



Your reliable networking solutions partner

User's Guide

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	• Read the installation guide thoroughly before you set up the modem.			
Instructions	 The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself 			
	 Do not place the modern in a damp or humid place a g a bathroom 			
	 Do not place the modeln in a damp of humid place, e.g. a bathoom. The modem should be used in a sheltered area, within a temperature range of 15. 			
	• The model should be used in a shellered area, within a temperature range of $+3$ 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 (nurchaser) that the modem will be free from any			
Trainanty	defects in workmanship or materials for a period of one (1) year from the date of			
	nurchase from the dealer. Please keep your nurchase receipt in a safe place as it serves			
	as proof of date of purchase. During the warranty period, and upon proof of purchase			
	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			
	naterials, we will, at our discretion, repair of replace the delective products of			
	components, without charge for either parts or labor, to whatever extent we deem			
	necessary tore-store 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	Web registration is preferred. You can register your Vigor modem via			
Owner	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			
	1 v			



European Community Declarations

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303Product: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



Preface	1	
1.1 Introduction	1	
1.2 LED Indicators and Connectors	2	
1.3 Hardware Installation	4	



Network Configuration	5
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 2.7.2 Configuring 2.4GHz Wireless Settings based on the Operation Mode 2.7.3 Configuring 2.4GHz Security Settings 2.7.4 Finishing the Wireless Settings Wizard 	
2.8 Online Status	21



Advanced Configuration	23
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. 3.4.2 Security. 3.4.3 Access Control. 3.4.4 WPS. 3.4.5 AP Discovery . 3.4.6 WMM Configuration . 3.4.7 Station List . 	
3.5 Wireless LAN Settings for AP Bridge-Point to Point/AP Bridge-Point to Multi-Point Me	ode 42
3.5.1 General Setup3.5.2 AP Discovery3.5.3 WDS AP Status	42 45 46



3.6 Wireless LAN Settings for AP Bridge-WDS Mode	. 46
 3.6.1 General Setup	. 46 . 51 . 54 . 55 . 56 . 57 . 57 . 59
3.7 Wireless LAN Settings for Universal Repeater Mode	. 60
 3.7.1 General Setup	. 60 . 64 . 67 . 68 . 69 . 70 . 72 . 74
3.8 RADIUS Server	. 75
3.9 Applications	. 76
3.9.1 Schedule 3.9.2 Apple iOS Keep Alive	. 76 . 78
3.10 System Maintenance	. 79
 3.10.1 System Status	. 79 . 80 . 82 . 83 . 84 . 85 . 85 . 86
3.11 Diagnostics	. 86
3.11.1 System Log 3.11.2 Speed Test	. 86 . 87
3.12 Support Area	. 87



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





1.1 Introduction

Thank you for purchasing this VigorAP 710, the concurrent dual band wirelessaccess 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	Connecter for xDSL / Cable modem or router.
Frank Market Dep PWR	Factory Reset	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	PWR: Connecter for a power adapter.
	ON OFF	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.)





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.

🖳 Local Area Connection Properties		
Networking Sharing		
Connect using:		
Realtek RTL8139/810x Family Fast Ethemet NIC		
Configure This connection uses the following items:		
Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv6)		
Install Uninstall Properties		
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.		
OK Cancel		

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

Internet Protocol Version 4 (TCP/IPv4) Properties	
General		
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.		
Obtain an IP address automatica	ally	
O Use the following IP address:	:	
IP address:	192.168.1.9	
Subnet mask:	255.255.255.0	
Default gateway:	192.168.1.1	
Obtain DNS server address automatically		
• Use the following DNS server ad	dresses:	
Preferred DNS server:	168 . 95 1 . 1	
Alternate DNS server:	• •	
Validate settings upon exit	Advanced	
	OK Cancel	

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**.

Local Area Connectio	on Properties	<u>? ×</u>
General		
Connect using:		
💷 Realtek RTL8	3029(AS) PCI Ethernet Ad	lapter
		Configure
Components checke	ed are used by this conne	ction:
Chent for Miles	Stosoft Networks iter Sharing for Microsoft Microsoft Microsoft (cocol (TCP/IP)	Networks

<u>I</u> nstall	<u>U</u> ninstall	Properties
Description	· · · · ·	
Transmission Con wide area networ across diverse int	trol Protocol/Internet Prot k protocol that provides c erconnected networks.	ocol. The default ommunication
Sho <u>w</u> icon in tas	kbar when connected	
	0	IK Cancel

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

Internet Protocol (TCP/IP) Properties	<u>? ×</u>
General	
You can get IP settings assigned automatically if this capability. Otherwise, you need to ask your n the appropriate IP settings.	your network supports etwork administrator for
Obtain an IP address automatically	
C Use the following IP address:	
IP address:	and the second sec
Sybnet mask:	
Default gateway:	
Obtain DNS server address automatically	
□ □ Use the following DNS server addresses:—	_
Preferred DNS server:	
Alternate DNS server:	
	OK Cancel

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**.

🕹 Local Area Connection Properties 🛛 🔹 💽
General Authentication Advanced
Connect using:
AMD PCNET Family PCI Ethernet Ad
This connection uses the following items:
Client for Microsoft Networks
Qa S Packet Scheduler
☑ Trinternet Protocol (TCP/IP)
Install Uninstall Properties
Transmission Control Protocol/Internet Protocol. The default
wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Votify me when this connection has limited or no connectivity
OK Cancel

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.

Internet Protocol (TCP/IP) Pr	operties 🛛 🛛 🛛
General	
You can get IP settings assigned a this capability. Otherwise, you nee the appropriate IP settings.	automatically if your network supports d to ask your network administrator for
Obtain an IP address automa	ıtically
O Use the following IP address]
IP address:	192.168.1.9
S <u>u</u> bnet mas	255 . 255 . 255 . 0
Default gateway:	· · ·
Obtain DNS server address a	utomatically
Output Server → Output Ser	r addresses:
Preferred DNS server:	
Alternate DNS server:	
	Advanced
	OK Cancel

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 Netwrok, 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.

eneral	
You can get IP settings assigne this capability. Otherwise, you i	d automatically if your network supports need to ask your network administrator
for the appropriate IP settings.	
🔘 Obtain an IP address auto	matically
• Use the following IP addre	ss:
IP at the st	192.168.1.9
onet mask:	255 . 255 . 255 . 0
Default gateway:	fr e s
Obtain DNS cerver addres	s sutomatically
Obtain one server address	ver addresses:
Preferred DNS server:	
Alternate DNS server:	Grab sele ed Region
	Advanced

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.



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. Pease type "admin/admin" on Username/Password and click Log In.

Authentication F	Required	>
The server http://19 The server says: Viş	2.168.1.2:80 requires a username and password. gorAP710.	
User Name:	admin	
Password:	****	

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

System Status	
art Wizard Model : Vig tatus Firmware Version : 1.1. Build Date Time : 1374 n Mode System Uptime : 00 C Operation Mode : Unix	AP710 RC2a 9 Thu Jan 16 17:05:53 CST 2014 Jo4:07 rsal Repeater
Server System	LAN
ions Memory Total : 62316 Maintenance Memory Left : 37824	B MAC Address : 00:0C:43:76:20:78 B IP Address : 192.168.1.2
lics Cached : 15420 Memory	:B / 62316 kB IP Mask : 255.255.255.0
Area Wireless	
lication Note MAC Address : 00:0C:	-3:76:20:78
Registration SSID : DrayTe	
Admin mode	
Admin mode sal 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.

Administrator Settings		
Account	admin	
Password	••••	
Confirm Password		

3. Enter the new login password on the field of **Password**. Then click **OK** to continue.

ОК

Cancel

4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.

Authentication	Required
The server http://19 The server says: Vi	92.168.1.2:80 requires a username and password. igorAP710.
User Name:	
Password	skoskoskosk
13350010.	

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 :	Universal Repeater 💉 VigorAP can act as a wireless repeater; it can be Station and AP at the same
Wireless Mode :	time. Mixed(11b+11q+11n) 💌
Main SSID :	DrayTek
	Multiple SSID
Channel :	2462MHz (Channel 11) 💌
Extension Channel :	2442MHz (Channel 7) 💌
Station List :	Display
AP Discovery :	Display
	Next > Cancel

Available settings are explained as follows:

Item	Description
Operation Mode	There are six operation modes for wireless connection. Settings for each mode are different.
Wireless Mode	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.
Main SSID	Set a name for VigorAP 710 to be identified.
	SSID4.
Channel	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



	frequency, please select AutoSelect to let system determine for
	you.
	2462MHz (Channel 11) AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 6) 2442MHz (Channel 7) 2447MHz (Channel 7) 2447MHz (Channel 8) 2452MHz (Channel 9) 2457MHz (Channel 10) 2462MHz (Channel 11) 2467MHz (Channel 12)
	With 202 11g, there is any action to double the bondwidth nor
Extension Channel	channel. The available extension channel options will be varied according to the Channel selected above.
Station List	Click the Display button to open the Station List dialog. It provides the knowledge of connecting wireless clients now along with its status code.
AP Discovery	Click this button to open the AP Discovery dialog. VigorAP 710 can scan all regulatory channels and find working APs in the neighborhood.
	This option is available when AP-Bridge/Universal Repeater is selected as the Operation Mode .

