710 while site surveying. The system allows you to set three sets of SSID for different usage.
<b>SSID</b>	Set a name for VigorAP 710 to be identified. Default settings are DrayTek.
<b>Isolate Member</b>	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
<b>VLAN ID</b>	<p>Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.</p> <p>If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.</p>
<b>Mac Clone</b>	Check this box and manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this MAC address.

<p><b>Channel</b></p>	<p>Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select <b>AutoSelect</b> to let system determine for you.</p> 
<p><b>Extension Channel</b></p>	<p>With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above. Configure the extension channel you want.</p>
<p><b>Rate</b></p>	<p>If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.</p>
<p><b>Packet-OVERDRIVE</b></p>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b>). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p><b>Note:</b> Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b>).</p> 

<b>Antenna</b>	<p>VigorAP 710 can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.</p> 
<b>Tx Power</b>	<p>The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.</p> 
<b>Channel Width</b>	<p><b>20 MHZ-</b> the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHZ-</b> the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.</p>

After finishing this web page configuration, please click **OK** to save the settings.



### 3.4.2 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

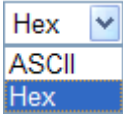
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (2.4GHz) >> Security Settings

The screenshot shows the 'Security Settings' page for SSID 1. At the top, there are tabs for SSID 1, SSID 2, SSID 3, and SSID 4. The 'Mode' dropdown is set to 'Mixed(WPA+WPA2)/PSK'. Below this, there is a section for 'RADIUS Server' with a 'Check' button. The 'WPA' section includes 'WPA Algorithms' with radio buttons for 'TKIP', 'AES', and 'TKIP/AES' (which is selected). There is a 'Pass Phrase' text field and a 'Key Renewal Interval' set to '3000 seconds'. The 'WEP' section has four rows for 'Key 1' through 'Key 4', each with a text input field and a 'Hex' dropdown menu. At the bottom, there are 'OK' and 'Cancel' buttons.

Available settings are explained as follows:

Item	Description
<b>Mode</b>	<p>There are several modes provided for you to choose.</p> <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p><b>WEP/802.1x</b> - The built-in RADIUS client feature enables</p>

	<p>VigorAP 710 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p><b>WPA/802.1x</b> - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p><b>WPA2/802.1x</b> - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>
<b>WPA Algorithms</b>	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Pass Phrase</b>	Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Key Renewal Interval</b>	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Key 1 – Key 4</b>	<p>Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ';'. Such feature is available for <b>WEP</b> mode.</p> 
<b>802.1x WEP</b>	<p><b>Disable</b> - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p><b>Enable</b> - Enable the WEP Encryption.</p> <p>Such feature is available for <b>WEP/802.1x</b> mode.</p>

Click the link of **RADIUS Server** to access into the following page for more settings.

**RADIUS Server**

Use Internal RADIUS Server

IP Address:

Port:

Shared Secret:

Session Timeout:

Available settings are explained as follows:

Item	Description
<b>Use internal RADIUS Server</b>	There is a RADIUS server built in VigorAP 710 which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, <b>3.9 RADIUS Server</b> to configure settings for internal server of VigorAP 710.
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
<b>Session Timeout</b>	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

After finishing this web page configuration, please click **OK** to save the settings.

### 3.4.3 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights (deny or allow).

Wireless LAN => Access Control

Available settings are explained as follows:

Item	Description
<b>Policy</b>	Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b> , so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 710. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">           Activate MAC address filter ▼            Disable            Activate MAC address filter            Blocked MAC address filter         </div>
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>Client's MAC Address</b>	Manually enter the MAC address of wireless client.
<b>Add</b>	Add a new MAC address into the list.
<b>Delete</b>	Delete the selected MAC address in the list.
<b>Edit</b>	Edit the selected MAC address in the list.

<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.

After finishing this web page configuration, please click **OK** to save the settings.

### 3.4.4 WPS

Open **Wireless LAN>>WPS** to configure the corresponding settings.

Wireless LAN >> WPS (Wi-Fi Protected Setup)

---

Enable WPS ⓘ

Wi-Fi Protected Setup Information

WPS Configured	Yes
WPS SSID	DrayTek
WPS Auth Mode	WPA2 (AES/TKIP/AES)
WPS Encryp Type	TKIP/AES

Device Configure

Configure via Push Button

Configure via Client PinCode

Status: Not Used

Note: WPS can help your wireless client automatically connect to the Access Point.

- ⓘ Access Point Info
- ⓘ WPS is Enabled
- ⓘ Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 710 is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current selected SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 710. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encryp Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 710.
<b>Configure via Push Button</b>	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. VigorAP 710 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 710 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
<b>Configure via Client</b>	Type the PIN code specified in wireless client you wish to

<b>PinCode</b>	connect, and click <b>Start PIN</b> button. The WLAN LED on VigorAP 710 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).
----------------	--

### 3.4.5 AP Discovery

VigorAP 710 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Please click **Scan** to discover all the connected APs.

Wireless LAN (2.4GHz) > Access Point Discovery

Access Point List

SSID	BSSID	RSSI	Channel	Encryption	Authentication
------	-------	------	---------	------------	----------------

Scan

Channel Statistics

Note: During the scanning process, VigorAP 710 will not allow any other wireless LAN client to connect.

Each item is explained as follows:

Item	Description
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 710.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 710.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 710.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>Channel Statistics</b>	It displays the statistics for the channels used by APs.

### 3.4.6 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC\_BE , AC\_BK, AC\_VI and AC\_VO for WMM.

Wireless LAN >> WMM Configuration

**WMM Configuration** | [Set to Factory Default](#)

WMM Capable  Disable  Enable

**WMM Parameters of Access Point**

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	LC	33	0		
AC_BK	7	LC	1023	0		
AC_VI	1	7	15	64		
AC_VO	1	3	7	17		

**WMM Parameters of Station**

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	LC	LC31	0	<input type="checkbox"/>
AC_BK	7	LC	LC31	0	<input type="checkbox"/>
AC_VI	3	7	LC	0	<input type="checkbox"/>
AC_VO	3	3	7	7	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
<b>WMM Capable</b>	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
<b>Aifsn</b>	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
<b>CWMin/CWMax</b>	<b>CWMin</b> means contention Window-Min and <b>CWMax</b> means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
<b>Txop</b>	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.

<b>ACM</b>	<p>It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked.</p> <p><b>Note:</b> VigorAP 710 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.</p>
<b>AckPolicy</b>	<p>“Uncheck” (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.</p> <p>“Check” the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.</p>

After finishing this web page configuration, please click **OK** to save the settings.



### 3.4.7 Station List

**Station List** provides the knowledge of connecting wireless clients now along with its status code.

Wireless LAN >> Station List

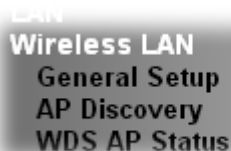
The screenshot shows the 'Station List' configuration interface. At the top, there are two tabs: 'General' and 'Advanced'. Below the tabs is a table with the following columns: 'MAC Address', 'SSID', 'Auth', and 'Encrypt'. The table is currently empty. Below the table is a 'Refresh' button. At the bottom of the page, there is a section titled 'Add to Access Control'. It contains a label 'Client's MAC Address' followed by three input fields for the MAC address components (XX:XX:XX). Below these fields is an 'Add' button.

Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>Auth</b>	Display the authentication that the wireless client uses for connection with such AP.
<b>Encrypt</b>	Display the encryption mode used by the wireless client.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .
<b>General/Advanced</b>	<b>General</b> – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. <b>Advanced</b> – Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

## 3.5 Wireless LAN Settings for AP Bridge-Point to Point/AP Bridge-Point to Multi-Point Mode

When you choose AP Bridge-Point to Point or Point-to Multi-Point Mode as the operation mode, the Wireless LAN menu items will include General Setup, AP Discovery and WDS AP Status.



AP Bridge-Point to Point allows VigorAP 710 to connect to **another** VigorAP 710 which uses the same mode. All wired Ethernet clients of both VigorAP 710s will be connected together.

Point-to Multi-Point Mode allows VigorAP 710 to connect up to **four** VigorAP 710s which uses the same mode. All wired Ethernet clients of every VigorAP 710 will be connected together.

### 3.5.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the Phy mode, security, Tx Burst and choose proper mode. Please refer to the following figure for more information.

Wireless LAN >> General Setup

---

General Setting | IEEE 802.11 |

Enable Wireless LAN

Mode:

Channel:

Basic Channel:

---

Note: Enter the coordinator of APs which AP710 want to connect

Phy Mode: 11N MIX

Security:

Disabled  WEP  TKIP  AES

Key:

Peer Mac Address:

:  :  :  :  :

Packet-COMPRESS

Enable

Note:

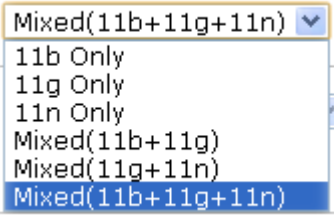
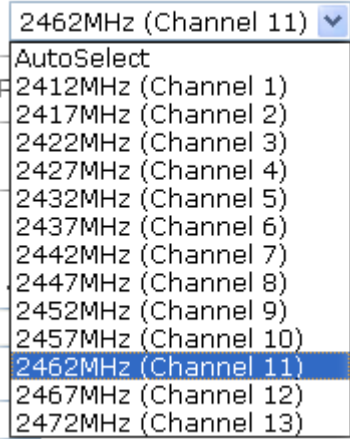
- 1. Tx Power may support 11g mode.
- 2. The same technology must also be supported in clients to boost WLAN performance.