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.

Note : Enter the configuration of APs which AP 900 want to connect. Phy Mode : HTMIX			
Security : O Disabled O WEP O TKIP O AES Key :			
Peer MAC Address :			
	<pre></pre>		

Available settings are explained as follows:

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

Phy Mode : HTMIX	
1. Security :	3. Security :
◯Disabled ◯WEP ◯TKIP ◯AES	◯ Disabled ◯ WEP ◯ TKIP ◯ AES
Кеу :	Key :
Peer MAC Address :	Peer MAC Address :
2. Security:	4. Security:
◯Disabled ◯WEP ◯TKIP ◯AES	◯ Disabled ◯ WEP ◯ TKIP ◯ AES
Key :	Key :
Peer MAC Address :	Peer MAC Address :

Available settings are explained as follows:

Quick Start Wizard >> Wireless LAN (2.4GHz)

Item	Description
Phy Mode	Data will be transmitted via HTMIX communication channel.
	Each access point should be setup to the same Phy mode for connecting with each other.
Security	Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required.
Peer MAC Address	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 : Enter the configuration of APs which AP Remote AP should always set LAN-A MA	9 900 want to connect. AC address to connect AP900 WDS.
Phy Mode : HTMIX	
1. Subnet LAN-A 💌 Security :	3. Subnet LAN-A 📝 Security :
◯Disabled ◯WEP ◯TKIP ◯AES	◯ Disabled ◯ WEP ◯ TKIP ◯ AES
Key :	Key :
Peer MAC Address :	Peer MAC Address :
2. Subnet LAN-A 🗹 Security :	4. Subnet LAN-A 💌 Security :
◯Disabled ◯WEP ◯TKIP ◯AES	O Disabled O WEP O TKIP O AES
Кеу :	Кеу :
Peer MAC Address :	Peer MAC Address :
	< Back Next > Cancel

Available settings are explained as follows:

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

SSID	DrayTek2860nnn
MAC Address (Optional)	00:1d:aa:ae:8c:68
Security Mode	WPA2/PSK 💌
Encryption Type	AES 💌
Pass Phrase	•••••

Available settings are explained as follows:

Item	Description
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
MAC Address (Optional)	Type the MAC address for the access point.
Security Mode	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. WPA/PSK Open Shared WPA/PSK WPA2/PSK
Encryption Type for Open/Shared	 This option is available when Open/Shared is selected as Security Mode. Choose None to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose WEP. None WEP WEP Keys - 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 ','.

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

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

SSID DrayTek Wireless Security Settings Mixed(WPA+WPA2)/PSK Mode Mixed(WPA+WPA2)/PSK WPA Algorithms TKIP Pass Phrase ••••••••••• Key Renewal Interval 3600 seconds PMK Cache Period 10 minutes Pre-Authentication ● Disable	SSID 1	SSID 2	SSID 3	SSID 4			
Wireless Security Settings Mode Mixed(WPA+WPA2)/PSK ▼ WPA Algorithms TKIP O AES O TKIP/AES Pass Phrase •••••••• Key Renewal Interval 3600 seconds PMK Cache Period 10 minutes Pre-Authentication • Disable O Enable	ssi	D	Di	rayTek			
Mode Mixed(WPA+WPA2)/PSK WPA Algorithms ○ TKIP ○ AES ⊙ TKIP/AES Pass Phrase •••••••••••••• Key Renewal Interval 3600 seconds PMK Cache Period 10 minutes Pre-Authentication ● Disable ○ Enable	Wir	eless Security Sett	ings				
WPA AlgorithmsTKIPAESTKIP/AESPass Phrase•••••••••••••••••••••••••••••••••	M	ode	٩	4ixed(WPA+WPA2	2)/PSK 🛛 🔽		
WPA AlgorithmsTKIPAESTKIP/AESPass Phrase•••••••••••Key Renewal Interval3600 secondsPMK Cache Period10 minutesPre-Authentication• Disable							
Pass Phrase••••••Key Renewal Interval3600 secondsPMK Cache Period10 minutesPre-Authentication	W	PA Algorithms	(TKIP OAES	⊙ TKIP/AES		
Key Renewal Interval3600 secondsPMK Cache Period10 minutesPre-AuthenticationIsable Enable	Pa	ass Phrase	•	•••••			
PMK Cache Period 10 minutes Pre-Authentication • Disable Enable	Ke	ey Renewal Interv	al 3	600 seconds			
Pre-Authentication Disable Enable 	PMK Cache Period		1	0 minutes			
	Pre-Authentication		0	Disable OEnal	ble		
						Novta	Cancel

Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose. Disable Image: Constraint of the second seco
	Disable - The encryption mechanism is turned off.
	WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.
	WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - 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.
	WEP/802.1x - 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.
	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.
	WPA/802.1x - 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.
	WPA2/802.1x - 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.
WPA Algorithm	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Internal	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 WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
PMK Cache Period	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 WPA2/802.1 mode.
Pre-Authentication	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) Enable - Enable IEEE 802.1X Pre-Authentication. Disable - Disable IEEE 802.1X Pre-Authentication.
Key 1 – Key 4	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 ','.
802.1x WEP	 Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted. Enable - Enable the WEP Encryption. Such feature is available for WEP/802.1x mode.

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				Syste	m Uptime: 0d 00:32:40
LAN Status					
IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes	
192.168.1.2	576	244	43778	12654	
Universal Repeate	rStatus				
IP		Gateway	SSID		Channel
10.28.60.13		10.28.60.254	DrayTek286	Onnn	11
Mac		Security Mode	TX Packets		RX Packets
00:1d:aa:ae:8c	:68	WPA2PSK	153394		17430

Detailed explanation is shown below:

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



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.

Dray Tek	VigorAP 710	
Quick Start Wizard Online Status	System Status Model : VigorAP710 Firmware Version : 1.1.0 Build Date/Time : r3805 Wed Feb 5 09:56:27	5 CST 2014
Operation Mode LAN Wireless LAN	System Uptime : 0d 00:01:25 Operation Mode : Universal Repeater	
RADIUS Server Applications System Maintenance Diagnostics	System Memory Total : 62344 kB Memory Left : 38232 kB Cached : 15424 kB / 62344 kB	LAN MAC Address 0.0:0C:43:76:20:78 IP Address 192.168.1.2 IP Mask 255.255.255.0
Support Area FAQ/Application Note Product Registration All Rights Reserved.	Memory VICETRE, CONTROL Wireless MAC Address : 00:0C:43:76:20:78 SSID : DrayTek Channel : 11	
Admin mode		
Universal Repeater Mode		

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 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

O AP Bridge-Point to Point :

VigorAP will connect to another VigorAP which uses the same mode, and all wired Ethernet clients of both VigorAPs will be connected together.

O AP Bridge-Point to Multi-Point :

VigorĂP will connect to up to four VigorAPs which uses the same mode, and all wired Ethernet clients of every VigorAPs will be connected together.

O AP Bridge-WDS :

VigorĀP will connect to up to four VigorAPs which uses the same mode, and all wired Ethernet clients of every VigorAPs will be connected together. This mode is still able to accept wireless clients.

O Universal Repeater :

VigorAP can act as a wireless repeater; it can be Station and AP at the same time.

OK

Available settings are explained as follows:

Item	Description
АР	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
AP Bridge-Point to Point	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.
AP Bridge-Point to Multi-Point	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.
AP Bridge-WDS	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.
Universal Repeater	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.

LAN General Setup

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

LAN IP Network Configuration		DHCP Server Configuratior	1
Specify an IP address		◯Enable Server ⊙Disat	ole Server
IP Address	192.168.1.2	○Relay Agent	
Subnet Mask	255.255.255.0	Start IP Address	
Default Gateway		End IP Address	
		Subnet Mask	
Enable Management	VLAN	Default Gateway	
VLAN ID	0	Lease Time	86400
		DHCP Server IP Address for Relay Agent	
		Primary DNS Server	
		Secondary DNS Server	
	ОК	Cancel	

Available settings are explained as follows:

Item	Description
IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.2).
Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
Default Gateway	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.
Enable Management VLAN	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. VLAN ID - Type the number as VLAN ID tagged on the

	transmitted packet. "0" means no VALN tag.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. DHCP server can automatically dispatch related IP settings to any local user configured as a DHCP client.
Enable Server / Disable Server	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.
Relay Agent	Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address	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.
End IP Address	Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
Default Gateway	Enter a value of the gateway IP address for the DHCP server.
Lease Time	It allows you to set the leased time for the specified PC.
DHCP Server IP Address for Relay Agent	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.
Primary DNS Server	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.
Secondary DNS Server	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.

Wireless LAN General Setup Security Access Control WPS AP Discovery WMM Configuration 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

🔲 Enable Limit	Client (3-64) 64 (default: 64)	
Mode :	Mixed(11b+11g+11n) 💌	
Hide SSID 1 D 2 C 3 C 4 C Hide SSID: Isolate Member:	SSID Isolate VLAN ID Mac Clone Member (0: Untagged) Mac Clone InayTek 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	each
MAC Clone:	Set the MAC address of SSID 1. The MAC addresses of other SSIL the Wireless client will also change based on this MAC address. Ple notice that the last byte of this MAC address must be a multiple of the set of	is an ease f g
MAC Clone: Channel : Extension Chann	Set the MAC address of SSID 1. The MAC addresses of other SSID the Wireless client will also change based on this MAC address. Ple notice that the last byte of this MAC address must be a multiple o 2462MHz (Channel 11) nel : 2442MHz (Channel 7)	s an ease f 8.
MAC Clone: Channel : Extension Chann Packet-OVERDRI	Set the MAC address of SSID 1. The MAC addresses of other SSID the Wireless client will also change based on this MAC address. Ple notice that the last byte of this MAC address must be a multiple o 2462MHz (Channel 11) V nel : 2442MHz (Channel 7) V	is an ase f 8.
MAC Clone: Channel : Extension Chann Packet-OVERDRI T x Burst	Set the MAC address of SSID 1. The MAC addresses of other SSID the Wireless client will also change based on this MAC address. Ple notice that the last byte of this MAC address must be a multiple o 2462MHz (Channel 11) V nel : 2442MHz (Channel 7) V	is an ease f 8.
MAC Clone: Channel : Extension Chann Packet-OVERDRI Tx Burst Note :	Set the MAC address of SSID 1. The MAC addresses of other SSIL the Wireless client will also change based on this MAC address. Ple notice that the last byte of this MAC address must be a multiple o 2462MHz (Channel 11) ♥ nel : 2442MHz (Channel 7) ♥	is an ease f 8.
MAC Clone: Channel : Extension Chann Packet-OVERDRI Tx Burst Note : 1.Tx Burst only s	Set the MAC address of SSID 1. The MAC addresses of other SSID the Wireless client will also change based on this MAC address. Ple notice that the last byte of this MAC address must be a multiple o 2462MHz (Channel 11) nel : 2442MHz (Channel 7) WE	is an ease f 8.
MAC Clone: Channel : Extension Chann Packet-OVERDRI Tx Burst Note : 1.Tx Burst only s 2.The same tech	Set the MAC address of SSID 1. The MAC addresses of other SSID the Wireless client will also change based on this MAC address. Ple notice that the last byte of this MAC address must be a multiple o 2462MHz (Channel 11) V nel : 2442MHz (Channel 7) V IVE	e,
MAC Clone: Channel : Extension Chann Packet-OVERDRI Tx Burst Note : 1.Tx Burst only s 2.The same tech Antenna :	Set the MAC address of SSID 1. The MAC addresses of other SSID the Wireless client will also change based on this MAC address. Ple notice that the last byte of this MAC address must be a multiple o 2462MHz (Channel 11) nel : 2442MHz (Channel 7) iVE supports 11g mode. noology must also be supported in clients to boost WLAN performanc 2T2R V	e.
MAC Clone: Channel : Extension Chann Packet-OVERDRI Tx Burst Note : 1.Tx Burst only s 2.The same tech Antenna : Tx Power :	Set the MAC address of SSID 1. The MAC addresses of other SSID the Wireless client will also change based on this MAC address. Ple notice that the last byte of this MAC address must be a multiple o 2462MHz (Channel 11) V hel : 2442MHz (Channel 7) V IVE supports 11g mode. noology must also be supported in clients to boost WLAN performanc 2T2R V 100% V	e.

Dray Tek

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Limit Client	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.
Mode	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.
	Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11b+11g+11n) Mixed(11b+11g+11n)
Hide SSID	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.
SSID	Set a name for VigorAP 710 to be identified. Default settings are DrayTek.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
VLAN ID	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.
Mac Clone	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.

Channel	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 AutoSelect to let system determine for you.			
	2437MHz (Channel 6) ✓ AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 3) 2427MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 5) 2442MHz (Channel 7) 2447MHz (Channel 7) 24452MHz (Channel 8) 2452MHz (Channel 9) 2457MHz (Channel 10) 2462MHz (Channel 11) 2467MHz (Channel 12) 2472MHz (Channel 13)			
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the Channel selected above. Configure the extension channel you want.			
Rate	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.			
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burs t). 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.			
	Note: 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 Enable for TxBURST on the tab of Option).			
	Vigor N61 802.11n Wireless USB Adapter Utility			
	Configuration Status Option About General Setting Advance Setting Auto launch when Windows start up Disable Redio Remember mini status position Disable Redio Auto hide mini status RTS Threshold : 2345 Set mini status always on top Frequency : 802.11b/g/n - 2.4GH Enable IP Setting and Proxy Setting in Profile Ad-hoc Channel: 1 Group Roaming Ad-hoc Disable Tx Burst :			
	WLAN type to connect Infrastructure and Ad-hoc network Infrastructure network only Ad-hoc network only A d-hoc network only			
	OK Cancel Apply			

Antenna	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. 2T2R 2T2R 1T1R
Tx Power	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless. 100% 100% 80% 60% 30% 20% 10%
Channel Width	 20 MHZ- the router will use 20Mhz for data transmission and receiving between the AP and the stations. Auto 20/40 MHZ- 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.

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

SSID 1	SSID 2	SSID 3	SSID 4			
Mo	de	Mixed(V	VPA+WPA2)	/PSK 🛛 💌		
Set WPA	: up <u>RADIUS Server</u> i	f 802.1x is er	nabled.			
WP	A Algorithms	🔿 ткір	○ AES	⊙ ΤΚΙΡ/ΑΕ	IS	
Pas	s Phrase	•••••	•••••			
Key	/ Renewal Interval	3600 s	econds			
WEP						
0	Кеу 1 :					Hex 💌
۲	Key 2 :					Hex 💟
	Кеу 3 :					Hex 💟
	Key 4 :					Hex 💟
802	2.1× WEP	🔿 Disab	ole 🔿 Ena	ble		
		ОК	Ca	ncel		

Item	Description
Mode	There are several modes provided for you to choose. Disable Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x Disable - The encryption mechanism is turned off. WEP - Accepts only WEP clients and the encryption key
	 should be entered in WEP Key. WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - 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. WEP/802.1x - 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.
	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.
	WPA/802.1x - 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.
	WPA2/802.1x - 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.
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/ PSK mode.
Key Renewal Interval	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 WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key 1 – Key 4	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 WEP mode. Hex ASCII Hex
802.1x WEP	Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.
	Enable - Enable the WEP Encryption.
	Such feature is available for WEP/802.1x mode.

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

RADIUS Server		
Use internal RADIUS Server		
IP Address	0	
Port	1812	
Shared Secret	DrayTek	
Session Timeout	0	

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	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, 3.9 RADIUS Server to configure settings for internal server of VigorAP 710.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	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.
Session Timeout	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.

Dray Tek

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).

SSID 1	SSID 2	SSID 3	SSID 4		
	S	SID: DrayTek olicy: Disable		×	
		MAG	C Address Filter		
	Inde>	(MAC A	Address	
	Client's M.	AC Address :	: : : : : : : : : : : : : : : : : : :	: : :	
		OK	Cance	el	
Backup ACL Cfg : Backup		Upload From Fil Restore	le: Choose File	No file chosen	

Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Blocked MAC address filter, 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. Activate MAC address filter Disable Activate MAC address filter Blocked MAC address filter
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.

Cancel	Give up the access control set up.
Backup	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
Restore	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.