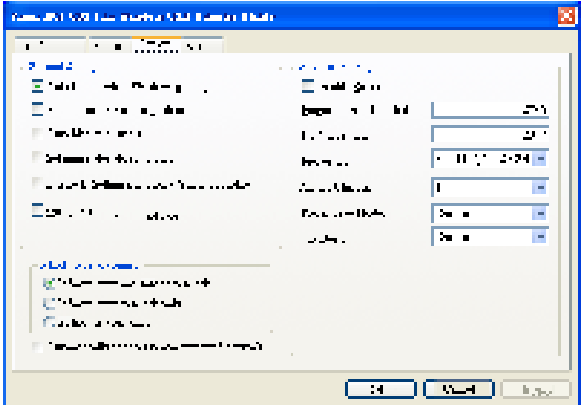

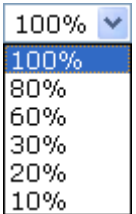
Antenna:

Tx Power:

Channel Width:  Auto 20/40 MHz  20 MHz

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Mode</b>	<p>At present, VigorAP 710 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.</p> 
<b>Channel</b>	<p>Means the channel of frequency of the wireless LAN. The default channel is 11. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select <b>AutoSelect</b> to let system determine for you.</p> 
<b>Extension Channel</b>	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above.
<b>Rate</b>	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.
<b>Phy Mode</b>	Data will be transmitted via communication channel, HTMIX.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required.
<b>Peer Mac Address</b>	Type the peer MAC address for the access point that VigorAP 710 connects to.

<p><b>Packet-OVERDRIVE</b></p>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b>). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p><b>Note:</b> Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b>).</p> 
<p><b>Antenna</b></p>	<p>VigorAP 710 can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.</p> 
<p><b>Tx Power</b></p>	<p>The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.</p> 
<p><b>Channel Width</b></p>	<p><b>20 MHZ-</b> the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHZ-</b> the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.</p>

After finishing this web page configuration, please click **OK** to save the settings.

### 3.5.2 AP Discovery

VigorAP 710 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to VigorAP 710.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of VigorAP 710 can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN >> Access Point Discovery

---

Access Point List

Select	SSID	BSSID	RSSI	Channel	Encryption	Authentication
<input type="button" value="Scan"/>						

See [Channel Statistics](#)

Note: During the scanning process (about 5 seconds), no client is allowed to connect with the AP.

---

AP's MAC Address:  :  :  :  :  :       AP's SSID:

Add to [WDS Settings](#):

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 710.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 710.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 710.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>Channel Statistics</b>	It displays the statistics for the channels used by APs.
<b>AP's MAC Address</b>	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
<b>AP's SSID</b>	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
<b>Add</b>	Type the MAC address of the AP. Click <b>Add</b> . Later, the MAC address of the AP will be added and be shown on WDS settings page.

### 3.5.3 WDS AP Status

VigorAP 710 can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.

Wireless LAN => WDS AP Status

WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth
-----	-------------	----------------------	------------	-----------

Refresh

### 3.6 Wireless LAN Settings for AP Bridge-WDS Mode

When you choose AP Bridge-WDS as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, AP Discovery, WDS AP Status, WMM Configuration and Station List.



#### 3.6.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the Phy mode, security, Tx Burst and choose proper mode. Please refer to the following figure for more information.

Wireless LAN >> General Setup

General Setting (VLL 002.11)

Enable Wireless LAN

Enable Limit Client:  (1-64)

---

Mode:

Mode	Rate	Rate (Mbps)	Max. Clients	Max. Tx Power	Max. Tx Power (dBm)
1	<input type="checkbox"/>	11b/g/n	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Hide SSID:  (SSID: 11b/g/n) (Default: Disabled)

Isolate LAN:  (Isolate LAN: 11b/g/n) (Default: Disabled)

Isolate Number:  (Isolate Number: 11b/g/n) (Default: 1)

MAC Clone:  (MAC Clone: 11b/g/n) (Default: Disabled)

---

Channel:

Extension Channel:

Note: To set the configuration, please refer to the following table.

Channel and Extension Channel: A valid address is 11b/g/n. Max. Tx Power: 11b/g/n.

Phy Mode: 11b/g/n

Subnet	Security	Key	Peer Mac Address
1. Subnet: 192.168.0.0	Security: <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES	Key: <input type="text" value=""/>	Peer Mac Address: <input type="text" value=""/>
2. Subnet: 192.168.0.0	Security: <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES	Key: <input type="text" value=""/>	Peer Mac Address: <input type="text" value=""/>
3. Subnet: 192.168.0.0	Security: <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES	Key: <input type="text" value=""/>	Peer Mac Address: <input type="text" value=""/>
4. Subnet: 192.168.0.0	Security: <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES	Key: <input type="text" value=""/>	Peer Mac Address: <input type="text" value=""/>

---

Antenna:  External

To:  Burst

Note: 1. The burst mode supports the mode.

2. The burst mode must also be supported by the client. Please refer to the manual.

---

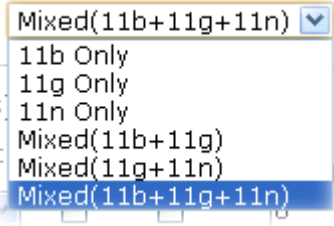
Antenna:

To:

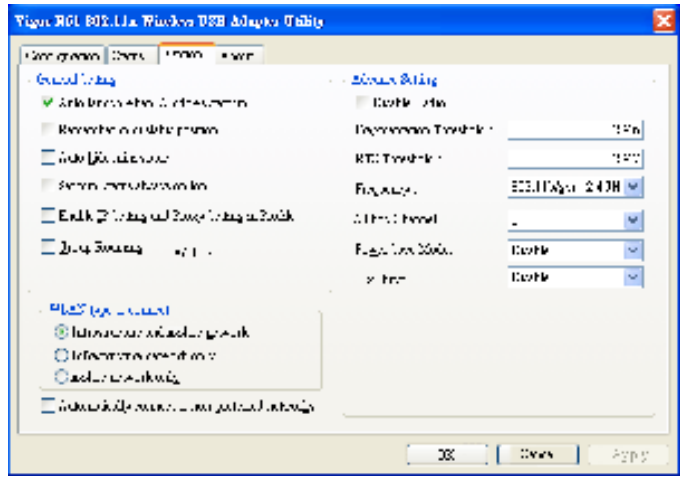
Channel Width:  20MHz  40MHz

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Enable Limit Client</b>	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor router. The number you can set is from 3 to 64.

<b>Mode</b>	<p>At present, VigorAP 710 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.</p> 
<b>Hide SSID</b>	<p>Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 710 while site surveying. The system allows you to set three sets of SSID for different usage.</p>
<b>SSID</b>	<p>Set a name for VigorAP 710 to be identified. Default settings is DrayTek.</p>
<b>Isolate LAN</b>	<p>Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.</p>
<b>Isolate Member</b>	<p>Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</p>
<b>VLAN ID</b>	<p>Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.</p> <p>If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.</p>
<b>Mac Clone</b>	<p>Check this box and manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this MAC address.</p>
<b>Channel</b>	<p>Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select <b>AutoSelect</b> to let system determine for you.</p>



	<p>243.000 Iz (Channel 6)</p> <p>AutoSelect</p> <p>241.200 Iz (Channel 1)</p> <p>241.400 Iz (Channel 2)</p> <p>242.200 Iz (Channel 3)</p> <p>242.400 Iz (Channel 4)</p> <p>243.200 Iz (Channel 5)</p> <p>243.000 Iz (Channel 6)</p> <p>244.200 Iz (Channel 7)</p> <p>244.400 Iz (Channel 8)</p> <p>245.200 Iz (Channel 9)</p> <p>246.000 Iz (Channel 10)</p> <p>246.200 Iz (Channel 11)</p> <p>246.400 Iz (Channel 12)</p> <p>247.200 Iz (Channel 13)</p>
<b>Extension Channel</b>	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above. Configure the extension channel you want.
<b>Rate</b>	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.
<b>Phy Mode</b>	Data will be transmitted via communication channel, HTMIX.
<b>Subnet</b>	LAN-A is specified for connection.
<b>Security</b>	Select WEP, TKIP or AES as the encryption algorithm.
<b>Peer Mac Address</b>	Four peer MAC addresses are allowed to be entered in this page at one time.
<b>Packet-OVERDRIVE</b>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b>). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p><b>Note:</b> Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b>).</p>
	

<b>Antenna</b>	<p>VigorAP 710 can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.</p> <div data-bbox="644 320 775 421"> <input type="text" value="2T2R"/> <ul style="list-style-type: none"> <li>2T2R</li> <li>1T1R</li> </ul> </div>
<b>Tx Power</b>	<p>The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.</p> <div data-bbox="644 533 775 745"> <input type="text" value="100%"/> <ul style="list-style-type: none"> <li>100%</li> <li>80%</li> <li>60%</li> <li>30%</li> <li>20%</li> <li>10%</li> </ul> </div>
<b>Channel Width</b>	<p><b>20 MHZ-</b> the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHZ-</b> the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.</p>

After finishing this web page configuration, please click **OK** to save the settings.