🔲 Enable WPS 😳	
Wi-Fi Protected Setup Information	
WPS Configured	Yes
WPS SSID	DrayTek
WPS Auth Mode	Mixed(WPA+WPA2)/PSK
WPS Encryp Type	TKIP/AES

Device Configure	
Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN
Status: Not used	

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

♀: WPS is Disabled.

◘: WPS is Enabled.

 \mathcal{C} : Waiting for WPS requests from wireless clients.

Available settings are explained as follow	ws:
--	-----

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 710 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 710. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 710.
Configure via Push Button	Click Start PBC 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)
Configure via Client	Type the PIN code specified in wireless client you wish to

PinCode	connect, and click Start PIN 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

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

See Channel Statistics

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

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

Each item is explained as follows:

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.

WMM Configurat	tion				Set to F	actory Default	
WMM Capable		(🕽 Enable 🛛 💿 Dis	able			
WMM Parameters of Access Point							
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy	
AC_BE	3	15 💌	63 💌	0			
АС_ВК	7	15 💌	102: 💌	0			
AC_VI	1	7 💌	15 💌	94			
AC_VO	1	3 💌	7 💌	47			
WMM Paramete	rs of Station						
	Aifsn	CW	/Min	CWMax	Тхор	ACM	
AC_BE	3	15	*	102: 💙	0		
AC_BK	7	15	v	102: 🔽	0		
AC_VI	2	7	*	15 💌	94		
AC_VO	2	3	*	7 💌	47		

Wireless LAN >> WMM Configuration

OK Cancel

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the Enable 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.
CWMin/CWMax	CWMin means contention Window-Min and CWMax 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.
Тхор	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.

ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. Note: 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.
AckPolicy	"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 \mathbf{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

Station List					
				General	Advanced
MAC Address	SSID	Auth	Encrypt	Tx Rate(Kbps)	Rx Rate(Kbps)
					<u>~</u>
					~
		Refresh			
Add to <u>Access Contro</u>	<u>)I</u> :				
Client's MAC Address	5:	: : :			
		Add			

Item	Description
MAC Address	Display the MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Auth	Display the authentication that the wireless client uses for connection with such AP.
Encrypt	Display the encryption mode used by the wireless client.
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.
Refresh	Click this button to refresh the status of station list.
Add to Access Control	Client's MAC Address - 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.
Add	Click this button to add current typed MAC address into Access Contro l.
General/Advanced	General – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. Advanced – 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

able Wireless LAN	
Mode :	Mixed(11b+11g+11n) 💌
Channel :	2462MHz (Channel 11) 💌
Extension Channel :	2442MHz (Channel 7) 💌
Note : Enter the configurati	ion of APs which AP710 want to connect.
Phy Mode : HTMIX	
Security:	
⊙Disabled ○WEP ○1	TKIP OAES
Key :	
Peer Mac Address:	
Packet-OVERDRIVE	
Tx Burst	
Note :	
1.Tx Burst only supports 11	g mode.
2.The same technology mus	t also be supported in clients to boost WLAN performance.
Antenna :	2121
Antenna : Tx Power :	

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	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) Mixed(11b+11g+11n) Mixed(11b+11g) Mixed(11b+11g) Mixed(11b+11g) Mixed(11b+11g+11n) Mixed(11b+11g+11n)
Channel	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 AutoSelect to let system determine for you. 2462MHz (Channel 1) 2417MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 3) 2437MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 5) 2447MHz (Channel 6) 2442MHz (Channel 7) 2447MHz (Channel 8) 2452MHz (Channel 10) 2462MHz (Channel 10) 2467MHz (Channel 11) 2467MHz (Channel 12) 2472MHz (Channel 13)
Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the Channel selected above.
Rate	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.
Phy Mode	Data will be transmitted via communication channel, HTMIX.
Security	Select WEP, TKIP or AES as the encryption algorithm. Type the key number if required.
Peer Mac Address	Type the peer MAC address for the access point that VigorAP 710 connects to.

Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burs t). 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.		
	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 Enable for TxBURST on the tab of Option).		
	Vigor M61 602.11n Wireless USB Adapter Utility Configuration Status Option Auto lanch when Windows gtart up Advace Setting Auto lanch when Windows gtart up Daable Edio Paymentation Threshold : 2346 Remember mini status gosition Auto lanch when Windows gtart up Baable Edio Engmentation Threshold : St gini status always on top Enable IP Setting and Proxy Setting in Profile Group Roaming Ad-hoc WLAN type to connect Image: Set we Mode: Infrastructure and Ad-hoc getwork Image: Set we Mode: WLAN type to connect Image: Set we mode: Infrastructure and Ad-hoc getwork Image: Set we mode: Automatically connect to non-preferred networgs OK OK Cancel		
Antenna	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.		
	2T2R 2T2R 1T1R		
Tx Power	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless. 100% 100% 80% 60% 30% 20% 10%		
Channel Width	20 MHZ- the router will use 20Mhz for data transmission and receiving between the AP and the stations.		
	Auto 20/40 MHZ – 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.		

After finishing this web page configuration, please click \mathbf{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.

Access Point List					
Select SSID	BSSID	RSSI	Channel	Encryption	Authentication
See <u>Channel</u> Note: Durina t	<u>Statistics</u> he scanning	process (a	Sc	an	lowed to connect with the AP.
				,,	
AP's MAC Add	ress	:	:	: AP	's SSID
Add to <u>WDS S</u>	ettings: 📃 A	dd			

Wireless LAN >> Access Point Discovery

Available settings are	explained as follows:
------------------------	-----------------------

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

VDS /	AP List				
AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth	

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.

Wireless LAN
General Setup
Security
Access Control
WPS
AP Discovery
WDS AP Status
WMM Configuration
Station List
DADILLE Convor

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

Epoble Limit	 	sul+: 64)
Coerault: 64)		
Mode : Mixed(11b+11g+11n) ♥		d(11b+11g+11n) 💌
Hide SSID 1 Dray 2	SSID Isolate LAN Tek	Isolate VLAN ID Mac Clone Member(0:Untagged) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Hide SSID: Isolate LAN: Isolate Member: MAC Clone:	Prevent SSID from being Wireless clients (station on LAN. Wireless clients (station other. Set the MAC address of the Wireless client will a notice that the last byte	scanned. s) with the same SSID cannot access wired PC s) with the same SSID cannot access for each SSID 1. The MAC addresses of other SSIDs an lso change based on this MAC address. Please a of this MAC address must be a multiple of 8.
Channel :	2462	MHz (Channel 11) 💌
Extension Chann	el : 2442	MHz (Channel 7) 💌
Note : Enter the (Remote AP Phy Mode : HTMI 1. Subnet LAN-/	configuration of APs which should always set LAN-A C Security:	AP710 want to connect. MAC address to connect AP710 WDS. 3. Subnet LAN-A Security:
Note : Enter the or Remote AP Phy Mode : HTMI 1. Subnet LAN Obisabled C Key : Peer Mac Addres	Configuration of APs which should always set LAN-A C Security: WEP OTKIP OAES S:	AP710 want to connect. MAC address to connect AP710 WDS. 3. Subnet AN-A Security: Oisabled WEP TKIP AES Key : Peer Mac Address:
Note : Enter the or Remote AP Phy Mode : HTMI 1. Subnet AN	C C C C C C C C C C C C C C C C C C C	AP710 want to connect. MAC address to connect AP710 WDS. 3. Subnet AN-A Security: • Disabled WEP TKIP AES Key : Peer Mac Address: : : : : : : : : :
Note : Enter the or Remote AP Phy Mode : HTMI 1. Subnet LAN- Disabled (Key : Peer Mac Address Disabled (Key : Disabled (Key : Peer Mac Address : :	<pre>configuration of APs which should always set LAN-A c Security: WEP O TKIP O AES s: C C C C C C C C C C C C C C C C C C C</pre>	AP710 want to connect. MAC address to connect AP710 WDS. 3. Subnet APA Security: Disabled WEP TKIP AES Key : Peer Mac Address: Disabled WEP TKIP AES Security: Disabled WEP TKIP AES :
Note : Enter the or Remote AP Phy Mode : HTMI 1. Subnet AN-7 Disabled Key : Peer Mac Address Disabled Key : Disabled Key : Peer Mac Address Peer Mac Address Peer Mac Address Tx Burst Note : 1. Tx Burst only s 2. The same tech	<pre>configuration of APs which should always set LAN-A c Security: DWEP OTKIP OAES S: C C C C C C C C C C C C C C C C C C C</pre>	AP710 want to connect. MAC address to connect AP710 WDS. 3. Subnet AN-A Security: • Disabled • WEP • TKIP • AES Key : Peer Mac Address: • : : : : : : : : : : : : : : : : : : :
Note : Enter the or Remote AP Phy Mode : HTMI 1. Subnet AN- Disabled Key : Peer Mac Addres 2. Subnet AN- Disabled Key : Peer Mac Addres Peer Mac Addres Peer Mac Addres Comparison of the order Packet-OVERDRI Tx Burst Note : 1.Tx Burst only s 2.The same tech Antenna :	<pre>ionfiguration of APs which should always set LAN-A (Security:) WEP O TKIP O AES : : : : : : : : : : : : : : : : : : :</pre>	AP710 want to connect. MAC address to connect AP710 WDS. 3. Subnet AN-A Security: Disabled WEP TKIP AES Key : Peer Mac Address: : : : : : : : : : : : : : : : : : : :
Note : Enter the or Remote AP Phy Mode : HTMI Disabled C Key : Peer Mac Address Disabled C Key : Peer Mac Address Disabled C Key : Peer Mac Address Peer Mac Address C Peer Mac Address T × Burst Note : 1. T × Burst only s 2. The same tech Antenna : T × Power :	<pre>ionfiguration of APs which should always set LAN-A (Security:) WEP O TKIP O AES : : : : : : : :) WEP O TKIP O AES S: : : : : : : : //E //E //E //E //E //E //E //E ///////</pre>	AP710 want to connect. MAC address to connect AP710 WDS. 3. Subnet AN-A Security: • Disabled • WEP • TKIP • AES Key : Peer Mac Address: • Disabled • WEP • TKIP • AES Key : • Disabled • WEP • TKIP • AES Key : • Peer Mac Address: • : : : : : : : : : : : : : : : : : : :