### 3.6.2 Security

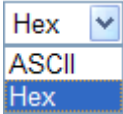
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

Wireless LAN (2.4GHz) => Security Settings

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Disable</p> <p>Disable</p> <p>WEP</p> <p>WPA/PSK</p> <p><b>WPA2/PSK</b></p> <p>Mixed(WPA+WPA2)/PSK</p> <p>WEP/802.1x</p> <p>WPA/802.1x</p> <p>WPA2/802.1x</p> <p>Mixed(WPA+WPA2)/802.1x</p> </div> <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> - Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p><b>WEP/802.1x</b> - The built-in RADIUS client feature enables</p>

	<p>VigorAP 710 to assist th1222222222222222222222222222e remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p><b>WPA/802.1x</b> - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p><b>WPA2/802.1x</b> - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>
<b>WPA Algorithms</b>	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Pass Phrase</b>	Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Key Renewal Interval</b>	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.
<b>Key 1 – Key 4</b>	<p>Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ';'. Such feature is available for <b>WEP</b> mode.</p> 
<b>802.1x WEP</b>	<p><b>Disable</b> - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p><b>Enable</b> - Enable the WEP Encryption.</p> <p>Such feature is available for <b>WEP/802.1x</b> mode.</p>

Click the link of **RADIUS Server** to access into the following page for more settings.

**RADIUS Server**

Use Internal RADIUS Server

IP Address:

Port:

Shared Secret:

Session Timeout:

Available settings are explained as follows:

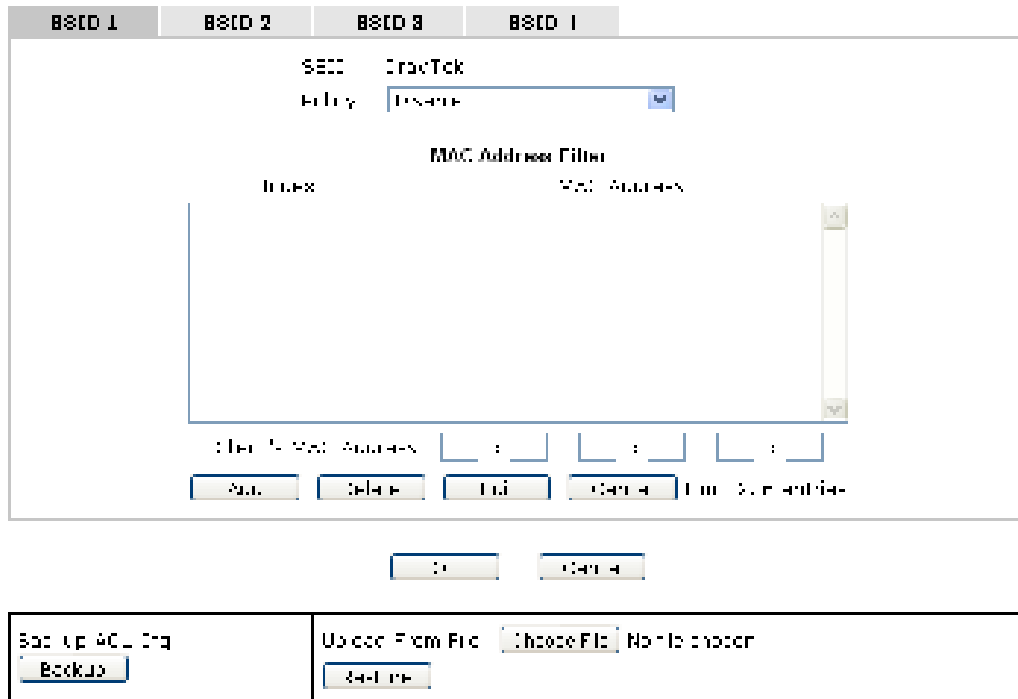
Item	Description
<b>Use internal RADIUS Server</b>	There is a RADIUS server built in VigorAP 710 which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, <b>3.9 RADIUS Server</b> to configure settings for internal server of VigorAP 710.
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
<b>Session Timeout</b>	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

After finishing this web page configuration, please click **OK** to save the settings.

### 3.6.3 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights (deny or allow).

Wireless LAN => Access Control



Available settings are explained as follows:

Item	Description
<b>Policy</b>	Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b> , so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 710. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">           Activate MAC address filter ▼            Disable            Activate MAC address filter            Blocked MAC address filter         </div>
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>Client's MAC Address</b>	Manually enter the MAC address of wireless client.
<b>Add</b>	Add a new MAC address into the list.
<b>Delete</b>	Delete the selected MAC address in the list.
<b>Edit</b>	Edit the selected MAC address in the list.

<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.


After finishing this web page configuration, please click **OK** to save the settings.

### 3.6.4 WPS

Open **Wireless LAN>>WPS** to configure the corresponding settings.

Wireless LAN >> WPS (WiFi Protected Setup)

---

Enable WPS 

WiFi Protected Setup Information

WPS Configured	Yes
WPS SSID	DrayTek
WPS Auth Mode	WPA2/PSK (AES)
WPS Encryp Type	TKIP/AES




Device Configure

Configure via Push Button

Configure via Client PinCode

Status: Not Used

Note: WPS can help your wireless client automatically connect to the access point.

- : WPS is disabled.
- : WPS is Enabled.
- : Waiting for AP to request a pin from wireless client.

Available settings are explained as follows:

Item	Description
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 710 is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current selected SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 710r. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encryp Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 710.
<b>Configure via Push Button</b>	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. VigorAP 710 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 710 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
<b>Configure via Client</b>	Type the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. The WLAN LED on

<b>PinCode</b>	VigorAP 710 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).
----------------	--

### 3.6.5 AP Discovery

VigorAP 710 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of VigorAP 710 can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN >> Access Point Discovery

Access Point List

Select	SSID	BSSID	RSSI	Channel	Encryption	Authentication
--------	------	-------	------	---------	------------	----------------

Note: During the scanning process (about 5 seconds), no station is allowed to connect with the AP

AP's MAC Address:  :  :  :  :  :       AP's SSID:

Add to WDS Settings:

Each item is explained as follows:

Item	Description
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 710.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 710.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 710.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>Channel Statistics</b>	It displays the statistics for the channels used by APs.
<b>AP's MAC Address</b>	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
<b>AP's SSID</b>	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
<b>Add</b>	Click <b>Add</b> . Later, the MAC address of the AP will be added and be shown on WDS settings page.



### 3.6.6 WDS AP Status

VigorAP 710 can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.

Wireless LAN => WDS AP Status

WDS AP List

AP ID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth
1	11:11:11:11:11:11	11B	Off	11M

### 3.6.7 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC\_BE , AC\_BK , AC\_VI and AC\_VO for WMM.

Wireless LAN => WMM Configuration

WMM Configuration

[Set to Factory Default](#)

WMM Capable  Enable  Disable

WMM Parameters of Access Point

AC	Aifsn	COVMin	COVMax	Txop	ACM	AckPolicy
AC_BE	1	15	51	1	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	2	15	112	1	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	3	2	15	54	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	4	2	2	42	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

AC	Aifsn	COVMin	COVMax	Txop	ACM
AC_BE	1	15	112	1	<input type="checkbox"/>
AC_BK	2	15	112	1	<input type="checkbox"/>
AC_VI	3	2	15	54	<input type="checkbox"/>
AC_VO	4	2	2	42	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.

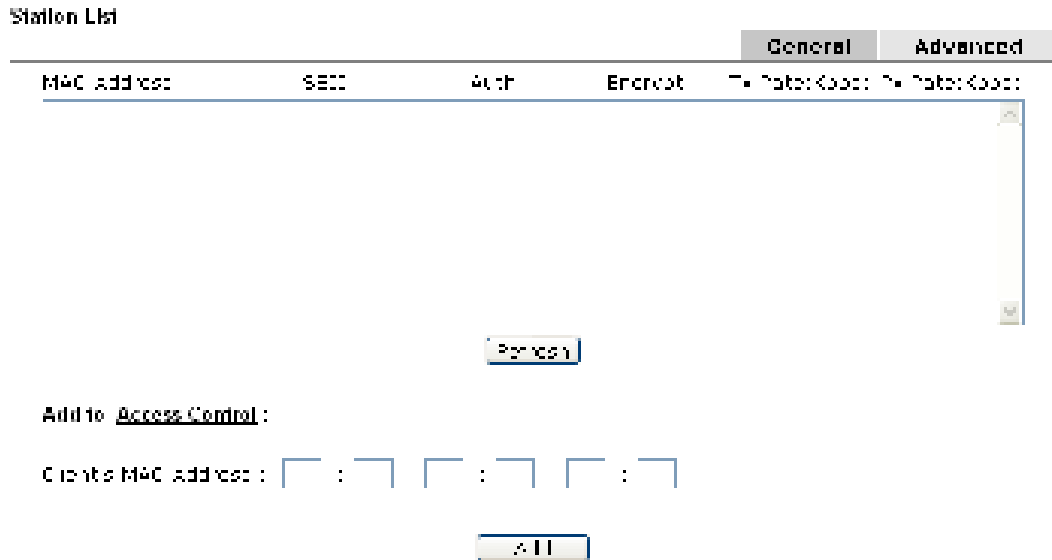
<b>CWMin/CWMax</b>	<b>CWMin</b> means contention Window-Min and <b>CWMax</b> means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
<b>Txop</b>	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
<b>ACM</b>	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. <b>Note:</b> VigorAP710 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
<b>AckPolicy</b>	“Uncheck” (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. “Check” the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

After finishing this web page configuration, please click **OK** to save the settings.

### 3.6.8 Station List

**Station List** provides the knowledge of connecting wireless clients now along with its status code.

Wireless LAN => Station List

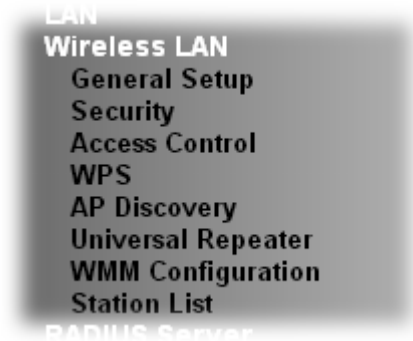


Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>Auth</b>	Display the authentication that the wireless client uses for connection with such AP.
<b>Encrypt</b>	Display the encryption mode used by the wireless client.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .
<b>General/Advanced</b>	<b>General</b> – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. <b>Advanced</b> – Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

## 3.7 Wireless LAN Settings for Universal Repeater Mode

When you choose Universal Repeater as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, AP Discovery, Universal Repeater, WMM Configuration and Station List.



### 3.7.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel.

Please refer to the following figure for more information.

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Limit Client (3-64) (default: 64)

Mode: Mixed (11b+11g+11n)

Hide SSID	SSID	Isolate LAN	Isolate Member	MAC Clone	MAC Clone
<input type="checkbox"/>	DrayTek	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Hide SSID: Prevent SSID from being scanned.

Isolate LAN: Wireless clients connected with the same SSID cannot access wired PCs or LAN.

Isolate Member: Wireless clients connected with the same SSID cannot access for each other.

MAC Clone: Set the MAC address of SSID 1. The MAC addresses of other SSIDs and the wireless client will also change based on this MAC address. Please notice that the last bits of this MAC address must be a multiple of 8.

Channel: 2 (24MHz Channel 1)

Extension Channel: 2 (24MHz Channel 7)

Radio Type: 802.11n

Tx Burst

Note:

1. Tx Burst only supports 11g mode.
2. The same radio type must be supported in order to ensure WLAN performance.

---

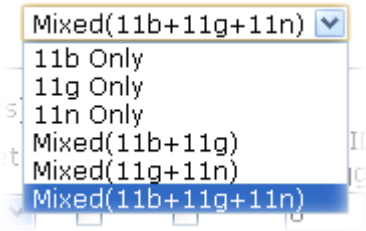
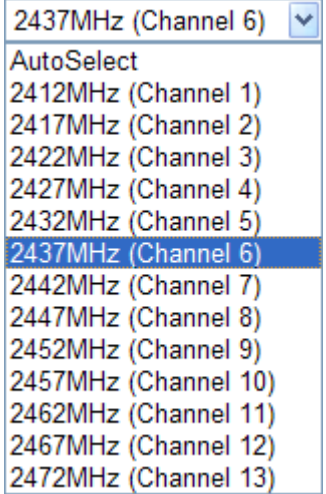
Antenna: 2.4d

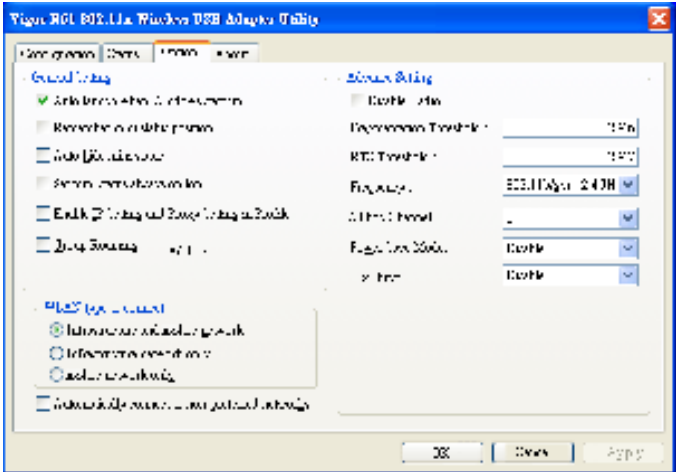
Tx Power: 100%

Channel Width: 20MHz 40MHz

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Enable Limit Client</b>	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor router. The number you can set is from 3 to 64.
<b>Mode</b>	At present, VigorAP 710 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

	
<b>Hide SSID</b>	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 710 while site surveying. The system allows you to set three sets of SSID for different usage.
<b>SSID</b>	Set a name for VigorAP 710 to be identified. Default setting is DrayTek.
<b>Isolate LAN</b>	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
<b>Isolate Member</b>	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
<b>VLAN ID</b>	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.  If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.
<b>Mac Clone</b>	Check this box and manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this MAC address.
<b>Channel</b>	Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select <b>AutoSelect</b> to let system determine for you.  

<b>Extension Channel</b>	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the <b>Channel</b> selected above. Configure the extension channel you want.
<b>Rate</b>	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.
<b>Packet-OVERDRIVE</b>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b>). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p><b>Note:</b> Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b>).</p> 
<b>Antenna</b>	<p>VigorAP 710 can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.</p> <p>2T2R 2T2R 1T1R</p>
<b>Tx Power</b>	<p>The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.</p> <p>100% 100% 80% 60% 30% 20% 10%</p>
<b>Channel Width</b>	<p><b>20 MHZ-</b> the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p><b>Auto 20/40 MHZ-</b> the router will use 20Mhz or 40Mhz for</p>

data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.

After finishing this web page configuration, please click **OK** to save the settings.

### 3.7.2 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

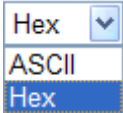
Wireless LAN >> Security Settings

The screenshot shows the 'Security Settings' page for SSID 1. At the top, there are tabs for SSID 1, SSID 2, SSID 3, and SSID 4. The 'Mode' is set to 'Mixed(WPA+WPA2)/PSK'. Below this, there are options for 'WPA Algorithms' (TKIP, AES, TKIP/AES), 'Pass Phrase', and 'Key Renewal Interval' (3000 seconds). Under the 'WEP' section, there are four radio buttons for 'Key 1' through 'Key 4', each with a corresponding input field and a 'Hex' checkbox. At the bottom, there are radio buttons for 'SSID 1-4' and 'None', along with 'OK' and 'Cancel' buttons.

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p> <p><b>Disable</b> - The encryption mechanism is turned off.</p> <p><b>WEP</b> - Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK -</b></p>



	<p>Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p><b>WEP/802.1x</b> - The built-in RADIUS client feature enables VigorAP 710 to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p><b>WPA/802.1x</b> - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p><b>WPA2/802.1x</b> - The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p>
<b>WPA Algorithms</b>	<p>Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>Pass Phrase</b>	<p>Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>Key Renewal Interval</b>	<p>WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for <b>WPA2/802.1, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK</b> mode.</p>
<b>Key 1 – Key 4</b>	<p>Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for <b>WEP</b> mode.</p> 

<b>802.1x WEP</b>	<p><b>Disable</b> - Disable the WEP Encryption. Data sent to the AP will not be encrypted.</p> <p><b>Enable</b> - Enable the WEP Encryption.</p> <p>Such feature is available for <b>WEP/802.1x</b> mode.</p>
-------------------	---

Click the link of **RADIUS Server** to access into the following page for more settings.

**RADIUS Server**

Use Internal RADIUS Server

IP Address:

Port:

Shared Secret:

Session Timeout:

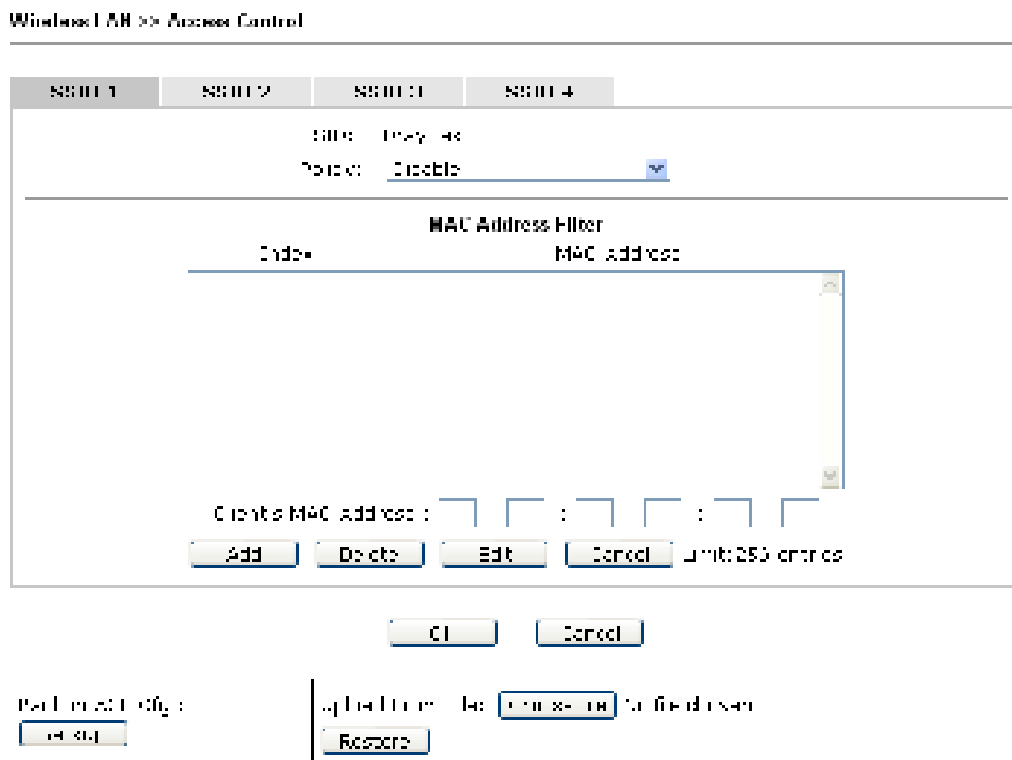
Available settings are explained as follows:

Item	Description
<b>Use internal RADIUS Server</b>	<p>There is a RADIUS server built in VigorAP 710 which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security.</p> <p>Besides, if you want to use the external RADIUS server for authentication, do not check this box.</p> <p>Please refer to the section, <b>3.9 RADIUS Server</b> to configure settings for internal server of VigorAP 710.</p>
<b>IP Address</b>	Enter the IP address of external RADIUS server.
<b>Port</b>	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
<b>Session Timeout</b>	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

After finishing this web page configuration, please click **OK** to save the settings.