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Limit Client	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.

Mode	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.
Hide SSID	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.
SSID	Set a name for VigorAP 710 to be identified. Default settings is DrayTek.
Isolate LAN	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
VLAN ID	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.
Mac Clone	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.
Channel	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 AutoSelect to let system determine for you.

Extension Channel	2437MHz (Channel 6) ✓ AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2422MHz (Channel 3) 2427MHz (Channel 4) 24337MHz (Channel 5) 2437MHz (Channel 6) 2442MHz (Channel 7) 2442MHz (Channel 8) 2452MHz (Channel 9) 2452MHz (Channel 10) 2462MHz (Channel 11) 2467MHz (Channel 12) 2472MHz (Channel 13) With 802, 11n, there is one option to double the bandwidth per		
	channel. The available extension channel options will be varied according to the Channel selected above. Configure the extension channel you want.		
Rate	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.		
Phy Mode	Data will be transmitted via communication channel, HTMIX.		
Subnet	LAN-A is specified for connection.		
Security	Select WEP, TKIP or AES as the encryption algorithm.		
Peer Mac Address	Four peer MAC addresses are allowed to be entered in this page at one time.		
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burs t). 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.		
	Note: 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 Enable for TxBURST on the tab of Option).		
	Virgor 1.101 BU22 11 m Wireless USB Adapter Utility Configuration Status Option About General Setting Advance Setting Auto launch when Windows gtart up Bable Badio Remember mini status position Advance Setting Auto hide mini status Configuration Threshold : 2346 RTS Threshold : 2347 Frequency : 802.11b/g/n - 2.4GH w Ad-hoc Ad-hoc WLAN type to connect Mathematically connect to non-preferred networks Infrastructure and Ad-hoc network only Ad-hoc chevork only Advice network only OK		

Antenna	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. 2T2R 2T2R 1T1R
Tx Power	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless. 100% 100% 80% 60% 30% 20% 10%
Channel Width	 20 MHZ- the router will use 20Mhz for data transmission and receiving between the AP and the stations. Auto 20/40 MHZ- 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.

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

SSID 1	SSID 2	SSID 3	SSID 4		
Mo	de	Mixed()	NPA+WPA2),	PSK 🔽	
Set	up <u>RADIUS Server</u>	if 802.1x is ei	nabled.		
WPA WP	A Algorithms	Οτκιρ	OAFS	• ΤΚΙΡ/ΔΕS	3
Pas	s Phrase	•••••	•••••		-
Кеу	/ Renewal Interval	3600	seconds		
WEP					
	Key 1 :				Hex 💌
۲	Key 2 :				Hex 💌
	Кеу 3 :				Hex 💌
	Кеу 4 :				Hex 💌
802	2.1× WEP	○ Disał	ole O Enat	ole	
		OK		icel	

Item	Description		
Mode	There are several modes provided for you to choose. Disable WEP WPA/PSK WPA2/PSK		
	Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x Disable - The encryption mechanism is turned off. WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key		
	 WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK - 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. WEP/802.1x - The built-in RADIUS client feature enables 		

	VigorAP 710 to assist th122222222222222222222222222222222222
	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.
	WPA/802.1x - 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.
	WPA2/802.1x - 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.
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/ PSK mode.
Key Renewal Interval	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 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 WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key 1 – Key 4	energy from 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 WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode. 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 WEP mode.
Key 1 – Key 4 802.1x WEP	 cheryption 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 WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode. 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 WEP mode. Hex ASCII Hex Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.
Key 1 – Key 4 802.1x WEP	energy prior key that is failed if y generated. This failed if y 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 WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode. 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 WEP mode. Hex Mascell Hex MEP Encryption. Data sent to the AP will not be encrypted. Enable - Disable the WEP Encryption.

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

RADIUS Server		
Use internal RADIUS Server		
IP Address	0	
Port	1812	
Shared Secret	DrayTek	
Session Timeout	0	

Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	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, 3.9 RADIUS Server to configure settings for internal server of VigorAP 710.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	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.
Session Timeout	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.

Dray Tek

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).

SSID 1	SSID 2	SSID 3	SSID 4		
	9	SID: DrayTek			
	F	Policy: Disable		~	
		MAG	C Address Filter		
	Index	<	MAC A	Address	
	Client's M	AC Address :] : 🛄 : 🛄		
	Add	Delete	Edit Ca	ncel Limit:256 entries	
		ОК	Cance	91	
Backup ACL Cfg Backup	:	Upload From Fi Restore	le: Choose File) No file chosen	

Wireless LAN >> Access Control

Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Blocked MAC address filter, 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. Activate MAC address filter Disable Activate MAC address filter Blocked MAC address filter
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.

Cancel	Give up the access control set up.
Backup	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
Restore	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	(Wi-FiProtected	Setup)
---------------------	-----------------	--------

Enable	whe	C5
Enable	WPS.	N 10

Wi-Fi Protected Setup Information

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

Device	Configure
000000	oomigaro

5	
Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN
Status: Not used	

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

 \mathfrak{Q} : WPS is Disabled.

♥: WPS is Enabled.

↔: Waiting for WPS requests from wireless clients.

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 710 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 710r. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 710.
Configure via Push Button	Click Start PBC 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)
Configure via Client	Type the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WLAN LED on

PinCode	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	
			Sc	an		
See <u>Channel</u>	Statistics 1 4 1					
Note: During the	he scanning	process (a	bout 5 second:	5), no station is allo	wed to connect with the AP.	
AP's MAC Addr	ress	::	:	: AP's	SSID	
Add to <u>WDS Se</u>	ettings: A	dd				

Each item is explained as follows:

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

The cost card and the status	Wirele	ess LAN	>>	WDS	AP	Status
------------------------------	--------	---------	----	-----	----	--------

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth
1	00:50:7F:C9:76:0C	CCK	OFF	20M

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

VMM Configurati	ion				Set to	Factory Default
WMM Capable		(🔾 Enable 🛛 💿 Di	sable		
WMM Parameter	s of Access Po	oint				
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy
AC_BE	3	15 💌	63 💌	0		
АС_ВК	7	15 💌	102: 💙	0		
AC_VI	1	7 💌	15 💌	94		
AC_VO	1	3 💌	7 💌	47		
WMM Parameter	s of Station					
	Aifsn	CV	/Min	CWMax	Тхор	ACM
AC_BE	3	15	*	1023 💌	0	
AC_BK	7	15	~	102: 💌	0	
AC_VI	2	7	~	15 💌	94	
AC_VO	2	3	~	7 💌	47	
			OK Ca	ncel		

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the Enable 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.