### 3.7.3 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights (deny or allow).



Available settings are explained as follows:

Item	Description
<b>Policy</b>	Select to enable any one of the following policy or disable the policy. Choose <b>Activate MAC address filter</b> to type in the MAC addresses for other clients in the network manually. Choose <b>Blocked MAC address filter</b> , so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 710. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">           Activate MAC address filter ▼            Disable            Activate MAC address filter            Blocked MAC address filter         </div>
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>Client's MAC Address</b>	Manually enter the MAC address of wireless client.
<b>Add</b>	Add a new MAC address into the list.
<b>Delete</b>	Delete the selected MAC address in the list.
<b>Edit</b>	Edit the selected MAC address in the list.

<b>Cancel</b>	Give up the access control set up.
<b>Backup</b>	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
<b>Restore</b>	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.

After finishing this web page configuration, please click **OK** to save the settings.

### 3.7.4 WPS

Open **Wireless LAN>>WPS** to configure the corresponding settings.

Wireless LAN >> WPS (Wi-Fi Protected Setup)

---

Enable WPS ⓘ

Wi-Fi Protected Setup Information

WPS Configured	Yes
WPS SSID	DrayTek
WPS Auth Mode	WPA2 (AES/TKIP) PSK
WPS Encrypt Type	TKIP/AES

Device Configure

Configure via Push Button

Configure via Client PinCode

Status: Not used

Note: WPS can help your wireless client automatically connect to the Access Point.

- ⓘ WPS is Disabled
- ⓘ WPS is Enabled
- ⓘ Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Configured</b>	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 710 is properly configured, you can see 'Yes' message here.
<b>WPS SSID</b>	Display current selected SSID.
<b>WPS Auth Mode</b>	Display current authentication mode of the VigorAP 710. Only WPA2/PSK and WPA/PSK support WPS.
<b>WPS Encrypt Type</b>	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 710.
<b>Configure via Push Button</b>	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. VigorAP 710 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 710 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
<b>Configure via Client PinCode</b>	Type the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. The WLAN LED on

VigorAP 710 will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).

### 3.7.5 AP Discovery

VigorAP 710 can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of VigorAP 710 can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN >> Access Point Discovery

---

Access Point List

Select	SSID	BSSID	RSSI	Channel	Encryption	Authentication
<input type="button" value="Scan"/>						

See [Channel Statistics](#)

Note: During the scanning process, the VigorAP 710 will blink fast when WPS is in progress.

---

AP's MAC Address:  AP's SSID:

Select as Universal Repeater:

Each item is explained as follows:

Item	Description
<b>SSID</b>	Display the SSID of the AP scanned by VigorAP 710.
<b>BSSID</b>	Display the MAC address of the AP scanned by VigorAP 710.
<b>RSSI</b>	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
<b>Channel</b>	Display the wireless channel used for the AP that is scanned by VigorAP 710.
<b>Encryption</b>	Display the encryption mode for the scanned AP.
<b>Authentication</b>	Display the authentication type that the scanned AP applied.
<b>Scan</b>	It is used to discover all the connected AP. The results will be shown on the box above this button
<b>Channel Statistics</b>	It displays the statistics for the channels used by APs.
<b>AP's MAC Address</b>	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
<b>AP's SSID</b>	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
<b>Select as Universal Repeater</b>	In <b>Universal Repeater</b> mode, WAN would work as station mode and the wireless AP can be selected as a universal repeater. Choose one of the wireless APs from the Scan list.

### 3.7.6 Universal Repeater

The access point can act as a wireless repeater; it can be Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to serve all wireless stations within its coverage.

**Note:** While using **Universal Repeater** mode, the access point will demodulate the received signal. Please check if this signal is noise for the operating network, then have the signal modulated and amplified again. The output power of this mode is the same as that of WDS and normal AP mode.

Wireless LAN >> Universal Repeater

---

**Universal Repeater Parameters**

SSID: \_\_\_\_\_

MAC Address (Optional): \_\_\_\_\_

Channel: 2.4G/5.8G/11G/13G [v]

Security Mode: WPA [v]

Encryption Type: None [v]

WEP Keys:

Key 1: \_\_\_\_\_ [11] [v]

Key 2: \_\_\_\_\_ [H2] [v]

Key 3: \_\_\_\_\_ [11] [v]

Key 4: \_\_\_\_\_ [H2] [v]

Note: Channel is used for the channel setting of AP. Multiple channels are allowed.

---

**Universal Repeater IP Configuration**

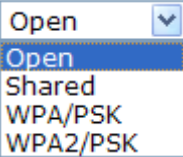
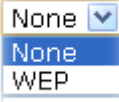
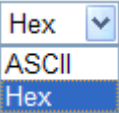
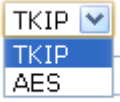
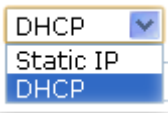
Connection Type: DHCP [v]

Interface Name: AP-1 [v]

[OK] [Cancel]

Available settings are explained as follows:

Item	Description
<b>SSID</b>	Set the name of access point that VigorAP 710 wants to connect to.
<b>MAC Address (Optional)</b>	Type the MAC address of access point that VigorAP 710 wants to connect to.
<b>Channel</b>	Means the channel of frequency of the wireless LAN. The default channel is 11. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select <b>AutoSelect</b> to let system determine for you.
<b>Security Mode</b>	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.

	
<b>Encryption Type for Open/Shared</b>	<p>This option is available when Open/Shared is selected as Security Mode.</p> <p>Choose <b>None</b> to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose <b>WEP</b>.</p>  <p><b>WEP Keys</b> - Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.</p> 
<b>Encryption Type for WPA/PSK and WPA2/PSK</b>	<p>This option is available when WPA/PSK or WPA2/PSK is selected as <b>Security Mode</b>.</p> <p>Select <b>TKIP</b> or <b>AES</b> as the algorithm for WPA.</p> 
<b>Pass Phrase</b>	<p>Either <b>8~63</b> ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
<b>Connection Type</b>	<p>Choose DHCP or Static IP as the connection mode.</p> <p><b>DHCP</b> – The wireless station will be assigned with an IP from Vigor router.</p> <p><b>Static IP</b> – The wireless station shall specify a static IP for connecting to Internet via Vigor router.</p> 
<b>Router Name</b>	<p>Type a name for the router as identification. Simply use the default name.</p>
<b>IP Address</b>	<p>This setting is available when <b>Static IP</b> is selected as <b>Connection Type</b>.</p>

	Type an IP address with the same network segment of the LAN IP setting of the router. Such IP shall be different with any IP address in LAN.
<b>Subnet Mask</b>	This setting is available when <b>Static IP</b> is selected as <b>Connection Type</b> . Type the subnet mask setting which shall be the same as the one configured in LAN for the router.
<b>Default Gateway</b>	This setting is available when <b>Static IP</b> is selected as <b>Connection Type</b> . Type the gateway setting which shall be the same as the default gateway configured in LAN for the router.

After finishing this web page configuration, please click **OK** to save the settings.

### 3.7.7 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC\_BE , AC\_BK, AC\_VI and AC\_VO for WMM.

Wireless LAN >> WMM Configuration

**WMM Configuration** | [Set to Factory Default](#)

WMM Capable:  Enable  Disable

**WMM Parameters of Access Point**

	Aifsn	QWMin	QWMax	Txop	ACM	AckPolicy
AC_BE	3	LC	33	0		
AC_BK	7	LC	1023	0		
AC_VI	1	7	15	04		
AC_VO	1	E	7	17		

**WMM Parameters of Station**

	Aifsn	QWMin	QWMax	Txop	ACM
AC_BE	3	LC	LC3	0	<input type="checkbox"/>
AC_BK	7	LC	LC3	0	<input type="checkbox"/>
AC_VI	3	7	LC	0	<input type="checkbox"/>
AC_VO	3	E	7	7	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
<b>WMM Capable</b>	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
<b>Aifsn</b>	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.



<b>CWMin/CWMax</b>	<b>CWMin</b> means contention Window-Min and <b>CWMax</b> means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
<b>Txop</b>	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
<b>ACM</b>	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. <b>Note:</b> Vigor2120 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
<b>AckPolicy</b>	“Uncheck” (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. “Check” the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

After finishing this web page configuration, please click **OK** to save the settings.

### 3.7.8 Station List

**Station List** provides the knowledge of connecting wireless clients now along with its status code.

Wireless LAN >> Station List

Station List

						General	Advanced
MAC Address	SSID	Auth	Encrypt	Tx Rate	Rx Rate	AP	Rate
Refresh							
Add to Access Control :							
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>							
Add							

Available settings are explained as follows:

Item	Description
<b>MAC Address</b>	Display the MAC Address for the connecting client.
<b>SSID</b>	Display the SSID that the wireless client connects to.
<b>Auth</b>	Display the authentication that the wireless client uses for connection with such AP.
<b>Encrypt</b>	Display the encryption mode used by the wireless client.
<b>Tx Rate/Rx Rate</b>	Display the transmission /receiving rate for packets.
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .
<b>General/Advanced</b>	<b>General</b> – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. <b>Advanced</b> – Display more information (e.g., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) for the station.