CWMin/CWMax	CWMin means contention Window-Min and CWMax 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.
Тхор	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.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. Note: 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.
AckPolicy	"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

ation List					
				General	Advanced
MAC Address	SSID	Auth	Encrypt	Tx Rate(Kbps)	Rx Rate(Kbps)
					<u>_</u>
					~
		Refrest	1		
Add to <u>Access Cont</u>	rol :				
Client's MAC Addres	s: 📄 : 📄 :	: : :			
		Add			

Available settings are explained as follows:

Description
Display the MAC Address for the connecting client.
Display the SSID that the wireless client connects to.
Display the authentication that the wireless client uses for connection with such AP.
Display the encryption mode used by the wireless client.
Display the transmission /receiving rate for packets.
Click this button to refresh the status of station list.
Client's MAC Address - 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.
Click this button to add current typed MAC address into Access Control.
General – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. Advanced – Display more information (e.g., AID, PSM, WMM, PSSI PbMd, BW, MCS, Pate) for the station

Dray Tek

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.

Wireless	LAN	>>	General	Setup
----------	-----	----	---------	-------

	N
🔲 Enable Limit	Client (3-64) 64 (default: 64)
Mode :	Mixed(11b+11g+11n) 💌
Hide SSID	SSID Isolate Isolate VLAN ID Mac Clone LAN Member(0:Untagged) Mac Clone
1 🔲 Dray	/Tek
2	
3	
4	
MAC Clone:	Set the MAC address of SSID 1. The MAC addresses of other SSIDs and
Channel :	the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8. 2462MHz (Channel 11) 2442MHz (Channel 7)
Channel : Extension Chann	the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8. 2462MHz (Channel 11) el : 2442MHz (Channel 7)
Channel : Extension Chanr Packet-OVERDRI	the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8. 2462MHz (Channel 11) tel : 2442MHz (Channel 7) VE
Channel : Extension Chanr ——— Packet-OVERDRI П Tx Burst	the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8. 2462MHz (Channel 11) tel : 2442MHz (Channel 7) VE
Channel : Extension Chann Packet-OVERDRI Tx Burst Note :	the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8. 2462MHz (Channel 11) 👻 tel : 2442MHz (Channel 7) 💙 YE
Channel : Extension Chanr Packet-OVERDRI Tx Burst Note : 1.Tx Burst only s	the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8. 2462MHz (Channel 11) tel : 2442MHz (Channel 7) VE
Channel : Extension Chanr Packet-OVERDRI Tx Burst Note : 1.Tx Burst only s 2.The same tech	the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8. 2462MHz (Channel 11) tel : 2442MHz (Channel 7) VE supports 11g mode. anology must also be supported in clients to boost WLAN performance.
Channel : Extension Chann Packet-OVERDRI Tx Burst Note : 1.Tx Burst only s 2.The same tech Antenna :	the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8. 2462MHz (Channel 11) tel : 2442MHz (Channel 7) VE Supports 11g mode. Inology must also be supported in clients to boost WLAN performance. 2T2R V
Channel : Extension Chann Packet-OVERDRI Tx Burst Note : 1.Tx Burst only s 2.The same tech Antenna : Tx Power :	the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8. 2462MHz (Channel 11) tel : 2442MHz (Channel 7) VE tupports 11g mode. nology must also be supported in clients to boost WLAN performance. 2T2R 100%

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Limit Client	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.
Mode	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.

	Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) II Mixed(11b+11g+11n) Mixed(11b+11g+11n)		
Hide SSID	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.		
SSID	Set a name for VigorAP 710 to be identified. Default setting is DrayTek.		
Isolate LAN	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.		
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.		
VLAN ID	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		
Mac Clone	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.		
Channel	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 AutoSelect to let system determine for you. 2437MHz (Channel 6) AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 3) 2427MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 5) 2437MHz (Channel 6) 2442MHz (Channel 7) 2447MHz (Channel 8) 2452MHz (Channel 10) 2462MHz (Channel 11) 2467MHz (Channel 12) 2472MHz (Channel 13)		

Extension Channel	With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the Channel selected above. Configure the extension channel you want.		
Rate	If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.		
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). 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. Note: 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 Enable for TxBURST on the tab of Option).		
	Yigor N61 802.11n Wireless USB Adapter Utility Configuration Status Option About General Setting Auto launch when Windows gtart up Remember mini status gosition A duto hide mini status Stet mini status Group Roaming Ad-hoc WLAN type to connect Onfinfarstructure and Ad-hoc network only Ad-hoc network only Ad-hoc network only OK		
Antenna	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.		
Tx Power	The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless. 100% 100% 100% 80% 60% 30% 20% 10%		
Channel Width	20 MHZ- the router will use 20Mhz for data transmission and receiving between the AP and the stations. Auto 20/40 MHZ – the router will use 20Mhz or 40Mhz for		

data transmission an capability. Such cha transit.	nd receiving according to the station annel can increase the performance for data
--	--

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

331D 1 331D 2	3310 3 3310 4	
SSID	DrayTek	
Mode	Mixed(WPA+WPA2)/PSK 💌	
Set up <u>RADIUS Server</u> i	f 802.1× is enabled.	
WPA		
WPA Algorithms	🔘 TKIP 🔘 AES 💿 TKIP/AES	
Pass Phrase	••••	
Key Renewal Interval	3600 seconds	
WEP		
○ Key 1 :		Hex 💌
Key 2 :		Hex 💌
🔾 Кеу 3 :		Hex 💌
○ Key 4 :		Hex 💌
802.1× WEP	O Disable O Enable	

Item	Description			
Mode	There are several modes provided for you to choose.			
	Disable 👻			
	Disable WEP WPA/PSK			
	WPA2/PSK			
	Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x			
	Disable - The encryption mechanism is turned off.			
	WEP - Accepts only WEP clients and the encryption key should be entered in WEP Key.			
	WPA/PSK or WPA2/PSK or M	WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK -		


	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.
	WEP/802.1x - 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.
	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.
	WPA/802.1x - 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.
	WPA2/802.1x - 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.
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Pass Phrase	Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key Renewal Interval	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 WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
Key 1 – Key 4	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 WEP mode.

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

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

RADIUS Server

Use internal RADIUS Server	
IP Address	0
Port	1812
Shared Secret	DrayTek
Session Timeout	0

ОК	
----	--

Available settings are explained as follows:

Item	Description	
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 710 which is use 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, 3.9 RADIUS Server to configure settings for internal server of VigorAP 710.	
IP Address	Enter the IP address of external RADIUS server.	
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.	
Shared Secret	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.	
Session Timeout	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).

Vireless LAN >> Access Control				
0010 1	0010 0	0010.0	0010 4	
5510 1	5510 2	881D 3	551D 4	
		SSID: DrayTek		
		Policy: Disable		*
		MAC	CAddress Filter	
	Inde	x	MAC A	Address
				<u>^</u>
				~
	Clientle M			
	Clients M	IAC AUURESS :		
	Add 🗌	Delete 🗌 🦲	Edit Ca	ancel Limit:256 entries
		1		2
ackup ACL Cfg	:	Upload From Fil	e: Choose File	No file chosen
Backup		Restore		

Available settings are explained as follows:

Item	Description	
Policy	Select to enable any one of the following policy or disable the policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Blocked MAC address filter, 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. Activate MAC address filter Disable Activate MAC address filter Blocked MAC address filter	
MAC Address Filter	Display all MAC addresses that are edited before.	
Client's MAC Address	Manually enter the MAC address of wireless client.	
Add	Add a new MAC address into the list.	
Delete	Delete the selected MAC address in the list.	
Edit	Edit the selected MAC address in the list.	

Dray Tek

Cancel	Give up the access control set up.
Backup	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
Restore	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	Mixed(WPA+WPA2)/PSK
WPS Encryp Type	TKIP/AES

Device Configure	
Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN
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.

Item	Description	
Enable WPS	Check this box to enable WPS setting.	
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 710 is properly configured, you can see 'Yes' message here.	
WPS SSID	Display current selected SSID.	
WPS Auth Mode	Display current authentication mode of the VigorAP 710. Only WPA2/PSK and WPA/PSK support WPS.	
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 710.	
Configure via Push Button	Click Start PBC 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)	
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WLAN LED on	



V	/igorAP 710 will blink fast when WPS is in progress. It will
r	eturn to normal condition after two minutes. (You need to
s	etup 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 >	/ireless LAN >> Access Point Discovery							
Access Point Li	st							
Select SSID	BSSID	RSSI	Channel	Encryption	Authentication			
			So	an				
See <u>Channel</u>	<u>Statistics</u>							
Note: During the	ne scanning	process (a	bout 5 second	s), no station is all	lowed to connect with the AP.			
AP's MAC Addi	ress	: :	: : : : : : : : : : : : : : : : : : : :	: AP'	's SSID			
Select as <u>Unive</u>	ersal Repeate	er: Select	:					

Each item is explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 710.
BSSID	Display the MAC address of the AP scanned by VigorAP 710.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 710.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Channel Statistics	It displays the statistics for the channels used by APs.
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	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.
Select as Universal Repeater	In Universal Repeater 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	2462MHz (Channel 11) 💌
Security Mode	Open 💌
Encryption Type	None 💌
WEP Keys	
○ Key 1 :	Hex 💌
О Кеу 2 :	Hex 💌
О Кеу 3 :	Hex 💌
О Кеу 4 :	Hex 💌

Note: If Channel is modified, the Channel setting of AP would also be changed.