## 3.8 RADIUS Server

VigorAP 710 offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 710. The AP can accept the wireless connection authentication requested by wireless clients.

### RADIUS Server Configuration

**Enable RADIUS Server**

**Users Profile (up to 96 users)**

Username	Password	Confirm Password	Configure
NO.	Username	Select	<input type="button" value="Add"/> <input type="button" value="Cancel"/>
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>			

**Authentication Client (up to 16 clients)**

Client IP	Secret Key	Confirm Secret Key	Configure
NO.	Client IP	Select	<input type="button" value="Add"/> <input type="button" value="Cancel"/>
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>			

---

Backup Radius Client <input type="button" value="Backup"/>	Upload From File: <input type="text" value="..."/> <input type="button" value="Browse"/>
	<input type="button" value="Upload"/>

Available settings are explained as follows:

Item	Description
<b>Enable RADIUS Server</b>	Check it to enable the internal RADIUS server.
<b>Users Profile</b>	<p><b>Username</b> – Type a new name for the user profile.</p> <p><b>Password</b> – Type a new password for such new user profile.</p> <p><b>Confirm Password</b> – Retype the password to confirm it.</p> <p><b>Configure</b></p> <ul style="list-style-type: none"> <li>● <b>Add</b> – Make a new user profile with the name and password specified on the left boxes.</li> <li>● <b>Cancel</b> – Clear current settings for user profile.</li> </ul> <p><b>Delete Selected</b> – Delete the selected user profile (s).</p> <p><b>Delete All</b> – Delete all of the user profiles.</p>
<b>Authentication Client</b>	<p>This internal RADIUS server of VigorAP 710 can be treated as the external RADIUS server for other users. Specify the client IP and secret key to make the wireless client choosing VigorAP 710 as its external RADIUS server.</p> <p><b>Client IP</b> – Type the IP address for the user to be authenticated by VigorAP 710 when the user tries to use VigorAP 710 as the external RADIUS server.</p>

	<p><b>Secret Key</b> – Type the password for the user to be authenticated by VigorAP 710 while the user tries to use VigorAP 710 as the external RADIUS server.</p> <p><b>Confirm Secret Key</b> – Type the password again for confirmation.</p> <p><b>Configure</b></p> <ul style="list-style-type: none"> <li>● <b>Add</b> – Make a new client with IP and secret key specified on the left boxes.</li> <li>● <b>Cancel</b> – Clear current settings for the client.</li> </ul> <p><b>Delete Selected</b> – Delete the selected client(s).</p> <p><b>Delete All</b> – Delete all of the clients.</p>
<b>Backup</b>	Click it to store the settings (RADIUS configuration) on this page as a file.
<b>Restore</b>	Click it to restore the settings (RADIUS configuration) from an existed file.

After finishing this web page configuration, please click **OK** to save the settings.

## 3.9 Applications

Below shows the menu items for Applications.

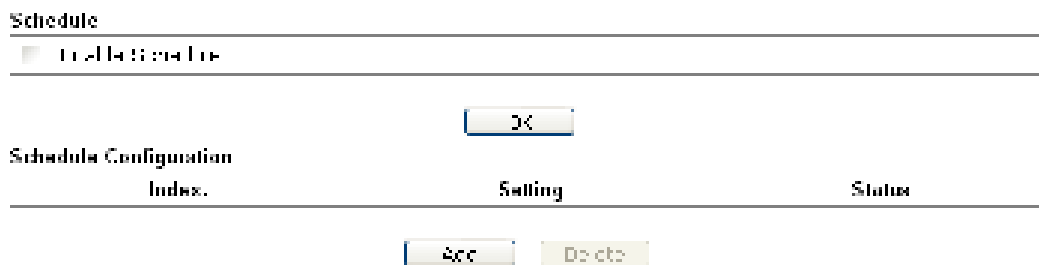


### 3.9.1 Schedule

The Vigor router has a built-in clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.

Applications >> Schedule



Available settings are explained as follows:

Item	Description
<b>Schedule</b>	<b>Enable Schedule</b> - Check it to enable the function of schedule configuration.
<b>Schedule Configuration</b>	<p><b>Index</b> – Display the sort number of the schedule profile.</p> <p><b>Setting</b> – Display the summary of the schedule profile.</p> <p><b>Status</b> – Display if the profile is enabled (V) or not (X).</p> <p><b>Add</b> – Such button is available when Enable Schedule is checked. It allows to add a new schedule profile.</p> <p><b>Delete</b> – Such button is used to remove the existed schedule profile.</p>

You can set up to **15** schedules. To add a schedule:

1. Check the box of **Enable Schedule**.
2. Click the **Add** button to open the following web page.

Applications >> Schedule

---

**Add Schedule**

Enable

Start Date: 2000 - 1 - 1 (Year - Month - Day)

Start Time: 1 : 1 (Hour - Minute)

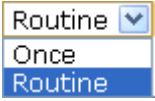
Action: Auto Reboot

Act: Routine

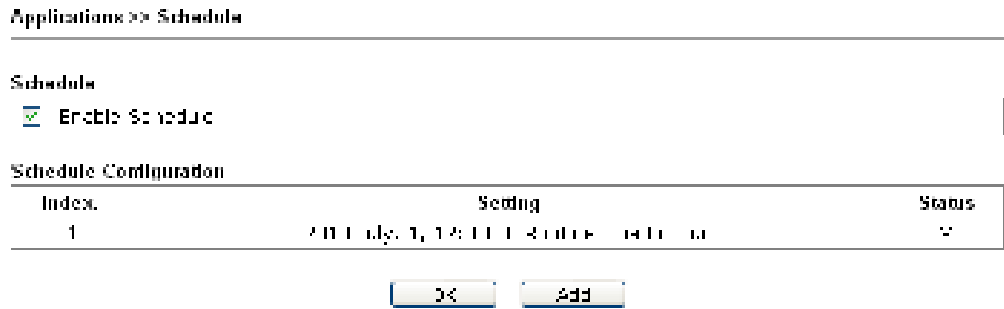
Weekly:  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

[ Add ] [ Cancel ]

Available settings are explained as follows:

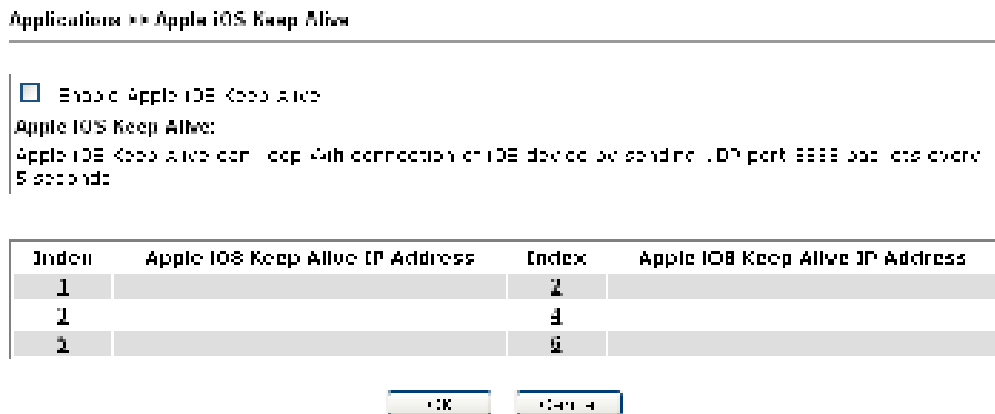
Item	Description
<b>Enable</b>	Check to enable such schedule profile.
<b>Start Date</b>	Specify the starting date of the schedule.
<b>Start Time</b>	Specify the starting time of the schedule.
<b>Action</b>	Specify which action should apply the schedule.
<b>Acts</b>	<p>Specify how often the schedule will be applied.</p> <p><b>Once</b> -The schedule will be applied just once</p> <p><b>Routine</b> -Specify which days in one week should perform the schedule.</p> 

- After finishing this web page configuration, please click **OK** to save the settings. A new schedule profile has been created and displayed on the screen.



### 3.9.2 Apple iOS Keep Alive

To keep the wireless connection (via Wi-Fi) on iOS device in alive, VigorAP 710 will send the UDP packets with 5353 port to the specific IP every five seconds.



Available settings are explained as follows:

Item	Description
<b>Enable Apple iOS Keep Alive</b>	Check to enable the function.
<b>Index</b>	Display the setting link. Click the index link to open the configuration page for setting the IP address.
<b>Apple iOS Keep Alive IP Address</b>	Display the IP address.

## 3.10 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, TR-069, Administrator Password, Configuration Backup, Time and Date, Management, Reboot System and Firmware Upgrade.

Below shows the menu items for System Maintenance.



### 3.10.1 System Status

The **System Status** provides basic network settings of Vigor modem. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

#### System Status

```

Model          : VigorAP710
Firmware Version : 1.10
Build Date/Time : 13805 Wed Feb 5 09:56:25 CST 2014
System Uptime   : 0d 00h 01m 25s
Operation Mode  : Universal Repeater
    
```

System		LAN	
Memory Total	: 05844 KB	MAC Address	: 00 0C 3C 7C 20 78
Memory left	: 11233 KB	IP Address	: 192 168 1 1
Cached	: 15464 KB	IP Mask	: 255 255 255 0
Memory	: 11233 KB		
Wireless			
MAC Address	: 00 0C 3C 7C 20 78		
IP	: 192 168 1 1		
Cache	: ...		

Each item is explained as follows:

Item	Description
<b>Model Name</b>	Display the model name of the modem.
<b>Firmware Version</b>	Display the firmware version of the modem.
<b>Build Date/Time</b>	Display the date and time of the current firmware build.
<b>System Uptime</b>	Display the period that such device connects to Internet.
<b>Operation Mode</b>	Display the operation mode that the device used.
<i>System</i>	
<b>Memory total</b>	Display the total memory of your system.
<b>Memory left</b>	Display the remaining memory of your system.

<i>LAN</i>	
<b>MAC Address</b>	Display the MAC address of the LAN Interface.
<b>IP Address</b>	Display the IP address of the LAN interface.
<b>IP Mask</b>	Display the subnet mask address of the LAN interface.
<i>Wireless</i>	
<b>MAC Address</b>	Display the MAC address of the WAN Interface.
<b>SSID</b>	Display the SSID of the device.
<b>Channel</b>	Display the channel that the station used for connecting with such device.

### 3.10.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS SI.

System Maintenance >> TR-069 Settings

#### ACS Settings

URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>

#### CPE Settings

Enable	<input type="checkbox"/>
CP	LAN 2
URL	http://102.138.1.2:8000/cp-mycp.html
Port	8080
Username	admin
Password	admin
DNS Server IP Address	<input type="text"/>
Primary IP Address	<input type="text"/>
Secondary IP Address	<input type="text"/>
Note:	Please set default gateway of the interface LAN 2 to LAN IP

#### Periodic Inform Settings

Enable	<input checked="" type="checkbox"/>
Interval (min)	500

#### STUN Settings

<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Server Address	<input type="text"/>
Server Port	8478
Maximum Keep Alive Period	60
Maximum Keep Alive Period	1



Available settings are explained as follows:

Item	Description
<b>ACS Settings</b>	<p><b>URL/Username/Password</b> – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user’s manual for detailed information. The setting for URL can be domain name or IP address.</p>
<b>CPE Settings</b>	<p>Such information is useful for Auto Configuration Server (ACS).</p> <p><b>Enable</b>– Check the box to allow the CPE Client to connect with Auto Configuration Server.</p> <p><b>On</b> – Choose the interface for VigorAP 710 connecting to ACS server.</p> <p><b>Port</b> – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.</p> <p><b>DNS Server IP Address</b> – Such field is to specify the IP address if a URL is configured with a domain name.</p> <ul style="list-style-type: none"> <li>● <b>Primary IP Address</b> –You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field.</li> <li>● <b>Secondary IP Address</b> –You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.</li> </ul>
<b>Periodic Inform Settings</b>	<p>The default setting is <b>Enable</b>. Please set interval time or schedule time for the AP to send notification to VigorACS server. Or click <b>Disable</b> to close the mechanism of notification.</p> <p><b>Interval Time</b> – Type the value for the interval time setting. The unit is “second”.</p>
<b>STUN Settings</b>	<p>The default is <b>Disable</b>. If you click <b>Enable</b>, please type the relational settings listed below:</p> <p><b>Server Address</b> – Type the IP address of the STUN server.</p> <p><b>Server Port</b> – Type the port number of the STUN server.</p> <p><b>Minimum Keep Alive Period</b> – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is “60 seconds”.</p> <p><b>Maximum Keep Alive Period</b> – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of “-1” indicates that no maximum period is specified.</p>

After finishing this web page configuration, please click **OK** to save the settings.

### 3.10.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administration Password

#### Administrator Settings

Account	<input type="text" value="admin"/>
Password	<input type="password" value="admin"/>
Confirm Password	<input type="password"/>

Note: Administrator can contain only a-z, A-Z, 0-9, ., - and \_.

Available settings are explained as follows:

Item	Description
<b>Account</b>	Type the name for accessing into Web User Interface.
<b>Password</b>	Type in new password in this field.
<b>Confirm Password</b>	Type the new password again for confirmation.

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

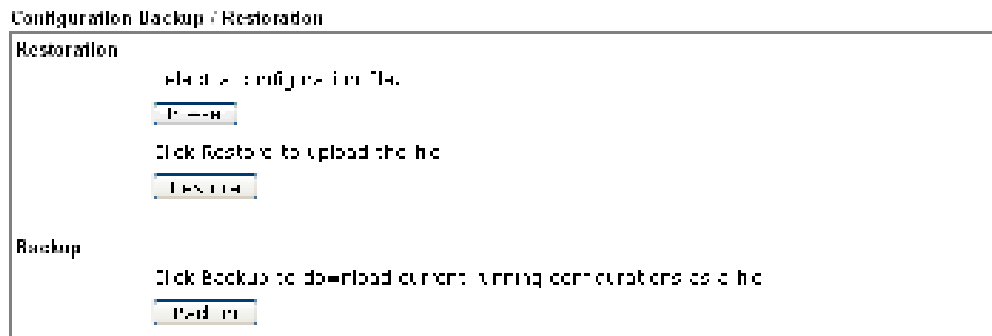
## 3.10.4 Configuration Backup

### Backup the Configuration

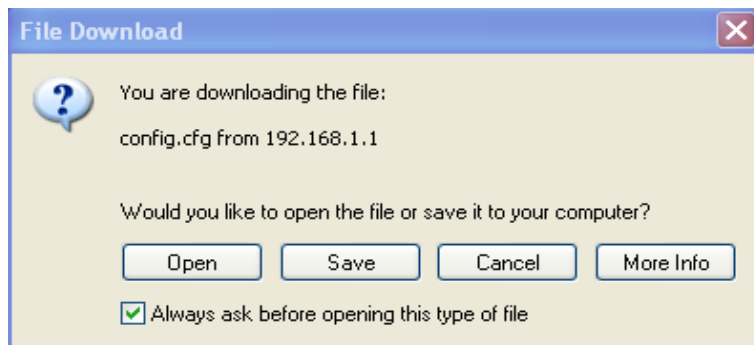
Follow the steps below to backup your configuration.

1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

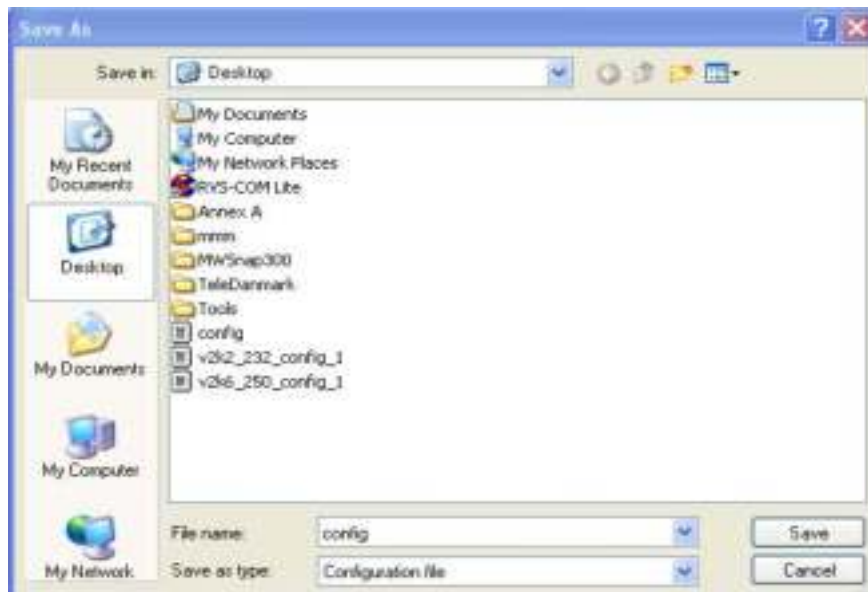
System Maintenance >> Configuration Backup



2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



- Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

**Note:** Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

## Restore Configuration

- Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup

- Click **Browse** button to choose the correct configuration file for uploading to the modem.
- Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

## 3.10.5 Time and Date

It allows you to specify where the time of the router should be inquired from.

System Maintenance >> Time and Date

Available parameters are explained as follows:

Item	Description
<b>Current System Time</b>	Click <b>Inquire Time</b> to get the current time.

Item	Description
<b>Use Browser Time</b>	Select this option to use the browser time from the remote administrator PC host as router's system time.
<b>Use NTP Client</b>	Select to inquire time information from Time Server on the Internet using assigned protocol.
<b>Time Zone</b>	Select a time protocol.
<b>NTP Server</b>	Type the IP address of the time server. <b>Use Default</b> – Click it to choose the default NTP server.
<b>Daylight Saving</b>	Check the box to enable the daylight saving. Such feature is available for certain area.
<b>NTP synchronization</b>	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

### 3.10.6 Management

This page allows you to manage the port settings for HTTP and HTTPS.

System Maintenance >> Management

Management Port Setup

HTTP	<input type="text" value="80"/>
HTTPS	<input type="text" value="443"/>

### 3.10.7 Reboot System

The Web Configurator may be used to restart your modem. Click **Reboot System** from **System Maintenance** to open the following page.

System Maintenance >> Reboot System

Reboot System

---

Do You want to reboot your router ?

Using current configuration  
 Using factory default configuration

If you want to reboot the modem using the current configuration, check **Using current configuration** and click **OK**. To reset the modem settings to default values, check **Using factory default configuration** and click **OK**. The modem will take 5 seconds to reboot the system.

**Note:** When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your modem for ensuring normal operation and preventing unexpected errors of the modem in the future.

### 3.10.8 Firmware Upgrade

Before upgrading your modem firmware, you need to install the Modem Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is [www.draytek.com](http://www.draytek.com) (or local DrayTek's web site) and FTP site is [ftp.draytek.com](ftp://ftp.draytek.com).