Universal Repeater IP Configuration

Connection Type	DHCP 💙	
Router Name	AP710	
	OK Cancel	

Item	Description
SSID	Set the name of access point that VigorAP 710 wants to connect to.
MAC Address (Optional)	Type the MAC address of access point that VigorAP 710 wants to connect to.
Channel	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 AutoSelect to let system determine for you.
Security Mode	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.

	Open Open Shared WPA/PSK WPA2/PSK
Encryption Type for Open/Shared	This option is available when Open/Shared is selected as Security Mode. Choose None to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose WEP .
	None 💌 None WEP
	WEP Keys - 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 ','. Hex ASCII Hex
Encryption Type for WPA/PSK and WPA2/PSK	This option is available when WPA/PSK or WPA2/PSK is selected as Security Mode . Select TKIP or AES as the algorithm for WPA.
Pass Phrase	Either 8~63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
Connection Type	Choose DHCP or Static IP as the connection mode. DHCP – The wireless station will be assigned with an IP from Vigor router. Static IP – The wireless station shall specify a static IP for connecting to Internet via Vigor router. DHCP Static IP DHCP
Router Name	Type a name for the router as identification. Simply use the default name.
IP Address	This setting is available when Static IP is selected as Connection Type .

	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.
Subnet Mask	This setting is available when Static IP is selected as Connection Type .
	Type the subnet mask setting which shall be the same as the one configured in LAN for the router.
Default Gateway	This setting is available when Static IP is selected as Connection Type .
	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.

MM Capable			🔾 Enable 💿 D	isable		
MM Parameter	s of Access P	oint				
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy
AC_BE	3	15 💌	63 💌	0		
АС_ВК	7	15 💌	102: 💌	0		
AC_VI	1	7 💌	15 💌	94		
AC_VO	1	3 💌	7 💌	47		
MM Parameter	s of Station					
	Aifsn	C	CWMin	CWMax	Тхор	ACM
AC_BE	3		15 💌	1023 💌	0	
AC_BK	7		15 💌	1023 💌	0	
AC_VI	2	5	7 💌	15 💌	94	
AC VO	2	3	3 💌	7 💌	47	

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the Enable 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.



CWMin/CWMax	CWMin means contention Window-Min and CWMax 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.
Тхор	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.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. Note: 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.
AckPolicy	"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

ation List									
						Ge	neral	Advan	ced
MAC Address	AID	RSSI	Rate	BW	PSM	WMM	PhMd	MCS	
									^
									~
L			R	efresh					
Add to <u>Access Co</u>	ntrol :								
Client's MAC Add	ress :	: 🔄 :	:	:	:				
				Add					

Item	Description		
MAC Address	Display the MAC Address for the connecting client.		
SSID	Display the SSID that the wireless client connects to.		
Auth	Display the authentication that the wireless client uses for connection with such AP.		
Encrypt	Display the encryption mode used by the wireless client.		
Tx Rate/Rx Rate	Display the transmission /receiving rate for packets.		
Refresh	Click this button to refresh the status of station list.		
Add to Access Control	Client's MAC Address - 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.		
Add	Click this button to add current typed MAC address into Access Control.		
General/Advanced	 General – Display general information (e.g., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) for the station. Advanced – 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.

username	Password	Confirm Password	Configure Add Cancel
NO.	Username		Select
Delete Selected	Delete All		
thentication Client (up Client IP	to 16 clients) Secret Key	Confirm Secret Key	Configure
nthentication Client (up Client IP	to 16 clients) Secret Key Client IP	Confirm Secret Key	Configure Add Cancel Select
thentication Client (up Client IP NO. Delete Selected	to 16 clients) Secret Key Client IP Delete All	Confirm Secret Key	Configure Add Cancel Select

Item	Description			
Enable RADIUS Server	Check it to enable the internal RADIUS server.			
Users Profile	Username – Type a new name for the user profile.			
	Password – Type a new password for such new user profile.			
	Confirm Password – Retype the password to confirm it.			
	Configure			
	• Add – Make a new user profile with the name and password specified on the left boxes.			
	• Cancel – Clear current settings for user profile.			
	Delete Selected – Delete the selected user profile (s).			
	Delete All – Delete all of the user profiles.			
Authentication Client	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 RADUIS server.			
	Client IP – 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.			

	Secret Key – 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.			
	Confirm Secrete Key – Type the password again for confirmation.			
	Configure			
	• Add – Make a new client with IP and secrete key specified on the left boxes.			
	• Cancel – Clear current settings for the client.			
	Delete Selected – Delete the selected client(s).			
	Delete All – Delete all of the clients.			
Backup	Click it to store the settings (RADIUS configuration) on this page as a file.			
Restore	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.

Applications			
Schedule			
Apple iOS	5 Keep Alive		

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			
chedule			
Enable Schedule			
	ОК		
chedule Configuration			
	C		

Available settings are explained as follows:

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

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 💌 - 🔟 💌 - 🔟 💌 (Year - Month - Day)
Start time	0 💌 : 0 💌 (Hour : Minute)
Action	Auto Reboot
Acts	Routine 💌
Weekday	🗌 Monday 🗹 Tuesday 🗋 Wednesday 🗋 Thursday 🗹 Friday 🗋 Saturday 🗹 Sunday

OK Cancel

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

3. 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.

Applications >> Schedule				
Schedule				
🗹 Enable Schedu	le			
Schedule Configurat	ion			
Index.	Setting	Status		
1	2013 July. 1, 12:0-0:0 Routine: Tue Fri Sun	۷		
	OK Add			

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.

Applications >> Apple iOS Keep Alive

Enable Apple iOS Keep Alive				
Apple iOS Keep Alive:				
Apple iOS Keep Alive can keep Wifi connection of iOS device by sending UDP port 5353 packets every 5 seconds.				
Index Apple iOS Kee	o Alive IP Address	Index	Apple iOS Keep Alive IP Address	
1		2		

Index	Apple iOS Keep Alive IP Address	Index	Apple iOS Keep Alive IP Address
1		2	
<u>3</u>		<u>4</u>	
<u>5</u>		<u>6</u>	

OK Cancel

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

System Maintenance
System Status
TR-069
Administration Password
Configuration Backup
Time and Date
Management
Reboot System
Firmware Upgrade
Diagnostias

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

Nodel	: Vigor AP710
irmware Version	: 1.1.0
Build Date/Time	: r3805 Wed Feb 5 09:56:25 CST 2014
System Uptime	: 0d 00:01:25
Operation Mode	: Universal Repeater

	System
Memory Total	: 62344 kB
Memory Left	: 38232 kB
Cached Memory	: 15424 kB / 62344 kB
	Wireless
MAC Address	: 00:0C:43:76:20:78
SSID	: DrayTek
Channel	: 11

	LAN
MAC Address	: 00:0C:43:76:20:78
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

Each item is explained as follows:

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

Dray Tek

LAN	
MAC Address	Display the MAC address of the LAN Interface.
IP Address	Display the IP address of the LAN interface.
IP Mask	Display the subnet mask address of the LAN interface.
Wireless	
MAC Address	Display the MAC address of the WAN Interface.
SSID	Display the SSID of the device.
Channel	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	
Username	
Password	
CPE Settings	
Enable	
On	LAN-A
URL	http://192.168.1.2:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	• • • • • • • •
DNS Server IP Address	
Primary IP Address	
Secondary IP Address	
Nete · Diance cet default estaur	nu na mattar abaaca Lébi é ar Lébi D

Note : Please set default gateway, no matter choose LAN-A or LAN-B.

Periodic Inform Settings		
Enable	V	
Interval Time	900	second(s)
STUN Settings		
○Enable ⊙Disable		
Server Address		
Server Port	3478	
Minimum Keep Alive Period	60	Second(s)
Maximum Keep Alive Period	-1	second(s)
	ОК (Cancel

	Т
Item	Description
ACS Settings	URL/Username/Password – 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.
CPE Settings	Such information is useful for Auto Configuration Server (ACS). Enable– Check the box to allow the CPE Client to connect with Auto Configuration Server.
	On – Choose the interface for VigorAP 710 connecting to ACS server.
	Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.
	DNS Server IP Address – Such field is to specify the IP address if a URL is configured with a domain name.
	• Primary IP Address –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.
	• Secondary IP Address – 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.
Periodic Inform Settings	The default setting is Enable . Please set interval time or schedule time for the AP to send notification to VigorACS server. Or click Disable to close the mechanism of notification.
	Interval Time – Type the value for the interval time setting. The unit is "second".
STUN Settings	The default is Disable . If you click Enable , please type the relational settings listed below:
	Server Address – Type the IP address of the STUN server.
	Server Port – Type the port number of the STUN server.
	Minimum Keep Alive Period – 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".
	Maximum Keep Alive Period – 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

Available settings are explained as follows:

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

maximum period is specified.

3.10.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administration Password

Administrator Settings

Account	admin
Password	•••••
Confirm Password	

Note: Authorization can contain only a-z A-Z 0-9 , ~ ` ! @ # \$ % ^ & * () _ + = { } [] | \ ; ' <> . ? /

Available settings are explained as follows:

Item	Description	
Account	Type the name for accessing into Web User Interface.	
Password	Type in new password in this filed.	
Confirm Password	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
--------	-------------	----	---------------	--------

Configuration	Backup / Restoration
Restoration	
	Select a configuration file.
	Browse
	Click Restore to upload the file.
	Restore
Backup	
	Click Backup to download current running configurations as a file.
	Backup

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

File Dov	vnload 🛛
?	You are downloading the file: config.cfg from 192.168.1.1
	Would you like to open the file or save it to your computer?
	Open Save Cancel More Info
	Always ask before opening this type of file

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

Save As		? 🗙
Save in:	🕼 Desktop 🔹 🔇 🎓 📂 🖽 •	
My Recent Documents Desktop My Documents	 My Documents My Computer My Network Places RVS-COM Lite Annex A mmm MWSnap300 TeleDanmark Tools config v2k2_232_config_1 v2k6_250_config_1 	
	File name: Config	Save
My Network	Save as type: Configuration file	Cancel

Dray Tek

4. 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

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

System Maintenance >> Configuration Backup		
Configuration Realism / Destanation		

Configuration Backup / Restoration		
Restoration		
	Select a configuration file.	
	Browse	
	Click Restore to upload the file.	
	Restore	
Backup		
	Click Backup to download current running configurations as a file.	
	Backup	

- 2. Click **Browse** button to choose the correct configuration file for uploading to the modem.
- 3. 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

System Maintenance >> Time and Date

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

Time Information	
Current System Time	Fri Jun 21 15:03:41 GMT 2013 Inquire Time
Time Setting	
OUse Browser Time	
⊙Use NTP Client	
Time Zone	(GMT-11:00) Midway Island, Samoa 💌
NTP Server	Use Default
Daylight Saving	
NTP synchronization	30 sec 💌
	OK Cancel

Available parameters are explained as follows:

Item	Description	
Current System Time	Click Inquire Time to get the current time.	

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

Svstem	Maintenance	>>	Management
oyotoini	maniconanco		management

System Maintenance >> Reboot System

Management Port Setup			
HTTP port	80		
HTTPS port	443		

OK Cancel

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.

Reboot System		
	Do You want to reboot your router ?	
	 Using current configuration Using factory default configuration 	
L	ОК	

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 (or local DrayTek's web site) and FTP site is ftp.draytek.com.

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

```
System Maintenance >> Firmware Upgrade
```

Firmware Update

```
Select a firmware file.
ChooseFile No file chosen
Click Upgrade to upload the file. Upgrade
```

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.

```
Diagnostics
System Log
Speed Test
```

3.11.1 System Log

At present, only System Log is offered.

Diagnostics >> System Log

System Log Information	<u>Clear</u> <u>Refresh</u> 🔲 Line wrap
Od 06:46:31 syslogd started: BusyBox v1.12.1	
Od 06:46:31 kernel: klogd started: BusyBox v1.12.1 (2	2013-04-22 11:06:44 CST)
Od O6:46:31 kernel: mng_vlan_en= 0x0	
Od O6:46:31 kernel: mng_vlan_vidl= 0x0	
Od O6:46:31 kernel: mng_vlan_vid2= 0x0	
Od 06:46:31 kernel: flag: 0x0	
Od 06:46:31 kernel: ravid 0: 0x0	
Od 06:46:31 kernel: ravid 1: 0x0	
0d 06:46:31 kernel: ravid 2: 0x0	
Od 06:46:31 kernel: ravid 3: 0x0	
0d 06:46:31 kernel: ravid 4: 0x0	
Od 06:46:31 kernel: ravid 5: 0x0	
0d 06:46:31 kernel: ravid 6: 0x0	
Od 06:46:31 kernel: ravid 7: 0x0	

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.

Diagnostics >> Speed Test

Speed Test Welcome to VigorAP710 Speed Test. This test allows you to find out the best place for VigorAP710. You can execute the speed test at different places of the building and select the best location for it. The performance test result is only for your reference. Start Note : Speed test could not work with chrome browser.

3.12 Support Area

When you click the menu item under **Support Area**, you will be guided to visit www.draytek.com and open the corresponding pages directly.



This page is left blank.

VigorAP 710 User's Guide

Dray Tek



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 stilled 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**.

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.

🕹 eth0 Properties 🛛 🔹 💽 🔀
General Authentication Advanced
Connect using:
ASUSTeK/Broadcom 440x 10/100 Ir
This connection uses the following items:
Elient for Microsoft Networks Elie and Printer Sharing for Microsoft Networks
Image: Strategy of Microsoft Networks Image: Strategy of Microsoft Networks Image: Strategy of Microsoft Networks
✓ 3 Internet Protocol (TCP/IP)
Install Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
 Show icon in notification area when connected Notify me when this connection has limited or no connectivity
OK Cancel

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

Internet Protocol (TCP/IP) Properties 🛛 🔹 🔀					
General	Alternate Configuration				
You car this cap the app	n get IP settings assigned automatically if your network supports ability. Otherwise, you need to ask your network administrator for ropriate IP settings.				
Obtain an IP address automatically					
-OU3	e the following IP address:				
<u>I</u> P ad	Idress:				
Subr	iet mask:				
Defa	ult gateway:				
⊙ Dbtain DNS server address automatically					
O Use the following DNS server addresses:					
Prefe	arred DNS server:				
Alter	nate DNS server:				
	Ad <u>v</u> anced				
OK Cancel					

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.

\bigcirc			Netv	vork		
	Displayer Sa		Etartus Dir	-k		
IOW AII	Displays So	und Network	Startup Dis	sĸ		
		ocation: A	utomatic			
			atomatic		·	
		Show: B	uilt-in Ethe	ernet	•	
	ТСР	/IP PPPoE	AppleT	alk Proxies	Ethernet	
Cor	figure IPv4:	Using DH	СР		•	
	IP Address:	192.168.1	.10		(Renew D	HCP Lease
Si	ubnet Mask:	255.255.2	55.0	DHCP Client I	D:	
	Boutor	102 169 1	1		(If require	ed)
	Kouter.	192.108.1	.1			_
0	ONS Servers:					(Optional)
Searc	ch Domains:					(Optional)
IP	v6 Address:	fe80:0000:	0000:0000	0:020a:95ff:fe8c	l:72e4	
		Configure	IPv6			0
		Conngare				0



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.



- 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.

$\Theta \Theta \Theta$	Terminal — bash — 80x24	2
Last login: Sat Jan Welcome to Darwin! Vigor10:~ draytek\$ PING 192.168.1.1 (1 64 bytes from 192.1 64 bytes from 192.1 64 bytes from 192.1 64 bytes from 192.1 64 bytes from 192.1	3 02:24:18 on ttyp1 ping 192.168.1.1 92.168.1.1): 56 data bytes 68.1.1: icmp_seq=0 ttl=255 time=0.755 ms 68.1.1: icmp_seq=1 ttl=255 time=0.697 ms 68.1.1: icmp_seq=2 ttl=255 time=0.716 ms 68.1.1: icmp_seq=3 ttl=255 time=0.731 ms 68.1.1: icmp_seq=4 ttl=255 time=0.72 ms	2
∧C 192.168.1.1 pin 5 packets transmitt round-trip min/avg/ Vigor10:~ draytek\$	g statistics ed, 5 packets received, 0% packet loss max = 0.697/0.723/0.755 ms	

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 loose 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

leboot System		
	Do You want to reboot your router ?	
	Osing current configuration	
	 Using factory default configuration 	

OK

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.