Click **System Maintenance**>> **Firmware Upgrade** to launch the Firmware Upgrade Utility.

System Maintenance >> Firmware Upgrade

---

#### Firmware Upgrade

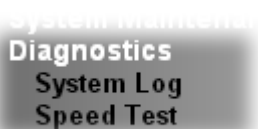
Select a firmware file.

File to upgrade (required):

Click **Browse** to locate the newest firmware from your hard disk and click **Upgrade**.

### 3.11 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your VigorAP 710.



#### 3.11.1 System Log

At present, only **System Log** is offered.

Diagnostics >> System Log

---

#### System Log Information

```

02/10/2014 01:52:01 [Debug] [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
02/10/2014 01:52:01 [Kernel] [Kernel] [Kernel] [Kernel] [Kernel]
    
```

4

### 3.11.2 Speed Test

Click the **Start** button on the page to test the speed. Such feature can help you to find the best installation place for Vigor AP.

Diagnoses **Speed Test**

---

#### Speed Test

Welcome to VigorAP's speed test.

This feature helps you to find out the best place for VigorAP to install a single Vigor AP. It is a different place of the building you selected. The test will help you to find the best performance for the test. Study for your reference.

**Start**

Note: Speed test cannot work with wireless router.

### 3.12 Support Area

When you click the menu item under **Support Area**, you will be guided to visit [www.draytek.com](http://www.draytek.com) and open the corresponding pages directly.

**Support Area**  
FAQ/Application Note  
Product Registration

All Rights Reserved

This page is left blank.



# 4

## Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the modem and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the modem from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the modem still cannot run normally, it is the time for you to contact your dealer for advanced help.

### 4.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and cable connections.  
Refer to “**1.3 Hardware Installation**” for details.
2. Power on the modem. Make sure the **POWER LED**, **ACT LED** and **SSID LED** are bright.
3. If not, it means that there is something wrong with the hardware status. Simply back to “**1.3 Hardware Installation**” to execute the hardware installation again. And then, try again.

## 4.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is still failed, please do the steps listed below to make sure the network connection settings is OK.

### For Windows



The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in [www.draytek.com](http://www.draytek.com).

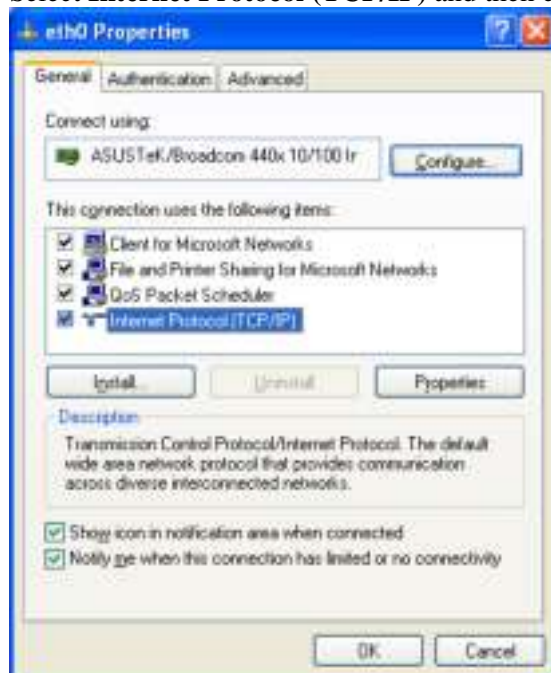
1. Go to **Control Panel** and then double-click on **Network Connections**.



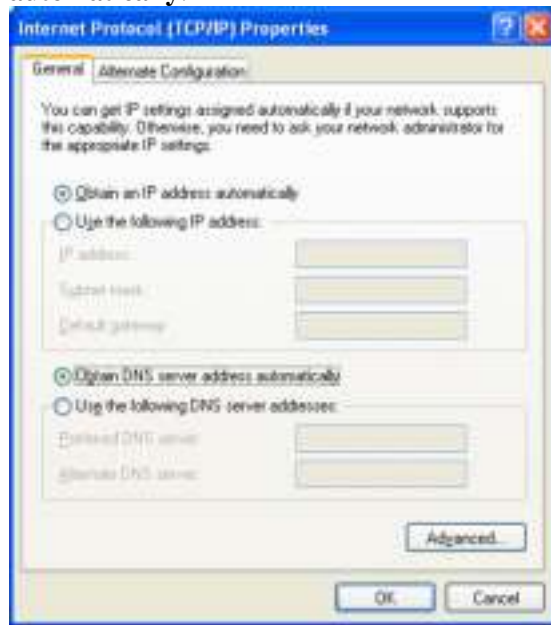
2. Right-click on **Local Area Connection** and click on **Properties**.



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

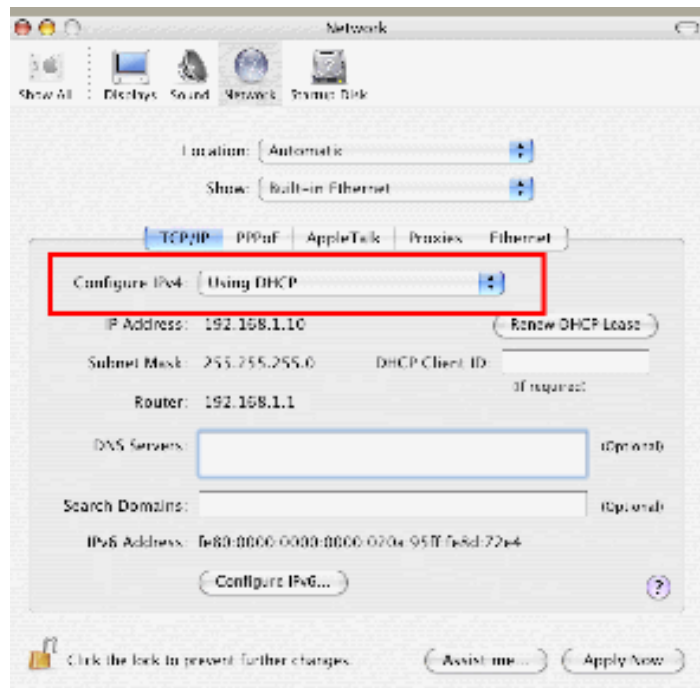


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



### For Mac Os

1. Double click on the current used Mac Os on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



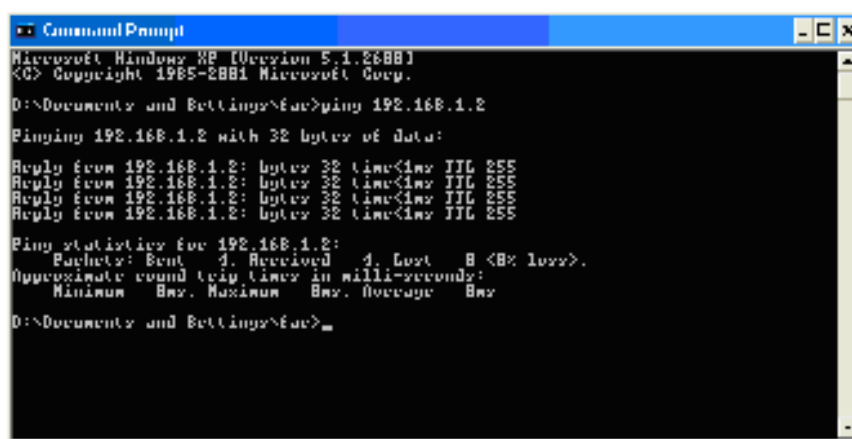
## 4.3 Pinging the Modem from Your Computer

The default gateway IP address of the modem is 192.168.1.2. For some reason, you might need to use “ping” command to check the link status of the modem. **The most important thing is that the computer will receive a reply from 192.168.1.2.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

Please follow the steps below to ping the modem correctly.

### For Windows

1. Open the **Command Prompt** window (from **Start menu**> **Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



```
Microsoft Windows [Version 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fac>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fac>
```

3. Type ping 192.168.1.2 and press [Enter]. If the link is OK, the line of **“Reply from 192.168.1.2:bytes=32 time<1ms TTL=255”** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

### For Mac Os (Terminal)

1. Double click on the current used Mac Os on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.2** and press [Enter]. If the link is OK, the line of **“64 bytes from 192.168.1.2: icmp\_seq=0 ttl=255 time=xxxx ms”** will appear.

```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

## 4.4 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the modem by software or hardware.



**Warning:** After pressing **factory default setting**, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

### Software Reset

You can reset the modem to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the modem will return all the settings to the factory settings.

System Maintenance => Reboot System

Reboot System

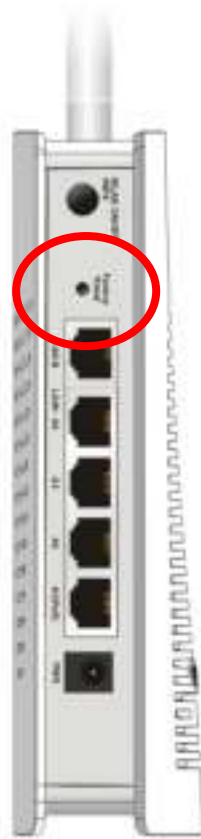
Do You want to reboot your router ?

- Using current configuration
- Using factory default configuration



### Hardware Reset

While the modem is running, press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the modem will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the modem again to fit your personal request.

## 4.5 Contacting Your Dealer

If the modem still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to [support@draytek.com](mailto:support@draytek.com).